SEGUNDO INFORME DE LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS, recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

BOLETÍN N° 14.847-06.

HONORABLE SENADO:

Las Comisiones de Defensa Nacional y de Seguridad Pública, unidas, tienen el honor de informar respecto del proyecto de ley individualizado en el epígrafe, iniciado en mensaje de S. E. el ex Presidente de la República, señor Sebastián Piñera Echenique, con urgencia calificada de discusión inmediata.

La iniciativa legal fue aprobada en general por la Corporación en sesión de 18 de octubre de 2022, oportunidad en la que se fijó como plazo para presentar indicaciones el 11 de noviembre de ese año. En dicha ocasión se determinó, además, que la proposición de ley fuera informada en particular por las Comisiones de Defensa Nacional y de Seguridad Pública, unidas.

Con posterioridad, el día 15 del mismo mes y año, la Sala abrió un nuevo plazo para formular indicaciones, hasta el 22 de noviembre, período en el que se presentaron otras. Dado que ello se produjo antes de iniciar el estudio de las primeras, esta Secretaría las reenumeró.

Finalmente, el 11 de abril de 2023, la Sala resolvió abrir un nuevo plazo, hasta las 16:30 horas del mismo día, indicaciones que fueron oportunamente incorporadas en el boletín correspondiente.

Cabe destacar que este proyecto de ley debe ser considerado, además, por la Comisión de Hacienda, en su caso, según el trámite conferido a su ingreso a esta Corporación.

A una o más de las sesiones en que se discutió este asunto **asistieron**, además de sus miembros, la Honorable Senadora señora Ximena Órdenes Neira.

Asimismo, concurrieron, especialmente invitados:

Del Ministerio del Interior y Seguridad Pública: Ministra, señora Carolina Tohá; Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez; asesoras legislativas de la Secretaría de Estado, señoras Leslie Sánchez, María de los Ángeles Fernández y Catalina Lagos, y asesora legislativa del Coordinador Nacional de Ciberseguridad, señora Michelle Bordachar.

De la Subsecretaría de Defensa: Jefe de la División de Desarrollo Tecnológico e Industria, señor Yerko Benavides; Jefe del Departamento de Ciberdefensa, Mayor de Ejército, señor Juan Pablo Cortés, y asesor legislativo, señor Daniel Andrade.

De la Comisión para el Mercado Financiero: Comisionado, señora Bernardita Piedrabuena; Director General (s) Jurídico, señora Claudia Soriano; Director Regulación Prudencial de Valores, Medios de Pago y Desarrollo de Mercado, señor Daniel Calvo, y Director Riesgo Operacional, señor José Mendoza.

Asesores parlamentarios: del Honorable Senador señor Araya, señores Roberto Godoy y Pedro Lazaeta; del Honorable Senador señor Cruz-Coke, señor Iván Reinoso; del Honorable Senador señor Flores, señora Carolina Allende; del Honorable Senador señor Huenchumilla, señora Alejandra Leiva; del Honorable Senador señor Insulza, señoras Javiera Gómez y Lorena Escalona y señores Guillermo Miranda y Carlos Fernández; del Honorable Senador señor Kast, señores José Astorga y Óscar Morales; del Honorable Senador señor Kusanovic, señores Hernán Maturana y Tomás Matheson; del Honorable Senador señor Macaya, señor Carlos Oyarzún; del Honorable Senador señor Ossandón, señor Ronald von der Weth; de la Honorable Senadora señora Provoste, señores Julio Valladares, Enrique Soler y Rodrigo Vega; del Honorable Senador señor Pugh, señores Pascal de Smet d`Olbecke y Michael Heavey; del Honorable Senador señor Quintana, señor Claudio Rodríguez; de la Honorable Senadora señora Rincón, señora Natalia Navarro; del Honorable Senador señor Van Rysselberghe, señor Juan Paulo Morales; del Comité Partido Socialista, señora Javiera Riquelme, y del Comité Unión Demócrata Independiente, señora Karin Luttecke y señor Camilo Sánchez.

De la Biblioteca del Congreso Nacional, el analista del Área Gobierno, Defensa y Relaciones Internacionales, señor Juan Pablo Jarufe.

De la Fundación Jaime Guzmán: asesor, señor Ignacio Rodríguez.

De Canal 13: periodista, señora Eliana Díaz.

\- - -

NORMAS DE QUÓRUM ESPECIAL

A. Normas orgánicas constitucionales:

1) Según el artículo 38 de la Constitución Política de la República, en relación con el artículo 66, inciso segundo, del mismo Texto Supremo:

- Artículos 1, inciso segundo; 8; 9 letras a), b), c), d), e), i), m), n), ñ), v) y x); 10; 13; 14; 16 (su inciso tercero en virtud de lo dispuesto en el artículo 8°, inciso tercero de la Carta Fundamental); 20; 21; 25; 26; 34; 36; 37; 39; 40; 41; 44 y 45.

- Artículos segundo; quinto y sexto de las disposiciones transitorias.

2) Según el artículo 99, inciso final, de la Carta Fundamental:

- Artículo 4, inciso final, y artículo octavo de las disposiciones transitorias.

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

- Artículo 35.

B. Normas de quórum calificado, de conformidad al artículo 8°, inciso segundo, y 66, inciso segundo, ambos de la Carta Fundamental:

Artículos 29; 30; 31 y 42.

- - -

Para los efectos de lo dispuesto en el artículo 124 del Reglamento del Senado, cabe dejar constancia de lo siguiente:

1.- Artículos del proyecto que no han sido objeto de indicaciones ni de modificaciones: 12; 31 y 32; y los artículos tercero; cuarto y séptimo de las disposiciones transitorias.

2.- Indicaciones aprobadas sin modificaciones: 5; 11; 13; 15; 16; 17; 18; 23; 25; 26; 27; 36; 38; 38 bis; 39; 42; 42 bis; 43 bis; 45; 46; 51; 53; 55 bis; 56; 58; 60; 61; 61 bis; 62; 63; 64; 65; 67; 71; 72; 76; 80; 81; 82; 83; 84; 86; 88; 89; 90; 94 bis; 95 bis; 97; 99 (en cuanto a los literales p), q), r), t), v) y w) que propone incorporar al artículo 9); 101 (en cuanto al primer literal propuesto, que pasa a ser x) en el artículo 9); 101 bis; 102; 103; 106; 107 bis; 109 bis; 110; 111; 115; 117; 119 bis; 126; 127; 128; 131; 132;135; 136; 139; 140 bis; 141 bis; 147; 148; 150; 151; 152; 154; 155; 156; 158; 165; 167; 169; 171; 172; 173; 174 bis; 177; 178 (en cuanto a la incorporación de los artículos 47 y 48, nuevos); 182 y 184.

3.- Indicaciones aprobadas con modificaciones: 2; 3; 6; 7; 8; 10; 22; 24; 28; 29 (en cuanto a la incorporación de las siguientes definiciones: “auditorías de seguridad”, “ciberhigiene”, “integridad”; “interagencialidad”, “interoperabilidad”, y “Sistema de Gestión de la Seguridad y

Riesgo de la Información – SGSRI"); 31; 32; 33; 34; 35; 43 (en cuanto a la inclusión del siguiente principio rector: "principio de actualización y reutilización"); 47; 52; 55; 57; 59; 66; 68; 69; 70; 73; 78; 87; 92; 94; 95; 99 (en cuanto a los literales s) y u) que propone incorporar al artículo 9); 105; 107; 109; 116; 118; 119; 120; 121; 123; 140; 141; 143; 144; 153; 157; 159; 161; 163; 164; 174; 175; 178 (en cuanto a la incorporación del artículo 46, nuevo); 179 y 185.

4.- Indicaciones rechazadas: 9; 12; 21; 29 (en cuanto a la incorporación de las siguientes definiciones: "amenaza persistente avanzada (APT)", "anonimización", "confianza digital", "registro de operadores de servicios de ciberseguridad", y "trazabilidad"); 37; 40; 41; 43 (en cuanto a la inclusión de los siguientes principios rectores: "principio de confianza cero", "principio de cooperación", "principio de interoperabilidad", y "principio de no obsolescencia tecnológica"); 44; 54; 75; 77; 93; 96; 100; 101 (en cuanto a los dos últimos literales que propone introducir al artículo 9); 108; 149; 160; 168; 170 y 180.

5.- Indicaciones retiradas: 1; 4; 14; 19; 20; 30; 48; 49; 50; 74; 79; 85; 91; 98; 104; 112; 113; 114; 122; 124; 125; 129; 130; 133; 134; 137; 138; 142; 145; 146; 162; 166; 176; 181 y 183.

6.- Indicaciones declaradas inadmisibles: no hay.

- - -

DISCUSIÓN EN PARTICULAR

Antes de dar inicio a la discusión en particular, estas instancias legislativas recibieron en audiencia a **la Ministra del Interior y Seguridad Pública, señora Carolina Tohá**, quien aseguró que para el Ejecutivo es fundamental avanzar en la tramitación de esta propuesta de ley, reflejándose así en la formulación de diversas indicaciones al texto aprobado en general por el Senado. Anunció que ellas recogen muchas de las observaciones planteadas durante el estudio de la iniciativa tanto en la Comisión de Defensa Nacional como en la de Seguridad Pública.

Destacó que, si bien el Gobierno siempre ha estado comprometido con el proyecto de ley en análisis, en los últimos meses este ha alcanzado mayor connotación producto de los ciberataques cometidos, lo que hace aún más pertinente y urgente su pronto despacho. Al respecto, anheló que la redacción que se apruebe cuente con un amplio respaldo.

En línea con lo anterior, sostuvo que la importancia de la temática conduce a la necesidad de tener una base legal para dar continuidad a esta política de Estado, que descanse en principios ampliamente compartidos.

Aclaró que el objetivo de la seguridad informática no radica en proteger equipos y programas, sino a las personas y a la sociedad en su conjunto. Los servicios digitales, alertó, cobran cada día más relevancia

-puesto que manejan datos sensibles-, resultando, la ciberseguridad, por lo tanto, esencial para el ejercicio de los derechos.

En consecuencia, subrayó que el Estado y los particulares tienen el deber de proteger la información que se les entrega, cuidando, de esta manera, la confianza de la ciudadanía. Advirtió que, si ellos no actúan de la forma prevista, los individuos, sus derechos, su patrimonio y su seguridad se verán afectados. En este punto, explicó que la propuesta legal da un estatus a esos deberes y los hace operables.

Continuando con el desarrollo de su exposición, se detuvo en las acciones llevadas a cabo por la Administración actual en materia de seguridad informática. Reveló que el Gobierno está evaluando la Política Nacional de Ciberseguridad 2018 a 2022, trabajo que permitirá formular una nueva para el periodo 2023-2028.

A la medida señalada, comentó, se suma la dictación del decreto supremo que establece la obligación para los servicios públicos de notificar los incidentes o ataques de ciberseguridad que sufran, en tanto no exista una norma legal que recoja tal deber.

Adicionalmente, informó, se ha reactivado el Comité Interministerial sobre Ciberseguridad y se ha designado al Coordinador Nacional, el señor Daniel Álvarez.

Por otro lado, declaró que se está ejecutando un préstamo del Banco Interamericano de Desarrollo, a fin de incrementar y mejorar las capacidades nacionales en seguridad informática.

Adentrándose en el análisis del proyecto de ley, recordó que contiene una propuesta de institucionalidad pública con funciones y atribuciones especificas en materia de ciberseguridad. En este contexto, consignó, se crea la Agencia Nacional de Ciberseguridad, la que se relacionará con el Presidente de la República a través del Ministerio del Interior y Seguridad Pública.

La iniciativa, dijo, establece un ámbito de aplicación acotado a los organismos públicos y a los privados que sean calificados como infraestructura crítica de la información y un régimen de sanciones. Asimismo, añadió, prescribe un régimen de organización de los centros de respuestas a incidentes de ciberseguridad -en adelante CSIRT-, diferenciando el CSIRT Nacional, los sectoriales y el de Defensa.

Tras definir algunos de los aspectos centrales del proyecto de ley aprobado en general por el Senado, aseveró que el Ejecutivo persistirá en su tramitación, habida consideración de que el área involucrada constituye una política de Estado.

En lo que atañe a las indicaciones formuladas por Su Excelencia el Presidente de la República, apuntó que persiguen un cambio de enfoque, haciendo énfasis en que la seguridad cibernética tiene por finalidad última la protección de las personas y sus derechos. Por eso, sentenció, se

recomienda incorporar expresamente el deber de velar por el resguardo, promoción y respeto a la ciberseguridad- idea matriz del proyecto-, y se suman dos nuevos principios, el de respuesta responsable y el de igualdad y no discriminación. Precisó que el primero busca que las reacciones a tal tipo de incidentes no agraven sus características, asegurando, en definitiva, proporcionalidad. El segundo, en tanto, detalló, tiene por objetivo que las distintas instituciones y normas permitan a todas las personas gozar de los derechos y las libertades cibernéticos, y que no generen brechas o profundicen las existentes.

De igual modo, hizo ver que las indicaciones apoyan la creación de la Agencia Nacional de Ciberseguridad y fortalecen sus atribuciones y funciones, ampliando el ámbito de aplicación a todo el sector público y privado, con obligaciones diferenciadas por riesgos y tamaño.

Por otra parte, adelantó que se sustituye el concepto de “infraestructura crítica de la información” por el de “servicios esenciales” y “operadores de importancia vital”. Adujo que estas últimas expresiones son más dinámicas y amplias, y hacen posible comprender, en toda su dimensión, la regulación.

En materia orgánica, observó, se simplifica el modelo de gobernanza, creando un solo CSIRT Nacional, sometiendo a su coordinación y supervisión a los otros que pudieran surgir.

Asimismo, develó, se consolida la Red de Conectividad Segura del Estado.

A reglón seguido, dio a conocer que se perfeccionan las normas relativas al deber de reportar vulnerabilidades e incidentes de ciberseguridad, tanto en el sector público como en el privado, incluyendo la protección del hacking ético.

Para concluir, planteó que se establecen obligaciones específicas para el Estado y para los particulares en ciberseguridad, incorporando la dimensión de la educación, la capacitación, las buenas prácticas y la higiene digital, entre otros temas, a fin de crear un ambiente de responsabilidad integral en torno a la temática.

Finalizada la exposición de la señora Ministra, algunos señores Senadores expresaron sus apreciaciones acerca de la iniciativa de ley y las indicaciones en ella recaídas.

El Honorable Senador señor Pugh connotó que los ciberataques han evidenciado que la dependencia de los sistemas digitales es total y se incrementa a diario. Por tal razón, juzgó que la transformación digital del país debe ir acompañada de la protección correspondiente.

Luego, alabó la decisión política del Ejecutivo de proseguir la tramitación de este proyecto de ley, presentado durante la Administración precedente, formulándole indicaciones. Tal determinación, complementó, revela que se está frente a una política de Estado. Sobre el

particular, puso de relieve que la seguridad cibernética es un dominio común y busca proteger a las personas en el nuevo espacio que se habita.

Reconoció que tal misión no será un asunto fácil, toda vez que la ciberseguridad es dinámica. Así, enunció, lo ha reconocido la experiencia comparada, siendo este el caso de España, país que ha señalado que todos los actores serán atacados y que, en consecuencia, la resiliencia se torna esencial.

En sintonía con lo expresado recientemente, expuso el ejemplo Ucrania, Estado que pese a la agresión de la que fue objeto a principios de este año por parte de Rusia, logró continuar con sus servicios básicos, utilizando la nube y el internet satelital, demostrando que es factible, incluso en la peor condición, seguir operando.

Refiriéndose a las indicaciones recaídas en la propuesta legal, opinó que las 185 formuladas dan cuenta del interés en alcanzar una ley adecuada. No obstante, clarificó, esta no es la ocasión para velar por gustos personales ni para demorar la tramitación legislativa, puesto que el país requiere una respuesta institucional a corto plazo.

Aseguró que el viaje realizado recientemente junto con el Honorable Senador señor Saavedra a Estonia, referente mundial en ciberseguridad, les ha permitido adquirir los conocimientos suficientes para contribuir a la construcción de esta ley marco.

Por último, llamó a conseguir acuerdos transversales, que den paso a una regulación clara y aplicable.

El Honorable Senador señor Macaya, a su turno, valoró también la disposición del Ejecutivo para tomar un proyecto ingresado por la Administración anterior. En este punto, arguyó que, habitualmente, cuando hay cambio de Gobierno, el nuevo presenta una indicación sustitutiva a la iniciativa de ley cuya tramitación quiere continuar.

En el mismo orden de ideas, estimó que la determinación adoptada constituye una buena manera de abordar un tema que es de importancia nacional, y que requiere apoyo transversal. Además, observó que muchas de las indicaciones de Su Excelencia el Presidente de la República coinciden con aquellas de autoría de los Honorables Senadores señor Pugh, señora Órdenes, señor Ossandón y de él mismo.

Finalmente, manifestó su disposición a despachar prontamente esta propuesta legal.

Sumándose a los dichos de los legisladores que le precedieron en el uso de la palabra, **el Honorable Senador señor Quintana** adhirió a la valoración de la decisión política adoptada.

Enseguida, hizo ver que el país está en deuda en asuntos de ciberseguridad. En efecto, recordó que S. E. la ex Presidenta de la República, señora Michelle Bachelet, durante su segundo mandato, elaboró la Política Nacional de Ciberseguridad para el periodo 2018-2022, instrumento que contiene aspectos formativos trascendentes y que no fueron tomados en cuenta sino hasta principios de este año, cuando se inició la tramitación de esta iniciativa de ley. Así, relevó, durante mucho tiempo no hubo atención a esta materia. Especificó que los únicos pasos dados radican en la aprobación del Convenio de Budapest.

A continuación, resaltó que una de las recomendaciones realizadas el 2018 fue la utilización de la nube para el almacenamiento y procesamiento de la información, tal como lo hacía el mundo privado.

Por otro lado, advirtió que esta proposición de ley va en línea con aquella que fortalece y moderniza el sistema de inteligencia del Estado (Boletín N° 12.234-02).

Adentrándose en el análisis de las indicaciones formuladas por el Ejecutivo, expresó aprensiones respecto a la idea de sustituir la expresión “infraestructura crítica de la información” por “servicios esenciales”. Al efecto, previno que el empleo de la primera no es un capricho de los últimos Gobiernos. Pormenorizó que fue el ex Presidente de los Estados Unidos de América, señor Bill Clinton, quien instauró, en los años ´90, este concepto que está consagrado no solo en la legislación norteamericana, sino también en la europea. En atención a lo expuesto, llamó al Ejecutivo a reconsiderar el cambio señalado. A mayor abundamiento, juzgó que utilizar el mismo lenguaje a nivel mundial en materia digital es fundamental.

El Honorable Senador señor Insulza advirtió que el Congreso Nacional ha abordado previo a este proyecto de ley otros vinculados a la ciberseguridad. Entre ellos, acotó, se encuentra la aprobación del Convenio de Budapest y la de 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 tratado referido.

Para terminar, llamó a adoptar las medidas indispensables para que el estudio de las indicaciones se realice lo más rápido posible; de lo contrario, vislumbró, esta iniciativa de ley no podrá despacharse con la celeridad requerida.

La Ministra del Interior y Seguridad Pública, señora Carolina Tohá, en relación con la primera observación del legislador que le antecedió en el uso de la palabra, consideró que quizás un orden inverso de tratar las propuestas legales mencionadas habría sido lo ideal. Con todo, planteó que hay proyectos paralelos que están vinculados. Entre ellos, puntualizó, el de modernización del Sistema de Inteligencia, respecto del cual el Gobierno presentará indicaciones, y el de infraestructura crítica, que resguarda las instalaciones en espacios públicos. Además, hizo hincapié en que el Ejecutivo se ha reunido con las compañías de servicios digitales, a fin de buscar una solución frente al robo de cables de cobre, ilícito que conlleva el

corte de conexiones. De esta manera, subrayó, esta proposición legal no se estudia aisladamente, mas constituye el marco para todas las demás.

En tanto, **el Honorable Senador señor Saavedra**, fijando su atención en los planteamientos de la Secretaria de Estado, sentenció que, si bien en esta oportunidad solo se discutirá la futura ley marco de ciberseguridad, debe hacerse con un enfoque sistémico, debido a la diversidad de elementos involucrados. En consecuencia, alertó, no puede tenerse una mirada meramente lineal, puesto que impedirá tener en cuenta las diversas variables que intervienen en el mundo actual, en donde la digitalización tiene un rol fundamental en la vida de los habitantes, sus derechos y su patrimonio.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, a su vez, informó que, tras el análisis efectuado por el Ejecutivo a las indicaciones, es posible concluir que, respecto de la mayoría de las enmiendas, hay consenso. Por tal razón, sugirió constituir una mesa de trabajo entre los asesores parlamentarios y los del Gobierno para avanzar en aquellos puntos en que hay acuerdo, con el propósito de no retardar la tramitación de esta importante y urgente proposición legal.

Centrando su atención en las indicaciones formuladas por Su Excelencia el Presidente de la República, aseveró que recogen parte de la discusión originada en el seno de estas Comisiones, particularmente en lo que dice relación con el modelo de organización. En efecto, puntualizó que el previsto en el texto aprobado en general es muy complejo, y dificulta la relación entre las diversas entidades.

Otro tema que también se aceptó, anunció, es el relativo a la situación laboral de quienes se desempeñarán en la Agencia Nacional de Ciberseguridad. Recordó que el proyecto de ley original dispone que se regirán por las normas del Estatuto Administrativo. Connotó que los Honorables Senadores señores Araya y Quintana hicieron ver lo dificultoso que podría llegar a ser contratar talento humano altamente especializado para dicha entidad bajo tales reglas. Por ello, justificó, se propone sujetarlos a los preceptos del Código del Trabajo, introduciendo algunas modificaciones.

Además, llamó a no olvidar que dicha institución tendrá el carácter de fiscalizador, lo que exige cierta estructura tradicionalmente consagrada en el Estado.

Atendiendo a la observación realizada por el Honorable Senador señor Quintana acerca de sustituir la expresión “infraestructura crítica de la información” por “servicios esenciales”, explicó que tal decisión descansa en que esta última es más dinámica y permite desvincularla del mundo militar. En efecto, ahondó, este concepto se acuñó durante la Segunda Guerra Mundial y dice relación con la planificación primaria de la defensa. En Chile, resaltó, nunca ha existido esa cultura, demostrándolo así la ausencia de un cuerpo legal sobre el particular.

En sintonía con lo relatado, apuntó que si se analiza la legislación de aquellos países que han avanzado de manera sustantiva en seguridad informática, lo primero que regularon fue la infraestructura crítica, abordando la ciberseguridad como un riesgo para ellas. Chile, por el contrario, continuó, comenzó por la ciberseguridad. Con todo, aseguró que la Secretaría del Interior y Seguridad Pública trabaja coordinadamente con los Ministerios Secretaría General de la Presidencia y de Hacienda, de modo que lo que resulte de este proyecto se refleje también en otras iniciativas, como la que moderniza el sistema de inteligencia.

Respaldando los planteamientos del Honorable Senador señor Saavedra, juzgó que para garantizar la ciberseguridad debe haber una respuesta sistémica, proveniente no solo de esta proposición legal, sino también de la ley de delitos informáticos, de la que moderniza el sistema de inteligencia y del proyecto de datos personales. Agregó que las indicaciones del Ejecutivo en esta oportunidad buscan hacer coherentes tales proyectos. Así, precisó, si se examinan las normas referidas a aspectos procedimentales, podrá concluirse que las reglas son las mismas aprobadas durante el año 2021 para la segunda iniciativa de ley, lo que permitirá tener un modelo coherente.

En cuanto a las indicaciones al texto aprobado en general, estimó que muchas de ellas lo armonizan, mientras que otras mejoran definiciones, acercándolas a los estándares internacionales. Avizoró que respecto de la mayoría habrá consenso. Las diferencias, adelantó, descansarán en temas como la relación entre la Agencia Nacional de Ciberseguridad y los sectores regulados. El reemplazo de la expresión “infraestructura crítica de la información” por “servicios esenciales”, en tanto, aseveró, será una discusión sobre títulos más que de contenido, toda vez que, probablemente, no habrá reparos a la redacción de las disposiciones que abordan el tema.

Por último, **el Honorable Senador señor Saavedra** fue tajante en manifestar la necesidad de dejar claramente consagrado en la proposición de ley que la Agencia Nacional de Ciberseguridad es un órgano de carácter estratégico, evitando con ello que, dentro del marco de las relaciones laborales regidas por el Código del Trabajo, la organización sindical acuerde paralizar sus funciones.

En una sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dando cuenta de los avances de la mesa de trabajo conformada por asesores parlamentarios y de Gobierno para asegurar el pronto despacho de esta proposición de ley, expresó que dicha instancia se ha reunido en dos oportunidades y ha alcanzado grandes acuerdos sobre las indicaciones formuladas a los artículos 1, 2 y 3 del texto aprobado en general por el Senado. No obstante, reconoció que en ciertos aspectos existen diferencias. Asimismo, comunicó, hay otros cuyo examen y votación se sugiere dejar pendiente en tanto no se estudie el precepto que aborda el tema de fondo.

Por último, consignó que de las decisiones adoptadas respecto de cada indicación se deja constancia en una minuta.

°°°°°

La indicación número 1, del Honorable Senador señor Insulza, es para reemplazar, todas las veces que aparece en el texto, la frase “incidentes de ciberseguridad” por la expresión “incidentes de ciberseguridad o ciberataques”.

- Esta indicación fue retirada por su autor.

°°°°°

°°°°°

La indicación número 2, del Honorable Senador señor Insulza, busca sustituir, todas las veces que aparece en el texto, la frase “sistema informático” por “red o sistema de información”.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que la mesa de trabajo constituida por los asesores sugiere aprobar con enmiendas tal indicación, reemplazando la expresión “sistema de información” por “sistema informático”, de modo que haya coherencia entre el lenguaje utilizado en este texto con aquel previsto en la ley N° 21.549, 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.

Pese al cambio propuesto, aclaró que, desde el punto de vista meramente técnico, las locuciones citadas son sinónimas.

- Las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana y Saavedra, aprobaron la indicación número 1 con la enmienda mencionada precedentemente.

°°°°°

ARTÍCULO 1

Consigna la finalidad perseguida por esta iniciativa. Al respecto, dispone que la presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos

casos, los mecanismos de control, supervisión y de responsabilidad por la infracción de la normativa.

Sobre este precepto recayeron las indicaciones números 3 y 4.

La indicación número 3, de Su Excelencia el Presidente de la República, es 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 estos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas y, en ambos casos, los mecanismos de control, supervisión y de responsabilidad ante infracciones.

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

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, puso de relieve que la indicación examinada determina el objeto de la ley -el que se recoge en el inciso primero del artículo 1 propuesto-; su ámbito de aplicación -contenido en el inciso segundo-, y su objetivo sustantivo -previsto en el inciso tercero-, consistente en que la institucionalidad de la ciberseguridad debe velar por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias.

Dando a conocer el acuerdo alcanzado por la mesa de trabajo, sostuvo que, acogiendo una observación de las Comisiones unidas, se decidió aprobar esta indicación con enmiendas, suprimiendo, en el inciso primero del artículo sugerido en la indicación, la frase ", en ambos casos,". Arguyó que esta última conducía a una interpretación equívoca de la norma.

Fijando su atención en el inciso segundo, sentenció que prescribe que la ley se aplicará a los organismos de la Administración del Estado, precisando cuáles son estos, y establece una regla especial para los órganos autónomos constitucionales; las empresas públicas creadas por ley, y las del Estado y sociedades en que este tenga participación accionaria superior al 50% o mayoría en el directorio.

El asesor legislativo del Honorable Senador señor Araya, señor Roberto Godoy, discrepó del acuerdo de la mesa de trabajo prelegislativa.

Profundizando en su afirmación, adelantó que la principal legislación existente en materia de ciberseguridad es la europea, conforme a la cual el bien jurídico protegido es el adecuado funcionamiento de los mercados internos de bienes y servicios y de los sistemas.

Consignado lo anterior, se adentró en el análisis de la indicación. Sobre el particular, notó que modifica el inciso único del artículo 1 y le incorpora dos nuevos.

En lo que atañe a la enmienda recaída en el primero de ellos -relativo al objeto de la ley-, connotó que la recomendación del Ejecutivo somete a esta legislación a todas las instituciones privadas, sin identificarlas ni definirlas.

Alertó que el inciso segundo, a su vez, al fijar el ámbito de aplicación, además de definir “Administración del Estado”-cuestión que por razones de técnica legislativa debe incluirse en el artículo 2-, excluye a las empresas públicas creadas por ley, a las del Estado y a las sociedades en que este tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.

A la luz de lo señalado, juzgó que se advierte la inconsistencia de que todas las entidades privadas deberán sujetarse a este cuerpo normativo, mientras que las recientemente citadas quedan al margen de él, a menos que sean catalogadas de la manera indicada.

Continuando con el análisis de la indicación, remarcó que, conforme a lo dispuesto en el inciso tercero, la institucionalidad de la ciberseguridad tendrá la misión de velar por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias. Al efecto, insistió en que, para la legislación europea, tal concepto está concebido desde una perspectiva funcional. De tal modo, precisó, se consagra en el Reglamento (UE) 2019/881, del Parlamento Europeo y del Consejo de la Unión Europea.

Plantear su regulación como un derecho subjetivo, acotó, introduce un modelo que no se aviene con el que suele tenerse como referente.

Para finalizar, hizo hincapié en que el artículo 1 constituye la piedra angular de esta futura ley, y no una mera disposición del proyecto.

Refiriéndose a las observaciones realizadas por el asesor que le antecedió en el uso de la palabra, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, recordó que, tal como lo expuso la Ministra del Interior y Seguridad Pública al dar inicio al estudio en particular de iniciativa, su ámbito de aplicación cambia sustancialmente luego de las indicaciones formuladas por Su Excelencia el Presidente de la República, señor Gabriel Boric.

Coincidió en que el texto aprobado en general por la Sala del Senado se basa en la norma de ciberseguridad identificada por el señor Godoy. Sin embargo, previno que esta fue modificada de forma radical recientemente. De hecho, ahondó, el Parlamento Europeo aprobó la Directiva de Seguridad de las Redes y de la Información 2 -NIS 2, por sus siglas en inglés- la que será publicada en las próximas semanas y contempla un giro significativo. Pormenorizó que la legislación citada propendía originalmente a la protección de los mercados, mas en la actualización aludida se busca la de los ciudadanos. Así, reiteró, la visión economicista fue abandonada.

Adicionalmente, relató que el derecho a la ciberseguridad nace en el mismo órgano que reconoció el de la autodeterminación informativa, el año 1978. En 2008, prosiguió, el tribunal federal alemán afirmó que las personas tienen derecho a la integridad, confidencialidad y disponibilidad de los datos contenidos en sistemas informáticos.

Por último, anunció que la iniciativa de ley, conforme a las indicaciones presentadas por el Ejecutivo, apunta a proteger los derechos de las personas y no los aparatos digitales. Por ello, agregó, un sistema coherente supone que el ámbito de aplicación de la ley se extiende a todo el sector público y al privado, estableciendo, posteriormente -entre los artículos 4 y 6-, sujetos especialmente obligados, que corresponden a los operadores de servicios esenciales y a los de importancia vital.

El Honorable Senador señor Galilea solicitó explicar por qué se decide someter a esta regulación a todas las instituciones privadas, mientras que, al tenor de lo prescrito en el inciso segundo, respecto de las públicas no se adopta igual criterio.

Atendiendo la consulta de Su Señoría, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aclaró que, en términos generales, el proyecto se aplica a los organismos del Estado, a las instituciones privadas y a las empresas públicas creadas por ley o en donde el Estado participe. No obstante, clarificó, las obligaciones especiales recaerán únicamente en quienes sean calificados como servicios esenciales y operadores de importancia vital, sin distinciones.

Aseguró que podrá ser declarado como un operador de servicios esenciales una empresa privada, una pública o una con participación del Estado. Al efecto, recalcó que el inciso segundo del artículo 3 propuesto señala que no se aplicarán las disposiciones de esta ley a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que este tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital. Igual criterio, reiteró, regirá para las empresas privadas.

El Honorable Senador señor Quintana consultó si los conceptos “servicios esenciales” y “operadores de importancia vital” son mundialmente utilizados.

Deteniéndose en la interrogante formulada por Su Señoría, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, subrayó que tradicionalmente se hablaba de infraestructura crítica para referirse a todo el universo de entidades. Sin embargo, actualmente, ha quedado acotada a las infraestructuras físicas propiamente tales; para lo demás se recurre a la locución “servicios esenciales”. Así se aprecia, continuó, en NIS 2, que emplea la expresión “operadores de servicios esenciales”.

Hizo ver que el texto analizado, en tanto, deja claramente establecido que, en materia digital, lo realmente trascendente son los servicios esenciales y los operadores de importancia vital.

Adicionalmente, enunció que el Ejecutivo buscará que las indicaciones que se formulen al proyecto de reforma constitucional de infraestructura crítica y al que modifica el sistema de inteligencia sean coherentes con esta nueva nomenclatura. En consecuencia, concluyó, la Constitución Política de la República abordará las capacidades físicas, mientras que esta iniciativa de ley, la prestación de servicios esenciales digitales.

El Honorable Senador señor Quintana discrepó de la tajante separación entre lo físico y lo cibernético expuesta por el personero de Gobierno. Sostuvo que basta con observar lo que ocurre con las criptomonedas para comprender la estrecha vinculación entre ambos mundos.

- En votación la indicación número 3, fue aprobada con la enmienda consignada anteriormente y otras de adecuación, por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana y Saavedra.

La indicación número 4, del Honorable Senador señor Insulza, busca sustituir la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”; y la expresión “órganos del Estado” por “organismos de la Administración del Estado”.

El Honorable Senador señor Huenchumilla previno que la Constitución Política de la República utiliza indistintamente ambas expresiones. Sin embargo, consignó, la ley de bases generales de la Administración del Estado emplea, mayoritariamente, la voz “órganos”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, afirmó que en el ordenamiento jurídico chileno se usan ambos términos.

Dicho lo anterior, informó que el Ejecutivo, luego de analizar la iniciativa de ley, distinguió dos tipos de obligaciones, unas que se aplicarán a todos los órganos del Estado y otras que solo recaerán en los que conforman la Administración del Estado.

En relación con los primeros, justificó que tal decisión obedece a la necesidad de incrementar los niveles de madurez en ciberseguridad.

Las Comisiones unidas optaron por resolver, en cada oportunidad en que el texto lo exija, cuál será la locución que corresponde emplear.

- La indicación número 4 fue retirada por su autor.

ARTÍCULO 2

Precisa, por medio de 17 numerales, la definición de algunas expresiones utilizadas en esta propuesta legal.

Número 1

Señala que por “Agencia” se entenderá la Agencia Nacional de Ciberseguridad.

Respecto de este numeral se presentó **la indicación número 5**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para intercalar entre la palabra “Ciberseguridad” y el punto final, la siguiente frase: “, que se conocerá en forma abreviada como ANCI”.

El Honorable Senador señor Insulza consultó si otros textos normativos -como la ley N° 19.974, sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia- consideran siglas.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, aseguró que para el Ejecutivo la indicación no reviste inconvenientes.

El Honorable Senador señor Quintana manifestó que las Comisiones unidas aún no han definido si el organismo encargado de la ciberseguridad se constituirá como una Agencia. De ser así, anunció su discrepancia, toda vez que “agenciar” implica encomendar un asunto de suma importancia para el Estado a un tercero.

El Honorable Senador señor Huenchumilla cuestionó el empleo de la voz “Agencia” en el derecho administrativo nacional. De hecho, recordó que la Ley de Bases Generales de la Administración del Estado no la incluye.

Para concluir, agregó que el vocablo referido proviene del modelo norteamericano. Ejemplo de ello es la Agencia Central de Inteligencia, sostuvo.

Deteniéndose en la inquietud del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, enfatizó que la palabra objeto de reparos se ha utilizado en los últimos años en el derecho administrativo chileno, demostrándolo así, verbigracia, la Agencia Nacional de Inteligencia.

Pese a lo señalado, develó que la discusión de fondo radica en la delegación en terceros de asuntos públicos.

Por último, llamó a tener presente que, no obstante la denominación conferida, se esconde detrás de la figura mencionada un servicio público sometido a la supervigilancia de Su Excelencia el Presidente de la República.

Discrepando de los planteamientos del Honorable Senador señor Quintana, **el Honorable Senador señor Ossandón** postuló que una Agencia dará mayor flexibilidad para atender asuntos que dicen relación con la ciberseguridad, los cuales evolucionan rápidamente. Además, recordó, la entidad dependerá del Primer Mandatario.

El Honorable Senador señor Quintana reconoció la importancia de que la estructura adoptada no dé paso a amarres. Con todo, recordó que la voz aludida no se encuentra consagrada en el derecho administrativo chileno, y que la figura implica que el Estado se desentiende del asunto. Tales razones, adujo, motivaron el reemplazo de la denominación de la Agencia Nacional de Acreditación por la de “Comisión Nacional de Acreditación”.

En atención a las diferencias existentes entre los integrantes de las Comisiones unidas, **el Honorable Senador señor Huenchumilla** aconsejó dejar pendiente el análisis de esta indicación en tanto no se examinen aquellas recaídas en el precepto referido a la naturaleza jurídica del órgano encargado de la ciberseguridad.

En una sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, manifestó que, tras una nueva revisión de esta indicación, el grupo de asesores conformado para facilitar la tramitación de la iniciativa de ley recomienda aprobarla.

- En consecuencia, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, respaldaron la indicación número 5.

Número 2

Dispone que el ciberataque consiste en la acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

Al respecto, se formularon las indicaciones números 6 y 7.

La indicación número 6, del Honorable Senador señor Insulza, es para reemplazar este numeral por el siguiente:

"2. Ciberataque: un incidente de ciberseguridad en el que una persona o grupo de ellas intenta destruir, exponer, alterar, deshabilitar, robar o ganar acceso no autorizado a un activo de información, o hacer uso no autorizado de un activo de información.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, comunicó que la mesa de trabajo constituida por asesores parlamentarios y del Ejecutivo propone aprobar la definición técnica sugerida, con enmiendas, a fin de perfeccionar su redacción y recoger, además, la dimensión física comprendida en la indicación que sigue. Consignó que, de acogerse la recomendación de la instancia mencionada, el tenor literal del número 2 del artículo 2 sería el que se transcribe a continuación:

"2. 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.".

El Honorable Senador señor Ossandón sugirió incorporar, luego de la palabra "persona", la locución ", natural o jurídica,", dejando claramente establecido que el ciberataque puede provenir también de estas últimas.

Sobre el punto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, estimó innecesario formular tal especificación, toda vez que la redacción actual comprende ambos tipos de personas.

El Honorable Senador señor Insulza manifestó interés por tener mayores antecedentes acerca de la voz “exfiltrar”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, explicó que la acción aludida corresponde a un concepto técnico, consistente en extraer de manera no autorizada datos desde un sistema.

- Puesta en votación la indicación número 6, fue aprobada con modificaciones, con la redacción consignada precedentemente, por la unanimidad de los miembros presentes de las instancias legislativas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas Comisiones-, Insulza, Ossandón, Saavedra y Van Rysselberghe.

La indicación número 7, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, agrega entre la palabra “soportan” y el punto final, la siguiente frase: “y/o que se vean afectados eléctrica o mecánicamente”.

- Sometida a votación, esta indicación fue respaldada con enmiendas, en los términos previstos con ocasión de la indicación anterior, por la totalidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Saavedra y Van Rysselberghe.

Número 3

Establece que el ciberespacio es el dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo y las interacciones sociales que se verifican en su interior.

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

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

En relación con este numeral se presentaron las indicaciones números 8 y 9.

La indicación número 8, del Honorable Senador señor Insulza, propone sustituir este numeral por el siguiente:

"3. Ciberespacio: ambiente formado por la interconexión e interrelación compleja entre las redes y sistemas de información, 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.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que la mesa de trabajo prelegislativa recomienda acoger esta indicación, toda vez que la definición prevista en ella es más exacta que la del texto aprobado en general. No obstante, detalló, al igual que en oportunidades anteriores y por la misma razón, sugiere reemplazar la expresión "sistemas de información" por "sistemas informáticos".

- Las Comisiones unidas, por la unanimidad de sus integrantes presentes, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe, aprobaron la indicación con la modificación señalada.

La indicación número 9, de Su Excelencia el Presidente de la República, busca suprimir la frase "que abarcan los dominios físico, virtual y cognitivo", del texto despachado en general.

- En atención a la aprobación de la indicación anterior, fue rechazada por la totalidad de los miembros presentes de las instancias legislativas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas Comisiones-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

Número 4

Define a la ciberseguridad como el conjunto de acciones destinadas al estudio y manejo de las amenazas y riesgos de incidentes de ciberseguridad; a la prevención, mitigación y respuesta frente a estos, así como para reducir sus efectos y el daño causado, antes, durante y después de su ocurrencia, respecto de los activos informáticos y de servicios.

Al efecto, se formuló **la indicación número 10**, del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

"4. Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas de información, con el objetivo de proteger a

las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que la mesa de trabajo conformada para el estudio preliminar de las indicaciones estima que la definición sugerida por el Honorable Senador señor Insulza para “ciberseguridad” es mejor que aquella aprobada en general por el Senado, motivo por el cual recomienda su aprobación. Con todo, al igual que en ocasiones anteriores, considera necesario reemplazar la expresión “sistemas de información” por “sistemas informáticos”.

- Puesta en votación la indicación número 10, resultó aprobada con la enmienda consignada precedentemente, por la totalidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

Número 5

Especifica que se entiende por equipo de respuesta a incidentes de seguridad informática o CSIRT a los centros conformados por especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, y que actúan según procedimientos y políticas predefinidas, coadyuvando asimismo a mitigar sus efectos.

Sobre este numeral recayeron las indicaciones números 11 y 12.

La indicación número 11, del Honorable Senador señor Insulza, es para reemplazarlo por el siguiente:

“5. 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 procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.”.

Las Comisiones unidas advirtieron la necesidad de incorporar, entre las palabras “conforme” y “procedimientos”, la preposición “a”.

- Sometida a votación la indicación número 11, fue respaldada con enmiendas meramente formales, por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

La indicación número 12, de Su Excelencia el Presidente de la República, busca sustituir la expresión “coadyuvando asimismo” por la palabra “ayudando”.

- En atención a la aprobación de la indicación anterior, fue rechazada por la totalidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

Número 6

Define la locución “estándares mínimos de ciberseguridad”, señalando que estos corresponden al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad, dictados por la Agencia o por el regulador sectorial competente, los cuales deben ser cumplidos por los órganos de la Administración del Estado y por quienes posean infraestructura de la información calificada como crítica.

Al respecto, se presentaron las indicaciones números 13 y 14.

La indicación número 13, de Su Excelencia el Presidente de la República, reemplaza la frase “el regulador sectorial competente, los cuales deben ser cumplidos por los órganos de la Administración del Estado y por quienes posean infraestructura de la información calificada como crítica”, por el siguiente texto: “la autoridad sectorial competente de conformidad con la presente ley”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, expresó que la mesa de asesores recomienda aprobar la sustitución aludida. Detalló que la enmienda propuesta por el Ejecutivo simplifica la definición de la expresión “estándares mínimos de ciberseguridad”, y la ajusta al nuevo modelo regulatorio diseñado. En definitiva, ahondó, podrán ser dictados por la Agencia Nacional de Ciberseguridad o por la autoridad sectorial competente.

El Honorable Senador señor Quintana advirtió que la indicación examinada suprime la referencia a la infraestructura crítica de la información, medida que aseguró no compartir. Por ese motivo, anunció que no la respaldaría.

El Honorable Senador señor Galilea, a su turno, puso de relieve que el reemplazo en estudio no solo simplifica la definición, sino que, además, elimina la posibilidad de que todos quienes posean infraestructura crítica de la información puedan dictar normas de ciberseguridad.

Atendiendo la observación realizada por el legislador que le precedió en el uso de la palabra, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aclaró que el texto aprobado en general por el Senado no faculta a tales actores a dictar reglas de seguridad informática. Esa función, remarcó, corresponde a la Agencia Nacional de Ciberseguridad o al regulador sectorial competente. Las entidades aludidas por Su Señoría, connotó, son los sujetos obligados a su cumplimiento.

En otro orden de ideas, solicitó dejar pendiente el debate y votación de este numeral mientras no se realice el de las indicaciones recaídas en el artículo 6.

En una sesión posterior y luego de zanjarse la redacción del precepto citado, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que la mesa de trabajo prelegislativo sugiere respaldar esta indicación, de manera que haya coherencia con la idea aprobada anteriormente por las Comisiones unidas, relativa a que la facultad normativa quede radicada en la Agencia Nacional de Ciberseguridad o en el regulador sectorial, según corresponda.

- Puesta en votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron esta indicación con enmiendas simplemente formales.

La indicación número 14, del Honorable Senador señor Insulza, sustituye la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

- Esta indicación fue retirada por su autor.

Número 7

Consigna que por gestión de incidente de ciberseguridad se entiende el conjunto ordenado de acciones enfocadas a prevenir en la medida de lo posible la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.

Sobre este numeral recayeron las indicaciones números 15 y 16.

La indicación número 15, del Honorable Senador señor Insulza, busca reemplazar la frase “Gestión de incidente de ciberseguridad” por su plural “Gestión de incidentes de ciberseguridad”.

- Puesta en votación, fue aprobada por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

La indicación número 16, de Su Excelencia el Presidente de la República, es para suprimir la frase “en la medida de lo posible”.

- Sometida a votación, fue respaldada por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

Número 8

Precisa que un incidente de ciberseguridad es todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos a través sistemas de telecomunicaciones y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

Al respecto, se presentó **la indicación número 17**, del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

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

El Honorable Senador señor Huenchumilla consultó si las redes o sistemas informáticos pueden ser resilientes.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, fue tajante en señalar que así debiera ser. Ello, justificó, porque inevitablemente serán objeto de ciberataques, y deben tener la capacidad de recuperarse prontamente.

- Puesta en votación la indicación número 17, fue aprobada por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Galilea, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Quintana, Saavedra y Van Rysselberghe.

Número 9

Señala que la infraestructura crítica de la información corresponde a aquellas instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción puede tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar.

Sobre este numeral recayeron las indicaciones números 18, 19 y 20.

La indicación número 18, de Su Excelencia el Presidente de la República, lo sustituye por el siguiente:

"9. 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 de información, y cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, propuso dejar pendiente el estudio de esta indicación en tanto no se analicen y voten aquellas recaídas en el artículo 4.

- En una sesión posterior, y luego de determinarse la redacción del artículo 4, las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe, respaldaron tal indicación, con una enmienda de adecuación.

La indicación número 19, del Honorable Senador señor Van Rysselberghe, elimina la palabra "instalaciones".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, solicitó no abordar esta indicación mientras no se examinen y resuelvan aquellas formuladas al artículo 4.

- En una sesión posterior, esta indicación fue retirada por su autor.

La indicación número 20, del Honorable Senador señor Van Rysselberghe, sustituye la frase ", y servicios y equipos físicos y de tecnología de la información", por la siguiente expresión: "y servicios".

Dando a conocer la opinión de la mesa de trabajo prelegislativo, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, llamó a dejar pendiente el estudio de esta indicación en tanto no se determine la redacción del artículo 4.

- En una sesión posterior, el Honorable Senador señor Van Rysselberghe retiró la indicación de su autoría.

Número 10

Dispone que la red o sistema de información es el medio en virtud del cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí.

Respecto de este numeral se formularon las indicaciones números 21 y 22.

La indicación número 21, de Su Excelencia el Presidente de la República, es para reemplazarlo por el que sigue:

“10. Red de datos: conjunto de dispositivos, cables y equipos de comunicaciones que almacenan, procesan o transmiten datos digitales.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, manifestó que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda rechazar esta indicación, de manera de acoger la siguiente.

- Respaldando tal sugerencia, las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe, desecharon esta indicación.

La indicación número 22, del Honorable Senador señor Insulza, busca sustituir este número por el siguiente:

“10. Red o sistema de información: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.”.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que la mesa de trabajo prelegislativo propone acoger esta indicación, reemplazando la expresión “sistema de información” por “sistema informático”, tal como se ha hecho en ocasiones precedentes, y por la misma razón.

- Puesta en votación, esta indicación resultó aprobada con la enmienda consignada anteriormente, por la totalidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe.

Número 11

Establece que se entiende por regulador o fiscalizador sectorial aquellos servicios públicos dentro de cuyas funciones se encuentra la regulación y/o supervigilancia de uno o más sectores regulados.

Sobre este numeral recayó **la indicación número 23**, de Su Excelencia el Presidente de la República, para consultar, en su lugar, el siguiente:

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

- Sometida a votación, esta indicación fue respaldada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe.

Número 12

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

Al respecto, se presentó **la indicación número 24**, del Honorable Senador señor Insulza, para reemplazarlo por el que sigue:

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

Adentrándose en el análisis de esta indicación, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, reveló que el grupo de asesores conformado para facilitar la tramitación del proyecto sugiere respaldarla. Con todo, resaltó que, al igual que en otras oportunidades, se propone sustituir la expresión "sistemas de información" por "sistemas informáticos".

- En votación, esta indicación fue aprobada con la enmienda citada precedentemente, por la totalidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe.

Número 13

Especifica que riesgo es toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes o sistemas de información. Puntualiza que se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto negativo en éstas.

Sobre este numeral recayó **la indicación número 25**, del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

"13. 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 incidente.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, recomendó aprobar esta indicación. No obstante, para evitar redundancias, llamó a reemplazar la locución "del incidente", la segunda vez que aparece, por "del mismo".

- Las Comisiones unidas, por la unanimidad de sus integrantes presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe, aprobaron esta indicación con la enmienda formal referida.

Número 14

Define sector regulado como aquel que representa alguna actividad económica estratégica nacional, que se encuentra sometido a la supervigilancia de un regulador o fiscalizador sectorial.

Respecto de este numeral se formuló **la indicación número 26**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

"14. 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.".

- Puesta en votación, esta indicación fue respaldada por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de

integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe.

Número 15

Consigna que se entiende por servicios esenciales todo aquel respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción de su infraestructura de la información pueda afectar gravemente algunos de las áreas indicadas entre los literales a) y e).

Letra a)

“a) La vida o integridad física de las personas;”

Letra b)

“b) La provisión de servicios sanitarios, energéticos o de telecomunicaciones;”

Letra c)

“c) Al normal funcionamiento de obras públicas fiscales y medios de transporte;”

Letra d)

“d) A la generalidad de usuarios o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que permitan la transacción de dinero o valores; y”

Letra e)

“e) De modo general, el normal desarrollo y bienestar de la población.”.

Sobre este numeral recayó **la indicación número 27**, de Su Excelencia el Presidente de la República, para sustituirlo por el que sigue:

“15. 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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, comunicó que la mesa de trabajo prelegislativo estima necesario dejar pendiente la votación de esta indicación en tanto no se determine la redacción del artículo 4 del proyecto.

- En una sesión posterior, y luego de definirse la redacción del artículo 4 de la iniciativa de ley, la unanimidad de los parlamentarios presentes de las Comisiones unidas, Honorables

Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe, aprobó esta indicación.

Número 16

Precisa que por sistema informático se entiende todo dispositivo aislado o el conjunto de ellos, interconectados o relacionados entre sí, incluidos sus soportes lógicos, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Al respecto, se presentó **la indicación número 28**, del Honorable Senador señor Insulza, para reemplazarlo por el siguiente:

"16. Activo informático: toda información almacenada en una red o sistema de información que tenga valor para una persona u organización.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, relató que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda respaldar esta indicación. Sin embargo, advirtió que, al igual que en ocasiones anteriores, sugiere sustituir la expresión "sistema de información" por "sistema informático".

- Sometida a votación, esta indicación fue aprobada con enmiendas por todos los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh y Van Rysselberghe.

°°°°°

Números nuevos

A continuación, se formuló **la indicación número 29**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para incorporar los siguientes números, nuevos:

"…. Amenaza persistente avanzada (APT): ataque informático sigiloso, continuo y oculto, dirigido por una compañía, un individuo, un grupo o un Estado, cuyo objetivo es observar, filtrar o modificar datos o recursos de una empresa, una organización o un Estado.".

Al respecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, sostuvo que la mesa de trabajo prelegislativo discrepa de la idea de incluir la definición del concepto aludido.

- Las Comisiones unidas, por la unanimidad de sus integrantes presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza,

Macaya, Ossandón, Pugh y Van Rysselberghe, rechazaron esta parte de la indicación.

Otro número, nuevo, cuya incorporación propone la indicación número 29, es el que sigue:

"…. Anonimización: proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere, protegiendo así los datos de carácter personal.".

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, manifestó que el grupo de asesores conformado para facilitar la tramitación del proyecto disiente de la idea de incorporar esta definición.

- En votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe, rechazaron la inclusión de tal término en esta parte de la indicación número 29.

Luego, la indicación número 29 propone introducir la locución que se transcribe:

"…. 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 y Riesgo de la Información y Ciberseguridad – SGSRI.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, anunció que la mesa de trabajo prelegislativo recomienda aprobar la incorporación de la expresión aludida, mas sugiere definirla de manera más técnica, de la forma que sigue:

"…. 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.".

- Puesta en votación, esta parte de la indicación número 29 fue aprobada en los términos expuestos, por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Asimismo, la indicación número 29 busca incluir el siguiente número, nuevo, al artículo 2:

"…. Ciberhigiene: conducta personal responsable referida a la actitud de cautela que debe tener un usuario al conectarse a los sistemas informáticos, incluyendo el cuidado de las claves personales, el visitar

sitios dudosos y conexiones en redes abiertas, establecer nexos con desconocidos a través de las redes sociales, o compartir información a través de medios extraíbles.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que el grupo de asesores conformado para facilitar la tramitación del proyecto valora la idea de agregar esta definición. Con todo, precisó, sugiere reemplazarla por la que sigue:

“…. 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.”.

- Sometida a votación, esta parte de la indicación número 29 fue respaldada con la redacción precedente, por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Adicionalmente, la indicación número 29 propone incorporar el siguiente número, nuevo, al artículo 2:

“…. Confianza digital: integridad, confidencialidad y trazabilidad de los datos e información proveniente de sistemas o equipos que intercambian información o realizan transacciones digitales de cualquier tipo.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, aseveró que la mesa de trabajo prelegislativo recomienda rechazar la incorporación del concepto consignado. Adujo que tal decisión descansa en que dicho término no es utilizado en el proyecto de ley, a diferencia de otras expresiones como confidencialidad, integridad, disponibilidad, autenticación y no repudio, respecto de las cuales, añadió, existe, además, amplio consenso, toda vez que se condicen con los estándares técnicos internacionales. En consecuencia, concluyó, se sugiere no incluir en la nómina del artículo 2 la referencia a la confianza digital, pero si las palabras citadas, como se detallará más adelante.

- Todos los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe, compartieron la idea de rechazar la inclusión de la definición transcrita en esta parte de la indicación número 29.

Por otro lado, la indicación número 29 considera la incorporación del número, nuevo, que sigue al artículo 2:

"…. Integridad: propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware, intervención humana o por condiciones medioambientales.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sostuvo que el grupo de asesores conformado para facilitar la tramitación del proyecto sugiere aprobar con modificaciones la propuesta anterior. Ahondando en su afirmación, puntualizó que se recomienda una nueva definición para la voz "integridad" y sumar la inclusión de los vocablos "confidencialidad", "disponibilidad", "autenticación" y "no repudio". Previno que todas ellas se emplean en el texto.

Adelantó que, de seguir el consejo de la instancia mencionada, se agregarían a la lista del artículo 2 las siguientes palabras con el significado que en cada caso se menciona:

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

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

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

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

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

- Puesta en votación, esta parte de la indicación número 29 fue respaldada con las enmiendas anteriores, por la totalidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

A continuación, la indicación número 29 propone la inclusión del siguiente número, nuevo, al artículo 2:

"…. Interagencialidad: coordinación que permite que dos o más agencias o instituciones actúen de forma conjunta, sinérgica y coherente para alcanzar un objetivo o tarea común del Estado, imposible de lograr de forma independiente.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, expresó que la mesa de trabajo prelegislativo sugiere aprobar la voz citada con modificaciones, reemplazando la locución “un objetivo o tarea común del Estado” por “objetivos comunes” y el vocablo “imposible” por su plural “imposibles”.

Pormenorizó que, de apoyarse el criterio del grupo de asesores, el número en análisis quedaría como sigue:

“…. 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.”.

- Sometida a votación, esta parte de la indicación número 29 fue aprobada con las enmiendas aludidas, por la unanimidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Más adelante, la indicación número 29 sugiere la incorporación del número, nuevo, siguiente:

“…. Interoperabilidad: capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos, en tiempo real, habilitando la confianza digital y asegurando la certeza jurídica de los actos digitales.”.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, planteó que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda aprobar con modificaciones la inclusión del concepto, en los términos que se transcribe:

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

- Las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe, respaldó esta parte de indicación número 29 con la enmienda referida.

Seguidamente, la indicación número 29 propone incorporar el siguiente número, nuevo, al artículo 2:

"…. Registro de proveedores de servicios de ciberseguridad: listado o repertorio de las personas naturales y/o jurídicas que realicen, con el fin de proteger las redes y sistemas informáticos, al menos una de las siguientes actividades: implementación de políticas, procedimientos y medidas, consultoría, capacitación, información, investigación, desarrollo, innovación, auditoría, evaluación, prueba de medidas implementadas, gestión de riesgos e incidentes de seguridad.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que la mesa de trabajo prelegislativo discrepa de la idea de incluir el término citado.

- Acogiendo la propuesta anterior, todos los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe, rechazaron esta parte de indicación número 29.

Por otra parte, la indicación número 29 sugiere considerar el siguiente número, nuevo, dentro del artículo 2:

"…. Sistema de Gestión de la Seguridad y Riesgo de la Información – SGSRI: sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información, y su Ciberseguridad. Incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos, los recursos y la infraestructura física.".

Pronunciándose sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que el grupo de asesores conformado para facilitar la tramitación del proyecto coincide en la necesidad de introducir la definición consignada. No obstante, acotó, se proponen ciertas modificaciones, de modo que su redacción quede así:

"…. 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.".

- Puesta en votación, esta parte de la indicación número 29 resultó aprobada en los términos expuestos, por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Finalmente, la indicación número 29 recomienda incluir el número que se indica al artículo 2:

"…. Trazabilidad: propiedad o característica consistente en que las actuaciones digitales de una entidad pueden ser imputadas exclusivamente a dicha entidad.".

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseguró que la mesa de trabajo prelegislativo está por desechar la inclusión de este concepto.

- Sometida a votación, esta parte de la indicación fue rechazada por la totalidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

°°°°°

°°°°°

Números nuevos

Seguidamente, el Honorable Senador señor Pugh, formuló **la indicación número 30**, para consultar los siguientes números, nuevos:

"…. Catálogo nacional de operadores esenciales: la información completa y actualizada relativa a las características específicas de cada uno de los operadores esenciales existentes en el territorio nacional, en los términos que señale la presente ley.

…. Operador de servicios esenciales – OSE: entidad pública o privada que se identifique considerando los factores establecidos en la presente ley.".

- Esta indicación fue retirada por su autor.

°°°°°

Artículo 3

Establece, por medio de ocho numerales, los principios rectores que deberán observarse en la aplicación de las disposiciones de esta ley.

Número 1

El texto aprobado en general dice lo siguiente:

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

Al respecto, se formuló **la indicación número 31**, del Honorable Senador señor Van Rysselberghe, para sustituir la expresión “ofrece u opera” por “desarrolla, ofrece u opera”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, expresó que el grupo de asesores conformado para facilitar la tramitación del proyecto valora la modificación anterior. Con todo, apuntó que recomienda reemplazar la voz “desarrolla” por “provee”.

En consecuencia, la redacción quedaría como se expresa a continuación:

“1. 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.”.

- Las Comisiones unidas, por la totalidad de sus legisladores presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe, aprobaron la indicación con la enmienda propuesta.

Número 3

Su tenor es el que sigue:

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

Sobre este numeral recayó **la indicación número 32**, del Honorable Senador señor Insulza, para reemplazar la frase “los datos, conectividad y sistemas deberán ser exclusivamente accedidos” por “la información almacenada o transmitida por redes y sistemas de información deberá ser conocida y accedida exclusivamente”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que la mesa de trabajo prelegislativo sugiere acoger tal indicación, pero sustituyendo la expresión “sistemas de información” por “sistemas informáticos”.

En virtud de tal recomendación, este principio quedaría como se señala:

“3. 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.”.

- En votación, esta indicación resultó respaldada con el texto antes referido, por la unanimidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Número 4

La redacción aprobada en general prescribe:

“4. Principio de integridad de los sistemas informáticos y de la información: los datos y elementos de configuración de un sistema solo podrán ser modificados por personas autorizadas en el ejercicio de sus funciones o por sistemas que cuenten con la autorización respectiva.”.

Respecto de este numeral se presentó **la indicación número 33**, del Honorable Senador señor Insulza, para sustituir la frase “los datos y elementos de configuración de un sistema” por “la información almacenada o transmitida por redes y sistemas de información, incluida la configuración de estos,”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, señaló que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda aprobar esta indicación, reemplazando la expresión “sistemas de información” por “sistemas informáticos”.

En consecuencia, el texto que se sugiere aprobar es el siguiente:

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

- Puesta en votación, esta indicación fue respaldada con la enmienda consignada, por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Número 5

Dispone lo que expresa a continuación:

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

En relación con este numeral, se formuló **la indicación número 34**, del Honorable Senador señor Insulza, para reemplazar la frase “los datos, conectividad y sistemas” por “la información almacenada o transmitida por redes y sistemas de información, y las redes y sistemas de información”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, declaró que la mesa de trabajo prelegislativo sugiere acoger tal indicación, pero sustituyendo la expresión “sistemas de información” por “sistemas informáticos”.

En virtud de lo anterior, la redacción de este numeral quedaría como sigue:

“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.”.

- Sometida a votación, esta indicación fue aprobada con la enmienda mencionada, por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Número 6

Establece lo que se transcribe:

“6. Principio de control de daños: los órganos del Estado y aquellas instituciones privadas que posean infraestructura de la información calificada como crítica, en el caso de un incidente de ciberseguridad o de un ciberataque, deben siempre actuar diligentemente y adoptar las medidas necesarias para evitar la escalada del incidente de ciberseguridad o del ciberataque y su posible propagación a otros sistemas

informáticos, notificando de igual forma el incidente de ciberseguridad al CSIRT respectivo.”.

Al respecto, se presentaron las indicaciones números 35, 36 y 37.

La indicación número 35, de Su Excelencia el Presidente de la República, es para sustituirlo por el siguiente:

“6. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad, todos los órganos 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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, comunicó que el grupo de asesores conformado para facilitar la tramitación del proyecto comparte la propuesta del Primer Mandatario. Sin embargo, observó, sugiere aprobarla con modificaciones, a fin de reemplazar la expresión “órganos del Estado” por “organismos del Estado”, como lo recomienda la indicación siguiente.

- Las Comisiones unidas, por la totalidad de sus legisladores presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron la indicación con la enmienda citada.

La indicación número 36, del Honorable Senador señor Insulza, busca reemplazar la expresión “órganos del Estado” por “organismos del Estado”.

- En votación, las Comisiones unidas, por la unanimidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron la indicación.

La indicación número 37, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, es para intercalar entre las palabras “necesarias” y “para”, la siguiente frase: “en un plazo no superior a 24 horas,”.

- Puesta en votación, las Comisiones unidas, por la totalidad de sus integrantes presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, rechazaron la indicación.

Número 7

El texto aprobado en general prescribe:

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

Sobre este numeral recayó **la indicación número 38**, del Honorable Senador señor Insulza, para sustituir la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, aseguró que la mesa de trabajo prelegislativo recomienda aprobar la indicación anterior.

Al efecto, **las Comisiones unidas** advirtieron que el reemplazo sugerido extiende el ámbito de aplicación de la ley, obligando a observar el principio de cooperación con la autoridad a todos los organismos del Estado y no solo a aquellos dependientes de su Administración. Por consiguiente, previno, la indicación en examen aborda una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República, conforme lo dispone el artículo 65, inciso cuarto, número 2°, de la Constitución Política de la República.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, anunció que el Ejecutivo acogerá la proposición analizada.

- Habida cuenta del compromiso enunciado, las Comisiones unidas aprobaron ad referéndum la indicación, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 38 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Asimismo, los miembros de las Comisiones unidas estimaron que la idea comprendida en la indicación número 38, se entiende recogida en la indicación número 38 bis.

Número 8

El texto aprobado en general reza lo que se expresa a continuación:

“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.”.

Respecto de este numeral se formularon las indicaciones números 39 y 40.

La indicación número 39, de Su Excelencia el Presidente de la República, lo reemplaza por el siguiente:

“8. 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.”.

- Sometida a votación, las Comisiones unidas, por la totalidad de sus integrantes presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron la indicación.

La indicación número 40, del Honorable Senador señor Van Rysselberghe, lo sustituye por el que sigue:

“8. Principio de especialidad: en materia regulatoria y sancionatoria, se preferirá la aplicación de lo dispuesto por el regulador o fiscalizador sectorial por sobre la establecida en esta ley.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, planteó que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda dejar pendiente el examen de esta indicación, a fin de abordarla de forma conjunta con el artículo 7.

- En una sesión posterior, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, rechazaron esta indicación.

°°°°°

Número nuevo

Asimismo, se presentó **la indicación número 41**, de Su Excelencia el Presidente de la República, para incorporar el siguiente numeral, nuevo, consultado como número 9:

"9. Principio de igualdad y no discriminación: para que todas las personas tengan garantizado el disfrute de sus derechos y libertades fundamentales en el entorno digital se deberán priorizar aquellos programas, proyectos y acciones dirigidos a la protección de la seguridad informática, especialmente de niños, niñas y adolescentes, mujeres, personas de la tercera edad, diversidades y disidencias sexuales y de género.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, declaró que la mesa de trabajo prelegislativo sugiere desechar esta indicación, a fin de acoger la que sigue.

- Las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, rechazaron esta indicación.

°°°°°

°°°°°

Número nuevo

También se formuló **la indicación número 42**, del Honorable Senador señor Insulza, para consultar el siguiente número 9, nuevo:

"9. 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.".

El Honorable Senador señor Huenchumilla preguntó por el empleo de la locución "disidencias sexogenéricas".

Atendiendo la inquietud del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que, actualmente, para hacer referencia a las diversidades sexuales y de identidad de género se utiliza la expresión mencionada. A mayor abundamiento, sentenció, es la más apropiada para evitar discriminaciones.

Las Comisiones unidas alertaron que la indicación en estudio aborda materias de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo dispuesto en el artículo 65, inciso cuarto, número 2°, del Texto Supremo.

En relación con el reparo consignado, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, anunció que el Ejecutivo acogerá la propuesta del Honorable Senador señor Insulza, en una futura indicación.

- Por consiguiente, puesta en votación ad referéndum, esta indicación contó con el voto favorable de la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 42 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Asimismo, los miembros de las Comisiones unidas estimaron que la idea comprendida en la indicación número 42, se entiende recogida en la indicación número 42 bis.

°°°°°

°°°°°

Números nuevos

Además, se presentó **la indicación número 43**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para incorporar los siguientes numerales, nuevos.

El primero de ellos es el que se transcribe:

“…. Principio de confianza cero: iniciativa de carácter estratégico que elimina el concepto de confianza en una red de datos, hasta que ésta sea vulnerada. Se basa en el concepto “No confiar nunca, verificar siempre”, y asume que cada transacción, entidad e identidad no son de confianza hasta que se establece la confianza y se mantiene a lo largo del tiempo.”.

En lo que concierne al principio referido, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, puso de relieve que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda rechazar su inclusión.

El Honorable Senador señor Pugh remarcó que el principio objeto de análisis es empleado en la legislación comparada, iluminando la operación de sistemas informáticos en la dirección señalada.

Reconoció que la confianza cero no queda adecuadamente articulada dentro del texto legal. Con todo, anheló su consideración en el reglamento de esta futura ley, de modo de incentivar el cambio de cultural y hacer ver los riesgos que se desprenden de la manipulación del conjunto de elementos físicos y lógicos capaces de guardar y procesar información.

- Sometida a votación, esta parte de la indicación número 43 fue rechazada por la totalidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Otro número cuya incorporación se propone al artículo 3 es el que se señala:

“…. Principio de actualización y reutilización: en cuya virtud los órganos de la Administración del Estado deberán actualizar sus plataformas a tecnologías no obsoletas o carentes de soporte, así como generar medidas que permitan el rescate de los contenidos de formatos de archivo electrónicos que caigan en desuso y el empleo de algoritmos que se mantengan vigentes.”.

En lo que atañe a este principio, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseguró que la mesa de trabajo prelegislativo celebra su inclusión. Con todo, puntualizó, sugiere modificar su redacción, quedando de la manera que sigue:

“…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.”.

Las Comisiones unidas estuvieron contestes en que este principio dice relación con materias de iniciativa exclusiva de Su Excelencia el Presidente de la República, según lo previsto en el artículo 65, inciso cuarto, número 2°, de la Carta Fundamental.

Pronunciándose sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, anunció que el Ejecutivo respaldará la indicación en estudio en lo que refiere a este principio.

- Habida cuenta del compromiso adquirido, las Comisiones unidas, por la unanimidad de sus integrantes presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron ad referéndum con enmiendas esta parte de la indicación número 43.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 43 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Asimismo, los miembros de las Comisiones unidas estimaron que la idea comprendida en la indicación número 43, se entiende recogida en la indicación número 43 bis.

El siguiente numeral que se sugiere considerar en el artículo 3 es el que se señala:

"…. Principio de cooperación: en cuya virtud los distintos órganos de la Administración del Estado deben cooperar efectivamente entre sí en la utilización de medios electrónicos, anonimizando datos cuando así sea necesario.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, hizo hincapié en que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda rechazar su inclusión.

- En votación esta parte de la indicación número 43, resultó rechazada por la totalidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Asimismo, la indicación número 43 recomienda incluir el siguiente numeral al artículo 3:

"…. Principio de interoperabilidad: consiste en que los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado, a través de estándares abiertos que permitan una segura y expedita interconexión entre ellos, dándole certeza jurídica a todos los actos digitales.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sostuvo que la instancia prelegislativa discrepa de la idea de incorporar el principio referido.

El Honorable Senador señor Pugh puso de relieve que la interoperabilidad constituye una materia de suma importancia que se vincula con la ley N° 21.180, sobre transformación digital del Estado. Sin embargo, connotó, requiere un cuerpo legal específico.

A la luz de lo expuesto, instó al Ejecutivo a presentar una iniciativa de ley sobre gobernanza de la interoperabilidad, siguiendo el modelo europeo, que es el que ha demostrado mejores resultados. Solo así, enfatizó, el Estado será exitoso en el mundo digital.

- Puesta en votación, esta parte de la indicación número 43 fue rechazada por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Por último, la indicación número 43 sugiere incorporar el siguiente numeral al artículo 3:

"…. Principio de no obsolescencia tecnológica: el uso de programas y equipos actualizados, de origen determinado, con procesos de mantención, actualización y certificaciones al día, propuestos por los proveedores o desarrolladores. Los equipos y programas que no cuenten con soporte técnico responsable, deberán ser reemplazados en un período no superior a 6 meses desde su caducidad.".

Acerca de tal propuesta, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que el grupo de asesores conformado para facilitar la tramitación del proyecto aún no ha alcanzado un acuerdo respecto de su redacción, motivo por el cual sugiere dejar pendiente su votación.

En la sesión posterior, **el Honorable Senador señor Pugh** sostuvo que la obsolescencia es una variable esencial en el marco de la ciberseguridad, puesto que el rápido avance de la tecnología conlleva que los equipamientos, procedimientos y protocolos queden en desuso de un momento a otro. Con todo, planteó que este principio debiera recogerse en el sistema integrado de gestión de riesgos del país.

Por su parte, **el Honorable Senador señor Saavedra** notó que la no obsolescencia tecnológica es una medida fundamental para la seguridad, y obliga a reemplazar oportunamente los equipos y softwares.

- Sometida a votación, esta parte de la indicación número 43 fue rechazada por seis votos en contra, de los Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Ossandón, Saavedra -en su condición de miembro de ambas Comisiones- y Van Rysselberghe, y una abstención, del Honorable Senador señor Pugh.

°°°°°

TÍTULO II

Lleva por epígrafe “De la determinación de Infraestructura Crítica de la Información”.

En relación con el título referido, se formuló **la indicación número 44**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para suprimirlo.

- Esta indicación fue rechazada por la unanimidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Ossandón, Pugh, Saavedra -en su condición de miembro de ambas Comisiones- y Van Rysselberghe.

EPÍGRAFE

Sobre él recayó **la indicación número 45**, de Su Excelencia el Presidente de la República, para sustituir su denominación por la siguiente:

“TÍTULO II
Obligaciones de ciberseguridad”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, explicó que esta indicación, así como aquellas formuladas por el Primer Mandatario a los artículos 4, 5 y 6 del texto aprobado en general, reemplazan la referencia a las infraestructuras críticas de la información por otras relativas a los servicios esenciales y operadores de importancia vital.

Adelantó que en el grupo de asesores conformado para facilitar la tramitación de la propuesta legal hay consenso respecto del cambio citado, pese a lo cual se introducen algunas modificaciones menores que se detallarán oportunamente.

- En votación, esta indicación fue respaldada por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

PÁRRAFO 1°

Se denomina “Determinación de la infraestructura crítica de la información”.

EPÍGRAFE

Al efecto, se presentó **la indicación número 46**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

“Párrafo 1°
Servicios esenciales y operadores de importancia vital”.

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe, aprobaron esta indicación.

ARTÍCULO 4

Señala el procedimiento y los factores a tener en consideración para determinar si un sector o institución posee infraestructura de la información que deba calificarse como crítica.

Inciso primero

Su tenor literal es el siguiente:

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

Inciso segundo

Especifica, por medio de cuatro literales, los factores a atender para determinar si en un sector o institución existe infraestructura de la información que deba calificarse como crítica.

Letra a)

Reza lo siguiente:

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

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

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

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

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

Letra b)

Consiga lo que sigue:

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

Letra c)

Prescribe lo que se indica:

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

Letra d)

Señala lo siguiente:

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

Inciso tercero

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

Inciso cuarto

Consigna que, sin perjuicio de lo dispuesto en los incisos anteriores, se entenderá que poseen infraestructura crítica de la información todos los órganos del Estado, incluidas las municipalidades, las entidades fiscales autónomas, las empresas del Estado o aquellas en las que el Fisco tenga intervención por aportes de capital.

En relación con el precepto referido se formularon las indicaciones números 47, 48, 49 y 50.

La indicación número 47, de Su Excelencia el Presidente de la República, es para sustituirlo por el siguiente:

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

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

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

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

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

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.

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

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

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, declaró que la mesa de trabajo prelegislativo recomienda aprobar la indicación con modificaciones. Estas, puntualizó, consisten en reemplazar, en el literal b) del inciso tercero, la expresión “de información” por “informáticos”, como se ha hecho en otras oportunidades; en sustituir, en el inciso cuarto, letra b), la voz “dependencia” por “interdependencia”, de manera hacer ver que la sujeción puede ser multidireccional y no solo jerárquica, y en incorporar dos nuevos factores que permitirán determinar si el impacto de un incidente de ciberseguridad puede ser perturbador. Estos últimos, relató, son la afectación relevante del funcionamiento del Estado y sus organismos y el daño reputacional que pueda ocasionarse.

Reveló que, de acogerse la sugerencia aludida, la redacción del artículo 4 del proyecto de ley quedaría como sigue:

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

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

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

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

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

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

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

a) La cantidad de usuarios potencialmente afectados;

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

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

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

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

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

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

h) El daño reputacional que pueda ocasionarse.

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

Transcurrido este plazo, con los antecedentes que hubiere recibido, la Agencia propondrá una lista actualizada de servicios esenciales y de operadores de importancia vital al Comité Interministerial sobre 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 sobre 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.”.

El Honorable Senador señor Pugh celebró el consenso alcanzado respecto de materias tan trascendentes como la interdependencia entre el sistema eléctrico y el informático, de modo que los operadores de importancia vital cuenten con todos los elementos para llevar a cabo adecuadamente sus funciones.

En línea con lo señalado, previno que es indispensable cambiar algunos aspectos. Detalló que en la actualidad ciertos medios de comunicación deben esperar la restitución el servicio eléctrico para asegurar su actividad. La idea, anheló, es que haya un solo estándar y que, por lo tanto, todos los servicios esenciales objeto de una afectación estén obligados a reaccionar de la misma manera.

Adicionalmente, destacó los dos nuevos literales incorporados al inciso cuarto. Fijando su atención en el segundo, pormenorizó que el daño reputacional debe afectar las actividades desarrolladas o la

disponibilidad de los servicios. Con todo, enunció que el reglamento proporcionará mayores antecedentes sobre el particular.

- Puesta en votación, la indicación número 47 fue aprobada con las enmiendas consignadas, por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

La indicación número 48, del Honorable Senador señor Van Rysselberghe, recaída en el inciso primero del artículo 4, es para reemplazar la expresión “al Consejo Técnico de”, por la vocal “a”.

- Esta indicación fue retirada por su autor.

La indicación número 49, del Honorable Senador señor Insulza, busca sustituir, en la letra b) del inciso segundo del artículo referido, la frase “del sistema informático, red o sistema de información” por “red o sistema de información”.

- Esta indicación fue retirada por su autor.

La indicación número 50, del Honorable Senador señor Insulza, es para suprimir el inciso final del precepto analizado.

- Al igual que la anterior, esta indicación fue retirada por su autor.

PÁRRAFO 2°

EPÍGRAFE

Esta parte del Título II reza lo que sigue:

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

Al respecto, se presentó **la indicación número 51**, de Su Excelencia el Presidente de la República, para sustituir su denominación por la siguiente:

“Párrafo 2°
Obligaciones de ciberseguridad”.

- Sometida a votación, esta indicación fue respaldada por la unanimidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

ARTÍCULO 5

Fija las obligaciones generales que deberán cumplir las instituciones que poseen infraestructura de la información calificada como crítica. Su tenor literal es el siguiente:

"Artículo 5. Deberes generales. Será obligación de los órganos del Estado y de las instituciones privadas que posean infraestructura de la información calificada como crítica, aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos, así como contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad e integridad del servicio prestado, de conformidad a lo prescrito en esta ley.".

Sobre la norma transcrita recayeron las indicaciones números 52, 53, 54 y 55.

La indicación número 52, de Su Excelencia el Presidente de la República, es para reemplazar este artículo por la siguiente:

"Artículo 5. Deberes generales. Será obligación de los órganos de la Administración 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 órganos 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.".

Explicando la propuesta del grupo de asesores conformado para facilitar la tramitación del proyecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que este recomienda

aprobar la indicación en análisis, con ciertas adecuaciones, para que haya coherencia con el texto aprobado previamente. Precisó que estas últimas son las siguientes:

- Reemplazar, en el inciso primero, la frase “órganos de la Administración del Estado” por “organismos del Estado”;

- Sustituir, en el inciso tercero, la voz “órganos” por “organismos”, y

- Agregar el siguiente inciso, nuevo:

“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.”.

Deteniéndose en la última enmienda, especificó que permite consagrar expresamente el deber de coordinación de la Agencia Nacional de Ciberseguridad con cualquier otra autoridad sectorial que requiera dictar normas técnicas en materia de seguridad informática.

Connotó que, de acogerse los planteamientos de la instancia prelegislativa, la redacción del artículo 5 quedaría de la manera que se transcribe a continuación:

“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 30 días hábiles, sin perjuicio de lo dispuesto en el artículo 22 respecto de las instituciones financieras fiscalizadas por la Comisión para el Mercado Financiero.”.

No obstante, anunció que la indicación número 55 propone incorporar al precepto transcrito un inciso final.

- En votación la indicación número 52, fue aprobada con las enmiendas referidas por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

La indicación número 53, del Honorable Senador señor Insulza, sustituye la expresión “órganos del Estado” por “organismos del Estado”.

- Esta indicación fue respaldada por la totalidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

La indicación número 54, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, reemplaza la frase “físicas e informativas”, por la siguiente: “físicas, informativas y de trazabilidad”.

- Puesta en votación, esta indicación fue rechazada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

La indicación número 55, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, agrega a continuación del punto final, que pasa a ser punto y seguido, el siguiente texto: “Se prohíbe a dichos órganos e instituciones, realizar pagos de cualquier tipo por rescate ante ataques de secuestro de datos o ransomware, así como de equipos o de dispositivos.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que el grupo de asesores conformado para facilitar la tramitación del proyecto recomienda aprobar con modificaciones esta indicación. Concretamente, concluyó, se propone transformar la oración sugerida en un inciso final, nuevo, del artículo 5, con el tenor que sigue:

"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.”.

Las Comisiones unidas advirtieron que la materia cuya regulación se propone constituye un asunto de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo dispuesto en el artículo 65, inciso cuarto, número 2°, de la Constitución Política de la República.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, anunció que el Ejecutivo acogerá esta propuesta en una futura indicación.

El Honorable Senador señor Pugh, en tanto, puso de relieve que el inciso final acordado busca erradicar el pago de los organismos del Estado y de las instituciones privadas ante el secuestro de sus datos. Tal medida, enfatizó, evitará que este ilícito siga escalando y posicionará a Chile como un pionero ético digital. Además, resaltó, obligará a considerar herramientas de protección efectiva.

- Habida cuenta del compromiso asumido por el Ejecutivo, la indicación número 55 fue aprobada con enmiendas, ad referéndum, por la totalidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 55 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Asimismo, los miembros de las Comisiones unidas estimaron que la idea comprendida en la indicación número 55, se entiende recogida en la indicación número 55 bis.

ARTÍCULO 6

El texto aprobado en general prescribe lo siguiente en su encabezamiento:

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

En relación con la denominación de este artículo -“Deberes específicos”-, se presentó **la indicación número 56**, para reemplazarla por la siguiente:

“Artículo 6. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales.”.

- Puesta en votación, esta indicación contó con el respaldo de la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Respecto del encabezamiento de la mencionada disposición, se formularon las indicaciones 57 y 58.

La indicación número 57, de Su Excelencia el Presidente de la República, es para sustituirlo por el siguiente: “Todos los órganos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital, deberán:”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, postuló que la mesa de trabajo prelegislativo propone reemplazar la voz “órganos” por “organismos”.

Aclarado lo anterior, afirmó que, de acogerse esta indicación, el encabezamiento del artículo 6 sería coherente con la redacción aprobada para los artículos 4 y 5, y quedaría de la siguiente manera:

“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:”.

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron la indicación con la enmienda aludida.

La indicación número 58, del Honorable Senador señor Insulza, busca reemplazar la expresión “órganos del Estado” por “organismos del Estado”.

- Esta indicación fue aprobada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra a)

Contempla como primer deber específico, el que se expresa:

"a) Implementar un sistema de gestión de riesgo permanente con el fin de determinar aquellos que pueden afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio y cuáles de ellos facilitan la ocurrencia de incidentes de ciberseguridad. Dicho sistema debe contar con la capacidad de determinar la gravedad de las consecuencias de un incidente de ciberseguridad.".

Sobre este literal recayeron las indicaciones números 59, 60 y 61.

La indicación número 59, de Su Excelencia el Presidente de la República, sustituye la voz "permanente", por la palabra "continuo".

El Honorable Senador señor Pugh celebró la propuesta del Ejecutivo. Sin embargo, estimó necesario aprobarla con enmiendas, a fin de reemplazar la frase "un sistema de gestión de riesgo permanente" por "un sistema de gestión de seguridad de la información continuo".

Las Comisiones unidas estuvieron contestes en respaldar la sugerencia de Su Señoría.

- Sometida a votación, esta indicación fue aprobada con la enmienda referida y otra de carácter formal por la totalidad de los legisladores presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 60, del Honorable Senador señor Insulza, suprime la frase "y cuáles de ellos facilitan la ocurrencia de incidentes de ciberseguridad."

- En votación, esta indicación contó con el voto favorable de la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 61, del Honorable Senador señor Insulza, reemplaza la expresión “determinar la gravedad” por “estimar tanto la probabilidad como el impacto”.

Las Comisiones unidas estimaron que la indicación analizada recae en una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo previsto en el artículo 65, inciso cuarto, número 2°, del Texto Supremo.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseguró que el Ejecutivo acompañaría la indicación pertinente.

- Habida cuenta del compromiso asumido por el representante del Gobierno, la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobó ad referéndum esta indicación.

Cabe destacar que, en virtud de los acuerdos anteriores, el literal en debate quedaría como sigue:

“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.”.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 61 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Asimismo, los miembros de las Comisiones unidas estimaron que la idea comprendida en la indicación número 61, se entiende recogida en la indicación número 61 bis.

Letra c)

Considera como segundo deber específico:

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

Al respecto, se presentaron las indicaciones números 62 y 63, ambas de Su Excelencia el Presidente de la República.

La indicación número 62 es para agregar, a continuación de la expresión “ciberseguridad”, la frase “,certificados por un centro de certificación acreditado o por la Agencia, según sea el caso”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, hizo presente que la indicación número 144, de Su Excelencia el Presidente de la República, que recae en el artículo 26, regula los centros de certificación acreditados.

- Puesta en votación, esta indicación fue respaldada por la totalidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 63, por su lado, busca sustituir la frase “periódicamente, a lo menos una vez al año”, por la siguiente: “y certificados periódicamente”.

El Honorable Senador señor Pugh celebró la decisión de no fijar una fecha para la actualización de los planes de continuidad operacional y ciberseguridad. Argumentó que tal medida permitirá renovarlos en la oportunidad que corresponda, lo que dependerá de las condiciones de riesgo, dando, por lo tanto, flexibilidad.

En sintonía con lo expuesto, relató que en algunos países dichos instrumentos se modernizan cada seis meses.

- Sometida a votación, esta indicación fue apoyada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Cabe mencionar que, en virtud de los acuerdos precedentes, el tenor de este literal sería:

“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.”.

Letra e)

Dispone lo siguiente:

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

En relación con este literal se formuló **la indicación número 64**, de Su Excelencia el Presidente de la República, para intercalar, entre las voces “Adoptar” y “las medidas”, la expresión “de forma oportuna y expedita”.

En consecuencia, el literal quedaría de la manera que se transcribe a continuación:

“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.”.

-Esta indicación contó con el voto favorable de todos los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

°°°°°

Letra nueva

Adicionalmente, se presentó **la indicación número 65**, de Su Excelencia el Presidente de la República, para agregar el siguiente literal, nuevo, contemplado como letra g):

“g) Informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes o 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.”.

- Las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación.

°°°°°

°°°°°

Letra nueva

Asimismo, Su Excelencia el Presidente de la República formuló **la indicación número 66**, para incorporar la siguiente letra, nueva, consultada como letra h):

“h) Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que la mesa de trabajo prelegislativo recomienda aprobar esta indicación con modificaciones, a fin de insertar, en la letra h) propuesta, luego de la voz “colaboradores”, la frase “, que incluyan campañas de ciberhigiene”.

En virtud de lo anterior, este literal quedaría:

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

- Sometida a votación, las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación con la enmienda señalada.

°°°°°

°°°°°

Letra nueva

Por otro lado, Su Excelencia el Presidente de la República presentó **la indicación número 67**, para agregar una letra, nueva, consultada como letra i):

“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.”.

- Las Comisiones unidas, por la unanimidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación.

°°°°°

°°°°°

Inciso nuevo

Finalmente, en relación con el artículo 6, Su Excelencia el Presidente de la República formuló **la indicación número 68**, para agregar el siguiente inciso segundo, nuevo:

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que el grupo de asesores conformado para facilitar la tramitación del proyecto sugiere acoger la indicación en estudio. Con todo, al igual que en oportunidades anteriores, se propone reemplazar la palabra "órganos" por "organismos".

De apoyarse tal recomendación, la redacción del inciso segundo del artículo 6 quedaría como sigue:

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

- Todos los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación con la enmienda consignada.

°°°°°

ARTÍCULO 7

Confiere facultades normativas a los reguladores o fiscalizadores sectoriales. Su redacción literal es la que se consigna:

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

Sobre este precepto recayó **la indicación número 69**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

“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. Este plazo podrá ser prorrogado por una sola vez y con la sola finalidad de recabar mayores detalles, siempre que la prórroga sea solicitada dentro del plazo original de tres horas.

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, plataformas y sistemas informáticos de los órganos 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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que la mesa de trabajo prelegislativo juzga indispensable aprobar la indicación con modificaciones, a objeto de precisar, en el inciso segundo, en qué oportunidad y con qué finalidad puede solicitarse la prórroga de la obligación de reportar. Para ello, pormenorizó, se sugiere sustituir la oración final del inciso segundo por la siguiente:

“La entidad informante podrá solicitar la prórroga de dicho plazo por una sola vez y mientras se encuentre este vigente, con la sola finalidad de recabar mayores antecedentes.”.

A mayor abundamiento, planteó que, de apoyarse el criterio referido, el tenor literal del artículo 7 sería el que sigue:

“Artículo 7. Deber de reportar. Todas las instituciones, sean públicas o privadas, e independiente de si son o no operadores de servicios esenciales, con la sola excepción de aquellos que la

Agencia hubiere eximido expresamente en sus instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley.

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

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

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

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

- Las Comisiones unidas, con el voto favorable de la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron la indicación número 69, con enmiendas.

ARTÍCULO 8

Crea la Agencia Nacional de Ciberseguridad. Su tenor literal es el que sigue:

“Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad y regular y fiscalizar las acciones de los órganos de la Administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o

fiscalizador sectorial, y que posea infraestructura de la información calificada como crítica, según los preceptos de esta ley. Se relacionará con el Presidente de la República por intermedio del Ministerio del Interior y Seguridad Pública.

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

Al respecto, se presentaron las indicaciones números 70 y 71.

La indicación número 70, de Su Excelencia el Presidente de la República, es para reemplazarlo por el siguiente:

“Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los órganos públicos en materia de ciberseguridad.

La Agencia deberá regular y fiscalizar las acciones de los órganos 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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sostuvo que la mesa de trabajo prelegislativo recomienda aprobar esta indicación, sin perjuicio de introducirle ciertas modificaciones. Puntualizó que estas últimas consisten en reemplazar, en el inciso primero, la expresión “órganos públicos” por “organismos de la Administración del Estado”, de modo de respetar el carácter autónomo de ciertas instituciones, y en sustituir, en el inciso segundo, la frase “regular y fiscalizar” por “regular, fiscalizar y sancionar”, además de la palabra “órganos” por “organismos”.

Detalló que, de apoyarse la sugerencia del equipo de asesores, la redacción del artículo 8 quedaría como sigue:

“Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

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

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

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

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

- Puesta en votación, esta indicación fue aprobada con las enmiendas referidas, por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 71, del Honorable Senador señor Insulza, recaída solo en el inciso primero del precepto referido, busca sustituir la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”.

- Las Comisiones unidas, con el voto favorable de todos sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación.

ARTÍCULO 9

Establece, por medio de dieciséis letras, las atribuciones con las que contará la Agencia Nacional de Ciberseguridad para dar cumplimiento a su objeto.

Letra a)

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

En relación con este literal, se formuló **la indicación número 72**, de Su Excelencia el Presidente de la República, para reemplazarlo por el que sigue:

"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.".

- En votación, las Comisiones unidas, con el voto favorable de todos sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación.

Letra b)

Contempla como atribución de la Agencia Nacional de Ciberseguridad dictar normas técnicas de carácter general y los estándares mínimos de ciberseguridad e impartir instrucciones particulares para los órganos de la Administración del Estado y para los privados cuya infraestructura de la información sea calificada como crítica y no se encuentren sometidos a la regulación o fiscalización de un regulador o fiscalizador sectorial, según corresponda.

Sobre este literal recayeron las indicaciones números 73, 74 y 75.

La indicación número 73, de Su Excelencia el Presidente de la República, lo sustituye por el siguiente:

"b) 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.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que el grupo de asesores conformado para facilitar la tramitación del proyecto sugiere aprobar la indicación en estudio, pero incorporando una oración inicial al literal b), con el objeto de dejar claramente establecido que la Agencia Nacional de Ciberseguridad podrá dictar las disposiciones para la aplicación y cumplimiento de las leyes y reglamentos.

Manifestó que, de apoyarse tal recomendación, la redacción de la letra b) del artículo 9 sería la que sigue:

"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.".

Para finalizar, observó que la oración cuya inclusión se sugiere es similar a la prevista en el número 1 del artículo 5° de la ley N° 21.000, que crea la Comisión para el Mercado Financiero.

- Sometida a votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación con la enmienda señalada.

La indicación número 74, del Honorable Senador señor Insulza, reemplaza la expresión "órganos de la Administración del Estado" por "organismos de la Administración del Estado".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, advirtió que la redacción del literal b), conforme a lo aprobado recientemente, no alude a la expresión cuya sustitución se propone.

- Por tal razón, esta indicación fue retirada por su autor.

La indicación número 75, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, agrega, a continuación del punto final de la letra b), que pasa a ser punto y seguido, lo siguiente: "Asimismo, podrá dictar normas de carácter general y las normas técnicas que sean necesarias para establecer los estándares particulares o mínimos de ciberseguridad que los reguladores o fiscalizadores sectoriales deban exigir respecto de sus regulados o fiscalizados, de conformidad a la regulación sectorial respectiva.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, comunicó que la mesa de trabajo sugiere dejar pendiente la discusión y la votación de esta indicación en tanto no se defina la redacción del artículo 22.

- En una sesión posterior, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, rechazaron esta indicación.

Letra c)

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

Respecto de este literal se presentaron las indicaciones números 76 y 77.

La indicación número 76, de Su Excelencia el Presidente de la República, es para reemplazarlo por el que se señala a continuación:

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, aseveró que la indicación en estudio simplifica el proceso de aplicación e interpretación administrativa de las normas sobre ciberseguridad.

El Honorable Senador señor Huenchumilla llamó a tener en cuenta que la interpretación administrativa de las disposiciones es materia de competencia de la Contraloría General de la República.

Atendiendo la observación del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, fue tajante en asegurar que tal función corresponde también a aquellos organismos públicos que tienen facultades fiscalizadoras y sancionadoras, sin perjuicio de las atribuciones del órgano autónomo citado.

Por su lado, **el Honorable Senador señor Insulza** consideró necesario introducir modificaciones de orden formal en la indicación, a fin de perfeccionar la redacción de la letra c) del artículo 9.

A su vez, **el Honorable Senador señor Huenchumilla** apuntó que el organismo a cargo de la seguridad informática tendrá la facultad de dictar normas, así como también la de interpretarlas y la de aplicarlas.

Al respecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, recordó que tal como acontece en el caso de las Superintendencias, habrá un control administrativo y judicial posterior de la cuestionada labor.

Acogiendo las observaciones de carácter formal del Honorable Senador señor Insulza, el texto de este literal quedaría como sigue:

"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.".

- Puesta en votación, las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación con las citadas enmiendas de orden formal.

La indicación número 77, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, busca sustituir la frase "al Ministro del Interior y Seguridad Pública", por la siguiente: "a los Ministros del Interior y Seguridad Pública, y de Transportes y Telecomunicaciones".

- Sometida a votación, esta indicación fue rechazada por siete votos en contra, de los Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh, Quintana, Saavedra y Van Rysselberghe, y una abstención, del Honorable Senador señor Ossandón.

Letra d)

El texto aprobado en general es el que se transcribe:

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

En relación con este literal se formularon las indicaciones números 78, 79 y 80.

La indicación número 78, de Su Excelencia el Presidente de la República, es para consultar, en su lugar, el siguiente:

“d) Coordinar y supervisar a los CSIRT Sectoriales existentes; a aquellos que pertenezcan a órganos del Estado; a instituciones privadas y al CSIRT Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, postuló que la mesa de trabajo prelegislativo sugiere aprobar esta indicación, sin perjuicio de introducirle ciertas adecuaciones. Estas últimas, puntualizó, consisten en reemplazar la expresión “órganos del Estado” por “organismos de la Administración del Estado” y en sustituir la frase “en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades”, por “en la forma que establece esta ley”. Esta última, adujo, permitirá ampliar la atribución de la Agencia Nacional de Ciberseguridad.

Concluyendo su intervención, especificó que, de respaldarse la propuesta anterior, la redacción de la letra d) del artículo 9 quedaría así:

“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.”.

- **Las Comisiones unidas, por la unanimidad de sus parlamentarios presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación con las mencionadas enmiendas.**

La indicación número 79, del Honorable Senador señor Van Rysselberghe, elimina el siguiente texto: “a los CSIRT Sectoriales y a aquellos que pertenezcan a órganos del Estado señalados en el inciso final del artículo 4º, a instituciones privadas y”.

- Esta indicación fue retirada por su autor.

La indicación número 80, del Honorable Senador señor Insulza, reemplaza la expresión “órganos del Estado” por “organismos de la Administración del Estado”.

- En votación, esta indicación fue aprobada por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

°°°°°

Letra nueva

Seguidamente, se formuló **la indicación número 81**, de Su Excelencia el Presidente de la República, para intercalar la siguiente letra e), nueva, ajustándose el orden correlativo de las letras subsiguientes:

"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.".

- Sometida a votación, esta indicación contó con el respaldo de la unanimidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

°°°°°

Letra e)

Contempla como facultad de la Agencia mencionada administrar el Registro Nacional de Incidentes de Ciberseguridad.

Sobre este literal recayó **la indicación número 82**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como letra f):

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

- Esta indicación fue aprobada por la totalidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra f)

Fija como atribución de la Agencia Nacional de Ciberseguridad fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad.

Al respecto, se formuló **la indicación número 83**, de Su Excelencia el Presidente de la República, para reemplazarla por la siguiente, contemplada como letra g):

“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.”.

- Puesta en votación, esta indicación fue respaldada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra g)

Considera como facultad de la Agencia referida requerir de los CSIRT Sectoriales y del CSIRT Nacional la información que sea necesaria para el cumplimiento de sus fines y que sea de responsabilidad de estas instituciones.

En relación con este literal se formularon las indicaciones números 84 y 85.

La indicación número 84, de Su Excelencia el Presidente de la República, es para sustituirlo por el que sigue, consultado como letra h):

“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.”.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 85, del Honorable Senador señor Van Rysselberghe, busca reemplazar la frase “de los CSIRT Sectoriales y del”, por la voz “al”.

- Esta indicación fue retirada por su autor.

Letra h)

Contempla como atribución de la Agencia Nacional de Ciberseguridad diseñar e implementar planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.

Sobre este literal recayó **la indicación número 86**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como letra i):

“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.”.

- Las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación.

Letra i)

Fija como facultad la Agencia suscribir convenios con órganos del Estado e instituciones privadas destinados a facilitar la colaboración y la transferencia de información que permita el cumplimiento de sus fines.

Respecto de este literal se presentaron las indicaciones números 87 y 88.

La indicación número 87, de Su Excelencia el Presidente de la República, lo reemplaza por el que sigue, consultado como letra j):

“j) Requerir a los órganos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sean necesarios 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 Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, manifestó que la mesa de trabajo prelegislativo sugiere aprobar esta indicación, sustituyendo, al igual que en oportunidades anteriores, la voz “órganos” por “organismos”; tal como lo recomienda, por lo demás, la propuesta de modificación siguiente.

Detalló que de acogerse lo anterior, el tenor literal de la letra j) sería el que se indica:

“j) Requerir a los organismos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sean necesarios 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.”.

- Todos los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación con la enmienda consignada.

La indicación número 88, del Honorable Senador señor Insulza, sustituye la expresión “órganos del Estado” por “organismos del Estado”.

- Las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación.

Letra j)

Considera como atribución de la Agencia Nacional de Ciberseguridad cooperar con organismos públicos, instituciones privadas y organismos internacionales, en materias propias de su competencia, en coordinación con el Ministerio de Relaciones Exteriores, cuando corresponda.

En relación con este literal se formuló **la indicación número 89**, de Su Excelencia el Presidente de la República, para reemplazarlo por el que sigue, consultado como letra k):

“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.”.

- En votación, las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación.

Letra k)

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

Sobre este literal recayeron las indicaciones números 90 y 91.

La indicación número 90, de Su Excelencia el Presidente de la República, es para sustituirlo por el siguiente, contemplado como letra l):

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

- Puesta en votación, las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación.

La indicación número 91, del Honorable Senador señor Insulza, busca reemplazar la expresión "órganos del Estado" por "organismos del Estado".

- Esta indicación fue retirada por su autor.

Letra l)

Fija como atribución de la Agencia Nacional de Ciberseguridad colaborar y coordinar con organismos de inteligencia, para enfrentar amenazas que puedan afectar a la infraestructura crítica de información e implementar acciones preventivas.

Al respecto, se presentaron las indicaciones números 92 y 93.

La indicación número 92, de Su Excelencia el Presidente de la República, la sustituye por la siguiente, contemplada como letra m):

"m) Coordinar y 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.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que el grupo de trabajo conformado para facilitar la tramitación de esta iniciativa de ley sugiere aprobar esta indicación. Con todo, pormenorizó, se propone incorporar, luego de la voz "colaborar" la palabra "interagencialmente". Recordó que el artículo 2 de la propuesta legal define tal expresión.

Sostuvo que, de respaldarse la recomendación señalada, la redacción de la letra m) del artículo 9 quedaría de la siguiente manera:

“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.”.

- En votación, las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación con la enmienda transcrita.

La indicación número 93, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, busca reemplazar la letra l) por la siguiente:

“l) Colaborar e interoperar con organismos de inteligencia y de persecución del delito, para enfrentar amenazas en forma interagencial, que puedan afectar a la infraestructura crítica de información e implementar acciones preventivas.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sugirió dejar pendiente el análisis de esta indicación.

- En una sesión posterior, las Comisiones unidas, por la unanimidad de sus miembros, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe, rechazaron esta indicación.

Letra m)

Considera como facultad de la Agencia referida fiscalizar y sancionar el cumplimiento de esta ley, sus reglamentos y la normativa técnica que se dicte en conformidad con la presente ley, cuando ello no corresponda a un regulador o fiscalizador sectorial, según sea el caso.

En relación con este literal se formuló **la indicación número 94**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como letra n):

“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.”.

Al igual que en el caso anterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, sugirió dejar pendiente esta indicación.

En una sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que la mesa técnica constituida para facilitar la tramitación de esta propuesta legal recomienda aprobar la indicación en estudio, con modificaciones, de manera de incorporar un párrafo segundo al literal, del tenor siguiente:

"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, 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.".

Explicó que la indicación en análisis entrega a la Agencia Nacional de Ciberseguridad la facultad de fiscalizar. Sin embargo, prosiguió, atendida la evolución que ha experimentado en el derecho administrativo tal atribución, se advierte la conveniencia de que la ley señale con exactitud en qué consistirá.

Las Comisiones unidas alertaron que el párrafo segundo cuya introducción se plantea aborda una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo prescrito en el artículo 65, inciso cuarto, N° 2°, de la Constitución Política de la República.

Al respecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseguró que el Ejecutivo haría llegar oportunamente la indicación, en los términos sugeridos por el grupo de asesores.

A continuación, **el Honorable Senador señor Huenchumilla** manifestó su preocupación ante el empleo de la expresión "entre otras". Al efecto, estimó que de acuerdo al artículo 7° del Texto Supremo, tal locución se aleja del derecho público.

Deteniéndose en la inquietud del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, sostuvo que, por regla general, en el caso de los órganos fiscalizadores, basta con declarar que tienen dicha atribución; así, puntualizó, ocurre en los textos normativos de varias Superintendencias. No obstante, en esta ocasión, y por las razones esgrimidas precedentemente, se ha decidido detallar su contenido. Para ello, connotó, se ha tenido a la vista la directiva europea NIS2.

En línea con lo expuesto, enfatizó que la expresión cuestionada determina el deber referido, además de cubrir otras acciones que sean imprescindibles a futuro.

Seguidamente, destacó que el ejercicio de la facultad mencionada estará sujeto a control administrativo y judicial. Asimismo, anunció que el artículo 34 de la iniciativa de ley establece reglas de procedimiento que evitarán que tal función pueda ser utilizada de forma abusiva o discrecional.

Por su parte, **el Honorable Senador señor Macaya** consultó cómo se cautelarán las garantías de las personas fiscalizadas.

Adicionalmente, puso de relieve que en ciertos casos esta atribución de la Agencia Nacional de Ciberseguridad podría colisionar con la del Ministerio Público.

El Honorable Senador señor Pugh, en tanto, respaldando los dichos del personero de Gobierno, postuló que la indicación analizada, en los términos sugeridos, adhiere a estándares internacionales en el ámbito de la ciberseguridad. Concretamente, acotó, a la directiva europea NIS2, publicada el 27 de diciembre de 2022.

En atención a lo señalado, juzgó que este futuro cuerpo normativo será una ley modelo en seguridad informática.

Insistiendo en su observación, **el Honorable Senador señor Huenchumilla** reiteró que, en virtud de lo dispuesto en el artículo 7° de la Carta Fundamental, los órganos públicos solo pueden actuar dentro de su competencia y en la forma que prescriba la ley.

Su Señoría consultó si el uso de la locución “entre otras” podría significar que la Agencia Nacional de Ciberseguridad tendrá, por ejemplo, la potestad de allanar un inmueble.

Para concluir, discutió la idea de encomendar a la entidad referida la atribución de “citar a declarar”, medida conferida a los tribunales de justicia y al Ministerio Público.

El Honorable Senador señor Insulza se sumó a la última aprensión del Presidente de las Comisiones unidas.

Abocándose a las dudas de los miembros de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó, en primer lugar, que el artículo 34 del proyecto de ley prescribe ciertas exigencias a las que se someterá el procedimiento sancionatorio. En ellas, pormenorizó, se distinguen diversas etapas y se señala quién investiga, quién formula cargos y quién sanciona. En consecuencia, vislumbró, está adecuadamente regulado, pese a lo cual podrían agregarse otras normas de control.

En lo que atañe a las garantías, remarcó que las medidas que adopte la Agencia Nacional de Ciberseguridad en el ejercicio de la atribución fiscalizadora quedarán sujetas a los recursos administrativos y judiciales respectivos. Dentro de los primeros, puntualizó, se encuentra el de reposición y el jerárquico, mientras que, dentro de los segundos, el de legalidad.

Aclaró que cualquier decisión que pueda afectar derechos fundamentales requiere expresa formulación legal. Agregó que la facultad de allanamiento obliga a identificar los casos y la forma en que procede. En esta oportunidad, subrayó, no tendrá cabida.

Para concluir, connotó que el artículo 34 junto con los recursos aludidos previamente permitirán resguardar el debido proceso.

A su vez, **el Honorable Senador señor Quintana** reveló que en la legislación chilena son diversos los órganos con atribuciones de control. Ejemplo de ellos, acotó, son las Superintendencias y la Inspección del Trabajo. De este modo, resaltó, la labor citada no es ajena al derecho administrativo nacional.

En sintonía con la explicación dada por el legislador que le antecedió en el uso de la palabra, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, recalcó que los organismos fiscalizadores de derecho público, en general, tienen facultades de dicha índole. Así, ahondó, se aprecia en materia laboral, bancaria, de telecomunicaciones y de consumidores, entre otras.

Con todo, previno que, si algún hecho reviste caracteres de delito, la Agencia deberá inhibirse y realizar la denuncia respectiva, derivando los antecedentes al Ministerio Público.

El Honorable Senador señor Macaya hizo hincapié en la necesidad de dejar claramente establecido que, en la última situación relatada por el representante del Ejecutivo, el órgano encargado de la ciberseguridad debe dar un paso al costado, inhibiéndose de intervenir.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, estimó redundante tal precisión, toda vez que el artículo 175 del Código Procesal Penal ya consagra la obligación de denunciar.

- En atención al compromiso asumido por el Ejecutivo, las Comisiones unidas, por la unanimidad de sus miembros, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de las dos Comisiones-, Saavedra y Van Rysselberghe, aprobaron ad referéndum, con la enmienda consignada, la indicación número 94.

Posteriormente, dando cumplimiento al compromiso asumido, Su Excelencia el Presidente de la República presentó una indicación, que fue individualizada como **indicación número 94 bis**, para reemplazar la letra m) del artículo 9 por la siguiente, consultada como letra n):

"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.".

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, aprobaron esta indicación.

Letra n)

Contempla como atribución de la Agencia Nacional de Ciberseguridad informar a la Agencia Nacional de Inteligencia sobre riesgos e incidentes de ciberseguridad.

Sobre este literal recayeron las indicaciones números 95 y 96.

La indicación número 95, de Su Excelencia el Presidente de la República, es para reemplazarlo por el siguiente, considerado como letra ñ):

"ñ) Determinar las infracciones e incumplimientos en que incurran las instituciones públicas y privadas respecto de los principios y obligaciones establecidos en esta ley, sus reglamentos y las 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.”.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, expresó que la mesa de trabajo prelegislativo recomienda aprobar con enmiendas esta indicación, a fin de sustituir la oración inicial de esta letra por la siguiente:

“Ordenar la realización de procedimientos sancionatorios a las entidades fiscalizadas, procediendo a sancionar las infracciones e incumplimientos en que incurran los instituciones públicas y privadas respecto de las disposiciones de esta ley, reglamentos, obligaciones e instrucciones generales y particulares que emita la Agencia.”.

Especificó que tal innovación busca clarificar el procedimiento para la aplicación de sanciones. Adicionalmente, advirtió, se emplea el lenguaje utilizado en otros textos normativos, a fin de que haya coherencia.

Agregó que, de respaldarse la propuesta del grupo de asesores, la redacción del literal ñ) quedaría así:

“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.”.

Las Comisiones unidas tuvieron en consideración que la modificación aborda materias de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo prescrito en el artículo 65, inciso cuarto, número 2°, de la Carta Fundamental.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, aseveró que el Ejecutivo presentaría posteriormente la indicación correspondiente.

El Honorable Senador señor Huenchumilla consultó si la enmienda aludida supondría la creación de nuevos procedimientos.

Abocándose a la consulta del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aclaró que las reglas procedimentales se regulan en el artículo 34 de la iniciativa de ley. Añadió que el lenguaje empleado simplemente busca evitar inconvenientes con el Tribunal Constitucional, suscitados en otras leyes

que establecen facultades sancionatorias. Por consiguiente, remarcó, se diferencia entre quien ordena la investigación y quien la lleva a cabo.

- En atención al compromiso asumido, las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe, aprobaron la indicación número 95, ad referéndum, con la enmienda consignada.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló una indicación, que fue individualizada como **indicación número 95 bis**, para reemplazarla la letra n) del artículo 9, considerada como letra ñ):

"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.".

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

La indicación número 96, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, busca sustituirlo por el siguiente:

"n) Interoperar con la Agencia Nacional de Inteligencia para el intercambio de información sobre riesgos e incidentes de ciberseguridad, incluidas las campañas de desinformación en línea.".

- Esta indicación fue rechazada por la unanimidad de los parlamentarios presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

Letra o)

Fija como facultad de la Agencia de la referencia diseñar, conjuntamente con el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, planes y acciones que fomenten la investigación, innovación y desarrollo de la industria de ciberseguridad local.

Al respecto, se presentaron las indicaciones números 97 y 98.

La indicación número 97, de Su Excelencia el Presidente de la República, es para reemplazarla por la siguiente:

"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.".

- Puesta en votación, esta indicación fue aprobada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Ossandón, Pugh, Saavedra y Van Rysselberghe.

La indicación número 98, del Honorable Senador señor Van Rysselberghe, busca sustituirla por la que sigue:

"o) Diseñar, planes y acciones que fomenten la investigación, innovación y desarrollo de la industria de la ciberseguridad nacional con los ministerios competentes.".

- Esta indicación fue retirada por su autor.

°°°°°

Letras nuevas

Enseguida, **la indicación número 99**, de Su Excelencia el Presidente de la República, es para incorporar las siguientes letra p), q), r), s), t), u), v) y w), nuevas, pasando la actual letra p) a ser x):

La letra p) es del siguiente tenor:

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

- Puesta en votación, la letra p) de esta indicación contó con el respaldo de la totalidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su

calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

La letra q) reza:

“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.”.

- Sometida a votación, la letra q) de esta indicación fue aprobada por la totalidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

El literal r) prescribe:

“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.”.

- Las Comisiones unidas, por la unanimidad de sus miembros, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe, respaldaron la letra r) de esta indicación.

La letra s) establece:

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

Al respecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que la mesa técnica conformada para facilitar la tramitación de este proyecto de ley recomienda aprobar la letra s) con modificaciones, a fin de reemplazar la voz “órganos” por “organismos”.

Detalló que, de acogerse tal sugerencia, el referido literal quedaría de la manera que se indica:

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

- Puesta en votación, la letra s) de esta indicación fue aprobada con la enmienda reproducida por la totalidad de

los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

El literal t) establece:

"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.".

- Sometida a votación, la letra t) de esta indicación contó con el respaldo de la totalidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

El texto de la letra u) es que se transcribe a continuación:

"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 órganos del Estado.".

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, expuso que el grupo de asesores conformado para facilitar la tramitación de este proyecto de ley recomienda aprobar la letra u) con modificaciones, a fin de reemplazar la voz "órganos" por "organismos".

Previno que, de acogerse tal sugerencia, el tenor literal de tal atribución sería el siguiente:

"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.".

- La letra u) de esta indicación fue aprobada con la enmienda referida por la totalidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

La letra v) dispone:

"v) Regular, en coordinación con el Servicio Nacional del Consumidor, estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales

disponibles a consumidores finales, cubriendo tanto la publicidad del producto como la obligación de incluir etiquetas en estos, pudiendo consistir en fechas de expiración, indicadores de riesgo, u otros indicadores similares.”.

- Puesta en votación, la letra v) de esta indicación fue aprobada por la totalidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

Finalmente, el literal w) prescribe:

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

- Sometida a votación, la letra w) de esta indicación fue aprobada por la totalidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

°°°°°

°°°°°

Letra nueva

Asimismo, se presentó **la indicación número 100**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para intercalar la siguiente letra p), nueva, pasando la actual letra p) a ser letra q):

“p) Proponer al Ministro del Interior y Seguridad Pública, participar en un programa de divulgación de vulnerabilidades que incluya un proceso de informe y divulgación. Se entiende por programa de divulgación de vulnerabilidades, aquel plan o proyecto que puede configurarse para permitir que investigadores de seguridad externos (o hackers éticos) aporten a identificar las vulnerabilidades de seguridad, también conocidas como errores de seguridad, usando una plataforma de intercambio segura y de ser necesaria anonimizada, junto a su reporte a los organismos internacionales encargados de numerarlas.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sugirió dejar pendiente el análisis y la votación de esta indicación en tanto no se examine la indicación número 178.

- En una sesión posterior, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas

instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, rechazaron esta indicación.

°°°°°

°°°°°

Letras nuevas

Adicionalmente, se formuló **la indicación número 101**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para agregar las siguientes letras, nuevas:

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

Las Comisiones unidas estuvieron contestes en que la función que se propone incorporar a la Agencia Nacional de Ciberseguridad recae en una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo prescrito en el artículo 65, inciso cuarto, N° 2°, de la Constitución Política de la República.

En relación con tal prevención, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseveró que el Ejecutivo haría llegar esta parte de la indicación examinada.

- Habida cuenta del compromiso asumido, las Comisiones unidas, por la unanimidad de sus miembros, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe, aprobaron ad referéndum la primera atribución de la indicación en análisis.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 101 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Asimismo, los miembros de las Comisiones unidas estimaron que la idea comprendida en la indicación número 101, se entiende recogida en la indicación número 101 bis.

La siguiente letra señala:

"…. Establecer el catálogo de clasificación y taxonomía de los incidentes de ciberseguridad, en base a estándares internacionales, para priorización de respuesta y luego análisis e intercambio de información.".

Sobre el particular, **el Honorable Senador señor Pugh** explicó que la atribución en debate tiene por objeto asegurar la existencia de un inventario de eventos que comprometan o perjudiquen la confidencialidad o la integridad de la información; la disponibilidad o resiliencia de las redes o sistemas informáticos, o la autenticación o no repudio de los procesos ejecutados o implementados en ellos, en base a modelos internacionales. Esto, subrayó, posibilitará contar con estadísticas respecto a tales episodios.

Con todo, se allanó a que esta medida sea recogida en el reglamento de la futura ley.

- Puesta en votación, esta parte de la indicación número 101 fue rechazada por la unanimidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de ambas Comisiones-, -Saavedra y Van Rysselberghe.

El último literal dispone:

"…. Definir el protocolo para manejo de información clasificada con organismos privados que operen infraestructura crítica de la información o realicen investigación avanzada de ciberseguridad.".

Al efecto, **el Honorable Senador señor Pugh** sentenció que la facultad examinada fija reglas para la gestión de información sensible, tal como lo contempla el protocolo de semáforo TLP -por sus siglas en inglés-, esquema creado para fomentar un mejor intercambio de aquella. A través de este instrumento, dijo, el autor de los datos puede decidir hasta dónde circulará.

No obstante, al igual que en el caso precedente, adelantó que esta medida podría considerarse a nivel reglamentario.

- Sometida a votación esta parte de la indicación número 101, fue rechazada por la unanimidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

°°°°°

ARTÍCULO 11

Precisa, en siete literales, las atribuciones del Director Nacional de la Agencia Nacional de Ciberseguridad.

Letra f)

Permite al director delegar atribuciones o facultades específicas en funcionarios de las plantas directiva, profesional o técnica de la Agencia.

Sobre este literal recayó **la indicación número 102**, de Su Excelencia el Presidente de la República, para reemplazar la expresión “funcionarios de las plantas directiva, profesional o técnica de la Agencia, y” por “los funcionarios que indique, e”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, puso de manifiesto que el cambio busca ajustar la redacción de la letra f) del artículo 11 al tenor del artículo 14 del proyecto de ley. En efecto, sostuvo, tal como se analizará prontamente, el personal de la Agencia Nacional de Ciberseguridad se regirá por las normas del Código del Trabajo y no por las del Estatuto Administrativo, como lo contempla el texto aprobado en general por el Senado. Por consiguiente, enfatizó, no habrá planta directiva, profesional ni técnica.

Adujo que, de aprobarse esta indicación, el literal f) quedaría de la manera se sigue:

“f) Delegar atribuciones o facultades específicas en los funcionarios que indique;”.

- Las Comisiones unidas, por la unanimidad de sus miembros, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -actuando como integrante de ambas Comisiones-, Saavedra y Van Rysselberghe, respaldaron esta indicación.

Letra g)

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

Al respecto, se presentaron las indicaciones números 103 y 104.

La indicación número 103, de Su Excelencia el Presidente de la República, suprime el texto: “, respecto de los órganos de la Administración del Estado, en los términos señalados en el artículo 32 y respecto de aquellos privados que posean infraestructura de la información calificada como crítica, que no estén sujetos a un regulador o fiscalizador sectorial específico”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, expuso que, habida cuenta de la sustitución del modelo de infraestructura crítica de la información por el de servicios esenciales y operadores de importancia vital, la locución transcrita pierde sentido, razón por la cual se propone su eliminación.

Acotó que, de respaldarse esta indicación, la redacción de la letra g) quedaría de la manera siguiente, con las adecuaciones formales correspondientes:

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

- Las Comisiones unidas, por la unanimidad de sus miembros, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe, aprobaron esta indicación.

La indicación número 104, del Honorable Senador señor Insulza, busca reemplazar la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”.

- Esta indicación fue retirada por su autor.

°°°°°

Letra nueva

A continuación, se formuló **la indicación número 105**, de Su Excelencia el Presidente de la República, para incorporar la siguiente letra h), nueva:

“h) Ejercer la representación judicial y extrajudicial de la Agencia.”.

Refiriéndose a esta indicación, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, declaró que, en atención al diseño previsto para la Agencia Nacional de Acreditación y dada su especialidad, se juzgó conveniente encomendar al Director Nacional de esta entidad su representación judicial y extrajudicial. Recordó que, tratándose de órganos públicos, por regla general, corresponden al Consejo de Defensa del Estado.

Afirmó que algo similar ocurre en el caso del Consejo para la Transparencia.

El Honorable Senador señor Macaya solicitó fundamentar la decisión, y señalar qué otros ejemplos existen en la legislación chilena en donde la representación de una entidad pública no recaiga en el Consejo de Defensa del Estado.

Atendiendo las consultas del legislador, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, reiteró que la idea de entregar al Director de la Agencia Nacional de Ciberseguridad la atribución obedece a que la especificidad de la materia involucrada hace razonable que su defensa quede radicada en esta organización. A mayor abundamiento, remarcó que los asuntos de su conocimiento y competencia son extremadamente técnicos.

En cuanto a los ejemplos requeridos, reiteró que el principal es el del Consejo para la Transparencia. Al efecto, sentenció que este ha motivado un tipo de litigación muy particular, que hace recomendable que el nuevo servicio, con sus capacidades, sea quien las aborde.

Por su lado, **el Honorable Senador señor Quintana** observó que el Director Nacional de la Agencia será quien determinará si se ejercen las acciones correspondientes. Su Señoría estimó prudente que la función encomendada no obste a la intervención del Consejo de Defensa del Estado.

A su turno, **el Honorable Senador señor Huenchumilla** evidenció que el artículo 10 aprobado en general por la Sala, que no fue objeto de indicaciones, ya confiere al Director Nacional la representación judicial y extrajudicial del órgano a su cargo.

En consideración a las dudas surgidas en el seno de las Comisiones unidas respecto de esta indicación, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, propuso dejar pendiente su examen y votación.

El Honorable Senador señor Huenchumilla valoró la disposición del personero de Gobierno, y recomendó tener a la vista la sugerencia del Honorable Senador señor Quintana, así como también recabar otros ejemplos de instituciones públicas en que se haya adoptado el mismo criterio.

En una sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que la mesa de trabajo prelegislativo, acogiendo la petición de los legisladores, sugiere aprobar esta indicación con modificaciones, de manera de incorporar, luego de la voz “Agencia”, la frase “, sin perjuicio de las atribuciones que pudieran corresponder al Consejo de Defensa del Estado”.

Detalló que de acogerse la propuesta, la redacción del literal h) del artículo 11 quedaría de la forma que sigue:

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

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron esta indicación con la enmienda consignada.

°°°°°

ARTÍCULO 13

Aborda el nombramiento de las autoridades de la Agencia Nacional de Ciberseguridad. Prescribe que 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.

En relación con esta norma, **la indicación número 106**, de Su Excelencia el Presidente de la República, es para intercalar, a continuación de la voz “indica”, la expresión “, hasta el segundo nivel jerárquico”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que, de respaldarse la propuesta del Ejecutivo, la redacción del artículo 13 sería la siguiente:

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

- Esta indicación fue apoyada por la unanimidad de los miembros de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana -en su condición de integrante de ambas Comisiones-, Saavedra y Van Rysselberghe.

ARTÍCULO 14

Prescribe las reglas legales a las que se someterá el personal de la Agencia Nacional de Ciberseguridad, señalando que se regirá por las normas del Estatuto Administrativo.

Sobre esta disposición recayeron las indicaciones números 107 y 108.

La indicación número 107, de Su Excelencia el Presidente de la República, es para sustituirlo por el que sigue:

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

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

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.

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, solo tendrán derecho a la indemnización contemplada en el artículo quincuagésimo octavo de dicha ley. Dichos trabajadores no tendrán derecho a las indemnizaciones establecidas en el Código del Trabajo.

El Director o Directora de la Agencia, sin perjuicio de lo que establezca el contrato, tendrá la facultad para aplicar las normas relativas a las destinaciones, comisiones de servicio y cometidos funcionarios de los artículos 73 a 78 del decreto con fuerza de ley N° 29, del Ministerio de Hacienda, promulgado el año 2004 y publicado el año 2005, 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, del Ministerio de Hacienda, de 1977, y al decreto supremo N° 1, del Ministerio de Hacienda, de 1991, 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.

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 del Servicio, indicando el número máximo de trabajadores que podrá ocupar según el régimen de remuneraciones.

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, relató que las observaciones realizadas durante la discusión en general respecto del régimen laboral del personal de la Agencia Nacional de Ciberseguridad; las particularidades de este organismo; las materias abordadas y la necesidad de contratar en ciertos casos a expertos sin título profesional, obligan a tener flexibilidad, capacidad que escapa al Estatuto Administrativo. En este contexto, subrayó, se concluyó que la mejor opción es el sistema propuesto. Conforme a él, acotó, quienes se desempeñen en la entidad encargada de la seguridad informática quedarán sujetos a las disposiciones del Código del Trabajo, con ciertas modificaciones.

Ahondando en las variaciones enunciadas, comunicó que la primera de ellas radica en la aplicación de las normas de probidad administrativa y las que regulan los conflictos de interés. Agregó que, dado que se trata de una institución fiscalizadora, se restringirá a los trabajadores la facultad de realizar actividades económicas en las áreas objeto de control.

Otro cambio, añadió, consiste en que se establece expresamente que el personal quedará sujeto a responsabilidad administrativa y civil.

Por otro lado, informó, se dispone que quienes ingresen a este servicio por el Sistema de Alta Dirección Pública solo tendrán derecho a la indemnización contemplada en la ley N° 19.882. En este punto, aclaró que quedarán en esa condición los que se desempeñen en el primer o segundo nivel jerárquico.

Los demás funcionarios, prosiguió, podrán acceder a las indemnizaciones reguladas en los artículos 161, 162 y 163 del Código del Trabajo.

Adicionalmente, consignó, se señala que las causales de término de contrato serán aquellas contempladas en el citado cuerpo normativo, y que no se podrán alterar las bases para el cálculo de las indemnizaciones.

Asimismo, notó, se consagra expresamente la posibilidad de que el Director Nacional aplique las normas relativas a las destinaciones, comisiones de servicio y cometido funcionario del Estatuto Administrativo. Patentizando su importancia, adujo que existen países que tienen un nivel de madurez mayor en ciberseguridad, lo que motivará la recepción de expertos extranjeros o el envío del personal a cursos de capacitación.

En lo que concierne a la estructura interna, expuso que se organizará mediante una resolución que dictará la máxima autoridad de la Agencia Nacional de Ciberseguridad, la que será visada por la Dirección de Presupuestos. Llamó a tener presente que, conforme al informe financiero que acompaña a esta iniciativa de ley, la dotación máxima de este órgano será de sesenta personas.

Tras dar a conocer el régimen aplicable al personal del organismo a cargo de la ciberseguridad, connotó que los modelamientos efectuados advierten la necesidad de realizar turnos, de manera de asegurar su funcionamiento ininterrumpido las veinticuatro horas del día, de lunes a domingo. Además, dijo, hay labores que tendrán una continuidad operacional de dieciocho horas. Tales particularidades, insistió, aconsejan respaldar la indicación.

Para concluir, apuntó que las disposiciones transitorias abordan el traspaso de trabajadores del Estado a la nueva institucionalidad. Con todo, afirmó, actualmente todos ellos se desempeñan a honorarios.

El Honorable Senador señor Pugh valoró la propuesta desarrollada por el Ejecutivo. Sin embargo, expresó dudas acerca del correcto tratamiento del acuerdo de no divulgación o NDA, por sus siglas en inglés (non disclosure agreement).

El Honorable Senador señor Quintana celebró también el régimen diseñado en la indicación, pues juzgó que los preceptos del Código del Trabajo aportan mayor flexibilidad.

No obstante, hizo ver la conveniencia de regular adecuadamente las incompatibilidades de los trabajadores, a fin de evitar el traspaso de información desde la Agencia a otros sectores.

El Honorable Senador señor Saavedra, a su turno, mostró interés por saber cómo se recoge el derecho a la libertad sindical y a la negociación colectiva. Previno que los conflictos de índole laboral podrían terminar en la paralización de las operaciones de la entidad encargada de la ciberseguridad.

Abordando la inquietud del Honorable Senador señor Pugh, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, recordó que el proyecto de ley contempla normas de secreto de la información para los funcionarios.

En cuanto a la pregunta del Honorable Senador señor Quintana, sentenció que la indicación número 109, recaída en el artículo 15, consagra prohibiciones e inhabilidades, las que excluyen cualquier tipo de servicios, con excepción de las labores docentes. Recordó que hoy se distingue entre estas y las de investigación, y que la redacción del precepto referido solo posibilita las primeras.

Deteniéndose en la interrogante del Honorable Senador señor Saavedra, en tanto, puso de relieve que, conforme lo ha resuelto la Contraloría General de la República, las instituciones públicas no tienen derecho a sindicalizarse sino a asociarse. Agregó que, por aplicarse las reglas de los servicios esenciales de otros cuerpos normativos, la Agencia será de aquellas entidades que no pueden paralizar sus actividades.

Sobre el particular, **el Honorable Senador señor Saavedra** solicitó establecer expresamente el impedimento en la ley, a fin de evitar dificultades.

El Honorable Senador señor Huenchumilla, a su vez, quiso saber si el régimen laboral propuesto constituye una innovación en la legislación nacional o, por el contrario, si existen otros organismos en donde se conjuguen las normas del Código del Trabajo con las del Estatuto Administrativo.

Fijando su atención en la pregunta formulada por el Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aclaró que el sistema previsto en la indicación en examen no es una novedad en el ordenamiento jurídico. En efecto, profundizó, rige en más de diez organismos públicos. El Ejecutivo, prosiguió, se limitó a recoger la experiencia de estos. Notó que el mayor exponente es el Consejo para la Transparencia.

A reglón seguido, comunicó que la única originalidad radica en que en esta oportunidad será un ente fiscalizador al que se le aplicarán las normas del Código del Trabajo. Por ello, declaró, se suman todas las disposiciones sobre inhabilidades e incompatibilidades del Estatuto Administrativo. Así, concluyó, quien se desempeñe en la Agencia Nacional de Ciberseguridad y sus parientes quedarán fuera del mercado de la seguridad informática.

El Honorable Senador señor Insulza pidió dedicar más tiempo al análisis de esta indicación.

El Honorable Senador señor Huenchumilla, por su parte, solicitó al señor Álvarez volver a examinar el régimen laboral expuesto, de ser indispensable. Enfatizó que, incluso, podría reabrirse el debate.

- En votación, la indicación número 107 contó con el respaldo de la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh, Quintana -actuando como miembro de ambas Comisiones- y Van Rysselberghe.

Advirtiendo la necesidad de perfeccionar la redacción del artículo 14 de la proposición legal, y al amparo del artículo 125 del Reglamento del Senado, en una sesión posterior, la totalidad de los parlamentarios presentes de las Comisiones unidas estuvieron contestes en reabrir el debate.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que la mesa de trabajo prelegislativo recomienda introducir los siguientes cambios a la disposición mencionada:

- Intercalar un inciso tercero, nuevo, pasando el actual inciso tercero a ser el cuarto, y así sucesivamente:

"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, del Ministerio de Hacienda, del año 2004, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.".

- Agregar una oración final al inciso tercero, que pasa a ser cuarto, del tenor que sigue:

"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, de 2004, del Ministerio de Hacienda que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.".

- Incorporar en el inciso sexto, que pasa a ser séptimo, la siguiente oración final:

"Para el caso de evaluación deficiente de su desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal.".

- Intercalar un inciso penúltimo del tenor que se indica:

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

Esclareció que las modificaciones introducidas apuntan a complementar la nueva redacción del artículo 15, que regula las prohibiciones e inhabilidades del personal de la Agencia. En efecto, prosiguió, los cambios señalan expresamente los derechos que tendrán los trabajadores del citado organismo.

Las Comisiones unidas advirtieron que las enmiendas recomendadas por la mesa de trabajo recaen en materias de iniciativa exclusiva de Su Excelencia el Presidente de la República.

Al respecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, anunció que el Ejecutivo haría llegar la indicación pertinente.

- En atención al compromiso adquirido por el representante del Gobierno, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, respaldaron, ad referéndum, la indicación número 107 con las enmiendas consignadas.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló una indicación, que fue individualizada como **indicación número 107 bis**, para sustituir el artículo 14 por el siguiente:

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

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

Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

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

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

El Director o Directora de la Agencia, sin perjuicio de lo que establezca el contrato, tendrá la facultad para aplicar las normas

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

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

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

Un reglamento expedido por el ministerio encargado de la seguridad pública, determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

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

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

La indicación número 108, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, busca reemplazar la expresión “Estatuto Administrativo” por “Código del Trabajo”.

- Habida cuenta de la aprobación de la indicación anterior, esta fue rechazada por ocho votos en contra, de los Honorables Senadores señores Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Quintana, Saavedra y Van Rysselberghe, y una abstención, del Honorable Senador señor Pugh.

ARTÍCULO 15

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

Respecto de este precepto se formuló **la indicación número 109**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

El personal de la Agencia no podrá intervenir, en razón de sus funciones, en asuntos en que tenga interés él o ella, su cónyuge, su conveniente civil, sus parientes consanguíneos del primer al cuarto grado inclusive, o por afinidad de primer 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, quedan exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañen personalmente al funcionario o que se refieran a la administración de su patrimonio. Además, será compatible con los cargos docentes hasta un máximo de doce horas semanales.

Igualmente, queda 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.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, solicitó dejar pendiente el debate y la votación de esta indicación. Justificando su petición, recordó que con ocasión de la aprobación de la indicación número 107, se advirtieron diversos aspectos vinculados al estatuto laboral que se aplicará a los trabajadores de la Agencia Nacional de

Ciberseguridad, que obligan a adecuar las prohibiciones e inhabilidades a las que quedarán sujetos.

En una sesión posterior, **el personero de Gobierno** informó que, tras un nuevo estudio, el grupo de asesores legislativo recomienda aprobar esta indicación con enmiendas, de manera que la redacción del artículo 15 del proyecto quede como se señala:

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

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

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

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

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

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

Analizando el artículo 15 propuesto, recordó que el personal de la Agencia Nacional de Ciberseguridad se regirá por las normas del Código del Trabajo. Con todo, acotó, se le aplicarán ciertas disposiciones del Estatuto Administrativo. Adujo que la razón de quedar sujeto a estas últimas descansa en el carácter de fiscalizador que tendrá.

Las Comisiones unidas estuvieron contestes en que el precepto sugerido por el grupo de asesores conformado para facilitar la tramitación de esta iniciativa de ley recae en materias de iniciativa exclusiva de Su Excelencia el Presidente de la República.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseguró que el Ejecutivo haría llegar la indicación pertinente.

- Habida cuenta del compromiso antedicho, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, respaldaron, ad referéndum, la indicación número 109 con las enmiendas consignadas.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló la correspondiente indicación, que fue individualizada con el **número 109 bis.**

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

PÁRRAFO 3°

Esta parte de la iniciativa de ley lleva por epígrafe “Registro Nacional de Incidentes de Ciberseguridad”.

En relación con ella, se formuló **la indicación número 110**, de Su Excelencia el Presidente de la República, para reemplazar su denominación por la siguiente:

“Párrafo 3°
Consejo Multisectorial sobre Ciberseguridad”.

- Puesta en votación, esta indicación contó con el respaldo de la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su

calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

ARTÍCULO 16

Refiere, por medio de dos incisos, al Registro Nacional de Incidentes de Ciberseguridad. Su tenor literal es el que sigue:

"Artículo 16. Del Registro Nacional de Incidentes de Ciberseguridad. Créase el Registro Nacional de Incidentes de Ciberseguridad, el que será administrado por la Agencia Nacional de Ciberseguridad y tendrá el carácter de reservado, por exigirlo el debido cumplimiento de las funciones de la Agencia, el debido resguardo de los derechos de las personas y la seguridad de la nación. En este registro se ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. Sobre la base de este registro se podrán realizar las respetivas investigaciones por parte de la Agencia, así como comunicar las alertas a los CSIRT Sectoriales, a los órganos del Estado señalados en el inciso final del artículo 4º y a las instituciones privadas que posean infraestructura de la información calificada como crítica, que corresponda al caso.

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

Sobre este artículo recayeron las indicaciones números 111, 112 y 113.

La indicación número 111, de Su Excelencia el Presidente de la República, es para suprimirlo.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 112, del Honorable Senador señor Van Rysselberghe, busca eliminar la frase "a los CSIRT Sectoriales,".

- Esta indicación fue retirada por su autor.

La indicación número 113, del Honorable Senador señor Insulza, reemplaza la locución "órganos del Estado señalados en el inciso final del artículo 4º y a las" por "organismos del Estado e".

- Al igual que la indicación anterior, esta fue retirada por su autor.

PÁRRAFO 4°

Esta parte del proyecto lleva por epígrafe “Consejo Técnico de la Agencia Nacional de Ciberseguridad”.

Al respecto, se formularon las indicaciones números 114 y 115.

La indicación número 114, del Honorable Senador señor Van Rysselberghe, lo elimina, junto con los artículos 17, 18, 19, 20 y 21, que lo integran.

- Esta indicación fue retirada por su autor.

La indicación número 115, de Su Excelencia el Presidente de la República, en tanto, suprime su epígrafe, pasando el actual Párrafo 5° a ser Párrafo 4°, y así sucesivamente.

- En votación, esta indicación contó con el respaldo de la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

ARTÍCULO 17

Regula, por medio de tres incisos, el Consejo Técnico de la Agencia Nacional de Ciberseguridad, rezando lo siguiente:

“Artículo 17. Consejo Técnico de la Agencia Nacional de Ciberseguridad. Créase el Consejo Técnico de la Agencia Nacional de Ciberseguridad, en adelante el “Consejo”, que tendrá como objeto asesorar y apoyar técnicamente a la Agencia en el análisis y revisión periódica de las políticas públicas propias de su ámbito de competencia, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad y, proponer posibles medidas para abordarlas.

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

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

En relación con este precepto se presentó **la indicación número 116**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como artículo 16:

“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 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 dos años, pudiendo ser reelegidos en sus cargos por una sola vez. La integración del Consejo deberá ser paritaria.

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.”.

Explicando esta indicación, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, sostuvo que la propuesta del Presidente de la República sustituye el Consejo Técnico de la Agencia Nacional de Ciberseguridad, cuyos miembros son 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.

A reglón seguido, manifestó que la razón de no incluir una disposición que precise las funciones del nuevo órgano -tal como lo hace el artículo 18 del texto aprobado en general- obedece a la conveniencia de contar con un espacio de diálogo público privado que, de manera permanente y amplia, apoye al Jefe de Estado en asuntos de ciberseguridad.

Dando a conocer la opinión de la mesa de trabajo prelegislativo, sentenció que esta sugiere aprobar con modificaciones esta

indicación, a fin de reemplazar en el inciso segundo, la locución “dos años” por “tres años”.

El Honorable Senador señor Pugh valoró la propuesta del Ejecutivo, pues juzgó que perfeccionará la composición de la entidad asesora, al incorporar la visión del mundo privado y vincular diferentes sectores, como son el industrial, el académico y el de las organizaciones de la sociedad civil. Además, destacó que sus miembros se desempeñarán ad honorem.

Otra diferencia respecto del proyecto aprobado en general, prosiguió, radica en el tiempo durante el cual los consejeros permanecerán en sus cargos. Al tenor de lo previsto en la indicación en análisis, puntualizó, ejercerán sus funciones durante seis años, pudiendo ser reelegidos por una vez. Añadió que su renovación se hará en tríos cada tres años.

A la luz de lo expuesto precedentemente, celebró que los integrantes trasciendan a los gobiernos de turno.

Con todo, calificó como esencial poseer reglas claras respecto a la conformación del primer Consejo Multisectorial sobre Ciberseguridad para garantizar que, a futuro, la alternancia se lleve a cabo adecuadamente.

Por su lado, **el Honorable Senador señor Ossandón** puso de relieve que, conforme a lo dispuesto en la oración final del inciso segundo del artículo en debate, la integración del consejo deberá ser paritaria. Al respecto, estimó que tal exigencia terminará por perjudicar a las mujeres. Profundizando en sus dichos, señaló que diversos estudios concluyen que cada vez son más las que trabajan en el área de la ciberseguridad.

Finalmente, reiteró que consejo citado debe estar compuesto por los mejores representantes de cada área, sin importar su género.

Discrepando de los planteamientos efectuados por el legislador que le antecedió en el uso de la palabra, **el Honorable Senador señor Insulza** hizo ver que la realidad del país obliga a contemplar normas que velen por la integración paritaria de ciertos órganos. Alcanzado un mejor nivel de igualdad entre hombres y mujeres, enunció, este modo de protección no será indispensable.

Fijando su atención en el carácter ad honorem de los integrantes del Consejo Multisectorial de Ciberseguridad, disintió de la idea de que quienes dedican su tiempo y conocimientos no reciban remuneración alguna a cambio. Pese a ello, declaró entender la razón por la cual se optó por este modelo.

Por último, recomendó que los miembros de la entidad cuya creación se propone sean aprobados por el Senado, tal como ocurre en otros casos.

Atendiendo la observación del Honorable Senador señor Ossandón, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, defendió la composición paritaria del consejo referido, afirmando que estará representada la mirada de hombres y mujeres.

También llamó a tener en consideración que en el área de la seguridad informática existe una fuerte concentración masculina. De hecho, acotó, los hombres representan cerca del 80%, lo que genera diversos efectos, entre ellos, sesgos en la visualización de este tipo de conflictos.

En sintonía con lo relatado recientemente, subrayó que las mujeres son las principales víctimas de acoso cibernético, no obstante lo cual las soluciones tecnológicas son diseñadas por personas del género opuesto, lo que impide dimensionar la amplitud del problema.

Luego, coincidió con el Honorable Senador señor Insulza en cuanto a que una norma que asegure paridad en la integración del Consejo Multisectorial sobre Ciberseguridad equilibrará las oportunidades para las mujeres, atendida la actual situación del mercado del sector.

Acerca de la intervención del Honorable Senador señor Pugh, en tanto, informó que el artículo sexto transitorio contempla reglas relativas a la integración del primer consejo para garantizar que, a futuro, la alternancia se realice de la forma prescrita.

En lo que atañe a la eventual aprobación de los miembros de la entidad por el Senado, anunció que dicha recomendación requeriría mayor análisis por parte del Ejecutivo.

A su turno, **el Honorable Senador señor Araya** compartió la importancia de que el país avance en paridad y en mayores espacios para las mujeres.

Sin embargo, opinó que en el caso del consejo no se observa con claridad por qué debe primar tal criterio. Por el contrario, reflexionó, simplemente es preciso velar porque quienes posean los mejores currículums en ciberseguridad lo conformen, sin atender al género.

El objetivo, declaró, es garantizar que el órgano asesor quede integrado apropiadamente. Relevó que la regla impuesta en la indicación podría conducir a que candidatos con más conocimientos y experiencia que otros queden fuera por su género, lo que incidirá en las políticas públicas sobre este fundamental tema. En conclusión, insistió, no es la paridad lo que hay que resguardar en esta ocasión, sino la capacidad técnica de los miembros del consejo.

El Honorable Senador señor Macaya, a su vez, juzgó fundamental incentivar la participación de las mujeres en todos los

espacios de la sociedad. Sin perjuicio de ello, especificó que hay ciertas áreas en las cuales, debido a su dificultad, se requiere la participación de personas que estén dotadas con las habilidades adecuadas. Así, profundizó, si se impusiera la exigencia de paridad en el Grupo de Operaciones Policiales Especiales, en las Fuerzas Armadas o en trabajos pesados mineros, se complejizaría el desarrollo de tales labores.

Su Señoría sentenció que en una materia tan compleja como es la ciberseguridad, lo que debe perseguirse es la participación de los mejores, independientemente del género. En consecuencia, concluyó, bien podrían ser solo mujeres.

Finalmente, expuso que imponer una limitación como la que es objeto de cuestionamientos, podría repercutir en la seguridad nacional.

El Honorable Senador señor Pugh alertó que los consejeros de la entidad cuya creación se propone en esta indicación serán designados por el Presidente de la República. Pormenorizó que el Primer Mandatario debe ser libre de nominar a quien quiera, pudiendo, por consiguiente, nombrar solo mujeres. En tal sentido, previno, la última oración del inciso segundo del artículo 16 limitaría la facultad de la máxima autoridad del país.

Recordó que hay lugares en los cuales la participación de las personas de género femenino es mayor a la de los hombres. Así, dijo, ocurre en el ámbito de la ciberinteligencia. En consecuencia, alertó, una regla como la cuestionada podría jugar en contra de aquellas. Con todo, reconoció que la fuerza laboral en ciberseguridad solo está compuesta en un 12% por mujeres.

El Honorable Senador señor Insulza reiteró que la exigencia discutida no es una arbitrariedad, sino simplemente el reconocimiento de una realidad y la defensa de la igualdad de oportunidades. De hecho, prosiguió, en la sociedad chilena actual impera aún la creencia de que los hombres están más preparados que las mujeres para asumir ciertas funciones.

Cuando el principio de paridad se haya asentado en la sociedad, connotó, no será imprescindible una imposición como la analizada.

Por último, resaltó que obligaciones como esta se han incorporado en diversos cuerpos del ordenamiento jurídico, incluso en la reforma constitucional.

El Honorable Senador señor Quintana, en tanto, puso de relieve que en seguridad preventiva está demostrado que la presencia de mujeres reporta beneficios significativos al trabajo de las policías. En efecto, ahondó, se ha verificado que patrullas mixtas facilitan las denuncias.

A reglón seguido, manifestó que el enfoque de género es aplicado en diversas áreas, y que no hay razones para no incorporarlo en esta, más aún cuando para las personas de género femenino

existen barreras de entrada para acceder a ciertos cargos. Añadió que su participación en el consejo mencionado allanará una visión distinta en ciberseguridad.

El Honorable Senador señor Ossandón postuló que la oración objeto de debate restringe la facultad del Presidente de la República para elegir a quienes están mejor preparados para integrar el órgano asesor aludido. La regla impuesta, observó, hará que la mitad de los cargos sean ocupados por mujeres, pero eso no implica, necesariamente, que sean las mejores candidatas para asumir tan significativa labor.

Para concluir, hizo ver la contradicción entre la propuesta en disputa y el actuar del Ejecutivo en los cambios realizados recientemente en la designación de quienes estarán a la cabeza del Ministerio de Desarrollo Social y Familia, y de la Secretaría de Estado de Justicia y Derechos Humanos.

Discrepando del legislador que le precedió en el uso de la palabra, **el Honorable Senador señor Saavedra** afirmó que la ausencia de reglas de paridad ha conducido a que sean hombres los que ejerzan gran parte de los cargos.

Al tenor de lo señalado, llamó a avanzar en la integración de hombres y de mujeres en la construcción de la sociedad. Añadió que mientras el país no madure en este sentido, exigencias como la cuestionada deberán permanecer.

En razón del debate suscitado, **el Honorable Senador señor Macaya** sugirió una redacción distinta para la última oración del inciso segundo, de manera de expresar que, en la elección, el Primer Mandatario procurará que se respeten los criterios de paridad de género, estableciéndolo como un principio. Consignó que tales términos evitarán rigidizar la decisión del Presidente de la República para nombrar a los más capacitados.

El Honorable Senador señor Van Rysselberghe respaldó los planteamientos de Su señoría.

Asimismo, resaltó que, debido a los talentos de las mujeres, la regla de paridad terminará por perjudicarlas.

El Honorable Senador señor Huenchumilla subrayó que la exigencia de representación balanceada en el Consejo Multisectorial sobre Ciberseguridad, al igual como ocurre en otras instituciones, encuentra su origen en el trato diferente y perjudicial que históricamente se ha dado a las personas de género femenino.

Hoy, prosiguió, los cambios en la sociedad obligan a dejar atrás dicha realidad. Una norma de discriminación positiva en favor de ellas les posibilitará acceder a cargos importantes y contribuir con sus talentos.

A pesar de sus dichos, reconoció que la imposición debatida resta flexibilidad al Primer Mandatario para nominar a quienes en un momento determinado estén mejor preparados.

En otro orden de ideas, cuestionó que los consejeros de la entidad creada se desempeñen ad honorem, y llamó a buscar algún mecanismo de remuneración que les permita palear el tiempo que dedicarán a un asunto tan significativo para el Estado, como es la seguridad informática.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, reiteró que la ciberseguridad es un espacio ocupado principalmente por hombres. Relató que el 78% de la fuerza laboral del área les corresponde. Estimó que, según el ritmo de crecimiento alcanzado, sin el requisito planteado, será imposible lograr la paridad, pese a que las mujeres constituyen más del 50% de la población chilena.

Connotó que la regla hará posible que el órgano asesor mencionado tenga la mejor representación de la sociedad. Su ausencia, añadió, reprimirá dicho objetivo, toda vez que, tradicionalmente, la balanza se ha inclinado en favor de las personas de género masculino.

Sostuvo que, si bien el número de mujeres abocadas a la ciberseguridad es aún bajo, puede afirmarse que las que asuman el cargo de consejera estarán muy bien calificadas.

Adicionalmente, recordó que las funciones de la entidad aludida apuntan a asesorar, analizar y formular recomendaciones respecto de las amenazas potenciales y existentes en seguridad informática. En este punto, destacó que el 99% de las víctimas de violencia digital de género son mujeres. De este modo, subrayó, se requiere una acción del Estado para equilibrar ese escenario.

Juzgó que el artículo examinado va en tal dirección. En consecuencia, invitó a aprobar la medida de paridad, para que el Presidente de la República pueda elegir como miembros del Consejo Multisectorial sobre Ciberseguridad a los mejores hombres y mujeres disponibles para asumir tal labor.

Enunció que, si en algunos años más la distribución de la fuerza laboral en ciberseguridad es similar, la exigencia podría suprimirse.

En lo que concierne a la inquietud de reconsiderar el carácter ad honorem de los consejeros, explicó que, si bien en el proyecto original se contempla un estipendio, se reparó que podría inhibir la participación de personas que suelen ser proveedoras del Estado. Verbigracia, comentó,

representantes de la industria, como es el caso de los de empresas de hacking contratadas por el Estado, no podrían ser miembros del citado órgano.

En sintonía con lo expuesto, opinó que el ejercicio a título gratuito otorgará más libertad. A mayor abundamiento, comentó que los académicos, en general, están impedidos de recibir remuneraciones de otros estamentos, salvo en casos excepcionales.

Por las razones detalladas, remarcó, el desempeño ad honorem consolidará un organismo asesor del más alto nivel.

Para concluir, aclaró que, a las razones precedentemente esgrimidas, se suman las restricciones presupuestarias para el financiamiento de la iniciativa de ley.

El Honorable Senador señor Ossandón instó al personero de Gobierno a buscar una redacción más flexible, como la sugerida por el Honorable Senador señor Macaya.

El Honorable Senador señor Huenchumilla concordó con los planteamientos del legislador que le precedió en el uso de la palabra. Al respecto, llamó a no olvidar que la mayoría de las enmiendas realizadas al texto aprobado en general han sido aprobadas por unanimidad.

Finalmente, las Comisiones unidas resolvieron votar separadamente la última oración del inciso segundo del artículo 16.

- Sometida a votación la indicación número 116, con excepción de la oración final del inciso segundo del artículo propuesto en ella, fue aprobada con la enmienda explicada al inicio del análisis -consistente en reemplazar la expresión “dos años” por “tres años”-, por la unanimidad de los miembros de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -actuando como integrante de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

- Puesta en votación la última oración del inciso segundo del artículo 16 propuesto, se registraron tres votos a favor, de los Honorables Senadores señores Insulza, Quintana y Saavedra; cuatro votos en contra, de los Honorables Senadores señores Araya, Ossandón, Pugh y Van Rysselberghe, y tres abstenciones, de los Honorables Senadores señores Huenchumilla -en su condición de miembros de ambas instancias legislativas- y Macaya.

- Repetida la votación de la última oración del inciso segundo del artículo 16 propuesto en la indicación, de conformidad a lo establecido en el artículo 178 del Reglamento del Senado, el resultado fue el mismo. Por consiguiente, al tenor de lo prescrito en el inciso segundo del citado precepto, las abstenciones se consideraron

como favorables a la posición que obtuvo mayor número de votos, quedando rechazada la mencionada oración por siete votos en contra, de los Honorables Senadores Araya, Huenchumilla -en su calidad de miembro de ambas Comisiones-, Macaya, Ossandón, Pugh y Van Rysselberghe, y tres votos a favor, de los Honorables Senadores señores Insulza, Quintana y Saavedra.

Como consecuencia de esta última votación, el artículo 16 quedaría de la manera que se transcribe:

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

El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, quienes permanecerán en su cargo durante seis años, renovándose en tríos cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.

Los integrantes del Consejo estarán obligados a presentar una declaración de intereses y patrimonio, en conformidad a lo dispuesto por la ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses, y estarán afectos al principio de abstención contenido en el artículo 12 de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.”.

ARTÍCULO 18

Establece las funciones del Consejo Técnico de la Agencia Nacional de Ciberseguridad. Su tenor literal es el que sigue:

“Artículo 18. Funciones del Consejo. Corresponderá al Consejo:

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

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

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

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

Sobre este precepto recayó **la indicación número 117**, de Su Excelencia el Presidente de la República, para suprimirlo.

- En votación, las Comisiones unidas, por la unanimidad de sus integrantes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación.

ARTÍCULO 19

Norma, por medio de cinco incisos, el funcionamiento del Consejo Técnico de la Agencia Nacional de Ciberseguridad. Al efecto, dispone que solo podrá sesionar con la asistencia de, al menos, tres de sus miembros, previa convocatoria del Director de la Agencia. Sin perjuicio de lo anterior, agrega, el Presidente del consejo estará obligado a convocar a una sesión extraordinaria cuando así lo requieran, por escrito, a lo menos tres de sus miembros. En todo caso, previene, el consejo podrá autoconvocarse en situaciones urgentes o necesarias conforme a la decisión de la mayoría de sus integrantes.

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

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

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

Finalmente, consigna que un reglamento expedido por el Ministerio del Interior y Seguridad Pública determinará las demás normas necesarias para el correcto funcionamiento del Consejo.

En relación con esta disposición, se formuló **la indicación número 118**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, consultado como artículo 17:

“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.

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.”.

El Honorable Senador señor Araya recomendó consignar en la redacción del nuevo artículo 17 que, en forma excepcional, el Consejo Multisectorial sobre Ciberseguridad podrá realizar recomendaciones de carácter reservado, en atención a que los temas involucrados versan sobre seguridad.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, observó que el artículo 29 de la iniciativa de ley consagra reglas referidas a la reserva de la información. Con todo, sugirió facultar al director de la Agencia Nacional de Ciberseguridad para declarar secretas algunas de las sesiones del consejo mencionado cuando los antecedentes así lo ameriten.

El Honorable Senador señor Huenchumilla propuso dejar pendiente la votación de esta indicación, a la espera de una redacción que recoja el planteamiento del Honorable Senador señor Araya.

En la sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que la mesa de trabajo prelegislativo, recogiendo las aprensiones suscitadas, acordó incorporar al inciso primero del artículo 17 contenido en la indicación analizada, la siguiente oración final:

“Excepcionalmente y mediante decisión fundada, el Director 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.”.

Acotó que, de acogerse tal sugerencia, la redacción del artículo 17 quedaría de la forma que se señala a continuación:

"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 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.".

- En votación, esta indicación fue aprobada, con la enmienda transcrita precedentemente y otras adecuaciones, por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Macaya, Pugh -actuando como miembro de ambas Comisiones- y Van Rysselberghe.

ARTÍCULO 20

Consagra las incompatibilidades de los miembros del Consejo Técnico de la Agencia Nacional de Ciberseguridad. Sobre el particular, indica que no podrán ser designados consejeros las personas que desempeñen empleos o comisiones retribuidos con fondos del Fisco, de las municipalidades, de las entidades fiscales autónomas, semifiscales, de las empresas del Estado o en las que el Fisco tenga aportes de capital, y con toda otra función o comisión de la misma naturaleza. Exceptúa a los empleos docentes y las funciones o comisiones de igual carácter de la enseñanza superior, media o especial.

Sobre este precepto recayó **la indicación número 119**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, contemplado como artículo 18:

"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. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.

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

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

Al respecto, **las Comisiones unidas** estuvieron contestes en la conveniencia de perfeccionar la redacción de la primera oración del inciso segundo del artículo 18 propuesto en la indicación, de modo que el deber de comunicación solo opere en las causales que posibilitan su cumplimiento. Para ello, acordaron incorporar, luego de la voz “Consejo”, la locución “cuando correspondiere”. En consecuencia, el tenor literal del artículo citado quedaría como sigue:

“Artículo 18. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro sesiones consecutivas.

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

El consejero respecto del cual se verificare alguna de las causales de cesación referidas anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.

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

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

El Honorable Senador señor Huenchumilla opinó que las causales individualizadas entre los literales a) y e) corresponden a situaciones que obviamente impedirán que el consejero afectado por ellas continúe en su cargo. Juzgó que no sería imprescindible contemplarlas.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sostuvo que los motivos considerados en la indicación objeto de análisis son las que habitualmente se señalan en la legislación para la cesación en el cargo de los miembros de órganos colegiados. Ellas, clarificó, no siempre operan de manera automática. Así, pormenorizó, la incapacidad física o síquica podría discutirse.

- Las Comisiones unidas, por la unanimidad de sus integrantes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron la indicación número 119 con la enmienda aludida.

°°°°°

Párrafo nuevo

Posteriormente, dando cumplimiento al compromiso adquirido, del cual se da cuenta en el debate de la indicación siguiente, Su Excelencia el Presidente de la República formuló una indicación, que fue individualizada como **indicación número 119 bis**, para intercalar en el Título III el siguiente párrafo 4°, nuevo, antes del artículo 21, que pasa a ser 19:

"Párrafo 4°
Red de Conectividad Segura del Estado."

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

°°°°°

ARTÍCULO 21

Indica las causales de cesación en el cargo de consejero técnico de la Agencia Nacional de Ciberseguridad. Su tenor literal es el que sigue:

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

a) Expiración del plazo por el que fue designado.

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

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

d) Fallecimiento.

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

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

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

i. Inasistencia injustificada a dos sesiones consecutivas.

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

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

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

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

Con relación a esta norma se formuló **la indicación número 120**, de Su Excelencia el Presidente de la República, para reemplazarla por la siguiente, consultada como artículo 19:

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

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

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

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, manifestó que la mesa de trabajo prelegislativo recomienda aprobar la indicación en análisis, con modificaciones, a fin de sustituir en los incisos primero y final la voz “órganos” por “organismos”, además enmiendas meramente formales.

Acotó que, de respaldarse tal propuesta, la redacción del artículo 19 quedaría como sigue:

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

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

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

El Honorable Senador señor Huenchumilla puso de manifiesto que, conforme a la indicación en estudio, el reglamento será expedido por el Ministerio encargado de la seguridad pública y visado por el Ministro de Hacienda.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que mientras se discute en el Congreso Nacional la creación del Ministerio de Seguridad Pública, se ha optado por emplear la fórmula mencionada. Sin embargo, en estricto rigor, acotó, debiera aludirse al Ministro de Seguridad Pública.

En otro orden de ideas, comunicó que la indicación formaliza la Red de Conectividad Segura del Estado, disponible en el país desde el Gobierno del ex Presidente, señor Ricardo Lagos, que permite que los servicios públicos contraten de manera centralizada acceso a Internet, lo que se ha traducido en ahorro de recursos para el país y un funcionamiento seguro.

A su vez, **el Honorable Senador señor Pugh** respaldó los dichos del personero de Gobierno. Adicionalmente, apuntó, se agrega la referencia a que la red deberá ser segura. Precisó que este último atributo dice relación no solo con que es de fiar, sino también con su capacidad de resiliencia.

Las Comisiones unidas, alertaron que el artículo cuya creación se propone en esta indicación queda bajo el alero del Párrafo 4°, del Título III, denominado “Consejo Multisectorial sobre Ciberseguridad”, por lo que en el texto definitivo deberá tener la ubicación pertinente.

Dicha observación fue recogida, como se dijo, en la indicación signada con el número 119 bis.

- Las Comisiones unidas, por la unanimidad de sus integrantes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron la indicación número 120 con las enmiendas consignadas oportunamente.

ARTÍCULO 22

Crea el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática dentro de la Agencia Nacional de Ciberseguridad y señala sus funciones.

Letra a)

Encomienda al CSIRT Nacional la función de responder ante incidentes de ciberseguridad o ciberataque que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información relativos a instituciones privadas no sometidas a la supervigilancia de un regulador o fiscalizador sectorial y que posean infraestructura de la información calificada como crítica, de conformidad a lo prescrito en esta ley.

Con respecto a este literal se presentó **la indicación número 121**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, afirmó que la indicación examinada persigue precisar las atribuciones del CSIRT Nacional.

El Honorable Senador señor Insulza observó que la iniciativa de ley utiliza en diversos artículos la sigla "CSIRT" para referirse al Equipo de Respuesta a Incidentes de Seguridad Informática.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que el empleo del acrónimo "CSIRT" responde a que se ha estandarizado técnicamente a nivel internacional, y encuentra su origen en la denominación original del grupo referido, llamado en inglés "computer security incident response team". Sin perjuicio de su uso en la iniciativa de ley, alertó, el título recurre a la expresión en español.

Luego, solicitó aprobar esta indicación con una modificación, a fin de reemplazar la expresión "impacto significativo" por "efecto significativo" para que haya coherencia entre este literal y el artículo 7 aprobado por las Comisiones unidas.

Detalló que, de acogerse tal requerimiento, la redacción del citado literal a) quedaría como sigue:

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

A su turno, **el Honorable Senador señor Pugh** dio a conocer que a nivel mundial existen dos formas para nombrar los equipos de respuesta citados; en primer lugar, la sigla “CSIRT”, y por otro la abreviatura “CERT”. No obstante, alertó, esta última corresponde a un término de marca registrada de la Universidad Carnegie Mellon.

Sostuvo que en Europa se utiliza la primera fórmula. Además, connotó, la OEA decidió emplear en todo el continente la misma opción. Así, relevó, la sigla citada no es extraña, y permite homologación con los estándares internacionales.

Asimismo, Su Señoría constató que el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática solo intervendrá ante ciberataques o incidentes que sean de consecuencias importantes. Por lo tanto, destacó, no estará permanentemente activo. Serán las CSIRT sectoriales los que tomarán el control, ejecuten las acciones correspondientes y reporten. Reiteró que solo en el evento de hechos mayores -y que tengan efectos significativos- operará el órgano nacional.

- Puesta en votación, esta indicación fue aprobada con la enmienda referida, por la unanimidad de los miembros de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra b)

Establece como función del CSIRT Nacional coordinar a los CSIRT Sectoriales frente a ataques, vulnerabilidades, incidentes y brechas de ciberseguridad.

Sobre este literal recayeron las indicaciones números 122 y 123.

La indicación número 122, del Honorable Senador señor Van Rysselberghe, es para eliminarlo.

- Esta indicación fue retirada por su autor.

La indicación número 123, de Su Excelencia el Presidente de la República, es para sustituirlo por el siguiente:

“b) Coordinar a los CSIRT Sectoriales frente a ciberataques o incidentes de ciberseguridad de impacto significativo. La misma coordinación deberá establecer con el CSIRT de la Defensa Nacional. En el

ejercicio de esta función, el CSIRT Nacional podrá realizar todas las acciones necesarias para asegurar una respuesta rápida por parte de los CSIRT Sectoriales, incluida la supervisión de las medidas adoptadas por estos.”.

Al igual que con ocasión de la indicación número 121, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, solicitó aprobar con modificaciones la enmienda en análisis para reemplazar la locución “impacto significativo” por “efecto significativo”, a fin de que exista coherencia entre la redacción del literal b) del artículo 22; el literal a) del mismo precepto y el artículo 7 de la iniciativa de ley.

Pormenorizó que, de acogerse tal sugerencia, el tenor literal del literal b) quedaría de la forma que se señala a continuación:

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

Seguidamente, informó que la indicación propone alcanzar un sistema coordinado de respuesta ante incidentes, a nivel sectorial, nacional y de defensa.

- Puesta en votación, esta indicación fue aprobada con la enmienda referida, por la unanimidad de los integrantes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra d)

Considera como función del CSIRT Nacional prestar colaboración o asesoría técnica a los CSIRT Sectoriales en la implementación de políticas y acciones relativas a ciberseguridad.

Al respecto, se formuló **la indicación número 124**, del Honorable Senador señor Van Rysselberghe, para suprimirla.

- Esta indicación fue retirada por su autor.

Letra e)

Entrega al CSIRT Nacional la función de ofrecer soporte a los CSIRT Sectoriales para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.

En relación con este literal se presentaron las indicaciones números 125 y 126.

La indicación número 125, del Honorable Senador señor Van Rysselberghe, es para eliminarlo.

- Esta indicación fue retirada por su autor.

La indicación número 126, de Su Excelencia el Presidente de la República, lo reemplaza por el siguiente:

"e) Supervisar incidentes a escala nacional.".

- Sometida a votación, esta indicación fue respaldada por la unanimidad de los integrantes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra f)

Encomienda al CSIRT Nacional la función de consolidar y tratar los datos técnicos y antecedentes que describen la ocurrencia de incidentes de ciberseguridad, ciberataques, vulnerabilidades y demás información para efectos de la alimentación del registro previsto en los términos del artículo 16.

Sobre este literal recayó **la indicación número 127**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

- En votación, esta indicación fue aprobada por la unanimidad de los integrantes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra g)

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

Respecto de este literal se formularon las indicaciones números 128 y 129.

La indicación número 128, de Su Excelencia el Presidente de la República, elimina el siguiente texto: “, con la finalidad de procurar que los órganos del Estado e instituciones privadas que posean infraestructura de la información calificada como crítica cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques”.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, comunicó que la supresión consignada busca alcanzar coherencia entre la letra g) del artículo 22 y el modelo previsto en el artículo 4 del proyecto de ley.

El Honorable Senador señor Quintana aseveró no compartir la idea de reemplazar el sistema de infraestructura crítica de la información por el de servicios esenciales y operadores de importancia vital. Por tal motivo, anunció que votaría en contra de esta indicación.

- La mayoría de los miembros de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Saavedra y Van Rysselberghe, respaldó esta indicación. El Honorable Senador señor Quintana, en tanto, votó en contra.

La indicación número 129, del Honorable Senador señor Insulza, reemplaza la expresión “órganos del Estado” por “organismos del Estado”.

- Esta indicación fue retirada por su autor.

Letra h)

Considera como función del CSIRT Nacional requerir a los CSIRT Sectoriales, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.

Al efecto, se presentaron las indicaciones números 130 y 131.

La indicación número 130, del Honorable Senador señor Van Rysselberghe, es para suprimirla.

- Esta indicación fue retirada por su autor.

La indicación número 131, de Su Excelencia el Presidente de la República, busca reemplazar la expresión “a los CSIRT Sectoriales, dentro del ámbito de su competencia”, por la siguiente: “a las instituciones afectadas o a los CSIRT correspondientes”.

De aprobarse esta indicación, el literal quedaría como sigue:

“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.”.

- Las Comisiones unidas, por la unanimidad de sus integrantes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, respaldaron esta indicación.

Letra i)

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

Sobre este literal recayeron las indicaciones números 132, 133 y 134.

La indicación número 132, de Su Excelencia el Presidente de la República, es para para sustituirlo por el siguiente:

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

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, puso de relieve que esta función es ejercida actualmente por el CSIRT de Gobierno.

- En votación, esta indicación contó con el apoyo de la totalidad de los integrantes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 133, del Honorable Senador señor Van Rysselberghe, suprime la frase “, conjuntamente con uno o más CSIRT Sectoriales,”.

- Esta indicación fue retirada por su autor.

La indicación número 134, del Honorable Senador señor Insulza, busca reemplazar, las dos veces en que aparece, la expresión “órganos del Estado”, por “organismos del Estado”.

- Al igual que la indicación anterior, esta fue retirada por su autor.

Letra j)

Establece como función del CSIRT Nacional generar y difundir información mediante campañas públicas y prestar asesoría técnica general a personas naturales o jurídicas, que no se encuentran reguladas por esta ley, que estén o se hayan visto afectadas por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o hayan afectado el funcionamiento de su operación.

En relación a este literal se formuló **la indicación número 135**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

“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.”.

- Puesta en votación, esta indicación contó con el respaldo de la unanimidad de los integrantes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

Letra k)

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

Respecto de este literal se presentaron las indicaciones números 136 y 137.

La indicación número 136, de Su Excelencia el Presidente de la República, es para eliminarlo.

- Sometida a votación, esta indicación contó con la aprobación de todos los integrantes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe.

La indicación número 137, del Honorable Senador señor Van Rysselberghe, busca reemplazar la expresión “los otros CSIRT Sectoriales, de Gobierno y Defensa” por “los reguladores o fiscalizadores sectoriales”.

- Esta indicación fue retirada por su autor.

TÍTULO IV

Lleva por epígrafe “De los equipos de respuesta a incidentes de seguridad informática sectoriales”.

Sobre esta parte del proyecto de ley recayeron las indicaciones 138 y 139.

La indicación número 138, del Honorable Senador señor Van Rysselberghe, es para suprimirlo, junto con los artículos 23, 24, 25 y 26, que lo integran.

- Esta indicación fue retirada por su autor.

La indicación número 139, de Su Excelencia el Presidente de la República, reemplaza su denominación por la siguiente:

“TÍTULO IV
Otras instituciones intervinientes”.

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de miembro de ambas instancias legislativas-, Insulza, Macaya, Ossandón, Pugh, Quintana, Saavedra y Van Rysselberghe, aprobaron esta indicación.

ARTÍCULO 23

Esta disposición refiere a los CSIRT Sectoriales. Su tenor literal es el que sigue:

“Artículo 23. CSIRT Sectoriales. Los reguladores o fiscalizadores sectoriales podrán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad dar respuesta a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de sus respectivos sectores regulados.

Un reglamento expedido por el Ministerio del Interior y Seguridad Pública establecerá las instancias de coordinación entre la Agencia Nacional de Ciberseguridad, los reguladores y fiscalizadores

sectoriales, así como de sus respectivos CSIRT, dentro del marco que fija esta ley.”.

Respecto de este precepto se formuló **la indicación número 140**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como artículo 21:

“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 dar respuesta a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de las instituciones privadas.

Las funciones de los CSIRT Sectoriales serán determinadas por la Agencia, y en su actuación quedarán sujetos a su coordinación e instrucción.

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.”.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que la mesa de trabajo prelegislativo recomienda aprobar con modificaciones esta indicación, de modo que la redacción del artículo 21 quede de la manera siguiente:

“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 a 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, y

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

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

Antes de interiorizarse en el contenido de la indicación y en los cambios introducidos, las Comisiones unidas acordaron escuchar la opinión de la Comisión para el Mercado Financiero, servicio público que solicitó ser recibido en audiencia para manifestar sus observaciones en relación con ciertos aspectos del proyecto de ley.

La Comisionada de la Comisión para el Mercado Financiero, señora Bernardita Piedrabuena, adujo que la entidad que integra valora la iniciativa de ley en examen, toda vez que es importante para el país contar con una Agencia Nacional de Ciberseguridad con facultades establecidas en la ley. Sin embargo, anunció, la institución tiene ciertas aprensiones respecto a cómo se coordinarán ambos organismos.

Recordó que la Comisión para el Mercado Financiero es un cuerpo regulador colegiado, de carácter técnico, autónomo y con patrimonio propio. Especificó que su directorio está compuesto por cinco miembros, cuatro de los cuales son elegidos por el Presidente de la República y ratificados por el Senado por los cuatro séptimos de sus parlamentarios en ejercicio. Agregó, asimismo, que las causales de remoción de los comisionados se encuentran taxativamente señaladas en la legislación, requiriéndose, además, la ratificación de la Corte Suprema.

Sostuvo que las cuatro personas aludidas precedentemente duran seis años en el cargo, pudiendo renovarse sus nombramientos. Adicionalmente, dijo, el presidente -que se desempeñará por un periodo de cuatro años- es elegido por el Primer Mandatario, y su separación supone una decisión fundamentada.

Puso de relieve que la creación del servicio público que representa responde a la conveniencia de que el país tenga un órgano ordenador técnico e independiente del ciclo político y de los regulados.

A la luz de lo expuesto, juzgó indispensable mantener la jerarquía institucional de dicha entidad, e hizo ver la preocupación que genera el que la Agencia Nacional de Ciberseguridad -cuyo director es elegido por medio del Sistema de Alta Dirección Pública y puede ser removido sin causales-, eventualmente coarte la autonomía de la que actualmente goza la Comisión para el Mercado Financiero.

Por otro lado, connotó que la indicación objeto de examen faculta, en términos amplios, al servicio que integra a dictar instrucciones generales y particulares sin conferir recursos para estas nuevas responsabilidades.

Siguiendo con el desarrollo de su exposición, afirmó que en la legislación comparada -España, Estados Unidos, Reino Unido, Brasil, México y Colombia, entre otros países- si bien existe una institución a cargo de los asuntos de ciberseguridad, se reconoce al sector financiero como uno relevante y con supervisión especial, haciéndose deferencia a sus potestades,

experiencias y capacidades. En definitiva, subrayó, se considera la competencia que tiene el organismo regulatorio para dictar normas sobre el particular y fiscalizarlas, tanto en tiempos normales como de crisis.

Asimismo, notó que la Comisión vela por la estabilidad financiera y la protección de los asegurados, depositantes e inversionistas. En este contexto, reflexionó, pese a que el órgano es nuevo, tiene una larga trayectoria en asuntos tecnológicos y de ciberseguridad. Ello, acotó, pues su origen se remonta a la unión de las Superintendencias de Bancos e Instituciones Financieras, y de Valores y Seguros.

A mayor abundamiento, pormenorizó que actualmente posee dos normas, la N° 2.010, que regula la gestión de riesgos y la ciberseguridad, particularmente en bancos, emisores de tarjetas y cooperativas, y la N° 454, que aborda la seguridad informática en las compañías de seguro.

En razón de lo indicado, manifestó su preocupación en torno a la continuidad operacional de las instituciones fiscalizadas. En efecto, profundizó, un posible contexto de ciberataque obligará a fijar reglas mínimas para que sigan funcionando y no se produzcan disrupciones en la atención a los clientes. Además, es necesario evitar el contagio de incidentes al interior de las organizaciones del sistema.

Por otra parte, expresó su inquietud frente a la posibilidad de que en eventos de crisis existan dos encargados de comunicar las instrucciones a los fiscalizados por la Comisión para el Mercado Financiero. Tal escenario, alertó, podría motivar la paralización. Estimó que, dada la experiencia y conocimiento del organismo en el funcionamiento del sistema financiero, este debiera ser el ente que lidere la labor supervisora en esos momentos. A mayor abundamiento, hizo presente que detener el sector tiene efectos nocivos sobre la economía y los ciudadanos.

Luego, aseveró que los incidentes de ciberseguridad focalizados al área financiera no se propagan a otras, como a las líneas aéreas, hospitales, colegios o entidades que puedan resultar de interés.

La Comisionada de la Comisión para el Mercado Financiero, señora Bernardita Piedrabuena, concluyó su participación sosteniendo que, si bien es importante la creación de la Agencia Nacional de Ciberseguridad, para la entidad que integra es fundamental conservar la autonomía respecto de sus supervisados en lo que atañe a la dictación de instrucciones y al ejercicio de las actividades fiscalizadoras.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, acerca de la intervención de la representante de la Comisión para el Mercado Financiero, reconoció que el proyecto de ley ingresado a tramitación no contemplaba distinciones entre los diversos sectores, por considerarse que era aconsejable tener una autoridad amplia que regulara de manera omnicomprensiva todo lo relacionado con la ciberseguridad. Ello, puntualizó, posibilitaría la respuesta coordinada desde el

Estado y, por lo tanto, gestionar adecuadamente los riesgos y amenazas del ciberespacio.

Sin embargo, previno, posteriormente, la mesa técnica incorporó dos excepciones. La primera, acotó, consiste en facultar al citado servicio público para 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. En definitiva, constató, se plasma en la ley el deber de coordinación. En este punto, informó, no hay diferencias con la Comisión para el Mercado Financiero.

La segunda innovación, continuó, radica en facultar al CSIRT del sector financiero sujeto a la fiscalización de la Comisión para el Mercado Financiero, para dar cumplimiento solo a los protocolos y estándares técnicos que la Agencia Nacional de Ciberseguridad comunique ante la ocurrencia de incidentes de ciberseguridad, salvo que pudieran tener efectos en todas las redes y sistemas informáticos del país, pues en esta situación deberán observarse también las instrucciones generales y particulares emanadas de la Agencia, con el objeto de lograr un nivel común de ciberseguridad y respuestas coordinadas. Con todo, clarificó, no se afectan las facultades fiscalizadoras, las normativas ni las de supervisión del mercado financiero.

A continuación, discrepó de la afirmación efectuada por la señora Piedrabuena relativa a que los ciberataques no se propagan fuera del área financiera, toda vez que dicho organismo tiene la capacidad de contenerlo. Justificando su parecer, señaló que basta con pensar en un incidente que afecta a un proveedor que presta, al mismo tiempo, servicios a la banca y a otra industria del país. En tal hipótesis, remarcó, la posibilidad de extensión es alta.

En consecuencia, postuló, el Ejecutivo estima que deben respetarse las instrucciones generales y particulares que la Agencia Nacional de Ciberseguridad dicte frente a un incidente que pueda tener efectos sistémicos, insistiendo en que el objetivo de crear un órgano especializado en ciberseguridad es lograr respuestas coordinadas.

En la misma línea argumental, disintió de la aseveración referida a que en tal evento habrá dos voces. Aclaró que la mayor parte del tiempo, cada cual se hará cargo de su ámbito de competencia, mas cuando se esté frente a una agresión con el potencial de transformarse en sistémico, habrá una sola autoridad, pues los riesgos para la seguridad de las redes del país serán mayores. Así, puntualizó, quedó en evidencia tras el ataque de ransomware WannaCry a nivel mundial, en el año 2017, que infectó a múltiples sectores.

Por las razones esgrimidas, llamó a aprobar la indicación en los términos sugeridos por el equipo de asesores.

El Honorable Senador señor Pugh reconoció la experiencia de la Comisión para el Mercado Financiero en materia de

ciberseguridad, y añadió que su normativa ha sido visionaria. Así queda de manifiesto, profundizó, con la exigencia que pesa sobre los fiscalizados de reportar, en treinta minutos, incidentes de dicha índole, en circunstancias de que el proyecto otorga tres horas a los CSIRT sectoriales ante tal tipo de circunstancias.

Su Señoría destacó que el fin perseguido por la iniciativa en estudio radica en tener un ecosistema digital que dé prosperidad al país -y que sea robusto y resiliente-, agregando que la infraestructura crítica de la información tiene dos características, la dependencia y la interdependencia.

Por otra parte, hizo ver que detrás de un ataque hay una autoría, la que debe ser determinada. Para ello, planteó, es imprescindible disponer de toda la información, lo que exige colaboración y no competición.

A fin de despejar dudas acerca del sector financiero, fue tajante en señalar que no está en el espíritu de la futura ley entrometerse en los procesos que él desarrolla, sino solo reaccionar coordinadamente para proteger a todos los ciudadanos de la mejor forma en situaciones muy particulares y difíciles.

En consecuencia, instó a respaldar la indicación en los términos propuestos por la mesa técnica.

El Honorable Senador señor Huenchumilla expresó interés por saber qué rol juega, en asuntos de ciberseguridad en la experiencia comparada, un órgano como la Comisión para el Mercado Financiero.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, respondió que en la Unión Europea -que constituye el marco de referencia para toda esta discusión- se ha avanzado en una regulación general sobre ciberseguridad; en una especial para el sector financiero, y una particular para las infraestructuras críticas. Indicó que, si bien el conjunto de normas más actualizado mantiene esa separación, propende a la coordinación entre las instituciones.

Relevó que el proyecto en debate sigue esa línea. Así, puntualizó, se observará al examinar las indicaciones que siguen. En esta oportunidad, reiteró, lo único que se prescribe es que en caso de incidentes que puedan tener efectos sistémicos, tan importante labor debe quedar, por deferencia, en la Agencia Nacional de Ciberseguridad.

El Honorable Senador señor Huenchumilla consultó si en la experiencia comparada existe algún organismo que vele por esa visión sistémica.

Atendiendo la inquietud del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor**

Daniel Álvarez, declaró que la labor suele recaer en los CSIRT Nacional, sin importar el sector de que se trate.

El Honorable Senador señor Huenchumilla declaró cerrado el debate y solicitó a los representantes de la Comisión para el Mercado Financiero que, de tener otras observaciones a la iniciativa legal, las hicieran llegar a la Secretaría de las Comisiones unidas. Si es necesario, adelantó, podría reabrirse el debate.

- Las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh -actuando como miembro de ambas Comisiones-, Saavedra y Van Rysselberghe aprobaron, ad referéndum, la indicación número 140 con las enmiendas transcritas anteriormente.

Posteriormente, dando cumplimiento al compromiso asumido, Su Excelencia el Presidente de la República presentó una indicación, que fue individualizada como **indicación número 140 bis**, para reemplazar el artículo 23 por el siguiente:

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

Los CSIRT Sectoriales tendrán las siguientes funciones:

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

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

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

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

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

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

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

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

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

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

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

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

Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las instancias de coordinación entre la Agencia y las autoridades sectoriales y sus respectivos CSIRT.”.

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, aprobaron esta indicación.

ARTÍCULO 24

Señala, por medio de 11 literales, las funciones de los CSIRT Sectoriales. Su redacción es la que se indica:

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

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

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

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

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

e) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos de la Administración de Estado de su sector y de las instituciones reguladas cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.

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

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

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

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

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

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

En relación con esta norma se presentó **la indicación número 141**, de Su Excelencia el Presidente de la República, para reemplazarla por la siguiente, contemplada como artículo 22:

“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 sectorial respectiva. Estas normas deberán ser sometidas a la aprobación previa de la Agencia, la que 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. Con todo, si las autoridades sectoriales dictan normas generales sobre gestión de riesgos, que estén basadas en estándares internacionales e incluyan elementos relativos a ciberseguridad, podrán mantener dichos elementos.

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

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, comentó que la disposición analizada dice relación con la facultad normativa especial de los órganos reguladores sectoriales. Ello, justificó, puesto que conocen sus capacidades y necesidades. Sin embargo, remarcó, dicha atribución debe ejercerse en coordinación con la Agencia Nacional de Ciberseguridad.

A reglón seguido, informó que el equipo de asesores conformado para facilitar la tramitación de esta iniciativa de ley recomienda aprobar la indicación en examen con las modificaciones que siguen:

- Suprimir la última oración del inciso segundo del artículo 22 propuesto, dado que resulta innecesaria, e

- Incorporar un inciso final, nuevo, a fin de reconocer la particularidad de la Comisión para el Mercado Financiero, del tenor que se transcribe:

"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 dictadas 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.".

Las Comisiones unidas advirtieron que el inciso final cuya incorporación se aboga recae en una materia de iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo dispuesto en el artículo 65, inciso cuarto, número 2, de la Constitución Política de la República.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, anunció que el Ejecutivo respaldaría oportunamente esta indicación.

- Habida cuenta del compromiso asumido, las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Araya, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh -actuando como miembro de ambas Comisiones-, Saavedra y Van Rysselberghe, aprobaron, ad referéndum, esta indicación con las enmiendas transcritas recientemente.

Posteriormente, dando cumplimiento al compromiso adquirido, Su Excelencia el Presidente de la República formuló una indicación, que fue individualizada como **indicación número 141 bis**, para reemplazar el artículo 24 por el siguiente:

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

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

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

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

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, respaldaron esta indicación.

Letra b)

Entrega a los CSIRT Sectoriales el deber de ofrecer soporte a los CSIRT de las instituciones reguladas para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.

Sobre este literal recayó **la indicación número 142**, del Honorable Senador señor Insulza, para sustituir la expresión “órganos del Estado” por “organismos del Estado”.

- Esta indicación fue retirada por su autor.

ARTÍCULO 25

Consagra el deber general de informar. Específicamente reza lo siguiente:

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

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

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

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

Al respecto, se formuló **la indicación número 143**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, considerado como artículo 23:

“Artículo 23. Incidentes de impacto significativo. Se considerará que un incidente de ciberseguridad tiene impacto 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 de información 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 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 prescrito 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 es 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.”.

Iniciando el estudio de esta indicación, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que el equipo de asesores conformado para facilitar la tramitación de este proyecto de ley sugiere aprobarla con modificaciones, reemplazando la voz “impacto” por “efecto”, las dos veces que aparece, de manera que haya coherencia con el articulado aprobado anteriormente.

Pormenorizó que se acogerse dicha recomendación, la redacción del artículo 23 quedaría de la siguiente forma:

“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 de información 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.”.

El Honorable Senador señor Insulza solicitó conocer la razón por la cual se propone reemplazar el artículo aprobado en general por la Sala.

Refiriéndose a la preocupación del legislador que le precedió en el uso de la palabra, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que los deberes de los CSIRT sectoriales están contenidos en el artículo 21. Agregó, además, que otras funciones serán desarrolladas a nivel reglamentario.

A continuación, puso de relieve que la norma sugerida en la indicación analizada, en tanto, persigue asegurar que los CSIRT sectoriales solo fijen su atención y capacidad de respuesta en los incidentes de efecto significativo. Argumentó que tal decisión descansa en que la notificación de todo ciberataque dificultará la gestión de aquellos.

- Puesta en votación, la indicación número 143 fue aprobada, con las enmiendas señaladas y otras adecuaciones, por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla -en su calidad de integrante de ambas instancias legislativas-, Insulza, Pugh -actuando como miembro de ambas Comisiones-, Saavedra y Van Rysselberghe.

ARTÍCULO 26

Establece el deber de los CSIRT Sectoriales de informar a la Agencia Nacional de Ciberseguridad cuando hayan vivido un incidente de seguridad informática. Su tenor literal es el que sigue:

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

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

a) Afecta a una gran cantidad de usuarios.

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

c) Afecta a una extensión geográfica considerable.

d) Afecta sistemas de información que contengan datos personales.

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

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

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

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

El procedimiento específico para notificar un incidente de ciberseguridad, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad serán establecidos en el reglamento de la presente ley.”.

En relación con esta disposición, se presentó **la indicación número 144**, de Su Excelencia el Presidente de la República, para sustituirla por la siguiente, consultada como artículo 24:

“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 órganos de la Administración del Estado, 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 órganos 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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, explicó que la norma persigue dos objetivos. El primero, detalló, consiste en regular la creación de los centros de certificación acreditados. Sostuvo que, conforme al modelo escogido, será la Agencia Nacional de Ciberseguridad la encargada de otorgarles dicha calidad.

El segundo, prosiguió, radica en establecer ciertos criterios respecto a la adquisición de tecnologías por parte del Estado.

Reveló que la mesa de trabajo prelegislativo recomienda aprobar la indicación analizada con enmiendas, de manera de reemplazar, en los incisos primero y final, la voz “órganos” por “organismos”, tal como se ha hecho en otras oportunidades; introducir en la oración final del inciso primero, luego de la palabra “Estado”, la expresión “que estén sujetos a las obligaciones del artículo 6”, y sustituir en el inciso cuarto la locución “deberán evaluar de mejor manera y” por “procurarán”.

El Honorable Senador señor Pugh hizo ver la relevancia de los centros de certificación acreditados. Al efecto, recordó que uno de los fines de la Política Nacional de Ciberseguridad es la creación de una industria chilena de esta naturaleza. En este marco, anheló la posibilidad de acceder a servicios, sistemas y equipamientos; sin embargo, alertó, ello supone asegurar los más altos estándares.

Deteniéndose en las enmiendas sustantivas cuya incorporación se propone, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, apuntó que aquella recaída en el inciso primero busca precisar que la entidad encargada de entregar certificación a los organismos del Estado que estén sujetos a los deberes específicos de los operadores de importancia vital será la Agencia Nacional de Ciberseguridad.

En lo que atañe a la modificación del inciso cuarto, en tanto, expresó que persigue introducir la variable de ciberseguridad en los procesos de adquisición de tecnología. Sostuvo que la decisión de perfeccionar la redacción de la indicación en estudio obedece a que las entidades vinculadas a la compra y contratación pública advirtieron que, muchas veces, las complejidades de las licitaciones no permiten la aplicación de una regla tan estricta. Así, manifestó, se optó por señalar que los organismos públicos,

simplemente, procurarán dar preferencia a los productos y servicios calificados con un nivel adecuado de seguridad por un centro certificador. Agregó que la Agencia Nacional de Ciberseguridad ahondará en el alcance de dicha exigencia.

Concluyó su intervención reconociendo que, si bien la recomendación del grupo de asesores conlleva a un estándar menor, con el paso del tiempo podrán incrementarse las pretensiones sobre este aspecto.

Fijando su atención en el reemplazo referido al inciso cuarto, **el Honorable Senador señor Macaya** lo cuestionó. A mayor abundamiento, observó que las compras involucradas implican gran cantidad de recursos y, en ese contexto, una norma imperativa como la contemplada originalmente en la indicación es a todas luces preferible.

El Honorable Senador señor Huenchumilla se sumó a los reparos del legislador que le antecedió en el uso de la palabra.

Abocándose a los comentarios efectuados por los parlamentarios, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, connotó que la decisión de rebajar la exigencia original se debe a la realidad del país. En efecto, pormenorizó, el nivel de madurez en ciberseguridad para la contratación pública es bajo. De hecho, resaltó, Chile sigue teniendo convenciones tecnológicas en donde asuntos como la propiedad intelectual aún no están bien resueltos.

Adicionalmente, recordó que la evaluación es una parte muy específica del proceso referido. En consecuencia, continuó, dar preferencia a productos y servicios calificados parece más oportuno.

Luego, postuló que la creación de la Agencia Nacional de Ciberseguridad, órgano que tendrá potestad normativa respecto de los organismos públicos, posibilitará mayor intensidad por la vía administrativa.

A su vez, **el Honorable Senador señor Pugh** coincidió en que el nivel de seguridad informática debiera ser más alto.

No obstante, juzgó que la entidad pública del artículo 8 tendrá el desafío de lograr que aquellas áreas de más alto riesgo eleven sus estándares, otorgando una mayor ponderación a la ciberseguridad. De esta manera, planteó, será ella quien lo determine, erradicando toda discrecionalidad.

A la luz de lo señalado, aseveró, pese a que se atenúa la exigencia a nivel legal, administrativamente podrá avanzarse en la dirección deseada.

Discrepando del razonamiento del legislador que le antecedió en el uso de la palabra, **el Honorable Senador señor Saavedra** llamó a optar por una norma imperativa, en los términos previstos en la indicación analizada. Su Señoría sugirió mantener la redacción relativa a que los organismos públicos deberán evaluar de mejor manera y dar preferencia a

los productos y servicios calificados con un nivel adecuado de seguridad por un centro certificador.

Acogiendo la propuesta antedicha, **el Presidente de la Comisiones unidas** cerró el debate respecto de la indicación analizada con las enmiendas aconsejadas por la mesa de trabajo prelegislativo, con excepción de aquella recaída en el inciso cuarto, toda vez que no concita el acuerdo de los integrantes de las Comisiones unidas. Anunció que, de respaldarse, el artículo 24 quedaría de la siguiente manera:

"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.".

- Las Comisiones unidas, por la totalidad de sus integrantes presentes, Honorables Senadores señores Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de miembro de ambas instancias legislativas- y Van Rysselberghe, aprobaron la indicación número 144 con enmiendas, en los términos previstos precedentemente.

°°°°°

Título nuevo

A continuación, se formuló **la indicación número 145**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para incorporar el siguiente Título, nuevo, consultado como Título V:

"Título V
De la Infraestructura Crítica de la Información

Párrafo 1°
De la calificación de la infraestructura de la información como crítica

Artículo …. La calificación de la infraestructura como crítica, será realizada por la Agencia Nacional de Ciberseguridad, en forma interagencial con los organismos que correspondan, debiendo efectuarse en un plazo inicial de 12 meses, un primer catastro de infraestructura crítica de la información.

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

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

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

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

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

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

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

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

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

e) El impacto que tenga sobre la economía de una comunidad, provincia o región a causa de la disrupción de los sistemas informáticos o de telecomunicaciones.

f) El daño reputacional que pueda ocasionarse por la vulnerabilidad en la infraestructura de la información, produciendo afectación de actividades o generando desconfianza respecto a su disponibilidad.

Transcurridos los 12 meses dispuestos para el catastro inicial, el Ministerio del Interior y Seguridad Pública, mediante la dictación de un decreto supremo bajo la fórmula “Por orden del Presidente de la República”, determinará aquellos sectores o instituciones que constituyen servicios esenciales y poseen infraestructura crítica de la información. Se entenderá que por el hecho de determinar que un sector posee infraestructura crítica de la información, las instituciones que conformen ese sector también poseerán infraestructura crítica de la información.

Sin perjuicio de lo dispuesto en los incisos anteriores, se entenderá que poseen infraestructura crítica de la información todos los órganos del Estado, incluidas las municipalidades, las entidades fiscales autónomas, las empresas del Estado o aquellas en las que el Fisco tenga intervención por aportes de capital.

Artículo …. Los Directorios de empresas que posean infraestructura crítica de la información en los términos de los incisos anteriores, deberán acreditar que al menos uno de sus directores posea:

a) Certificación o título en ciberseguridad, o

b) Conocimientos, habilidades u otros antecedentes profesionales en ciberseguridad, tales como: áreas de política y gobierno de seguridad, gestión de riesgos, evaluación de seguridad, evaluación de control, arquitectura e ingeniería de seguridad, operaciones de seguridad, manejo de incidentes o planificación de continuidad comercial.

Artículo …. El catastro de Infraestructuras Críticas de la Información se actualizará anualmente, incluyendo a los criterios, los incidentes e impactos que se hayan registrado entre cada actualización, y remitirá su informe al Ministerio respectivo para su vigencia y aplicación.

Asimismo, se mantendrá un listado actualizado de todos los Directores de Informática de las empresas e instituciones calificadas como Infraestructura Crítica, y sus datos de contacto.

La Agencia Nacional de Ciberseguridad tendrá facultades de regulación sobre los organismos que posean infraestructura crítica, pudiendo establecer, entre otros, los contenidos mínimos de los Sistemas de Gestión de la Seguridad y Riesgo de la Información – SGSRI de los regulados, controlando que los mismos se encuentren correctamente auditados por entidades externas debidamente habilitadas para tal efecto por la Agencia.

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

Artículo …. Deberes generales. Será obligación de los órganos del Estado y de las instituciones privadas que posean infraestructura de la información calificada como crítica, aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas, informativas y de trazabilidad necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos, así como contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad e integridad del servicio prestado, de conformidad a lo prescrito en esta ley. Se prohíbe a dichos órganos e instituciones, realizar pagos de cualquier tipo por rescate ante ataques de secuestro de datos o ransomware, así como de equipos o de dispositivos.

Artículo …. Deberes específicos. Los órganos del Estado, las municipalidades, las entidades fiscales autónomas, las empresas del Estado o aquellas en las que el Fisco tenga intervención por aportes de capital, y las instituciones privadas cuya infraestructura de la información sea calificada como crítica, deberán:

a) Implementar un Sistema de Gestión de la Seguridad y Riesgo de la Información – SGSRI, permanente y actualizado regularmente, cada 180 días a lo menos, con el fin de determinar aquellos que pueden afectar la seguridad de las redes, sistemas informáticos y datos, cuáles afectarían la continuidad operacional del servicio y cuáles de ellos facilitan la ocurrencia de incidentes de ciberseguridad. Dicho sistema deberá contar con la capacidad de determinar la gravedad de las consecuencias de un incidente de ciberseguridad.

EL SGSRI debe además considerar el entorno operacional de la o las instalaciones, tales como las vulnerabilidades físicas a las que puede estar expuesta la información producto de acciones de la naturaleza, actos vandálicos que interrumpan comunicaciones, vulnerabilidad física y otros.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de la seguridad y riesgos de la información – SGSRI, 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) Establecer un plan de capacitación y actualización del personal en las tecnologías en uso, así como planes de inducción y procedimientos de administración del cambio al introducir modificaciones o actualizaciones relevantes de los sistemas.

d) Elaborar e implementar planes de continuidad operacional y ciberseguridad. Dichos planes deberán ser actualizados periódicamente, a lo menos cada 180 días, o cada vez que sean actualizados los sistemas o procesos. Los planes de ciberseguridad deberán contemplar los protocolos de acción inmediata frente a incidentes de ciberseguridad, y de la forma de comunicar la ocurrencia de estos.

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

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

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

Sobre el particular, **el Honorable Senador señor Pugh** anunció que esta indicación fue retirada por sus autores. Sin embargo, relevó la importancia de que al menos uno de los directores de las empresas que posean infraestructura crítica de la información tenga certificación o título en ciberseguridad, o conocimientos, habilidades u otros antecedentes profesionales en la materia, tal como lo contempla la letra b) del segundo artículo considerado en la propuesta de enmienda.

Afirmó que tal exigencia ha ido cobrando fuerza poco a poco, y que en muchas organizaciones ya opera, siendo este el caso de Esval, en la Región de Valparaíso.

Por las razones esgrimidas, hizo un llamado al Ejecutivo a ponderar la inclusión de una norma como la citada. No obstante, a fin de no retardar la tramitación de esta iniciativa de ley, instó a hacerlo en otra oportunidad.

- Esta indicación fue retirada por sus autores.

°°°°°

TÍTULO V

Lleva por epígrafe “De los CSIRT del sector público”.

Sobre este título recayeron las indicaciones números 146 y 147.

La indicación número 146, del Honorable Senador señor Van Rysselberghe, es para suprimirlo, junto con los artículos 27 y 28, que lo integran.

- Esta indicación fue retirada por su autor.

La indicación número 147, de Su Excelencia el Presidente de la República, busca reemplazar su denominación por la siguiente:

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

- Esta indicación fue aprobada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe.

ARTÍCULO 27

Crea el Equipo de Respuesta ante Incidentes de Seguridad Informática del Sector Gobierno y señala sus principales funciones. Su redacción es la siguiente:

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

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

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

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

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

Este precepto fue objeto de **la indicación número 148**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, contemplado como artículo 25:

“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 Ministerio de Defensa Nacional y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y seguridad nacional.

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

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

El Honorable Senador señor Pugh puso de relieve que la indicación en estudio solo se hace cargo de los incidentes que afectan al sector de la defensa nacional, y evidenció la necesidad de que exista una adecuada coordinación con otros órganos, de manera de determinar las atribuciones correspondientes.

Su Señoría resaltó que un Estado agredido por otro en el ciberespacio debe tener la capacidad de actuar; para ello, reunir toda la información nacional en un solo centro es esencial, sentenció.

Dirigiéndose al Coordinador Nacional de Ciberseguridad, solicitó que este tema siga desarrollándose, así como también todo lo vinculado a la Política Nacional de Ciberdefensa.

- Puesta en votación, esta indicación fue respaldada con enmiendas de carácter meramente formal por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

Letra a)

Encomienda al Equipo de Respuesta ante Incidentes de Seguridad Informática del Sector Gobierno responder a los incidentes de ciberseguridad que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información que afecten a los órganos de la Administración del Estado.

Respecto de este literal se presentó **la indicación número 149**, del Honorable Senador señor Insulza, para reemplazar la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

- Habida cuenta de la aprobación de la indicación anterior, esta fue rechazada por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe.

ARTÍCULO 28

Regula el Centro Coordinador del Equipo de Respuesta ante Incidentes de Seguridad Informáticos del Sector Defensa. Su tenor literal es el que sigue:

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

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

Sus funciones principales serán las siguientes:

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

disponibilidad de la infraestructura de la información calificada como crítica del sector Defensa.

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

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

Sobre esta disposición recayó **la indicación número 150**, de Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como artículo 26:

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

a) Responsable de 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.”.

El Jefe de División de Desarrollo Tecnológico e Industria de la Subsecretaría de Defensa, señor Yerko Benavides, aseguró que la disposición contenida en la indicación en análisis, así como aquellas contempladas en las dos indicaciones siguientes formalizan un sistema de trabajo que opera actualmente en el sector. En efecto, acotó, existe el CSIRT de Defensa Nacional y Equipos de Respuesta a Incidentes de Ciberseguridad en cada una de las ramas de las Fuerzas Armadas.

Agregó que el organismo cuya creación se considera en esta indicación se vinculará con la Agencia Nacional de Ciberseguridad, informándole aquellos ataques que no afecten la seguridad nacional. Además, notó, ofrecerá todas sus capacidades para enfrentar agresiones masivas que pongan en riesgo al país.

El Honorable Senador señor Pugh respaldó los dichos del representante del Ejecutivo. Remarcó que las instituciones de la defensa nacional comenzaron a resguardar la seguridad informática por medio del empleo de NOC y de SOC. A ellos, continuó, les siguió el Equipo de Respuesta ante Incidentes de Ciberseguridad. En definitiva, confirmó, los artículos 26 y 27 reconocen a nivel legal algo que ya existe.

Posteriormente, Su Señoría observó que, para efectos presupuestarios, el CSIRT de la Defensa Nacional dependerá de la Cartera de Estado de la misma denominación. En consecuencia, instó a considerar los recursos necesarios, a fin de renovar los equipos informáticos y entrenar al personal a cargo.

En sintonía con el último punto, juzgó esencial que quienes se desempeñen en esas áreas tengan adiestramiento e intercambios con otros países. Al efecto, enfatizó que los ejercicios más importantes son los que se llevan a cabo en el Centro de Excelencia de la OTAN, en Estonia.

- Sometida a votación, esta indicación fue respaldada con enmiendas de carácter meramente formal por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

°°°°°

Artículo nuevo

Seguidamente, se formuló **la indicación número 151**, de Su Excelencia el Presidente de la República, para introducir el siguiente artículo, nuevo, consultado como artículo 27:

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

Dando inicio al análisis de esta indicación, **el Honorable Senador señor Huenchumilla** advirtió que, al tenor de la disposición, las funciones de tales equipos serán establecidas por la reglamentación que al efecto dicte el Ministerio de Defensa Nacional. Sobre el particular, consultó si no debieran consignarse a nivel legal. Asimismo, solicitó clarificar si la voz cuestionada alude a la potestad del artículo 32, número 6°, de la Carta Fundamental, o a meras instrucciones de la citada Secretaría de Estado.

Atendiendo las interrogantes del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, señaló que las labores de los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional están en la ley. En efecto, observó, el inciso primero de la norma sugerida en la indicación prescribe 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, plataformas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional. Aclaró que el Ministerio, por su lado, se limitará a determinar qué funciones desempeñará específicamente cada uno de los CSIRT.

Profundizando en sus comentarios, sostuvo que, si bien todas estas entidades atienden ciberataques, algunos podrían realizar otras labores, como análisis forense. En este caso, la Cartera de Estado nombrada puntualizará si esta última misión será ejercida de forma compartida o por cada institución por separado.

Para concluir, aclaró que la expresión puesta en duda refiere a la potestad reglamentaria del Primer Mandatario.

Complementando la intervención del personero de Gobierno, **el Jefe de División de Desarrollo Tecnológico e Industria de la Subsecretaría de Defensa, señor Yerko Benavides**, connotó que la regla en debate evitará la duplicidad de funciones. Adicionalmente, recalcó que, atendidas las características del sector de que se trata, pueden encomendarse a los CSIRT otras atribuciones no estrechamente vinculadas a la ciberseguridad. Así, concluyó, las establecidas en la ley son las mínimas que deberán realizar.

- Esta indicación fue apoyada con enmiendas de adecuación por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

°°°°°

°°°°°

Artículo nuevo

A continuación, se presentó **la indicación número 152**, de Su Excelencia el Presidente de la República, para agregar el siguiente artículo, nuevo, consultado como artículo 28:

"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.".

- Las Comisiones unidas, con el voto conforme de la totalidad de sus miembros presentes, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe, respaldaron esta indicación.

°°°°°

ARTÍCULO 29

Norma, por medio de cinco incisos, la reserva de la información. Su tenor literal es el que se indica:

"Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de los CSIRT, sean el CSIRT Nacional, de Gobierno, Defensa o los CSIRT Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales órganos de la Administración del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

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

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

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de riesgos y los registros previstos en el artículo 6º, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

Adicionalmente, serán considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad;

ii. Los planes de continuidad operacional y planes ante desastres;

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

iv. Los reportes de incidentes de ciberseguridad.”.

Inciso primero

Sobre esta parte del artículo referido recayeron las indicaciones números 153, 154 y 155.

La indicación número 153, del Honorable Senador señor Van Rysselberghe, es para reemplazar la frase “los CSIRT, sean el CSIRT Nacional, de Gobierno, Defensa o los CSIRT Sectoriales”, por la siguiente: “la Agencial Nacional de Ciberseguridad”.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que el grupo de asesores conformado para facilitar la tramitación de esta iniciativa de ley recomienda aprobar con modificaciones esta indicación, a fin de agregar, luego de la locución “en poder de”, la expresión “la Agencia,”, de manera que también pese sobre ella el deber de reserva a que se alude en este precepto.

- Esta indicación fue aprobada en los términos explicados por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

La indicación número 154, de Su Excelencia el Presidente de la República, busca suprimir la expresión “de Gobierno,”.

- Puesta en votación, esta indicación fue respaldada por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe.

La indicación número 155, del Honorable Senador señor Insulza, reemplaza la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que la mesa de trabajo prelegislativo sugiere aprobar esta indicación. Declaró que de acogerse esta y las dos anteriores, la redacción del inciso primero del artículo 29 quedaría de la siguiente manera:

“Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con estos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de estas.”.

- Sometida a votación, esta indicación fue aprobada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

Inciso segundo

Con respecto al inciso segundo, se formuló **la indicación número 156**, de Su Excelencia el Presidente de la República, para intercalar, entre las palabras “autorización” y “su”, el vocablo “de”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, adelantó que, de acogerse esta indicación, el tenor literal del inciso segundo del artículo 29 sería el siguiente:

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

- Las Comisiones unidas, por la totalidad de sus miembros presentes, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe, respaldaron esta indicación, con adecuaciones.

Inciso tercero

Al efecto, se presentaron las indicaciones números 157 y 158.

La indicación número 157, del Honorable Senador señor Van Rysselberghe, es para sustituir la frase “CSIRT, sean del CSIRT

Nacional, de Gobierno, Defensa o de los CSIRT Sectoriales," por "la Agencia Nacional de Ciberseguridad".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sostuvo que el grupo de asesores conformado para asegurar el pronto despacho de esta iniciativa de ley recomienda aprobar esta indicación con modificaciones, a fin de reemplazar la expresión "CSIRT, sean del" por "la Agencia y del".

Adelantó que, de acogerse tal enmienda, así como aquella contenida en la indicación número 158, el tenor del inciso tercero del artículo 29 quedaría de la forma que se indica:

"Los funcionarios 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.".

El Honorable Senador señor Pugh haciendo ver la importancia de una norma como la examinada, subrayó que una exigencia tal es clave para la protección de sistemas que son vitales para el país. Por ello, estimó, la selección del personal constituye un paso esencial. Además, observó que la disposición está en sintonía con las obligaciones que pesan sobre quienes que se desempeñan en la Agencia Nacional de Inteligencia.

- Esta indicación fue aprobada con la enmienda antedicha por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe.

La indicación número 158, de Su Excelencia el Presidente de la República, suprime la locución "de Gobierno,".

- Puesta en votación, esta indicación fue respaldada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

Inciso cuarto

Pese a que esta parte del artículo 29 no fue objeto de indicaciones, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, manifestó la conveniencia de sustituir la expresión "sistemas de gestión de riesgos" por "sistemas de gestión de seguridad de la información", de modo que este inciso esté en sintonía con los artículos 2, 6 y 9, letra n), de esta proposición de ley.

Acotó que, de acogerse dicha enmienda, la redacción del inciso cuarto del artículo 29 quedaría de la manera que se expone:

"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.".

- La enmienda se acordó en mérito de lo dispuesto en el inciso final del artículo 121 del Reglamento del Senado, por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -quien se pronunció como integrante de ambas instancias legislativas- y Van Rysselberghe.

Inciso quinto

Si bien sobre esta parte del artículo 29 no recayeron indicaciones, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, informó que la mesa de trabajo prelegislativo recomienda suprimir su numeral iv.

Reveló que se respaldarse tal propuesta, el tenor literal del inciso quinto del artículo 29 sería el que a continuación se transcribe:

"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.".

- La enmienda al inciso referido fue acordada en mérito de lo dispuesto por el artículo 121, inciso final, del Reglamento de la Corporación, por la unanimidad de los integrantes presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -quien votó como miembro de ambas instancias legislativas- y Van Rysselberghe.

ARTÍCULO 33

Esta disposición consagra las infracciones a este cuerpo normativo. Su tenor literal es el que sigue:

“Artículo 33. De las infracciones. Serán consideradas infracciones para efectos de esta ley:

a) Retardar o entregar fuera del plazo señalado la información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;

b) Negar injustificadamente información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;

c) Entregar maliciosamente información falsa o manifiestamente errónea, e;

d) Incumplir los deberes previstos en el párrafo 2° del Título II.

Podrán imponerse, a beneficio fiscal, multas entre 10 y 20.000 Unidades Tributarias Mensuales, de conformidad a la gravedad de la infracción. Para determinar la cuantía de la multa, se entenderá por:

a) Faltas gravísimas: aquellas señaladas en los literales b) y c) del inciso precedente. En este caso, la multa será de hasta a 20.000 Unidades Tributarias Mensuales.

b) Faltas graves: aquellas señaladas en el literal a) del inciso precedente. En este caso, la multa será de hasta 10.000 Unidades Tributarias Mensuales.

c) Faltas leves: aquellas obligaciones señaladas en esta ley cuyo incumplimiento negligente o injustificado no tenga señalada una sanción especial, caso en el que la multa será de 10 a 5.000 Unidades Tributarias Mensuales.

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

Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.

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

Este precepto fue objeto de las indicaciones números 159 y 160.

La indicación número 159, de Su Excelencia el Presidente de la República, lo reemplaza por el siguiente:

“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) Retardar o entregar fuera de plazo la información a la autoridad u órgano 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 órgano de la Administración del Estado habilitado para requerirla.

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

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

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

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

Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre esta.”.

Comenzando el estudio de esta indicación, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que el artículo 33 contempla el régimen infraccional al que se sujetará el incumplimiento de las obligaciones consagradas en este proyecto de ley.

Afirmó que el grupo de trabajo conformado para acelerar el despacho de esta iniciativa legal concuerda en los términos sugeridos por el Ejecutivo, con excepción del inciso final. Este último, declaró, se recomienda reemplazarlo por otros que reconocen de manera expresa la aplicación del principio non bis in ídem en sede administrativa. Remarcó que su inclusión constituye una innovación. Recordó que en el sistema jurídico nacional su ausencia ha motivado diversas interpretaciones tanto por parte de la Contraloría General de la República como por los tribunales de justicia.

Por otro lado, informó, se propone establecer una regla específica de prescripción, a fin de evitar discusiones acerca de este punto, toda vez que en el derecho administrativo chileno no existe una disposición en tal sentido, lo que ha conducido a discrepancias.

Ahondando en los acuerdos de la mesa de trabajo, expuso que los incisos por los cuales se aconseja sustituir el final son los que se consignan a continuación:

“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.”.

El Honorable Senador señor Huenchumilla constató que el precepto contenido en la indicación en estudio solo dice relación con infracciones y sanciones de las instituciones privadas.

Refiriéndose a la observación del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, enunció que para los servicios públicos se contemplan dos

normas, una que aborda la responsabilidad del jefe del servicio y otra, la del funcionario.

En un orden distinto de consideraciones, y teniendo a la vista la indicación número 161, del Honorable Senador señor Van Rysselberghe, sugirió suprimir, en el inciso segundo, letra a), del precepto propuesto, la locución “Retardar o”.

Con respecto a este último punto, **el Honorable Senador señor Pugh** manifestó su apoyo. Juzgó que tal voz es imprecisa y que basta con comenzar la redacción del literal aludido con la locución “entregar fuera de plazo”.

A su turno, **el Honorable Senador señor Huenchumilla** coincidió con el legislador que le antecedió en el uso de la palabra.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, detalló que, de acogerse todas las enmiendas, la redacción del artículo 33 quedaría de la manera que se expresa a continuación:

“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 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 órgano 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 órgano de la Administración del Estado habilitado para requerirla.

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

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

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

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

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

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

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

- **Sometida a votación, esta indicación fue aprobada con las enmiendas consignadas precedentemente y otras adecuaciones por la totalidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe.**

La indicación número 160, del Honorable Senador señor Insulza, sustituye el artículo 33 aprobado en general por el que sigue:

“Artículo 33. De las infracciones. Serán consideradas infracciones leves para efectos de esta ley, las siguientes:

a) Retardar o entregar fuera del plazo señalado la información a la autoridad u órgano del Estado habilitado para requerirla.

b) Incumplir el plazo previsto en el artículo 25, para efectos de reportar incidentes.

c) Incumplir los deberes generales previstos en el artículo 5.

Serán consideradas infracciones graves para efectos de esta ley, las siguientes:

a) Negar injustificadamente información a la autoridad u órgano del Estado habilitado para requerirla.

b) Incumplir los deberes específicos previstos en el artículo 6.

Serán consideradas infracciones gravísimas para efectos de esta ley, las siguientes:

a) Entregar información falsa o manifiestamente errónea.

b) Incumplir el deber de reportar previsto en el artículo 25.

Podrán imponerse, a beneficio fiscal, multas entre 10 y 20.000 Unidades Tributarias Mensuales, de conformidad a la gravedad de la infracción y a la siguiente escala:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 10 a 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.

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

Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.

Las infracciones cometidas por funcionarios del Estado se regirán por su respectivo estatuto sancionatorio.”.

- Habida cuenta de la aprobación de la indicación anterior, esta fue rechazada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -en su calidad de integrante de ambas instancias legislativas- y Van Rysselberghe.

Inciso primero

Adicionalmente, en relación con el inciso primero del artículo 33 aprobado en general se presentaron las indicaciones números 161 y 162, **ambas del Honorable Senador señor Van Rysselberghe.**

La indicación número 161 elimina, en la letra a) del referido inciso, la expresión “Retardar o”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, hizo presente que esta indicación fue recogida en el marco de la discusión de la indicación número 159.

- En consecuencia, las Comisiones unidas, por la unanimidad de sus miembros presentes, Honorables Senadores señores Araya, Huenchumilla, Macaya, Ossandón, Pugh, Saavedra -actuando como integrante de ambas instancias legislativas- y Van Rysselberghe, aprobaron con enmiendas esta indicación, en los términos previstos en la número 159.

La indicación número 162, en tanto, suprime, en el literal b) del mismo inciso, la palabra “injustificadamente”.

- Esta indicación fue retirada por su autor.

ARTÍCULO 34

Regula el procedimiento al que se sujetarán las infracciones previstas en la disposición anterior. Su redacción es la que se transcribe a continuación:

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

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

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

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

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

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

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

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

Sobre este precepto recayó **la indicación número 163**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

“Artículo 34. Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan las instituciones privadas por incumplimiento o vulneración de los principios y obligaciones establecidas en esta ley y 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 responsable de la instrucción del procedimiento, que recibirá el nombre de instructor.

c) La Agencia deberá presentar una formulación de cargos en contra de la institución privada, la que señalará una descripción clara y precisa de los hechos que se estimen constitutivos de infracción y la fecha de su verificación, así como los principios, obligaciones, protocolos, estándares técnicos, instrucciones generales y particulares eventualmente infringidos por la institución privada, la disposición que establece la infracción, la sanción y cualquier otro antecedente que sirva para sustentar la formulación.

d) La formulación de cargos debe 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 puede 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 hubiera 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

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 emitirá, dentro de diez días un dictamen en el cual propondrá la absolución o 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 de las sanciones que estimare procedente aplicar o de la absolución de uno o más de los infractores.

k) Emitido el dictamen, el instructor elevará los antecedentes al Director, quien resolverá en el plazo de quince días dictando al efecto una resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. No obstante, el Director podrá ordenar la realización de nuevas diligencias o la corrección de vicios de procedimiento, fijando un plazo de tres días 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 debe 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 el incumplimiento o vulneración de los principios y obligaciones establecidos en la ley por la institución privada 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 el incumplimiento o vulneración a los principios y obligaciones de esta ley 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 5 días hábiles contados desde la notificación, el que deberá ser resuelto por el Director dentro del plazo de 30 días hábiles.

n) El procedimiento administrativo de infracción de ley no podrá superar los seis meses. Cuando hayan transcurrido más de seis meses desde la fecha de la certificación indicada en la letra b) de este artículo sin que la Agencia haya resuelto la reclamación, la institución privada podrá presentar un reclamo de ilegalidad en los términos previstos en el siguiente artículo.”.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dio a conocer que la instancia de trabajo conformada para facilitar la tramitación de esta propuesta aún no ha alcanzado consenso respecto a esta indicación. Con todo, relevó que en la legislación existen diversos procedimientos administrativos por infracción de ley, y que el Ejecutivo anhela estandarizarlos.

El Honorable Senador señor Huenchumilla consultó si se prevén normas jurídicas especiales que ordenen y regulen el proceso jurídico y sus distintos trámites para las transgresiones a las obligaciones contempladas en esta ley.

Abocándose a la duda del Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, sentenció que luego del fallo del Tribunal Constitucional sobre las atribuciones del Servicio Nacional del Consumidor, en los cuerpos normativos aprobados con posterioridad se ha exigido que los procedimientos administrativos estén estrictamente descritos en la ley, resultando insuficiente un mero enunciado y su desarrollo a nivel reglamentario, como era habitual.

El Honorable Senador señor Huenchumilla instó a tener en vista la ley N° 19.880 recientemente actualizada y sus respectivos reglamentos.

En una sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, dando cuenta de los acuerdos alcanzados por el grupo de trabajo conformado para facilitar la tramitación de esta iniciativa, informó que la indicación analizada se propone aprobar con las enmiendas que siguen:

- Reemplazar, en el inciso primero del artículo 34, la frase “incumplimiento o vulneración de los principios y obligaciones establecidas en esta ley y”, 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”.

- Agregar, en el literal b) del inciso primero, a continuación de la expresión “un funcionario”, la locución “o una funcionaria”, y luego del vocablo “instructor”, lo siguiente: “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”.

- Sustituir, en la letra c), la frase “deberá presentar una formulación de” por “podrá formular”; reemplazar la expresión “la que señalará” por “señalando tanto”, y sustituir “los principios, obligaciones, protocolos, estándares técnicos, instrucciones generales y particulares eventualmente infringidos por la institución privada, la disposición que establece la infracción” por “las normas que se estimen infringidas”.

- Reemplazar, en el literal f), la conjunción “y”, la primera vez que aparece, por una coma, e incorporar a continuación de la locución “inspecciones que sean pertinentes”, “y la recepción de los demás medios probatorios que procedan”.

- Eliminar, en la letra k), la expresión “de tres días”.

- Suprimir, en el literal l), la frase “el incumplimiento o vulneración de los principios y obligaciones establecidos en la ley”, y agregar, a continuación de la expresión “institución privada”, “la infracción a la normativa aplicable,”.

- Reemplazar, en la letra m), la locución “el incumplimiento o vulneración a los principios y obligaciones de esta ley” por “la infracción a la normativa sobre ciberseguridad”.

- Sustituir, en el literal n), el punto seguido y la oración final por la frase “contados desde la notificación a que se refiere el literal d) anterior.”.

El personero de Gobierno sentenció que las modificaciones apuntan a hacer coherente esta iniciativa con el proyecto de ley sobre protección de datos personales, contenido en el Boletín N° 11.092-07, además de recoger las observaciones formuladas por la Excelentísima Corte Suprema en su oficio N° 62-2023, por el que da respuesta a la consulta

efectuada por las Comisiones unidas en cumplimiento de lo prescrito en los artículos 77 de la Constitución Política de la República y el artículo 16 de la ley orgánica constitucional del Congreso Nacional.

Además, **las Comisiones unidas** estuvieron contestes en precisar si los plazos previstos en las letras f), j) y k) serán de días hábiles o corridos.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, aseguró que debería optarse por la primera alternativa, a fin de uniformar los períodos establecidos en el articulado.

Anunció que, de acogerse los cambios sugeridos por la mesa de trabajo prelegislativo y la observación referida a los plazos, el artículo 34 quedaría de la manera que sigue:

“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 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 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, 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 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 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.”.

- Las Comisiones unidas, por la unanimidad de sus parlamentarios presentes, Honorables Senadores señores Araya, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, aprobaron la indicación número 163 con las enmiendas consignadas y otras adecuaciones.

°°°°°

Artículos nuevos

A continuación, se formuló **la indicación número 164**, de Su Excelencia el Presidente de la República, para incorporar los siguientes artículos, nuevos, consultados como artículos 35, 36 y 37, pasando el actual artículo 35 a ser artículo 38 y así sucesivamente:

“Artículo 35. Procedimiento de reclamación judicial. Las personas jurídicas 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 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, según 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 confirmar o revocar 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) 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.”.

En lo que atañe a este primer precepto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, enfatizó que el proyecto de ley ingresado a tramitación no contemplaba una norma relativa al procedimiento de reclamación judicial ante la decisión administrativa, pese a que en esta rama del derecho existe y es útil para la mejor protección de los derechos.

Previno que el precepto analizado es similar al de la ley sobre protección de datos personales.

El Honorable Senador señor Macaya alertó la necesidad de poner esta norma en conocimiento de la Excelentísima Corte Suprema, de conformidad a lo prescrito en el artículo 77, inciso segundo, de la Constitución Política de la República y en el artículo 16, inciso primero, de la ley orgánica constitucional del Congreso Nacional.

El Honorable Senador señor Huenchumilla remarcó que el artículo examinado solo posibilita la reclamación de las personas jurídicas. Solicitó al representante del Ejecutivo justificar tal decisión.

Fijando su atención en la interrogante planteada por el Presidente de las Comisiones unidas, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, adujo que el proyecto está concebido en términos que sus obligaciones solo sean aplicables a tales entidades, según se aprecia en sus primeras normas.

Respaldando la explicación dada anteriormente, **el Honorable Senador señor Pugh** sostuvo que son las personas jurídicas a quienes la ley encomienda la función de proveer servicios esenciales.

Por otra parte, notó que ellas tendrán el deber de gestionar riesgos y de adoptar las acciones vinculadas a aquel.

Seguidamente, celebró la incorporación de una disposición para que quienes sean afectados con una decisión administrativa puedan reclamar ante la Corte de Apelaciones que corresponda.

Finalmente, valoró la idea que el artículo incorporado sea similar al previsto en la ley N° 19.628.

El Honorable Senador señor Macaya cuestionó que solo las personas jurídicas puedan ser proveedores de servicios esenciales y, consecuentemente, actores en el sistema de ciberseguridad. Hizo hincapié en que un individuo natural bien podría estar organizado tributariamente para desarrollar este tipo de prestaciones.

A la luz de lo expuesto, requirió mayor profundidad por parte del Coordinador Nacional de Ciberseguridad.

Aportando más antecedentes, **el Honorable Senador señor Huenchumilla** abogó que tener en cuenta que el criterio adoptado podría infringir el principio de igualdad ante la ley.

En atención a los reparos surgidos, **las Comisiones unidas** acordaron dejar pendiente la votación del artículo 35 propuesto en la indicación número 164.

En una sesión posterior, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, comunicó que la mesa de trabajo prelegislativo, acogiendo las observaciones realizadas por la Excelentísima Corte Suprema, recomienda las siguientes enmiendas al artículo 35 en examen:

- En el inciso primero, eliminar la voz “jurídicas”.

- En el literal g), reemplazar la expresión “confirmar o revocar” por “rechazar o acoger”.

- Intercalar la siguiente letra h), nueva, pasando la actual a ser la letra i):

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

En relación con esta última modificación, **las Comisiones unidas** tuvieron en consideración que el oficio del Máximo Tribunal recomienda establecer expresamente que la sentencia dictada sea inapelable, porque de esta forma procederían en su contra los recursos de casación, acorde con lo dispuesto en los artículos 766 y 767 del Código de Procedimiento Civil.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que el grupo de trabajo constituido para acelerar la tramitación de esta proposición legal optó por emplear la misma fórmula de la ley N° 20.285, sobre acceso a la información pública. Agregó que garantiza que no procederá la mayoría de los recursos, pero si los de casación en la forma y en el fondo.

Adicionalmente, **las Comisiones unidas** estuvieron por uniformar el carácter de los plazos, de modo que todos sean de días hábiles.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, enunció que, de respaldarse los cambios citados, la redacción del artículo 35 quedaría de la siguiente manera:

“Artículo 35. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

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

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

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

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

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

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

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

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

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

- Puesto en votación el artículo 35 de la indicación número 164, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Araya, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, aprobaron esta indicación con las enmiendas consignadas precedentemente.

En tanto, el artículo 36 contemplado en la indicación en debate reza lo siguiente:

“Artículo 36. Responsabilidad administrativa del jefe superior del órgano público. El jefe superior de un órgano público deberá velar porque el órgano 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 órganos de la Administración del Estado deberán someterse a las medidas tendientes a subsanar o prevenir 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 órgano 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 órgano público persiste en la infracción, se le aplicará al jefe superior del órgano público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días.

Las infracciones en que incurra un órgano 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 respectivo órgano o servicio dentro del plazo de cinco días hábiles contados desde que la respectiva resolución quede firme.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que la mesa de trabajo prelegislativo sugiere aprobar la norma transcrita con enmiendas, reemplazando, al igual que en oportunidades anteriores, las voces “órgano” por “organismo” y “órganos” por “organismos”, todas las veces que aparecen en el texto.

Las Comisiones unidas, en aras de uniformar los plazos prescritos en esta iniciativa de ley, estuvieron por especificar que aquel aludido en el inciso cuarto será de días hábiles.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, concordó con la sugerencia precedente, y detalló que de acogerse todas las modificaciones el artículo 36 quedaría como se señala a continuación:

“Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente.

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

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

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

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

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

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

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

En relación con los cambios sugeridos por la mesa técnica, **la Honorable Senadora señora Provoste** juzgó que las expresiones “órgano” y “organismo” son diferentes. En efecto, recordó que el Texto Supremo al referirse a los cuerpos autónomos, como el Poder Judicial, emplea la primera.

Su Señoría consultó la razón de la modificación acordada.

Deteniéndose en la interrogante de la legisladora que le antecedió en el uso de la palabra, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, sostuvo que la Constitución Política de la República utiliza ambos vocablos.

Añadió que el proyecto de ley, al aludir a las instituciones de la Administración del Estado recurre al vocablo “organismo”.

Resaltó que, en el caso de las entidades autónomas constitucionales, en tanto, la proposición de ley emplea la expresión “órganos”.

Clarificado el punto, subrayó que la responsabilidad administrativa de los funcionarios de estos últimos se perseguirá conforme a sus propias reglas estatutarias.

- Sometido a votación el artículo 36 comprendido en la indicación número 164, las Comisiones unidas, por la unanimidad de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias

legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, aprobaron esta indicación con las enmiendas consignadas precedentemente y otras de carácter meramente formal.

Por su lado, el tenor literal del artículo 37 contenido en la indicación número 164 dispone lo siguiente:

"Artículo 37. Responsabilidad del funcionario 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 del órgano público, la Contraloría General de la República, a petición de la Agencia, iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado, en su caso. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en el Estatuto Administrativo.

En caso de que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios 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 Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que el grupo de asesores conformado para facilitar la tramitación de este proyecto de ley recomienda reemplazar "órgano público, la Contraloría General de la República, a petición de la Agencia, iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado, en su caso", y la oración final del inciso primero de la norma en estudio, por la locución "organismo público, la responsabilidad administrativa se hará efectiva con sujeción a las normas estatutarias que rijan al órgano u organismo en que se produjo la infracción.".

Profundizando en el cambio antedicho, pormenorizó que se sustituye el texto por uno genérico, de manera de asegurar que la responsabilidad administrativa se perseguirá conforme a la norma estatutaria que sea aplicable, eliminando, además, la referencia a la investigación sumaria, tal como lo sugirió la Excelentísima Corte Suprema.

Detalló que, de acogerse la recomendación mencionada, el artículo 37 quedaría así:

"Artículo 37. Responsabilidad del funcionario 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 del organismo público, la responsabilidad administrativa se hará efectiva con sujeción a las

normas estatutarias que rijan al órgano u organismo en que se produjo la infracción.

En caso de que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios 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 artículo 37 de la indicación número 164, con la enmienda consignada anteriormente y otras adecuaciones, contó con el apoyo transversal de los parlamentarios de las Comisiones unidas, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra.

°°°°°

ARTÍCULO 35

Establece una agravante especial. Al respecto, dispone que, si como consecuencia de la perpetración de un delito resultare la destrucción, inutilización o alteración grave del funcionamiento de infraestructura crítica de la información, se impondrá la pena que corresponda, aumentada en un grado.

Agrega, en su inciso segundo, que lo mismo se observará cuando el delito consistiere en la alteración o supresión de los datos soportados por infraestructura de la información calificada como crítica o en la obstaculización del acceso o la alteración perjudicial del funcionamiento de un sistema informático que formare parte de la infraestructura crítica de la información.

En relación con esta disposición se formuló **la indicación número 165**, de Su Excelencia el Presidente de la República, para reemplazarla por la siguiente, consultada como artículo 38:

“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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, explicó que la razón de la decisión plasmada en el precepto descansa en que los servicios esenciales y los operadores de

importancia vital serán los que, conforme a este futuro texto legal, tendrán los más altos estándares de ciberseguridad y de protección.

En atención a su reciente incorporación a la Comisión de Defensa Nacional, **el Honorable Senador señor Cruz-Coke** consultó quiénes podrán ser calificados como operadores de importancia vital.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, respondió que, al tenor de lo dispuesto en el artículo 4 del proyecto, la Agencia Nacional de Ciberseguridad determinará a aquellos servicios que sean considerados como esenciales y dentro de estos identificará a los operadores de importancia vital.

Apuntó que los criterios para establecer a los últimos son los siguientes:

a) Se trata de un operador que presta un servicio esencial;

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

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

Continuando con el desarrollo de su intervención, ejemplificó que algunos operadores de telecomunicaciones -solo los que sean vitales para el funcionamiento del sector-, quedarán en esta categoría, de manera que el país no se paralice en caso de un ciberataque. Así, vislumbró, probablemente serán calificados como tales los prestadores de servicios públicos de telecomunicaciones y aquellos que ofrecen servicios privados de datos.

El Honorable Senador señor Cruz-Coke manifestó interés por conocer quién será el encargado de atribuirles tal condición.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, enfatizó que la proposición legal considera una disposición transitoria que identifica, a priori, cuáles son los servicios esenciales. Al respecto, puso de relieve que la experiencia comparada ha permitido advertir que cuando se da tal calificación, es muy difícil salir de ella; así, adelantó, verbigracia, el sector eléctrico siempre lo será.

Por otro lado, prosiguió, el artículo 4 contempla un procedimiento para que la Agencia Nacional de Ciberseguridad, en conjunto con el Comité Interministerial de Ciberseguridad, establezcan quiénes quedan en esa condición. Tal determinación, puntualizó, se hará por medio de un decreto supremo.

- Las Comisiones unidas, por la totalidad de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast

-actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, respaldaron esta indicación.

TÍTULO VIII

Esta parte de la iniciativa de ley lleva por epígrafe "Del Comité Interministerial de Ciberseguridad".

El título fue objeto de **la indicación número 166**, del Honorable Senador señor Van Rysselberghe, para suprimirlo, junto con los artículos 36, 37, 38, 39 y 40, que lo integran.

- Esta indicación fue retirada por su autor ante la Secretaría de las Comisiones unidas el día 30 de enero de 2023.

ARTÍCULO 36

Crea el Comité Interministerial de Ciberseguridad, encomendándole la función de asesorar al Ministro del Interior y Seguridad Pública en materias de ciberseguridad relevantes para el funcionamiento de los órganos de la Administración del Estado y de servicios esenciales.

Sobre esta norma recayeron las indicaciones números 167 y 168.

La indicación número 167, de Su Excelencia el Presidente de la República, es para reemplazarla por la siguiente, contemplada como artículo 39:

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

En el ejercicio de sus funciones, el Comité deberá:

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

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

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

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

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

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

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

Habida cuenta de la falta de uniformidad advertida en el inciso primero de la norma propuesta, **las Comisiones unidas** consultaron si la nueva organización se denominará “Comité Interministerial de Ciberseguridad” o “Comité Interministerial sobre Ciberseguridad”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que actualmente, en virtud del decreto supremo N° 533, del Ministerio del Interior y Seguridad Pública, existe el organismo mencionado y que sobre él recaen dos de las decisiones más importantes de la iniciativa de ley; a saber, la declaración de los servicios esenciales y la de los operadores de importancia vital. A ellas, subrayó, se sumarán las individualizadas en la disposición examinada. En relación con estas últimas, especial relevancia atribuyó a la labor de asesorar al Presidente de la República en el análisis y definición de la Política Nacional de Ciberseguridad y a la de implementar dicho instrumento.

Sostuvo que, conforme a la norma aludida, dicha entidad recibe la denominación de Comité Interministerial sobre Ciberseguridad, y afirmó que el Ejecutivo la mantendrá en el futuro texto legal. A mayor abundamiento, esclareció que el título del artículo 39 solo constituye un error de redacción.

En el mismo orden de consideraciones, **la Honorable Senadora señora Provoste** estimó que la discusión debiera centrarse en si se trata de un Comité Interministerial sobre Ciberseguridad o un Comité Interministerial acerca de Ciberseguridad, discusión que, a su juicio, no es un tema baladí. Connotó que la primera nomenclatura tendría un impacto menor, motivo por el cual instó a preferir la segunda.

- Puesta en votación, las Comisiones unidas, por la totalidad de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, aprobaron esta indicación con la referida enmienda de carácter formal.

La indicación número 168, del Honorable Senador señor Insulza, por su parte, sustituye la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

- En atención a la aprobación de la indicación anterior, esta fue rechazada por la unanimidad de los parlamentarios de las Comisiones unidas, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra.

ARTÍCULO 37

Este precepto está referido a la composición del Comité Interministerial sobre Ciberseguridad. Prescribe, en su inciso primero, que dicho órgano será presidido por el Subsecretario del Interior y estará integrado por los siguientes miembros permanentes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Respecto de este artículo se presentaron las indicaciones números 169 y 170.

La indicación número 169, de Su Excelencia el Presidente de la República, lo reemplaza por el siguiente, contemplado como artículo 40:

“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 Nacional de la Agencia Nacional de Inteligencia.

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

Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios de la Administración del Estado u otras autoridades

públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.”.

Analizando la norma, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, reiteró que la organización cuya integración aborda este artículo existe desde el año 2015, en virtud del decreto supremo N° 533, del Ministerio del Interior y Seguridad Pública.

Acerca de las diferencias entre el artículo 37 aprobado en general por el Senado y el contenido en la indicación en estudio, observó que este último limita la integración. La razón, argumentó, obedece a que la actual es excesivamente amplia y la experiencia desde su creación ha advertido que reunir a tantos subsecretarios es complejo. Además, prosiguió, en la práctica solo concurren aquellos vinculados al tema tratado.

Por último, centrándose en la letra a), adelantó que una vez que se publique la ley que crea el Ministerio de Seguridad Pública será el Subsecretario de dicha Cartera quien componga la citada instancia.

A su turno, **el Honorable Senador señor Cruz-Coke** manifestó interés por conocer la razón de la incorporación del Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación al referido comité.

Justificando su consulta, hizo ver que el presupuesto de la citada Secretaría de Estado es acotado, lo que le resta fuerza para atender materias como la ciberseguridad. Además, concluyó, se aboca a asuntos muy específicos.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, relató que la inclusión del aludido personero de Gobierno no estaba originalmente contemplada. No obstante, remarcó, se reparó que los países que han logrado avanzar en ciberseguridad son aquellos que tienen una política estatal de fomento a la investigación y al desarrollo de esta industria. Además, apuntó, conforme a la ley N° 21.105, que creó dicha Cartera de Estado, es ella la encargada de esta política. De hecho, resaltó, actualmente hay mesas específicas porque se innovará en ciberseguridad.

En línea con lo expresado, detalló que si lo que se pretende es orientar la inversión estatal en tecnología de punta, el Ministerio referido es, orgánicamente, el llamado a tal labor. Agregó que el decreto supremo N° 533, anteriormente reseñado, fue modificado para asegurar la integración del Subsecretario por cuya participación se consulta.

Por su parte, **el Honorable Senador señor Pugh**, respaldando la decisión del Ejecutivo, subrayó que a la Cartera de Estado mencionada se le encomienda no solo las ciencias, sino también la tecnología, el conocimiento y la innovación. Connotó que la seguridad informática supone conocimientos, y que la ciberdefensa, verbigracia, ha acudido a la inteligencia

artificial, la que debe desarrollarse y programarse en base a lo que cada país realiza en el área.

Su Señoría hizo presente de la política nacional de ciberseguridad considera, dentro de sus objetivos, fomentar una industria nacional sobre la materia. Eso, notó, es innovación.

Subrayó, además, que la Organización de Estados Americanos tiene un capítulo especial dedicado a la innovación en ciberseguridad.

Asimismo, resaltó que la investigación en seguridad informática es una de las áreas estratégicas del nombrado Ministerio, y que para ello tiene recursos asignados en la Ley de Presupuestos del Sector Público. Asimismo, sostuvo, se ha estado analizado la posibilidad de crear un instituto nacional de ciberseguridad.

Tras las razones esgrimidas por el personero de Gobierno y por el Presidente de las Comisiones unidas, **el Honorable Senador señor Cruz-Coke** valoró la idea de sumar a la referida Cartera de Estado.

Enseguida, preguntó por los integrantes que, estando en el texto aprobado en general por la Sala, no figuran en el artículo en debate.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, explicó que la composición en discusión excluye a los Ministerios de Minería, de Energía y de Justicia y Derechos Humanos.

Con respecto a la decisión de prescindir de la última Secretaría de Estado aludida, **el Honorable Senador señor Cruz-Coke** observó que, probablemente, la ciberseguridad se traducirá en normas y, por lo tanto, su contribución resultará esencial.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, reiteró que el Comité Interministerial sobre Ciberseguridad existe hace ocho años, lapso durante el cual ha acumulado experiencia suficiente. Conforme a ella, dijo, la participación del Ministerio de Justicia y Derechos Humanos ha sido muy acotada, salvo cuando se han abordado temas relativos a los delitos informáticos.

Explicó que su escasa intervención se explica por la gran carga de trabajo que sobre él pesa. Con todo, insistió, cuando ha sido convocado para atender ciertas materias, ha asistido.

Para concluir recordó que, de acuerdo a lo prescrito en el inciso final de la norma examinada, el Comité podrá invitar a participar de sus sesiones a tales autoridades, de estimarse necesario.

- Sometida a votación, las Comisiones unidas, por la totalidad de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, aprobaron la indicación número 169 con enmiendas meramente formales y otras adecuaciones.

La indicación número 170, del Honorable Senador señor Insulza, sustituye, en el inciso final del artículo 37 aprobado en general, la expresión “funcionarios de la Administración del Estado” por “funcionarios del Estado”.

- Habida cuenta de la aprobación de la indicación anterior, esta fue rechazada por la unanimidad de los parlamentarios de las Comisiones unidas, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra.

ARTÍCULO 38

Esta norma alude a la Secretaría Ejecutiva del Comité Interministerial sobre Ciberseguridad.

Inciso segundo

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

Al efecto, se formuló **la indicación número 171**, de Su Excelencia el Presidente de la República, para reemplazarlo por el que sigue:

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

Deteniéndose en la enmienda propuesta, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, adujo que simplifica la redacción aprobada en general, y confiere al Director Nacional de la Agencia Nacional de Ciberseguridad la conducción del Comité.

- Las Comisiones unidas, con el apoyo transversal de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas

Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, respaldaron esta indicación con adecuaciones.

ARTÍCULO 40

Prescribe que un reglamento expedido por el Ministerio del Interior y Seguridad Pública fijará las normas de funcionamiento del Comité.

Respecto de esta norma se presentó **la indicación número 172**, de Su Excelencia el Presidente de la República, para sustituir la expresión “Ministerio del Interior y Seguridad Pública” por “Ministerio encargado de la seguridad pública”.

- Puesta en votación esta indicación, las Comisiones unidas, por la totalidad de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, aprobaron esta indicación.

°°°°°

Título nuevo

A continuación, se formuló **la indicación número 173**, de Su Excelencia el Presidente de la República, para incorporar el siguiente Título IX, nuevo, pasando el actual Título IX a ser Título X, y así sucesivamente:

“Título IX
Órganos autónomos constitucionales”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que la inclusión del título apunta a contemplar reglas particulares para las entidades mencionadas, a fin de regular -de manera más precisa- la forma en que deberán hacerse cargo de sus obligaciones en asuntos de ciberseguridad. Actualmente, alertó, los órganos autónomos constitucionales son tan importantes como los organismos de la Administración del Estado para el funcionamiento del país. Sin embargo, habida cuenta de que la Agencia Nacional de Ciberseguridad forma parte de dicha Administración, carece de competencia sobre los primeros. Por tal motivo, razonó, resulta fundamental fijar ciertas pautas, en función del estándar normativo regulado en esta iniciativa de ley.

- Sometida a votación, las Comisiones unidas, por la totalidad de sus parlamentarios, Honorables Senadores señores Araya, Cruz-Coke, Kast -actuando como miembro de ambas instancias legislativas-, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como representante de ambas instancias legislativas- y señor Saavedra, respaldaron esta indicación.

°°°°°

°°°°°

Artículo nuevo

A continuación, se presentó **la indicación número 174**, de Su Excelencia el Presidente de la República, para consultar el siguiente artículo 44, nuevo, pasando el actual artículo 41 a ser artículo 45:

“Artículo 44. Regímenes especiales. Corresponde 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 establecidas en esta ley, pudiendo requerir para ello la asistencia técnica de la Agencia Nacional de Ciberseguridad.

Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios, en relación con las infracciones a esta ley que se produzcan.

Las instituciones y organismos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que la mesa de trabajo prelegislativo sugiere aprobar esta disposición con las siguientes modificaciones:

- Agregar, en el inciso primero del artículo 44 propuesto, la siguiente oración final “En este caso, las referencias al reglamento contenidas en el artículo 6, se entenderán efectuadas a las normas que adopten los respectivos órganos internos.”.

- Incorporar, en el inciso segundo, a continuación de la voz “produzcan”, la expresión: “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".

- Agregar, en el inciso tercero, las siguientes oraciones finales: "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 sistemas o redes informáticas 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 parte que los reciba deberá conservarlos en ese carácter.".

- Incorporar los siguientes incisos finales, nuevos:

"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.".

Anunció que, de acogerse las enmiendas antedichas, la redacción del artículo 44 quedaría de la manera que sigue:

"Artículo 44. Regímenes especiales. Corresponde 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 establecidas 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, 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 sistemas o redes informáticas 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 parte que los reciba 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.”.

Las Comisiones unidas estuvieron contestes en que las enmiendas introducidas abordan materias de la iniciativa exclusiva de Su Excelencia el Presidente de la República, de conformidad a lo dispuesto en el artículo 65, inciso cuarto, N° 2, de la Constitución Política de la República.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, enunció que el Primer Mandatario respaldaría los cambios sugeridos por la mesa técnica, formulando la indicación pertinente.

La Honorable Senadora señora Provoste expresó interés por saber qué ocurrirá en el evento de que un órgano autónomo de los mencionados en el precepto no dé cumplimiento a las obligaciones establecidas; entre ellas, la de adoptar las medidas señaladas en el artículo 6, reportar los incidentes de seguridad informática, intercambiar información y conformar o participar en CSIRT. En este punto, hizo ver que la ausencia de sanción se traducirá en la falta de observancia de la ley.

Abocándose a la inquietud manifestada por la legisladora, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, reconoció que la creación de la Agencia Nacional de Ciberseguridad como un organismo de la Administración del Estado impide que las entidades autónomas constitucionales queden sujetas a su regulación, fiscalización y supervigilancia.

No obstante, ahondó, se proponen algunos ajustes al texto para garantizar el respeto a las obligaciones de ciberseguridad, tal como lo recomendó la Excelentísima Corte Suprema. En efecto, subrayó, se les impone el deber de coordinarse. Aseveró que ello ha demostrado ser más útil que avanzar en cuerpos normativos más estrictos respecto de las organizaciones públicas no dependientes del Gobierno.

Remarcó que algunos de los órganos autónomos, entre ellos el Poder Judicial y el Congreso Nacional, serán calificados como operadores de importancia vital. Agregó que, si bien la Agencia Nacional de Ciberseguridad no podrá sancionarlos, serán sus organismos internos de control los que, recurriendo a las normas sustanciales, determinarán si hubo incumplimiento de una obligación legal. Sin embargo, insistió, el procedimiento a aplicar será aquel previsto en la entidad de que se trate.

Siguiendo con el desarrollo de su exposición, puso de relieve que la experiencia ha permitido concluir que en asuntos de seguridad informática prima la colaboración. Añadió que difícilmente los cuerpos con autonomía constitucional lograrán desarrollar todas sus capacidades, lo que supondrá que gran parte de las mismas descansen en la Agencia, mediante un convenio de colaboración.

Para concluir, reconoció que el artículo 44 contemplado en la indicación número 174 motivó observaciones tanto por parte del Banco Central como del Poder Judicial, en orden consignar expresamente la obligación de dar cumplimiento a ciertos deberes. Producto de ello, enfatizó, quedarán sujetos a lo dispuesto en los artículos 4 y 6, asegurando, de este modo, altos estándares de ciberseguridad.

A su turno, **el Honorable Senador señor Araya** juzgó indispensable dar mayores pasos en seguridad informática en lo que respecta a los órganos autónomos. Planteó que las regulaciones emanadas de la Agencia Nacional de Ciberseguridad debieran serles obligatorias, y aclaró que estas no persiguen interferir en sus atribuciones sino, simplemente, afianzar un mínimo de ciberseguridad en todo el Estado.

Su Señoría resaltó que episodios como los experimentados por el Poder Judicial y por el Estado Mayor Conjunto hacen conveniente que la citada Agencia cuente con facultades normativas respecto de todos los organismos y órganos autónomos considerados en la iniciativa de ley. Apuntó que las de supervigilancia y de fiscalización, en tanto, deberían quedar radicadas en los referidos órganos, a fin de no vulnerar su independencia.

Llamó a ponderar que dejar entregada una materia tan importante a un eventual convenio de colaboración no parece razonable, toda vez que dependerá de la voluntad de quien dirija cada órgano.

A la luz de lo expuesto, instó por introducir cambios en el título IX del proyecto, e insistió en disipar la posibilidad de que su propuesta sea entendida como una coartación a la autonomía de tales entidades.

Atendiendo las inquietudes develadas por los legisladores que le antecedieron en el uso de la palabra, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, afirmó concordar con las apreciaciones del Honorable Senador señor Araya. Ahondando en su aseveración, destacó que las normas de los artículos 4 y 6 del proyecto en estudio serán obligatorias para los órganos autónomos, cumpliendo así con el estándar de esta legislación.

En lo que concierne a cómo la Agencia Nacional de Ciberseguridad controla y fiscaliza la observancia de tales estándares, esclareció que no puede avanzarse más, debido a la limitación constitucional existente.

Comentó que el Ejecutivo ha consultado a diversos especialistas acerca de la fórmula apropiada para garantizar el cumplimiento de la regulación contenida en esta proposición legal por parte de los órganos autónomos, sin vulnerar su carácter. Acotó que todos han coincidido en la complejidad de tal objetivo. Sin embargo, opinó que el modelo al que arribó la mesa técnica parece ser el más adecuado, puesto que, si alguna de las organizaciones públicas no dependientes del Gobierno contraviene las obligaciones de los preceptos mencionados, tendrá que asumir las responsabilidades correspondientes, de acuerdo a lo contemplado en su normativa interna.

Evidenció que solo hasta ese punto es posible avanzar, habida cuenta de que la Agencia Nacional de Ciberseguridad será un servicio público perteneciente a la Administración del Estado. Para lograr más, postuló, debería crearse como una institución autónoma.

En relación con el último comentario realizado, hizo hincapié en que en la experiencia comparada no hay países que hayan optado por esa alternativa, porque consagrarlo en tal carácter rigidizaría a un organismo eminentemente técnico.

Para concluir, arguyó que las diversas entidades autónomas coinciden en la importancia que reviste la ciberseguridad y, en consecuencia, el cumplimiento mínimo de ciertas medidas, las que, reiteró, se encuentran en los artículos 4 y 6 de la iniciativa de ley.

El Honorable Senador señor Pugh valoró la solución ofrecida por el grupo de asesores conformado para facilitar la tramitación de este proyecto, señalando que de acuerdo con la redacción propuesta para el artículo 44, las organizaciones públicas no dependientes del Gobierno deberán observar los deberes de este futuro texto legal, entre ellos, el de cooperación, el de coordinación y el de reporte de incidentes.

- En atención al compromiso asumido por el Ejecutivo y luego de disiparse las inquietudes expresadas, las Comisiones unidas, por la unanimidad de sus parlamentarios presentes, Honorables Senadores señores Araya, Cruz-Coke, Kusanovic, Pugh -en su calidad de integrante de ambas Comisiones-, señora Provoste -como

representante de ambas instancias legislativas- y señor Saavedra, respaldaron, ad referéndum, la indicación número 174 con las modificaciones señaladas.

Posteriormente, dando cumplimiento al compromiso asumido, Su Excelencia el Presidente de la República presentó una indicación, que fue individualizada como **indicación número 174 bis**, para consultar el siguiente artículo 44, nuevo:

"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.”.

- Las Comisiones unidas, por la totalidad de sus integrantes, Honorables Senadores señores Araya, Cruz-Coke -actuando como miembro de ambas instancias legislativas-, Insulza, Kusanovic, Macaya y Ossandón, señora Provoste -en su calidad de miembro de ambas instancias legislativas- y señor Pugh, aprobaron esta indicación.

°°°°°

°°°°°

Artículo nuevo

Asimismo, se formuló **la indicación número 175**, del Honorable Senador señor Insulza, para agregar el siguiente artículo, nuevo:

“Artículo…. Derecho general al 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.”.

La totalidad de los integrantes presentes de las Comisiones unidas estuvo conteste en la idea de considerar el derecho en discusión dentro del artículo 3 de la iniciativa de ley.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, aseveró que la mesa de trabajo prelegislativo comparte la indicación del Honorable Senador señor Insulza. Con todo, adhirió a la propuesta de las instancias legislativas. Pormenorizó que, de incluirse como un principio de aquellos que deberán observarse en la aplicación de este futuro texto legal, su redacción sería la siguiente:

“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.”.

El Honorable Senador señor Saavedra valoró la decisión adoptada, y añadió que el derecho en cuestión fortalecerá a otros tradicionales, como el de privacidad, el de libertad de expresión y el de asociación en el mundo de la digitalización.

El Honorable Senador señor Pugh hizo ver que la criptografía constituye una forma de mantener las comunicaciones privadas. Al efecto, recordó que el artículo 19 N° 4° de la Carta Fundamental asegura el

respeto y la protección a la vida privada, así como también la de sus datos personales. Por la razón esgrimida, celebró la inclusión de este derecho.

No obstante, alertó que, para hacer frente a ciertos delitos, el Estado debe tener capacidad de análisis criptográfica que permita a las policías, en ciertas ocasiones y con la debida autorización, realizar adecuadamente sus investigaciones.

Para concluir, advirtió que el desarrollo tecnológico avanza rápidamente, y que el arte citado puede quedar obsoleto con el advenimiento de la computación cuántica. En consecuencia, Su Señoría instó a anticipar cuáles serán las fórmulas para proteger a futuro las comunicaciones.

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya, Ossandón, Pugh y Saavedra, respaldaron esta indicación con la enmienda antedicha.

°°°°°

TÍTULO IX

Esta parte del proyecto de ley se denomina “De las modificaciones a otros cuerpos legales”.

Sobre el referido título recayó **la indicación número 176**, del Honorable Senador señor Van Rysselberghe, para eliminarlo, junto con el artículo 41, que lo integra.

- Esta indicación fue retirada por su autor ante la Secretaría de las Comisiones unidas el día 30 de enero de 2023.

ARTÍCULO 41

Inserto en el título mencionado anteriormente, este precepto introduce un literal k), nuevo, al artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, con el objeto de encomendar al Estado Mayor conjunto la conducción del Centro Coordinador CSIRT del Sector Defensa en coordinación con la Subsecretaría de Defensa.

Este artículo fue objeto de **la indicación número 177**, de Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como 45:

“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.”.”.

Sobre el particular, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, planteó que la enmienda al artículo 25 de la ley N° 20.424 persigue confiar al Estado Mayor Conjunto la labor de dirigir el CSIRT de la Defensa Nacional, tal como lo contempla el artículo 25 del proyecto de ley.

- Puesta en votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya, Ossandón, Pugh y Saavedra, aprobaron esta indicación.

°°°°°

Artículos nuevos

A continuación, se formuló **la indicación número 178**, de Su Excelencia el Presidente de la República, para agregar los siguientes artículos, nuevos, consultados como 46, 47 y 48.

El primero de ellos es del siguiente tenor:

“Artículo 46. Modificaciones a la ley N° 21.459, sobre delitos informáticos. Incorpóranse las siguientes modificaciones 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 el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que reporte inmediatamente al responsable de las redes o sistemas informáticos afectados y a la Agencia Nacional de Ciberseguridad el acceso y las vulnerabilidades de seguridad detectadas en su investigación.”.

Centrando su atención en el primer numeral del artículo 46, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez,** informó que el grupo de asesores conformado para facilitar la tramitación de esta iniciativa de ley sugiere aprobarlo con modificaciones, de manera de agregar al artículo 2° de la ley N° 21.459 los siguientes incisos finales:

“No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los

hechos tipificados en el inciso primero, siempre que se cumplan las siguientes condiciones:

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

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

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

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

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

El personero de Gobierno explicó que la enmienda al artículo 2° de la ley sobre delitos informáticos fue discutida largamente durante la tramitación de dicho cuerpo normativo. En esa oportunidad, recordó, se debatió la opción de otorgar una protección legal al investigador en seguridad informática que descubre una vulnerabilidad y sigue un procedimiento para notificar al afectado a fin de resolverla. En otras palabras, ilustró, al “*hacking ético*”.

Relató que producto de la entrada en vigor del texto aludido, el CSIRT de Gobierno dejó de recibir reportes relativos a las debilidades presentes en los sistemas públicos. La razón de este cambio, subrayó, obedece a que ello podría conllevar sanciones penales. Tal realidad, prosiguió, motivó a la mesa técnica a proponer un resguardo legal a la piratería ética, erradicando la posibilidad de que una norma en ese sentido sea mal utilizada. Para ello, detalló se establecen ciertas condiciones a cumplir.

Asimismo, puso de relieve que la redacción sugerida recoge las exigencias previstas en la experiencia comparada. Concretamente, enunció, el estándar de la Directiva NIS2, de la Unión Europea, y el belga; las prácticas incorporadas recientemente en Israel, y las reformas introducidas en la legislación dominicana.

Juzgó que la enmienda al artículo 2° de la ley N° 21.459 hará posible brindar resguardo legal a las labores de investigación en seguridad informática, lo que, remarcó, es significativamente beneficioso para la sociedad.

El Honorable Senador señor Macaya estimó que toda eximente de responsabilidad penal obliga a un análisis mayor.

Su Señoría consultó qué se considerará "labores de investigación en ciberseguridad". Preguntó si la expresión está concebida en términos amplios o si, por el contrario, existe una definición específica a su respecto.

Adicionalmente, manifestó interés por saber si el "*hacking ético"* ampara solo a quienes se desempeñan en reparticiones públicas o a cualquier persona que afirma realizar indagaciones de dicha índole.

Razonó que el mal uso de la figura citada podría abrigar el el acceso a sistemas informáticos ajenos y a su manipulación.

Por los motivos esgrimidos, hizo ver la necesidad de garantizar que las labores mencionadas tengan cierto nivel de trazabilidad.

Atendiendo las inquietudes planteadas por Su Señoría, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, declaró que los investigadores en seguridad informática pueden ser de dos tipos, académicos o empresas dedicadas a la ciberseguridad.

Fijando su atención en los primeros, especificó que se trata de personas pertenecientes a instituciones de educación superior que efectúan indagaciones sobre ciertos temas específicos. Tal es el caso, precisó, de quien escanea una red determinada para detectar posibles anomalías y, en consecuencia, brechas de seguridad. Sin embargo, adelantó, son muy pocos en el país.

En relación con las empresas dedicadas a ciberseguridad, arguyó que esta figura es la que opera en los diversos servicios públicos. Aquellas, continuó, pueden encontrar vulnerabilidades en las redes de quien las contrató. No obstante, alertó, habitualmente la tecnología empleada por el Estado es la misma y, por lo tanto, el hallazgo en cierto ministerio también estará presente en otros. Reiteró que este acontecimiento solía comunicarse, mas ante la posibilidad de incurrir en un delito, ya no se hace.

Postuló que, si bien podría ponderarse la obligación de registro, suele ser un paso engorroso. Además, añadió, no tiene un beneficio directo. Por ese motivo, observó, se prefirió considerar una eximente de responsabilidad, para la cual deberán cumplirse ciertas exigencias.

Por último, hizo hincapié en que la construcción de una barrera que permita que los investigadores de ciberseguridad tengan

confianza y notifiquen las fragilidades detectadas redundará en mejores niveles de seguridad informática.

El Honorable Senador señor Macaya consultó cual será el plazo para formalizar el deber de reporte.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, sostuvo que, de acuerdo con lo prescrito en el numeral 1, deberá efectuarse en forma inmediata y a más tardar en el momento que alerte a la Agencia Nacional de Ciberseguridad.

Agregó que, el numeral 2, consigna que deberá dar cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que hubiere dictado el organismo encargado de la ciberseguridad.

El Honorable Senador señor Macaya demostró interés por el empleo de la expresión “a más tardar en el momento que alerte a la Agencia Nacional de Ciberseguridad”.

Al efecto, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, explicó que no siempre los sistemas informáticos tienen a quien reportar. De ser este el caso, concluyó, deberá recurrirse a la Agencia.

El Honorable Senador señor Pugh celebró las enmiendas a la indicación en estudio. Profundizando en su apreciación, relevó que la redacción sugerida por el grupo de asesores conformado para acelerar la tramitación de esta iniciativa de ley transformará a Chile en un país proactivo en ciberseguridad, puesto que recoge la directiva europea NIS2, y las experiencias belga y dominicana.

- Sometido a votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron el numeral 1 del artículo 46 propuesto en la indicación número 178 con las enmiendas consignadas y otras de carácter formal.

El numeral 2 del artículo 46, en tanto, deroga el artículo 16 de la ley N° 21.459, que reza lo siguiente:

“Artículo 16.- Autorización e Investigación Académica. Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.”.

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, respaldaron el numeral 2 del artículo 46 propuesto en la indicación número 178.

El artículo 47, a su vez, incorpora, en el artículo 8° de la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia, el siguiente literal h), nuevo:

"h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, señaló que la letra cuya inclusión se sugiere en el artículo 8° de la ley N° 19.974 es fruto de la aprobación del artículo 4 de esta iniciativa.

- Puesto en votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron el artículo 47 propuesto en la indicación número 178, con adecuaciones formales.

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

El Honorable Senador señor Pugh consultó la razón por la cual el Primer Mandatario propone suprimir esta facultad que le otorga el citado texto normativo.

Sobre la inquietud de Su Señoría, **el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez**, adujo que la eliminación del literal indicado obedece a que la ley referida fue derogada completamente, con excepción de su artículo 8°. A lo anterior, añadió, se suma el hecho de que este nunca ha tenido aplicación, y que las tecnologías a las que alude están obsoletas. Asimismo, connotó, los sistemas de cifrado operan por defecto en

casi todas las tecnologías de comunicación y, en consecuencia, si quisiera aplicarse tal norma, tampoco sería posible.

Al respecto, **el Honorable Senador señor Pugh** puso énfasis en el poder que posee internet en la actualidad. En efecto, ahondó, resulta prácticamente imposible suprimir el acceso a este servicio digital, demostrándolo así la experiencia ucraniana.

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron el artículo 48 propuesto en la indicación número 178.

°°°°°

ARTÍCULO PRIMERO TRANSITORIO

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

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

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

Además, prosigue, podrá establecer las normas para el encasillamiento del personal en la planta que fije, las que podrá incluir a los funcionarios que se traspasen desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.

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

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

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

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

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

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

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

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

b) No podrá significar pérdida del empleo, disminución de remuneraciones respecto del personal titular de un cargo de planta, modificación de los derechos estatutarios y previsionales del personal traspasado. Tampoco importará cambio de la residencia habitual de los

funcionarios fuera de la Región en que estén prestando servicios, a menos que se lleve a cabo con su consentimiento.

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

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

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

En relación con esta disposición transitoria se presentó **la indicación número 179**, de Su Excelencia el Presidente de la República, para reemplazarla por la siguiente:

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

1. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

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

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

4. El personal que a la fecha de inicio de actividades de la Agencia se encuentre prestando servicios a honorarios en la Subsecretaría del Interior y cuyo traspaso se determine de conformidad a los incisos tercero y cuarto de este numeral, podrá optar por modificar su estatuto

laboral al Código del Trabajo, siempre que cumpla con los requisitos respectivos y otorgue previamente su consentimiento.

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

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

La individualización del personal traspasado conforme al inciso anterior, se realizará a través de decretos expedidos bajo la fórmula “Por orden del Presidente de la República”, por intermedio del Ministerio del Interior y Seguridad Pública.

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

5. Determinar la estructura de la Agencia y su dotación máxima de personal.

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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, informó que la mesa de trabajo prelegislativo recomienda aprobar esta indicación con una modificación, consistente en reemplazar el número 5 del precepto en examen por el siguiente:

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

Justificó que el cambio anterior obedece a que la estructura interna de la Agencia Nacional de Ciberseguridad se establecerá en un decreto.

El personero de Gobierno anunció que, de respaldarse la propuesta citada, la redacción del artículo primero transitorio quedaría de la manera que sigue:

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

1. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

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

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

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

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

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

La individualización del personal traspasado conforme al inciso anterior, se realizará a través de decretos expedidos bajo la fórmula "Por orden del Presidente de la República", por intermedio del Ministerio del Interior y Seguridad Pública.

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

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

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

- Puesta en votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron la indicación número 179 con la enmienda consignada precedentemente y otras de carácter formal.

ARTÍCULO SEGUNDO TRANSITORIO

Se refiere al nombramiento del primer Director de la Agencia Nacional de Ciberseguridad. Sobre el particular, señala que 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, a dicha autoridad, 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. Detalla que, en el acto de nombramiento, el Primer Mandatario fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director, siempre que no se encuentre vigente la respectiva planta de personal. Concluye expresando que la remuneración de aquel se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese solo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal.

Sobre esta norma recayó **la indicación número 180**, de los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para sustituir la expresión “un año”, por la frase: “dieciocho meses, prorrogables por necesidades del servicio,”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, dio a conocer que el grupo de asesores conformado para facilitar la tramitación de este proyecto de ley recomienda rechazar esta indicación, toda vez que el primer Director de la Agencia Nacional de Ciberseguridad solo tendrá la misión de llevar a cabo la instalación de dicha entidad, labor para la cual el plazo aprobado en general por el Senado es suficiente.

- Por la razón esgrimida precedentemente, esta indicación fue desechada por la unanimidad de los miembros presentes de las Comisiones unidas, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra.

ARTÍCULO QUINTO TRANSITORIO

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

En relación con esta disposición se presentaron las indicaciones números 181 y 182.

La indicación número 181, del Honorable Senador señor Van Rysselberghe, la elimina.

- Esta indicación fue retirada por su autor ante la Secretaría de las Comisiones unidas el día 30 de enero de 2023.

La indicación número 182, del Honorable Senador señor Insulza, reemplaza la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

- Sometida a votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, respaldaron esta indicación.

ARTÍCULO SEXTO TRANSITORIO

Refiere a la renovación parcial de los miembros del Consejo Técnico de la Agencia Nacional de Ciberseguridad. Concretamente, prescribe que, para tales efectos, sus miembros durarán en los cargos el número de años que a continuación se transcribe, sin perjuicio de que podrán ser designados por un nuevo período:

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

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

Respecto de este precepto se formularon las indicaciones números 183 y 184.

La indicación número 183, del Honorable Senador señor Van Rysselberghe, es para eliminarlo.

- Esta indicación fue retirada por su autor ante la Secretaría de las Comisiones unidas el día 30 de enero de 2023.

La indicación número 184, de Su Excelencia el Presidente de la República, busca reemplazarlo por el siguiente:

"Artículo sexto transitorio.- 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.".

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, puso de relieve que la disposición en estudio regula la primera designación de los integrantes del Consejo Multisectorial sobre Ciberseguridad.

- Las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, aprobaron esta indicación con adecuaciones formales.

°°°°°

Artículo transitorio nuevo

Finalmente, se presentó **la indicación número 185**, de Su Excelencia el Presidente de la República, para incorporar la siguiente norma transitoria, nueva:

"Artículo octavo transitorio.- 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; 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.”.

El Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, recordó que el artículo 4 del proyecto prescribe que mediante la dictación de un decreto del ministerio encargado de la seguridad pública se determinarán aquellos servicios que serán considerados esenciales y a los operadores de importancia vital. La indicación en estudio, por su parte, persigue incorporar una disposición transitoria para la fijación de aquellos mientras no se dicte la norma jurídica señalada.

Fijando su atención en el trabajo desarrollado por la mesa de trabajo prelegislativo, declaró que dicha instancia sugiere aprobar esta indicación con enmiendas, de manera de excluir de esta categoría inicial a los prestadores de salud operados por municipios o corporaciones municipales. Justificó el planteamiento en su falta de capacidad para adoptar medidas técnicas en materia de ciberseguridad. No obstante, enunció, en los próximos años podrán incorporarse.

Especificó que, de acogerse la modificación mencionada, la redacción del artículo octavo transitorio quedaría de la forma que sigue:

“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.”.

El Honorable Senador señor Pugh postuló que la precisión del grupo de asesores permite que aquellos que están más débiles en seguridad informática tengan mayor tiempo para adaptarse a las exigencias derivadas de esta iniciativa legal.

Sin embargo, remarcó, lo ideal es que los municipios sean capaces de dar cumplimiento a los deberes de ciberseguridad; objetivo que requerirá el trabajo conjunto de las asociaciones que los agrupan.

- Sometida a votación, las Comisiones unidas, por la totalidad de sus parlamentarios presentes, Honorables Senadores señores Cruz-Coke -en su calidad de integrante de ambas instancias legislativas-, Kusanovic, Macaya y Ossandón, señora Provoste -actuando como miembro de ambas instancias legislativas- y señores Pugh y Saavedra, respaldaron esta indicación con la enmienda antedicha y otras de carácter formal.

Al término de la última sesión celebrada por las Comisiones unidas para conocer las indicaciones formuladas a esta iniciativa, las instancias legislativas, en virtud de lo dispuesto en el artículo 121, inciso final, del reglamento del Senado, y a solicitud del representante del Ejecutivo, acordaron eliminar del texto el vocablo “plataforma”, y sustituir la expresión “redes o sistemas informáticos” y “red o sistema informático” por “redes y sistemas informáticos” y “red y sistema informático”, respectivamente.

°°°°°

- - -

MODIFICACIONES

De conformidad a los acuerdos adoptados, las Comisiones de Defensa Nacional y de Seguridad Pública, unidas, tienen el honor de proponer las siguientes modificaciones al proyecto de ley aprobado en general por el Senado:

ARTÍCULO 1

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 estos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para los efectos de esta ley, se entenderá por Administración del Estado a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. Los

órganos autónomos constitucionales se ajustarán a las disposiciones de esta ley que así lo señalen. No se aplicarán las disposiciones de esta ley a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que este tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.

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

(Unanimidad 7x0. Indicación número 3, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 2

Sustituirlo por el que se señala a continuación:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20. Operadores de importancia vital: institución pública o privada, identificada como tal por la Agencia de conformidad con esta ley, por prestar algún servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, que depende de las redes y sistemas informáticos, y cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar.

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

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

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

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

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

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

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

(Encabezamiento, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Número 1, unanimidad 7x0. Indicación número 28, y artículo 121, inciso final, del Reglamento del Senado).

(Número 2, unanimidad 9x0. Indicación número 5).

(Número 3, unanimidad 8x0. Indicación número 29).

(Número 4, unanimidad 8x0. Indicación número 29).

(Número 5, unanimidad 7x0. Indicación número 23).

(Número 6, unanimidad 7x0. Indicaciones números 6 y 7).

(Número 7, unanimidad 8x0. Indicación número 8).

(Número 8, unanimidad 8x0. Indicación número 29).

(Número 9, unanimidad 8x0. Indicación número 10).

(Número 10, unanimidad 8x0. Indicación número 29).

(Número 11, unanimidad 8x0. Indicación número 29).

(Número 12, unanimidad 8x0. Indicación número 11).

(Número 13, unanimidad 9x0. Indicación número 13).

(Número 14, unanimidad 8x0. Indicaciones números 15 y 16).

(Número 15, unanimidad 8x0. Indicación número 17, y artículo 121, inciso final, del Reglamento del Senado).

(Número 16, unanimidad 8x0. Indicación número 29).

(Número 17, unanimidad 8x0. Indicación número 29).

(Número 18, unanimidad 8x0. Indicación número 29).

(Número 19, unanimidad 8x0. Indicación número 29).

(Número 20, unanimidad 7x0. Indicación número 18, y artículo 121, inciso final, del Reglamento del Senado).

(Número 21, unanimidad 7x0. Indicación número 22, y artículo 121, inciso final, del Reglamento del Senado).

(Número 22, unanimidad 7x0. Indicación número 24, y artículo 121, inciso final, del Reglamento del Senado).

(Número 23, unanimidad 7x0. Indicación número 25).

(Número 24, unanimidad 7x0. Indicación número 26).

(Número 25, unanimidad 7x0. Indicación número 27).

(Número 26, unanimidad 8x0. Indicación número 29).

(Número 27, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 3

Reemplazarlo por el que se transcribe:

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

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

2. Principio de confidencialidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas

informáticos deberá ser conocida y accedida exclusivamente por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.

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

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

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

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

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

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

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

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

11. Principio del cifrado: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere

necesarias, incluyendo el cifrado. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio de este derecho.”.

(Encabezamiento, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Número 1, unanimidad 9x0, indicación número 43, y 10x0, indicación número 43 bis).

(Número 2, unanimidad 8x0. Indicación número 32).

(Número 3, unanimidad 9x0. Indicaciones números 35 y 36).

(Número 4, unanimidad 9x0, indicación número 38, y 10x0, indicación número 38 bis).

(Número 5, unanimidad 8x0. Indicación número 34).

(Número 6, unanimidad 9x0, indicación número 42, y 10x0, indicación número 42 bis).

(Número 7, unanimidad 8x0. Indicación número 33).

(Número 8, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Número 9, unanimidad 8x0. Indicación número 31).

(Número 10, unanimidad 9x0. Indicación número 39).

(Número 11, unanimidad 7x0. Indicación número 175).

TÍTULO II

Considerar como tal el siguiente:

“TÍTULO II
Obligaciones de ciberseguridad”.

(Unanimidad 7x0. Indicación número 45).

Párrafo 1°

Contemplar, en su lugar, el que se indica a continuación:

"Párrafo 1°
Servicios esenciales y operadores de importancia vital".

(Unanimidad 7x0. Indicación número 46).

ARTÍCULO 4

Reemplazarlo por el que sigue:

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

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

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

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

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

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

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

a) La cantidad de usuarios potencialmente afectados;

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

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

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

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

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

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

h) El daño reputacional que pueda ocasionarse.

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

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

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

(Unanimidad 7x0. Indicación número 47).

Párrafo 2°

Contemplar, en su lugar, el que se transcribe a continuación:

“Párrafo 2°
Obligaciones de ciberseguridad”.

(Unanimidad 7x0. Indicación número 51).

ARTÍCULO 5

Sustituirlo por el que se señala:

“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.”.

(Unanimidad 7x0, indicaciones números 52 y 53; 8x0, indicación número 55, y 10x0, indicación número 55 bis).

ARTÍCULO 6

Reemplazarlo por el siguiente:

“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.”.

(Denominación y encabezamiento del artículo: 8x0 y 7x0, respectivamente. Indicaciones número 56, 57 y 58).

(Letra a), unanimidad 8x0, indicaciones números 59, 60 y 61, y 10x0, indicación número 61 bis).

(Letra b), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Letra c), unanimidad 8x0. Indicaciones números 62 y 63).

(Letra d), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Letra e), unanimidad 8x0. Indicación número 64).

(Letra f), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Letra g), unanimidad 8x0. Indicación número 65, y artículo 121, inciso final, del Reglamento del Senado).

(Letra h), unanimidad 8x0. Indicación número 66).

(Letra i), unanimidad 8x0. Indicación número 67).

(Inciso final, unanimidad 8x0. Indicación número 68).

ARTÍCULO 7

Considerar como tal el que sigue:

“Artículo 7. Deber de reportar. Todas las instituciones, sean públicas o privadas, e independiente de si son o no

operadores de servicios esenciales, con la sola excepción de aquellos que la Agencia hubiere eximido expresamente en sus instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley.

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

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

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

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

(Unanimidad 8x0. Indicación número 69, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 8

Reemplazarlo por el siguiente:

“Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

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

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

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

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

(Unanimidad 8x0. Indicaciones números 70 y 71).

ARTÍCULO 9

Sustituirlo por el que se transcribe a continuación:

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

a) Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.

b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.

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

d) Coordinar y supervisar a los CSIRT Sectoriales existentes; a aquellos que pertenezcan a organismos de la Administración del

Estado; a instituciones privadas y al CSIRT Nacional, en la forma que establece esta ley.

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

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

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

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

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

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

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

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

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

n) Fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones

generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley.

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

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

o) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.

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

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

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

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

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

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

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

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

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

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

(Encabezamiento, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

(Letra a), unanimidad 8x0. Indicación número 72).

(Letra b), unanimidad 8x0. Indicación número 73).

(Letra c), unanimidad 8x0. Indicación número 76).

(Letra d), unanimidad 8x0. Indicaciones números 78 y 80).

(Letra e), unanimidad 8x0. Indicación número 81).

(Letra f), unanimidad 8x0. Indicación número 82).

(Letra g), unanimidad 8x0. Indicación número 83).

(Letra h), unanimidad 8x0. Indicación número 84).

(Letra i), unanimidad 8x0. Indicación número 86).

(Letra j), unanimidad 8x0. Indicaciones números 87 y 88).

(Letra k), unanimidad 8x0. Indicación número 89).

(Letra l), unanimidad 8x0. Indicación número 90).

(Letra m), unanimidad 8x0. Indicación número 92).

(Letra n), unanimidad 10x0. Indicaciones números 94 y 94 bis).

(Letra ñ), unanimidad 7x0, indicación número 95, y 10x0, indicación número 95 bis).

(Letra o), unanimidad 7x0. Indicación número 97).

(Letras p), q), r), s), t), u), v) y w), unanimidad 10x0. Indicación número 99).

(Letra x), unanimidad 10x0. Indicaciones número 101 y 101 bis).

(Letra y), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 10

Incorporar, a continuación de la expresión “un Director” la locución “o Directora”.

(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 11

Encabezamiento

Sustituirlo por el siguiente:

“Artículo 11. Atribuciones del Director o Directora Nacional. Corresponderá especialmente al Director o Directora Nacional:”.

(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

Letra f)

Reemplazarla por la siguiente:

“f) Delegar atribuciones o facultades específicas en los funcionarios y funcionarias que indique;”.

(Unanimidad 10x0. Indicación número 102, y artículo 121, inciso final, del Reglamento del Senado).

Letra g)

Sustituirla por la que sigue:

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

(Unanimidad 10x0. Indicación número 103, y artículo 121, inciso final, del Reglamento del Senado).

ººººº

Luego, incorporar la siguiente letra h), nueva:

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

(Unanimidad 9x0. Indicación número 105).

ººººº

ARTÍCULO 13

Considerar como tal el que se transcribe a continuación:

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

(Unanimidad 10x0. Indicación número 106).

ARTÍCULO 14

Reemplazarlo por el siguiente:

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

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

Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

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

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

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

La Agencia no podrá celebrar contratos de trabajo estableciendo el pago de indemnizaciones por causas distintas a las indicadas en los artículos 161, 162 y 163 del Código del Trabajo, y en caso alguno se

podrá alterar el monto que entregue la base de cálculo dispuesta en dichas normas. Para el caso de evaluación deficiente de su desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal.

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

Un reglamento expedido por el ministerio encargado de la seguridad pública, determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

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

(Unanimidad 9x0, indicación número 107, y 10x0 indicación número 107 bis).

ARTÍCULO 15

Sustituirlo por el que sigue:

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

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

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

En todo caso, quedarán exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañan personalmente al funcionario o funcionaria, o que se refieran a la

administración de su patrimonio. El desempeño de funciones en la Agencia será de dedicación exclusiva y será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley. No obstante, será compatible con cargos docentes en instituciones públicas o privadas reconocidas por el Estado hasta un máximo de doce horas semanales, para lo cual deberá prolongar su jornada para compensar las horas durante las cuales no haya podido desempeñar su cargo.

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

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

(Unanimidad 9x0, indicación número 109, y 10x0 indicación número 109 bis).

Párrafo 3°(del Título III)

Sustituir su denominación por la que se indica a continuación:

“Párrafo 3°
Consejo Multisectorial sobre Ciberseguridad”.

(Unanimidad 9x0. Indicación número 110).

ARTÍCULO 16

Eliminarlo.

(Unanimidad 9x0. Indicación número 111).

Párrafo 4°(del Título III)

Suprimirlo en esta parte, para ubicarlo más adelante, antes del artículo 21 que pasa a ser 19, con la denominación que se señalará en su oportunidad.

(Unanimidad 9x0. Indicación número 115).

ARTÍCULO 17

Pasa a ser artículo 16, reemplazado por el que sigue:

“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.”.

(Unanimidad 10x0, todo el artículo, salvo la oración final del inciso segundo que fue eliminada por 7 votos en contra y 3 a favor, en segunda votación, de conformidad al artículo 178 del Reglamento del Senado. Indicación número 116, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 18

Suprimirlo.

(Unanimidad 10x0. Indicación número 117).

ARTÍCULO 19

Pasa a ser artículo 17, sustituido por el que sigue:

“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.”.

(Unanimidad 7x0. Indicación número 118, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 20

Pasa a ser artículo 18, reemplazado por el que se transcribe a continuación:

“Artículo 18. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro sesiones consecutivas.

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

El consejero respecto del cual se verificare alguna de las causales de cesación referidas anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.

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

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

(Unanimidad 10x0. Indicación número 119).

°°°°°

Como se dijo, incorporar luego un párrafo 4°, nuevo, del siguiente tenor:

“Párrafo 4°
Red de Conectividad Segura del Estado”.

(Unanimidad.10x0. Indicación número 119 bis).

°°°°°

ARTÍCULO 21

Pasa a ser artículo 19, sustituido por el que sigue:

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

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

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

(Unanimidad 10x0. Indicación número 120).

ARTÍCULO 22

Pasa a ser artículo 20, con las siguientes enmiendas:

En su encabezamiento, sustituir “ante Incidentes” por “a Incidentes”.

(Adecuación formal).

Letra a)

Reemplazarla por la siguiente:

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

(Unanimidad 10x0. Indicación número 121).

Letra b)

Sustituirla por la que sigue:

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

(Unanimidad 10x0. Indicación número 123).

Letra e)

Considerar como tal la que se señala continuación:

“e) Supervisar incidentes a escala nacional.”.

(Unanimidad 10x0. Indicación número 126).

Letra f)

Reemplazarla por la que sigue:

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

(Unanimidad 10x0. Indicación número 127).

Letra g)

Sustituirla por la siguiente:

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

(Mayoría 9x1. Indicación número 128).

Letra h)

Contemplar en su lugar la que sigue:

“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.”.

(Unanimidad 10x0. Indicación número 131).

Letra i)

Reemplazarla por la que se transcribe:

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

(Unanimidad 10x0. Indicación número 132).

Letra j)

Sustituirla por la siguiente:

“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.”.

(Unanimidad 10x0. Indicación número 135).

Letra k)

Eliminarla.

(Unanimidad 10x0. Indicación número 136).

TÍTULO IV

Reemplazar su denominación, para que quede del siguiente modo:

“TÍTULO IV
Otras instituciones intervinientes”.

(Unanimidad 10x0. Indicación número 139).

ARTÍCULO 23

Pasa a ser artículo 21, sustituido por el siguiente:

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

Los CSIRT Sectoriales tendrán las siguientes funciones:

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

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

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

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

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

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

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

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

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

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

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

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

Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las instancias de coordinación entre la Agencia y las autoridades sectoriales y sus respectivos CSIRT.”.

(Unanimidad 8x0, indicación número 140, y 10x0, indicación número 140 bis).

ARTÍCULO 24

Pasa a ser artículo 22, consultado con el siguiente texto:

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

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

En el ejercicio de estas facultades normativas, las autoridades sectoriales deberán considerar, a lo menos, los protocolos y estándares técnicos y las instrucciones generales y particulares dictados por la Agencia Nacional de Ciberseguridad. Lo anterior, sin perjuicio de que estos

últimos serán obligatorios para todos los regulados aun cuando la autoridad sectorial omita referirse a ellos.

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

(Unanimidad 8x0, indicación número 141, y 10x0, indicación número 141 bis).

ARTÍCULO 25

Pasa a ser artículo 23, reemplazado por el que se transcribe a continuación:

“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.”.

(Unanimidad 8x0. Indicación número 143).

ARTÍCULO 26

Pasa a ser artículo 24, sustituido por el siguiente:

"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.".

(Unanimidad 7x0. Indicación número 144).

TÍTULO V

Reemplazar su denominación, para que quede del siguiente modo:

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

(Unanimidad 8x0. Indicación número 147).

ARTÍCULO 27

Pasa a ser artículo 25, reemplazado por el que sigue:

“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.”.

(Unanimidad 8x0. Indicación número 148).

ARTÍCULO 28

Pasa a ser artículo 26, sustituido por el que se indica:

“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.”.

(Unanimidad 8x0. Indicación número 150).

°°°°°

A continuación, incorporar los siguientes artículos 27 y 28, nuevos:

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

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

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

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

(Artículo 27, nuevo, unanimidad 8x0. Indicación número 151, y artículo 121, inciso final, del Reglamento del Senado).

(Artículo 28, nuevo, unanimidad 8x0. Indicación número 152).

°°°°°

ARTÍCULO 29

Consultar en su lugar el que se señala a continuación:

“Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con estos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de estas.

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

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

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 6, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

Adicionalmente, serán considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad;

ii. Los planes de continuidad operacional y planes ante desastres, y

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

(Inciso primero, unanimidad 8x0. Indicaciones números 153, 154, y 155).

(Inciso segundo, unanimidad 8x0. Indicación números 156, y artículo 121, inciso final, del Reglamento del Senado).

(Inciso tercero, unanimidad 8x0. Indicaciones números 157 y 158, y artículo 121, inciso final, del Reglamento del Senado).

(Incisos cuarto y quinto, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 30

Agregar, a continuación de la voz “funcionarios” la expresión “o funcionarias”.

(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 33

Reemplazarlo por el siguiente:

“Artículo 33. De las infracciones. Las sanciones a las infracciones de la presente ley cometidas por instituciones privadas serán las siguientes:

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

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

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

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

Se consideran infracciones graves, las siguientes:

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

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

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

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

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

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

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

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

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

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

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

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

(Unanimidad 8x0. Indicaciones número 159 y 161).

ARTÍCULO 34

Sustituirlo por el que se señala a continuación:

“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.”.

(Unanimidad 9x0. Indicación número 163, y artículo 121, inciso final, del Reglamento del Senado).

°°°°°

Luego, incorporar los siguientes artículos 35, 36 y 37, nuevos:

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

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

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

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

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

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

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

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

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

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

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

Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente.

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

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

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

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

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

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

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

Artículo 37. Responsabilidad del funcionario o funcionaria infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios o funcionarias del organismo público, la responsabilidad administrativa se hará efectiva con sujeción a las normas estatutarias que rijan al organismo en que se produjo la infracción.

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

(Artículo 35, nuevo, unanimidad 9x0. Indicación número 164).

(Artículos 36 y 37, nuevos, unanimidad 10x0. Indicación número 164, y artículo 121, inciso final, del Reglamento del Senado).

°°°°°

ARTÍCULO 35

Pasa a ser artículo 38, sustituido por el que se indica a continuación:

"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.".

(Unanimidad 10x0. Indicación número 165).

ARTÍCULO 36

Pasa a ser artículo 39, reemplazado por el que sigue:

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

En el ejercicio de sus funciones, el Comité deberá:

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

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

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

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

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

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

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

(Unanimidad 10x0. Indicación número 167).

ARTÍCULO 37

Pasa ser artículo 40, consultando en su lugar el siguiente texto:

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

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

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

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

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

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

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

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

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

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

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

(Unanimidad 10x0. Indicación número 169, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 38

Pasa a ser artículo 41.

Inciso segundo

Sustituirlo por el que sigue:

“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.”.

(Unanimidad 10x0. Indicación número 171, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 39

Pasa a ser artículo 42.

Agregar, a continuación de la voz “funcionarios” la expresión “o funcionarias”.

(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO 40

Pasa a ser artículo 43, sustituyendo la expresión “Ministerio del Interior y Seguridad Pública” por “Ministerio encargado de la seguridad pública”.

(Unanimidad 10x0. Indicación número 172).

°°°°°

Luego, intercalar el siguiente Título IX, nuevo:

“Título IX
Órganos autónomos constitucionales”.

(Unanimidad 10x0. Indicación número 173).

°°°°°

°°°°°

A continuación, introducir un artículo 44, nuevo, del tenor que sigue:

“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.”.

(Unanimidad 8x0, indicación número 174, y 10x0, indicación número 174 bis).

°°°°°

TÍTULO IX

Pasa a ser Título X, sin cambios en su denominación.

ARTÍCULO 41

Pasa a ser artículo 45, reemplazado por el que sigue:

“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.”.”.

(Unanimidad 7x0. Indicación número 177).

°°°°°

Luego, incorporar los siguientes artículos 46, 47 y 48, nuevos:

“Artículo 46. Introdúcense las siguientes enmiendas a la ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest:

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

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

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

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

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

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

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

2. Derógase el artículo 16.

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

“h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.”.

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

(Unanimidad 9x0. Indicación número 178).

°°°°°

TÍTULO X

Pasa a ser Título XI, sin cambios en su denominación.

ARTÍCULO PRIMERO TRANSITORIO

Reemplazarlo por el siguiente:

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

1. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

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

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

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

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

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

La individualización del personal traspasado conforme al inciso anterior, se realizará a través de decretos expedidos bajo la fórmula “Por orden del Presidente de la República”, por intermedio del Ministerio del Interior y Seguridad Pública.

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

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

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

(Unanimidad 9x0. Indicación número 179).

ARTÍCULO SEGUNDO TRANSITORIO

Sustituir su denominación por “Artículo segundo”.

Agregar, a continuación de la voz “Director” la expresión “o Directora”, las tres veces que aparece.

(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO TERCERO TRANSITORIO Y ARTÍCULO CUARTO TRANSITORIO

Considerarlos como artículos tercero y cuarto, respectivamente, sin enmiendas.

(Adecuación formal).

ARTÍCULO QUINTO TRANSITORIO

Reemplazarlo por el que sigue:

“Artículo quinto. En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás organismos del Estado

reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de estos, de conformidad a lo dispuesto en el artículo 21, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.”.

(Unanimidad 9x0. Indicación número 182, y artículo 121, inciso final, del Reglamento del Senado).

ARTÍCULO SEXTO TRANSITORIO

Sustituirlo por el que se transcribe a continuación:

“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.”.

(Unanimidad 9x0. Indicación número 184).

ARTÍCULO SÉPTIMO TRANSITORIO

Considerarlo como artículo séptimo.

(Adecuación formal).

°°°°°

Introducir la siguiente disposición transitoria, nueva:

“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.”.

(Unanimidad 9x0. Indicación número 185).

°°°°°

- - -

TEXTO DEL PROYECTO

En virtud de las modificaciones anteriores, el proyecto de ley queda como sigue:

PROYECTO DE LEY:

“TÍTULO I
Disposiciones generales

Artículo 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

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

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

Artículo 2. Definiciones. Para efectos de esta

ley se entenderá por:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20. Operadores de importancia vital: institución pública o privada, identificada como tal por la Agencia de conformidad con esta ley, por prestar algún servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, que depende de las redes y sistemas informáticos, y cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar.

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

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

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

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

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

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

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

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

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

2. Principio de confidencialidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos deberá ser conocida y accedida exclusivamente por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.

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

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

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

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

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

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

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

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

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

TÍTULO II
Obligaciones de ciberseguridad

Párrafo 1°
Servicios esenciales y operadores de importancia vital

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

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

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

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

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

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

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

a) La cantidad de usuarios potencialmente afectados;

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

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

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

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

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

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

h) El daño reputacional que pueda ocasionarse.

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

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

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

Párrafo 2°
Obligaciones de ciberseguridad

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

Asimismo, estas medidas tendrán por objeto la gestión de riesgos asociados a la ciberseguridad y la contención y mitigación del impacto que los incidentes puedan tener sobre la

continuidad operacional, la confidencialidad y la integridad del servicio prestado, de conformidad con lo prescrito en la presente ley.

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

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

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

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

Artículo 6. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales. Todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital, deberán:

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

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, de conformidad a lo que señale el reglamento. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores de los protocolos de ciberseguridad y la aplicación de los mismos, tanto

durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad.

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

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

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

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

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

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

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

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

Artículo 7. Deber de reportar. Todas las instituciones, sean públicas o privadas, e independiente de si son o no operadores de servicios esenciales, con la sola excepción de aquellos que la Agencia hubiere eximido expresamente en sus instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan

tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley.

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

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

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

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

TÍTULO III
De la Agencia Nacional de Ciberseguridad

Párrafo 1°
Objeto, naturaleza y atribuciones

Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

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

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

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

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

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

a) Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.

b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.

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

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

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

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

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

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

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

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

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

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

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

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

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

ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza, respecto de algún hecho cuyo conocimiento estime necesario para el cumplimiento de sus funciones.

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

o) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.

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

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

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

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

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

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

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

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

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

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

Párrafo 2°
Dirección, organización y patrimonio

Artículo 10. Dirección de la Agencia. La dirección y administración superior de la Agencia estará a cargo de un Director **o Directora** Nacional, quien será el jefe superior del Servicio, tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta Dirección Pública establecidas en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.

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

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

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

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

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

e) Ejecutar los actos y celebrar los convenios necesarios para el cumplimiento de los fines de la Agencia. En el ejercicio de

esta facultad, podrá libremente administrar, adquirir y enajenar bienes de cualquier naturaleza;

f) Delegar atribuciones o facultades específicas en los funcionarios y funcionarias que indique;

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

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

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

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

b) Los recursos otorgados por leyes generales o especiales;

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

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

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

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

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

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

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

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

Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

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

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

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

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

desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal.

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

Un reglamento expedido por el ministerio encargado de la seguridad pública, determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

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

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

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

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

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

jornada para compensar las horas durante las cuales no haya podido desempeñar su cargo.

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

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

Párrafo 3°
Consejo Multisectorial sobre Ciberseguridad

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

El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, quienes permanecerán en su cargo durante seis años, renovándose en tríos cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.

Los integrantes del Consejo estarán obligados a presentar una declaración de intereses y patrimonio, en conformidad a lo dispuesto por la ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses, y estarán afectos al principio de abstención contenido en el artículo 12 de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

Artículo 17. Funcionamiento del Consejo. El Consejo sesionará a lo menos cuatro veces al año; sus recomendaciones serán de carácter público, y deberán recoger la diversidad de opiniones existentes en él cuando no haya unanimidad respecto de las mismas. Excepcionalmente y mediante decisión fundada, el Director o Directora podrá decretar secreta o reservada una parte o toda una sesión del

Consejo, de lo cual se deberá dejar constancia en el acta respectiva. En este caso, se aplicará lo dispuesto en el artículo 42.

El Consejo sesionará todas las veces que sea necesario para el cumplimiento de sus funciones. La Agencia prestará el apoyo técnico y administrativo indispensable para el adecuado funcionamiento del Consejo.

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

Artículo 18. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro sesiones consecutivas.

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

El consejero respecto del cual se verificare alguna de las causales de cesación referidas anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.

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

Si quedare vacante el cargo de consejero deberá procederse al nombramiento de uno nuevo de conformidad con el

procedimiento establecido en esta ley. El consejero nombrado en reemplazo durará en el cargo solo por el tiempo que falte para completar el período del consejero reemplazado.

Párrafo 4°
Red de Conectividad Segura del Estado

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

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

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

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

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

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

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

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

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

e) Supervisar incidentes a escala nacional.

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

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

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

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

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

TÍTULO IV
Otras instituciones intervinientes

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

Los CSIRT Sectoriales tendrán las siguientes funciones:

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

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

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

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

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

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

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

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

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

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

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

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

Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las instancias de coordinación entre la Agencia y las autoridades sectoriales y sus respectivos CSIRT.

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

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

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

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

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

a) El número de personas afectadas.

b) La duración del incidente.

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

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

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

El procedimiento específico para notificar un incidente de ciberseguridad, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad, serán establecidos en el reglamento de la presente ley.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 27. De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. En el sector de la defensa nacional se constituirán Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales de la Defensa Nacional, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que

pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional.

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

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

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

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

Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con estos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de estas.

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

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

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 6, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

Adicionalmente, serán considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad;

ii. Los planes de continuidad operacional y planes ante desastres, y

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

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

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

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

TÍTULO VII
De las infracciones y sanciones

Artículo 33. De las infracciones. Las sanciones a las infracciones de la presente ley cometidas por instituciones privadas serán las siguientes:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 1.000 unidades tributarias

mensuales. En caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 5.000 unidades tributarias mensuales.

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

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

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

Se consideran infracciones graves, las siguientes:

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

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

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

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

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

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

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

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

La multa será fijada teniendo en consideración si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del riesgo, la gravedad de los efectos de los ataques, la reiteración en la

infracción dentro del plazo de tres años contados desde el momento en que se produjo el incidente y la capacidad económica del infractor.

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

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

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

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

a) El procedimiento sancionatorio será instruido por la Agencia.

b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Junto con la apertura del expediente, la Agencia deberá designar un funcionario o una funcionaria responsable de la instrucción del procedimiento, que recibirá el nombre de instructor o instructora. En el evento de que producto de una denuncia se iniciare un procedimiento administrativo sancionador, el denunciante tendrá la calidad de interesado, para todos los efectos legales.

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

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

e) La institución privada tendrá un plazo de quince días hábiles para presentar sus descargos. En esa oportunidad, la institución privada podrá acompañar todos los antecedentes que estime

pertinentes para desacreditar los hechos imputados. Junto con los descargos, la institución privada deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones, si no lo hubiere hecho previamente.

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

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

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

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

j) Cumplidos los trámites señalados en los literales anteriores, el instructor o instructora emitirá, dentro de diez días hábiles, un dictamen en el cual propondrá la absolución o la sanción que a su juicio corresponda aplicar. Dicho dictamen deberá contener la individualización del o de los infractores; la relación de los hechos investigados y la forma como se ha llegado a comprobarlos, y la proposición al Director o Directora de las sanciones que estimare procedente aplicar o de la absolución de uno o más de los infractores.

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

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

en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida.

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

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

Artículo 35. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

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

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

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

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

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

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

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

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

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

Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente.

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

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

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

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

Habiéndose configurado la infracción, las sanciones administrativas señaladas en este artículo serán aplicadas por

la Agencia. Con todo, la Contraloría General de la República, a petición de la Agencia podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y proponer las sanciones que correspondan.

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

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

Artículo 37. Responsabilidad del funcionario o funcionaria infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios o funcionarias del organismo público, la responsabilidad administrativa se hará efectiva con sujeción a las normas estatutarias que rijan al organismo en que se produjo la infracción.

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

Artículo 38. Agravante especial. Si como consecuencia de la perpetración de un delito resultare afectada gravemente la continuidad operativa de un operador de importancia vital, se impondrá la pena que corresponda, aumentada en un grado.

Lo mismo se observará cuando el delito consistiere en la alteración o supresión de los datos informáticos relevantes del operador de importancia vital o en la obstaculización del acceso o la alteración perjudicial del funcionamiento de su sistema informático.

TÍTULO VIII
Del Comité Interministerial de Ciberseguridad

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

En el ejercicio de sus funciones, el Comité deberá:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 41. De la secretaría ejecutiva. El Comité contará con una Secretaría Ejecutiva radicada en la Agencia, la que prestará el apoyo técnico, administrativo y de contenidos para el desarrollo de las reuniones del Comité.

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

Artículo 42. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios **o funcionarias** que estén en conocimiento de información reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición.

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

Artículo 43. Del reglamento. Un reglamento expedido por el **Ministerio encargado de la seguridad pública** fijará las normas de funcionamiento del Comité.

Título IX
Órganos autónomos constitucionales

Artículo 44. Regímenes especiales. Corresponderá a las autoridades superiores de los órganos internos del Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral y el Consejo Nacional

de Televisión adoptar las medidas especiales de ciberseguridad señaladas en el artículo 6 de la presente ley, debiendo dictar para ello las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, pudiendo requerir para ello la asistencia técnica de la Agencia Nacional de Ciberseguridad. En este caso, las referencias al reglamento contenidas en el artículo 6, se entenderán efectuadas a las normas que adopten los respectivos órganos internos.

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

Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia. Sin perjuicio de ello, deberán acordar mecanismos de coordinación, cooperación, reporte de incidentes e intercambio de información sobre ciberseguridad, respecto de la Agencia y las demás autoridades o instancias previstas en esta ley, incluyéndose la conformación o participación en equipos de respuesta a incidentes de ciberseguridad. En este contexto, si además fuere requerido el acceso por parte de la Agencia a redes y sistemas informáticos de los referidos órganos, deberá contarse con su autorización previa, debiendo cautelarse para ello la continuidad de sus operaciones. En caso de que los antecedentes que se soliciten o la información a la que se acceda sean confidenciales o reservados, la Agencia deberá conservarlos en ese carácter.

Corresponderá a los señalados órganos determinar e informar a la Agencia sobre su carácter de operador de importancia vital, en los términos del artículo 4, e informarle, con la periodicidad que se acuerde, las infraestructuras, servicios o funciones específicos que se identifiquen en esta condición.

Asimismo, si el órgano autónomo constitucional revistiere además el carácter de autoridad sectorial, deberá considerarse su opinión previa en relación con las personas o entidades reguladas o supervisadas por ella, que pudieren calificarse como operadores de importancia vital.

TÍTULO X

De las modificaciones a otros cuerpos legales

Artículo 45. Incorpórase, en el artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, la siguiente letra k), nueva:

“k) Conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa.”.

Artículo 46. Introdúcense las siguientes enmiendas a la ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest:

1. Incorpórase, en el artículo 2°, los siguientes incisos finales, nuevos:

“No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que se cumplan las siguientes condiciones:

1) Haber reportado el acceso y las vulnerabilidades de seguridad detectadas en su investigación al responsable de las redes y sistemas informáticos afectados, en forma inmediata y a más tardar en el momento en que alerte a la Agencia Nacional de Ciberseguridad;

2) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia Nacional de Ciberseguridad;

3) Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, ex filtración o destrucción de datos, y

4) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad.

Tampoco será objeto de sanción penal la persona que comunique a la Agencia información una vulnerabilidad potencial de la que haya tomado conocimiento en su contexto laboral o con ocasión de la prestación de sus servicios, ni se considerará que ha incumplido con ello su obligación de secreto profesional.”.

2. Derógase el artículo 16.

Artículo 47. Incorpórase, en el artículo 8° de la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia, el siguiente literal h), nuevo:

“h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.”.

Artículo 48. Derógase la letra a) del artículo 8° de la ley N° 7.401, que reprime las actividades que vayan contra la seguridad exterior del Estado.

TÍTULO XI
Disposiciones transitorias

Artículo primero. Entrada en vigencia y personal. Facúltase al Presidente de la República para que en el plazo de un año de publicada en el Diario Oficial la presente ley, establezca mediante uno o más decretos con fuerza de ley expedidos a través del Ministerio del Interior y Seguridad Pública, los que también deberán ser suscritos por el Ministro de Hacienda, las normas necesarias para regular las siguientes materias:

1. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

2. Fijar el sistema de remuneraciones del personal de la Agencia y las normas necesarias para la fijación de las remuneraciones variables, en su aplicación transitoria.

3. Fijar la planta de personal de Directivos de la Agencia, pudiendo al efecto fijar el número de cargos, los requisitos para el desempeño de los mismos, sus denominaciones y los cargos que se encuentren afectos al Título VI de la ley N° 19.882. Además, determinará la fecha de entrada en vigencia de dicha planta.

4. El personal que a la fecha de inicio de actividades de la Agencia se encuentre prestando servicios a honorarios en la Subsecretaría del Interior y cuyo traspaso se determine de conformidad a los incisos tercero y cuarto de este numeral, podrá optar por modificar su estatuto laboral al Código del Trabajo, siempre que cumpla con los requisitos respectivos y otorgue previamente su consentimiento.

En la medida que el personal señalado en el inciso anterior cumpla con los requisitos respectivos y dé su consentimiento, las modificaciones de estatuto laboral señaladas en el inciso precedente deberán incluirse en la dotación máxima de personal del primer presupuesto que se fije para la Agencia.

En el respectivo decreto con fuerza de ley, se determinará la forma y el número de personas a honorarios a traspasar sin solución de continuidad, desde la Subsecretaría del Interior a la Agencia, además, el plazo en que se llevará a cabo este proceso. Conjuntamente con el traspaso del personal, se traspasarán los recursos presupuestarios que se liberen por este hecho y, a su vez, un número equivalente al de los honorarios traspasados deberá ser reducido del número máximo de personas a ser contratadas a honorarios fijado en las glosas presupuestarias correspondientes de la Subsecretaría del Interior.

La individualización del personal traspasado conforme al inciso anterior, se realizará a través de decretos expedidos bajo la fórmula "Por orden del Presidente de la República", por intermedio del Ministerio del Interior y Seguridad Pública.

El personal a honorarios que pase a ser Código del Trabajo de acuerdo a lo señalado en este artículo, mantendrá una remuneración líquida mensualizada que le permita mantener su honorario líquido mensual.

5. Determinar la dotación máxima de personal de la Agencia.

6. Podrá disponer el traspaso, en lo que corresponda, de toda clase de bienes, desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.

Artículo segundo. El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº 19.882, podrá nombrar, a partir de la publicación de la presente ley, al primer Director **o Directora** de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección

Pública. En el acto de nombramiento, el Presidente de la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director **o Directora**, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director **o Directora** se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese solo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal.

Artículo tercero. El Presidente de la República, por decreto supremo expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia Nacional de Ciberseguridad y podrá modificar el presupuesto del Ministerio del Interior y Seguridad Pública. Para los efectos anteriores podrá crear, suprimir o modificar las partidas, capítulos, programas, ítems, asignaciones y glosas presupuestarias que sean pertinentes.

Artículo cuarto. Dentro del plazo de ciento ochenta días posteriores a la publicación de la ley, el Ministerio del Interior y Seguridad Pública deberá expedir los reglamentos señalados en esta ley.

Artículo quinto. En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás organismos del Estado reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de estos, de conformidad a lo dispuesto en el artículo 21, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.

Artículo sexto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 16, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período:

a) Tres consejeros durarán en sus cargos un plazo de tres años.

b) Tres consejeros durarán en sus cargos un plazo de seis años.

Artículo séptimo. El mayor gasto fiscal que represente la aplicación de la presente ley durante su primer año presupuestario de vigencia se financiará con cargo al presupuesto el Ministerio

del Interior y Seguridad Pública. No obstante lo anterior, el Ministerio de Hacienda con cargo a la partida presupuestaria Tesoro Público podrá suplementar dicho presupuesto en la parte del gasto que no pudiere financiar con esos recursos. Para los años siguientes, se financiará de acuerdo con lo determinen las respectivas leyes de Presupuestos del Sector Público.

Artículo octavo. Sobre los servicios esenciales. Hasta que no se dicten los respectivos decretos señalados en el artículo 4 de la ley, serán calificados como servicios esenciales para los efectos de esta ley, los servicios públicos de telecomunicaciones, incluyendo los servicios de transmisión de datos; los servicios de generación, transmisión y distribución eléctrica; los servicios sanitarios y de suministro de agua potable, excluyendo los servicios sanitarios rurales; los servicios bancarios y financieros; las prestaciones de salud, incluyendo cualquier institución pública o privada que realice tratamiento de datos personales de salud, salvo aquellos prestados por municipios o corporaciones municipales; los órganos de la administración del Estado, excluyendo a las municipalidades y gobernaciones provinciales y regionales; el Poder Judicial, y el Poder Legislativo. La Agencia identificará, mediante resolución exenta, los operadores de importancia vital que quedarán sujetos a las obligaciones establecidas en el artículo 6 de esta ley.".

- - -

Acordado en las siguientes sesiones celebradas **los días 29 de noviembre de 2022**, con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, José Miguel Insulza Salinas, Javier Macaya Danús, Manuel José Ossandón Irarrázabal, Kenneth Pugh Olavarría, Jaime Quintana Leal, Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **13 de diciembre de 2022**, con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Rodrigo Galilea Vial (en reemplazo del Honorable Senador Kenneth Pugh Olavarría), José Miguel Insulza Salinas, Manuel José Ossandón Irarrázabal, Jaime Quintana Leal, Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **20 de diciembre de 2022,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), José Miguel Insulza Salinas, Javier Macaya Danús, Manuel José Ossandón Irarrázabal, Kenneth Pugh Olavarría, Jaime Quintana Leal, Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **3 de enero de 2023,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), José Miguel Insulza Salinas, Manuel José Ossandón Irarrázabal, Kenneth Pugh Olavarría, Jaime Quintana Leal, Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **10 de enero de 2023,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), José Miguel Insulza Salinas, Javier Macaya Danús, Manuel José Ossandón Irarrázabal, Kenneth Pugh Olavarría, Jaime Quintana Leal (también en

reemplazo del Honorable Senador señor Pedro Araya Guerrero), Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **17 de enero de 2023,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, José Miguel Insulza Salinas, Javier Macaya Danús, Manuel José Ossandón Irarrázabal, Kenneth Pugh Olavarría, Jaime Quintana Leal, Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **24 de enero de 2023,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, José Miguel Insulza Salinas, Javier Macaya Danús, Kenneth Pugh Olavarría (también en reemplazo del Honorable Senador señor Manuel José Ossandón Irarrázabal), Gastón Saavedra Chandía y Enrique Van Rysselberghe Herrera; **7 de marzo de 2023,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Javier Macaya Danús, Manuel José Ossandón Irarrázabal, Kenneth Pugh Olavarría, Gastón Saavedra Chandía (también en reemplazo del Honorable Senador señor José Miguel Insulza Salinas) y Enrique Van Rysselberghe Herrera; **21 de marzo de 2023,** con asistencia de los Honorables Senadores señores Kenneth Pugh Olavarría (Presidente) (también en reemplazo del Honorable Senador señor Manuel José Ossandón Irarrázabal), Pedro Araya Guerrero, Luciano Cruz-Coke Carvallo, Felipe Kast Sommerhoff (también en reemplazo del Honorable Senador señor Javier Macaya Danús) y Alejandro Kuzanovic Glusevic, señora Yasna Provoste Campillay (también en reemplazo del Honorable Senador señor Iván Flores García) y señor Gastón Saavedra Chandía (en reemplazo del Honorable Senador señor José Miguel Insulza Salinas); **4 de abril de 2023,** con asistencia de los Honorables Senadores señores Kenneth Pugh Olavarría (Presidente), Luciano Cruz-Coke Carvallo (también en reemplazo del Honorable Senador señor Felipe Kast Sommerhoff), Alejandro Kuzanovic Glusevic, Javier Macaya Danús y Manuel José Ossandón Irarrázabal, señora Yasna Provoste Campillay (también en reemplazo del Honorable Senador señor Iván Flores García) y señor Gastón Saavedra Chandía (en reemplazo del Honorable Senador señor José Miguel Insulza Salinas), **y 18 de abril de 2023,** con asistencia de los Honorables Senadores señores Kenneth Pugh Olavarría (Presidente), Pedro Araya Guerrero, Luciano Cruz-Coke Carvallo (también en reemplazo del Honorable Senador señor Felipe Kast Sommerhoff), Alejandro Kuzanovic Glusevic, Javier Macaya Danús y Manuel José Ossandón Irarrázabal, señora Yasna Provoste Campillay (también en reemplazo del Honorable Senador señor Iván Flores García) y señor José Miguel Insulza Salinas.

Valparaíso, a 20 de abril de 2023.


MILENA KARELOVIC RÍOS
Abogada Secretaria

RESUMEN EJECUTIVO

SEGUNDO INFORME DE LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS, RECAÍDO EN EL PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL, QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN (BOLETÍN N° 14.847-06).

I. OBJETIVO DEL PROYECTO PROPUESTO POR LAS COMISIONES UNIDAS: establecer la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, formar una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

II. ACUERDOS: Indicaciones:

Número 1: Retirada.
Número 2: Aprobada con enmiendas (8x0).
Número 3: Aprobada con enmiendas (7x0).
Número 4: Retirada.
Número 5: Aprobada (9x0).
Número 6: Aprobada con enmiendas (7x0).
Número 7: Aprobada con enmiendas (7x0).
Número 8: Aprobada con enmiendas (8x0).
Número 9: Rechazada (8x0).
Número 10: Aprobada con enmiendas (8x0).
Número 11: Aprobada (8x0).
Número 12: Rechazada (8x0).
Número 13: Aprobada (9x0).
Número 14: Retirada.
Número 15: Aprobada (8x0).
Número 16: Aprobada (8x0).
Número 17: Aprobada (8x0).
Número 18: Aprobada (7x0).
Número 19: Retirada.
Número 20: Retirada.
Número 21: Rechazada (7x0).
Número 22: Aprobada con enmiendas (7x0).
Número 23: Aprobada (7x0).
Número 24: Aprobada con enmiendas (7x0).
Número 25: Aprobada (7x0).
Número 26: Aprobada (7x0).
Número 27: Aprobada (7x0).
Número 28: Aprobada con enmiendas (7x0).
Número 29: (referida a definiciones)
Amenaza persistente avanzada (APT): Rechazada (7x0).
Anonimización: Rechazada (8x0).
Auditorías de seguridad: Aprobada con enmiendas (8x0).
Ciberhigiene: Aprobada con enmiendas (8x0).
Confianza digital: Rechazada (8x0).

Integridad: Aprobada con enmiendas (8x0).
Interagencialidad: Aprobada con enmiendas (8x0).
interoperabilidad: Aprobada con enmiendas (8x0).
Registro de proveedores de servicios de seguridad: Rechazada (8x0).
Sistema de Gestión de la Seguridad y Riesgo de la Información (SGSRI): Aprobada con enmiendas (8x0).
Trazabilidad: Rechazada (8x0).

Número 30: Retirada.
Número 31: Aprobada con enmiendas (8x0).
Número 32: Aprobada con enmiendas (8x0).
Número 33: Aprobada con enmiendas (8x0).
Número 34: Aprobada con enmiendas (8x0).
Número 35: Aprobada con enmiendas (9x0).
Número 36: Aprobada (9x0).
Número 37: Rechazada (9x0).
Número 38: Aprobada (9x0).
Número 38 bis: Aprobada (10x0).
Número 39: Aprobada (9x0).
Número 40: Rechazada (9x0).
Número 41: Rechazada (9x0).
Número 42: Aprobada (9x0).
Número 42 bis: Aprobada (10x0).
Número 43:

Principio de confianza cero: Rechazado (9x0).
Principio de actualización y reutilización: Aprobado con enmiendas (9x0).
Principio de cooperación: Rechazado (9x0).
Principio de interoperabilidad: Rechazado (9x0).
Principio de no obsolescencia tecnológica): Rechazado (6x1 abstención).

Numero 43 bis: Aprobada (10x0).
Número 44: Rechazada (7x0).
Número 45: Aprobada (7x0).
Número 45: Aprobada (7x0).
Número 46: Aprobada (7x0).
Número 47: Aprobada con enmiendas (7x0).
Número 48: Retirada.
Número 49: Retirada.
Número 50: Retirada.
Número 51: Aprobada (7x0).
Número 52: Aprobada con enmiendas (7x0).
Número 53: Aprobada (7x0).
Número 54: Rechazada (7x0).
Número 55: Aprobada con enmiendas (8x0).
Número 55 bis: Aprobada (10x0).
Número 56: Aprobada (8x0).
Número 57: Aprobada con enmiendas (7x0).
Número 58: Aprobada (7x0).
Número 59: Aprobada con enmiendas (8x0).
Número 60: Aprobada (8x0).
Número 61: Aprobada (8x0).

Número 61 bis: Aprobada (10x0).
Número 62: Aprobada (8x0).
Número 63: Aprobada (8x0).
Número 64: Aprobada (8x0).
Número 65: Aprobada (8x0).
Número 66: Aprobada con enmiendas (8x0).
Número 67: Aprobada (8x0).
Número 68: Aprobada con enmiendas (8x0).
Número 69: Aprobada con enmiendas (8x0).
Número 70: Aprobada con enmiendas (8x0).
Número 71: Aprobada (8x0).
Número 72: Aprobada (8x0).
Número 73: Aprobada con enmiendas (8x0).
Número 74: Retirada.
Número 75: Rechazada (9x0).
Número 76: Aprobada (8x0).
Número 77: Rechazada (7x1 abstención).
Número 78: Aprobada con enmiendas (8x0).
Número 79: Retirada.
Número 80: Aprobada (8x0).
Número 81: Aprobada (8x0).
Número 82: Aprobada (8x0).
Número 83: Aprobada (8x0).
Número 84: Aprobada (8x0).
Número 85: Retirada.
Número 86: Aprobada (8x0).
Número 87: Aprobada con enmiendas (8x0).
Número 88: Aprobada (8x0).
Número 89: Aprobada (8x0).
Número 90: Aprobada (8x0).
Número 91: Retirada.
Número 92: Aprobada con enmiendas (8x0).
Número 93: Rechazada (10x0).
Número 94: Aprobada con enmiendas (10x0).
Número 94 bis: Aprobada (10x0).
Número 95: Aprobada con enmiendas (7x0).
Número 95 bis: Aprobada (10x0).
Número 96: Rechazada (7x0).
Número 97: Aprobada (7x0).
Número 98: Retirada.
Número 99: Letra p) propuesta: Aprobada (10x0).
Letra q) propuesta: Aprobada (10x0).
Letra r) propuesta: Aprobada (10x0).
Letra s) propuesta: Aprobada con enmiendas (10x0).
Letra t) propuesta: Aprobada (10x0).
Letra u) propuesta: Aprobada con enmiendas (10x0).
Letra v) propuesta: Aprobada (10x0).
Letra w) propuesta: Aprobada (10x0).
Número 100: Rechazada (9x0).
Número 101: Primera atribución propuesta: Aprobada (10x0).
Segunda atribución propuesta: Rechazada (10x0).
Tercera atribución propuesta: Rechazada (10x0).

Número 101 bis: Aprobada (10x0).
Número 102: Aprobada (10x0).
Número 103: Aprobada (10x0).
Número 104: Retirada.
Número 105: Aprobada con enmiendas (9x0).
Número 106: Aprobada (10x0).
Número 107: Aprobada con enmiendas (9x0).
Número 107 bis: Aprobada (10x0).
Número 108: Rechazada (8x1 abstención).
Número 109: Aprobada con enmiendas (9x0).
Número 109 bis: Aprobada (10x0).
Número 110: Aprobada (9x0).
Número 111: Aprobada (9x0).
Número 112: Retirada.
Número 113: Retirada.
Número 114: Retirada.
Número 115: Aprobada (9x0).
Número 116: Todo el artículo 16 propuesto, con excepción de la oración final de su inciso segundo: Aprobado con enmiendas (10x0). Oración final del inciso segundo del artículo propuesto: Rechazada (7x3 a favor).
Número 117: Aprobada (10x0).
Número 118: Aprobada con enmiendas (7x0).
Número 119: Aprobada con enmiendas (10x0).
Número 119 bis: Aprobada (10x0).
Número 120: Aprobada con enmiendas (10x0).
Número 121: Aprobada con enmiendas (10x0).
Número 122: Retirada.
Número 123: Aprobada con enmiendas (10x0).
Número 124: Retirada.
Número 125: Retirada.
Número 126: Aprobada (10x0).
Número 127: Aprobada (10x0).
Número 128: Aprobada (9x1 en contra).
Número 129: Retirada.
Número 130: Retirada.
Número 131: Aprobada (10x0).
Número 132: Aprobada (10x0).
Número 133: Retirada.
Número 134: Retirada.
Número 135: Aprobada (10x0).
Número 136: Aprobada (10x0).
Número 137: Retirada.
Número 138: Retirada.
Número 139: Aprobada (10x0).
Número 140: Aprobada con enmiendas (8x0).
Número 140 bis: Aprobada (10x0).
Número 141: Aprobada con enmiendas (8x0).
Número 141 bis: Aprobada (10x0).
Número 142: Retirada.
Número 143: Aprobada con enmiendas (8x0).
Número 144: Aprobada con enmiendas (7x0).
Número 145: Retirada.

Número 146: Retirada.
Número 147: Aprobada (8x0).
Número 148: Aprobada (8x0).
Número 149: Rechazada (8x0).
Número 150: Aprobada (8x0).
Número 151: Aprobada (8x0).
Número 152: Aprobada (8x0).
Número 153: Aprobada con enmiendas (8x0).
Número 154: Aprobada (8x0).
Número 155: Aprobada (8x0).
Número 156: Aprobada (8x0).
Número 157: Aprobada con enmiendas (8x0).
Número 158: Aprobada (8x0).
Número 159: Aprobada con enmiendas (8x0).
Número 160: Rechazada (8x0).
Número 161: Aprobada con enmiendas (8x0).
Número 162: Retirada.
Número 163: Aprobada con enmiendas (9x0).
Número 164: Artículo 35 propuesto: Aprobado con enmiendas (9x0).
Artículo 36 propuesto: Aprobado con enmiendas (10x0).
Artículo 37 propuesto: Aprobado con enmiendas (10x0).
Número 165: Aprobada (10x0).
Número 166: Retirada.
Número 167: Aprobada (10x0).
Número 168: Rechazada (10x0).
Número 169: Aprobada (10x0).
Número 170: Rechazada (10x0).
Número 171: Aprobada (10x0).
Número 172: Aprobada (10x0).
Número 173: Aprobada (10x0).
Número 174: Aprobada con enmiendas (8x0).
Número 174 bis: Aprobada (10x0).
Número 175: Aprobada con enmiendas (7x0).
Número 176: Retirada.
Número 177: Aprobada (7x0).
Número 178: Artículo 46, N° 1: Aprobado con enmiendas (9x0).
Artículo 46, N° 2: Aprobado (9x0).
Artículo 47: Aprobado (9x0).
Artículo 48: Aprobado (9x0).
Número 179: Aprobada con enmiendas (9x0).
Número 180: Rechazada (9x0).
Número 181: Retirada.
Número 182: Aprobada (9x0).
Número 183: Retirada.
Número 184: Aprobada (9x0).
Número 185: Aprobada con enmiendas (9x0).

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN: consta de 48 artículos permanentes y de 8 disposiciones transitorias.

IV. NORMAS DE QUÓRUM ESPECIAL:
A. Normas orgánicas constitucionales:

1) Según el artículo 38 de la Constitución Política de la República, en relación con el artículo 66, inciso segundo, del mismo Texto Supremo:
- Artículos 1, inciso segundo; 8; 9 letras a), b), c), d), e), i), m), n), ñ), v); x); 10; 13; 14; 16 (su inciso tercero en virtud de lo dispuesto en el artículo 8°, inciso tercero de la Carta Fundamental); 20; 21; 25; 26; 34; 36; 37; 39; 40; 41; 44 y 45.
- Artículos segundo; quinto y sexto de las disposiciones transitorias.

2) Según el artículo 99, inciso final, de la Carta Fundamental:
- Artículo 4, inciso final y artículo octavo de las disposiciones transitorias.

3) Según el artículo 77 de la Constitución Política de la República:
- Artículo 35.

B. Normas de quórum calificado, de conformidad al artículo 8°, inciso segundo, y 66, inciso segundo, ambos de la Carta Fundamental:

Artículos 29; 30; 31 y 42.

V. URGENCIA: discusión inmediata.

VI. ORIGEN INICIATIVA: Senado. Mensaje de S.E. el ex Presidente de la República, señor Sebastián Piñera Echenique.

VII. TRÁMITE CONSTITUCIONAL: primero.

VIII. INICIO TRAMITACIÓN EN EL SENADO: 15 de marzo de 2022.

IX. TRÁMITE REGLAMENTARIO: segundo informe.

XI. LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: 1.- Constitución Política de la República. 2.- Código del Trabajo. 3.- Código Penal. 4.- Decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.834, sobre Estatuto Administrativo. 5.- Decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado. 6.- Ley N° 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del consumo de drogas y alcohol, y modifica diversos cuerpos legales. 7.- Decreto 2.421, de 1964, del Ministerio de Hacienda, que fija el texto refundido de la ley de organización y atribuciones de la Contraloría General de la República. 8.- Ley N° 20.416, que fija normas especiales para las empresas de menor tamaño. 9.- Ley N° 21.000, que crea la Comisión para el Mercado Financiero. 10.- Ley N° 21.105, que crea el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. 11.- Ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional. 12.- Ley N° 21.180, sobre transformación digital del Estado. 13.- Ley N° 20.285, sobre

acceso a la información pública. 14.- Ley N° 19.882, que regula nueva política de personal a los funcionarios públicos que indica. 15.-Ley N° 19.628, sobre protección de la vida privada. 16.- Ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia. 17.- Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado. 18.- Ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses. 19.- Ley N° 7.401, que reprime las actividades que vayan contra la seguridad exterior del estado. 20.- Decreto con fuerza de ley N° 1, de 1993, del Ministerio de Hacienda, fija el texto refundido, coordinado y sistematizado de la ley orgánica del Consejo de Defensa del Estado. 21.- Decreto con fuerza de ley N° 262, de 1977, del Ministerio de Hacienda, que aprueba el reglamento de viáticos para el personal de la administración pública. 22.- Decreto supremo N° 1, de 1991, del Ministerio de Hacienda, que fija monto de viáticos en dólares para el personal que debe cumplir comisiones de servicio en el extranjero. 23.- Decreto ley N° 1.263, de 1975, de administración financiera del Estado. 24.- Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest). 25.- Ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. 26.- Ley N° 21.113, que declara el mes de octubre como el de la ciberseguridad. 27.- Ley N° 18.168, general de telecomunicaciones. 28.- Decreto N° 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad. 29.- Instructivo Presidencial 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad. 30.- Decreto N° 3, de 2018, del Ministerio de Defensa Nacional, que aprueba la Política de Ciberdefensa. 31.- Ley N° 21.130, que moderniza la legislación bancaria. 32.- Ley N° 20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet. 33.- Decreto N° 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, reglamento para la interoperación y difusión de mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones. 34.- Decreto supremo N° 83, promulgado en 2004 y publicado en 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

Valparaíso, a 20 de abril de 2023.

ÍNDICE