INFORME DE LA COMISIÓN DE DEFENSA NACIONAL 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.

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

HONORABLE SENADO:

La Comisión de Defensa Nacional tiene 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.

Esta proposición legal debe ser conocida, enseguida, por la Comisión de Seguridad Pública. Posteriormente, durante el segundo trámite reglamentario, deberá ser analizada por la Comisión de Hacienda, en su caso, según la tramitación acordada por la Sala.

Se hace presente que, de conformidad a lo dispuesto en el artículo 36 del Reglamento de la Corporación, la Comisión discutió solo en general esta iniciativa de ley, la que resultó aprobada por la unanimidad de sus miembros (5X0).

\- - -

OBJETIVOS DEL PROYECTO

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

\- - -

CONSTANCIAS

- Normas de quórum especial: sí tiene.

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

\- - -

- - -

NORMAS DE QUÓRUM ESPECIAL

A. Normas orgánicas constitucionales, según el artículo 38 de la Constitución Política de la República, en relación con el artículo 66, inciso segundo, del mismo Texto Supremo:

- Artículos 8; 9 letras a), b), d), h), l) y m); 10; 13; 17; 22; 23; 24 letra b); 27; 28; 34; 36; 37; 38 y 41, permanentes.

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

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

- Artículos 16; 29; 30; 31 y 39, permanentes.

- - -

ASISTENCIA

- Senadores y Diputados no integrantes de la Comisión: Honorable Senadora señora Ximena Órdenes.

- Representantes del Ejecutivo e invitados: del Ministerio del Interior y Seguridad Pública: la exministra, señora Izkia Siches.

De la Subsecretaría de Defensa: el exsubsecretario, señor Fernando Ayala.

De la Subsecretaría de Telecomunicaciones: el Subsecretario, señor Claudio Araya.

De Carabineros de Chile: el General Subdirector, General Inspector, señor Esteban Díaz.

De la Policía de Investigaciones de Chile: el Jefe Nacional de Gestión Estratégica, Prefecto, señor Erick Menay.

El exsubsecretario de Telecomunicaciones, señor Jorge Atton.

El exsubsecretario de Telecomunicaciones y docente del Centro de Investigación en Ciberseguridad de la Universidad Mayor, señor Pedro Huichalaf.

De la Cámara Chilena de Infraestructura Digital: la Directora Ejecutiva, señora Corina Gómez.

El profesor de Derecho Informático de la Pontificia Universidad Católica de Valparaíso, señor Renato Jijena.

La profesora de la Universidad Adolfo Ibáñez, señora Romina Garrido.

El profesor de la Universidad del Desarrollo, señor Juan Pablo González.

El experto internacional en seguridad cibernética, señor Israel Reyes.

Del Comité Chileno del Consejo Internacional de Grandes Redes Eléctricas: el Coordinador de Ciberseguridad en Sistemas Eléctricos, señor Eduardo Morales.

De la Fundación País Digital: el Presidente, señor Pelayo Covarrubias.

- Otros: del Ministerio del Interior y Seguridad Pública: la ex Jefa de Gabinete de la exministra, señora Ana Lya Uriarte; la ex Jefa de Comunicaciones, señora Vanessa Azócar; la asesora legislativa, señora Leslie Sánchez, y el ex asesor legislativo, señor Tomás Razazi.

De la Subsecretaría de Defensa: el Jefe de la División de Desarrollo Tecnológico e Industria, señor Yerko Benavides, y el exasesor, señor Gonzalo Díaz de Valdés.

De Carabineros de Chile: el Jefe de Gabinete Técnico de la Subdirección General, Coronel, señor Jorge Montre; el Director de la Dirección de Tecnología, Información y Comunicaciones, Coronel, señor Enrique Villarroel, y el encargado de ciberseguridad, señor Jonathan Ponce.

De la Policía de Investigaciones de Chile: el Jefe de la Brigada Congreso Nacional, Subprefecto, señor Rodrigo Carreño, y la ayudante de la Jefatura Nacional de Gestión Estratégica, Comisario, señora Paulina González.

- Asesores parlamentarios: del Honorable Senador señor Araya, señor Pedro Lezaeta; del Honorable Senador señor Macaya, señor Carlos Oyarzún; del Honorable Senador señor Pugh, señores Pascal de Smet d´Olbecke y Michael Heavey, y del Comité Unión Demócrata Independiente, señora María Teresa Urrutia.

- - -

- - -

ANTECEDENTES DE HECHO

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

I. Antecedentes

El mensaje que da origen a esta iniciativa pone de relieve que las tecnologías emergentes de la sociedad digital han generado un cambio cultural amplio, el que se ha acelerado y ahondado en el contexto de diversas medidas sanitarias -como el confinamiento-, producto de la pandemia del COVID-19. Así, previene, se ha alterado la forma de ser y estar en el mundo.

En este escenario, asegura que ha sido indispensable que el Estado profundice su transformación digital. Esta, recuerda, comenzó con la publicación de la ley Nº 21.180, el año 2019, y ha continuado con el decreto supremo Nº 4, del Ministerio Secretaría General de la Presidencia, promulgado en 2020 y publicado en 2021, el cual contiene el reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en el texto legal anteriormente mencionado. Señala que reflejo de ello es, asimismo, el decreto con fuerza de ley N° 1, del Ministerio Secretaría General de la Presidencia, de igual fecha, que establece normas de aplicación del artículo 1° de la ley N° 21.180, respecto de los procedimientos administrativos regulados en leyes especiales que se expresan a través de medios electrónicos y determina la gradualidad para la aplicación de la misma ley a los órganos de la Administración del Estado que indica y las materias que les resulten aplicables.

Esta modernización, sostiene, es una tarea incesante y permanente, enmarcada dentro del principio consagrado en el artículo 1° de la Carta Fundamental, conforme al cual el Estado está al servicio de las personas. Asevera que los pasos encaminados a robustecer el acceso a diversos servicios públicos mediante canales digitales deben ir acompañados de garantías para que dichas prestaciones sean entregadas con los resguardos y estándares de seguridad necesarios.

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

Manifestaciones concretas de lo anterior, precisa, se encuentran en numerosas plataformas que proveen acceso a trámites que tradicionalmente debían realizarse de forma presencial, como la Comisaría Virtual o las solicitudes de beneficios estatales por medio de la Clave Única.

Sin embargo, advierte que esta evolución implica enfrentar desafíos en distintos ámbitos, como los relativos al área de la tecnología y aquellos referidos a habilidades relacionales y al analfabetismo digital, pero, además, subraya, obliga a afrontar retos en materia de ciberseguridad, lo que requiere convergencia, coordinación y articulación público-privada para la gestión de alertas preventivas y de incidentes de dicha índole.

Para el adecuado funcionamiento de la seguridad informática en el país, afirma, es imprescindible administrar los riesgos y poner en marcha los más exigentes estándares que otorguen confianza y certeza, tanto en las instituciones públicas como privadas. Para esto, acota, se requiere planificación, implementación, seguimiento y evaluación constante en el desarrollo de la ciberseguridad, con un marco integrado que considere una nueva visión de lo multisectorial y transectorial, enfatizando el trabajo conjunto de los sectores mencionados, para beneficio mutuo y general.

Esta mirada, declara, prioriza la colaboración y la coordinación, permitiendo la labor mancomunada de todos los actores, tanto locales como globales, valorando el importante rol de la ciencia, la tecnología y la investigación en la ciberseguridad.

El vertiginoso desarrollo de la sociedad digital, hace ver, conlleva un mayor riesgo de vulnerabilidad en todas las estructuras, pero especialmente en aquellos sectores estratégicos donde existe infraestructura crítica de la información.

Por este motivo, explica, el proyecto establece el marco regulatorio para el desarrollo robusto de la seguridad informática, tanto en su dimensión operativa como regulatoria.

II. Fundamentos

1. Relevancia de la ciberseguridad

El mensaje destaca que la ciberseguridad es un tema recurrente en la discusión pública. Ello, ahonda, porque en una sociedad que transita desde los soportes físicos hacia la infraestructura de la información, el permanente peligro de incidentes y ciberataques comienza a formar parte de los elementos que deben considerarse. En este sentido, sentencia, la gestión del riesgo y el control de la vulnerabilidad son elementos de suyo relevantes.

Recalca que la seguridad es clave en el período de adaptabilidad para la aplicación y el desarrollo de tecnologías, como la inteligencia artificial, en los diversos procesos socio-relacionales, en la generación de servicios y las cadenas productivas. Sin embargo, connota, toda esa potencialidad se puede transformar en amenaza si no se adoptan los estándares de una cultura de ciberseguridad, con enfoque colaborativo y sistémico.

En ese marco, apunta que la Administración del ex Presidente de la República, señor Sebastián Piñera, asumió el compromiso de abordar esta temática en su programa de Gobierno para embarcar al país en la revolución tecnológica, y estableció dentro de sus objetivos la creación de condiciones para que Chile pueda insertarse, exitosamente y de manera protagónica, en la cuarta revolución industrial. Con tal objetivo, detalla, se propuso adaptar las regulaciones a los desafíos impuestos, contemplando el desarrollo de políticas de ciberseguridad. De esta forma, con el proyecto de ley se procura llevar adelante esas políticas y, al mismo tiempo, dar cumplimiento a las medidas que dispone la Política Nacional de Ciberseguridad.

2. Relevancia de la institucionalidad en materia de ciberseguridad

Con posterioridad, el ex Primer Mandatario pone de manifiesto que Chile precisa con urgencia una institucionalidad en ciberseguridad para coordinar esfuerzos que permitan enfrentar nuevos retos, atendido el uso masivo y extensivo de las tecnologías. Alerta que este es un problema de creciente importancia que se mantendrá y agudizará en el futuro, debido al acelerado despliegue de infraestructura digital.

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

En este contexto, insiste, el país demanda una institucionalidad pública coordinadora, capaz de prevenir los delitos informáticos y proteger los activos referidos.

Adicionalmente, prosigue, se necesita una gobernanza clara y una orgánica definida en sus roles, con amplias competencias, tecnológicamente robusta, confiable, de interacción nacional y global, altamente profesional, eficiente en su gestión y experimentada.

III. Objetivo del proyecto de ley

Expone que la iniciativa de ley tiene como propósito establecer la institucionalidad para robustecer la ciberseguridad; ampliar y fortalecer el trabajo preventivo; formar una cultura pública en materia de seguridad digital; enfrentar las contingencias y resguardar la seguridad de las personas en el ciberespacio.

En virtud de lo anterior, nota, a través de esta proposición legal:

- Se protegerá al Estado, sus redes y los sistemas informáticos e infraestructura de la información del sector público, especialmente aquellas que son esenciales y críticas para los ciudadanos;

- Se resguardará la Seguridad Nacional;

- Se prevendrán ciberamenazas, al mejorar las instancias de comunicación, coordinación y colaboración entre diversas instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos que se originan en el ciberespacio, y

- Se gestionarán los peligros del espacio virtual, lo que permitirá identificar las vulnerabilidades, amenazas y riesgos en el uso, procesamiento, almacenamiento y transmisión de la información. Para ello, especifica, se procurará generar las capacidades para la prevención, mitigación y efectiva y pronta recuperación ante incidentes que afecten a instituciones que posean infraestructura crítica de la información.

IV. Contenido del proyecto de ley

Luego, describe que la iniciativa de ley se estructura en base a diez títulos, con cuarenta y un artículos permanentes y siete disposiciones transitorias.

Comunica que el ámbito de aplicación de la proposición legal serán los órganos de la Administración del Estado; los demás de carácter público, y las instituciones privadas que posean infraestructura crítica de la información. Añade que esta propuesta de ley establece un marco normativo en materia de ciberseguridad, responsabilidades y deberes asociados para las entidades referidas, considerando requisitos mínimos para la prevención y resolución de incidentes de ciberseguridad y contingencias. En particular, ahonda, consagra lo siguiente:

1. Título I

Contiene las disposiciones generales, definiendo el objeto del proyecto y fijando ciertas definiciones y principios rectores, entendiendo estos últimos como aquellos criterios normativos de aplicación general que cumplen, además, una función integradora e interpretativa, determinando el sentido y alcance del texto en su conjunto.

2. Título II

Se divide en dos párrafos, los cuales consagran la forma de especificación de la infraestructura crítica de la información y las obligaciones de las instituciones que la posean.

Para considerar como crítica una infraestructura de la información, se contemplan diversos factores que posibilitarán realizar dicha calificación, tales como el impacto de una posible interrupción o mal funcionamiento de los componentes; la capacidad del sistema informático para ser sustituido o reparado en un corto tiempo; las pérdidas financieras potenciales por fallas o ausencia del servicio a nivel nacional o regional asociada al producto interno bruto (PIB), y la afectación relevante del funcionamiento del Estado y sus órganos.

Pormenoriza que el Ministerio del Interior y Seguridad Pública, mediante la dictación de un decreto supremo, señalará aquellos sectores o instituciones que constituyen servicios esenciales, según lo dispuesto en esta iniciativa y que, por lo tanto, tienen este tipo de activos.

Además, se dispone que 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.

Adicionalmente, da a conocer, se regulan los deberes generales de los órganos del Estado cuya infraestructura de la información sea calificada como tal.

Por último, indica que este título prescribe las facultades normativas de los fiscalizadores sectoriales, brindándoles la facultad para dictar instrucciones, circulares, órdenes, normas técnicas y de carácter general, las que deberán tener a la vista los estándares establecidos por la Agencia Nacional de Ciberseguridad.

3. Título III

El ex Primer Mandatario hace saber que esta parte de la propuesta legal crea y regula 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 es asesorar al Presidente de la República en asuntos propios de ciberseguridad; colaborar en la protección de los intereses nacionales en el ciberespacio; coordinar el actuar de las instituciones con competencia en la materia, 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 fiscalizador sectorial.

Agrega que la Agencia se relacionará con el Jefe de Estado por intermedio del Ministerio del Interior y Seguridad Pública, y que tendrá su domicilio en la ciudad de Santiago, sin perjuicio de contar con oficinas en otras regiones del país.

Entre las atribuciones de la Agencia Nacional de Ciberseguridad, adelanta, destacan: asesorar al Presidente de la República en el análisis y definiciones de la política nacional de ciberseguridad, así como en los planes y programas de acción específicos para su ejecución y cumplimiento. Además, podrá dictar normas técnicas de carácter general y estándares mínimos de ciberseguridad, y coordinar 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 sectorial.

Hace presente que la dirección y administración de la Agencia estará a cargo de un Director Nacional, quien será el jefe superior del servicio, y que esta institución estará afecta al Sistema de Alta Dirección Pública.

Por otro lado, informa que la iniciativa crea el Registro Nacional de Incidentes de Ciberseguridad, de carácter reservado. Puntualiza que en él se ingresarán los datos técnicos y antecedentes para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. Previene que sobre la base de este inventario se podrán efectuar las respetivas investigaciones, así como comunicar las alertas a CSIRT Sectoriales, a los órganos del Estado y a las instituciones que posean infraestructura de la información calificada como crítica.

A continuación, señala que este título crea y regula el Consejo Técnico de la Agencia Nacional de Ciberseguridad, el cual tiene por finalidad 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.

Pone de relieve que también se establece el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, denominado “CSIRT Nacional”, el cual tendrá entre sus funciones responder ante casos 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 fiscalizador sectorial y que posean infraestructura crítica de la información; coordinar a los CSIRT Sectoriales y prestarles colaboración técnica; servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes, y 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 Nacional de Incidentes de Ciberseguridad, entre otras.

4. Título IV

El mensaje manifiesta que en este título se regulan los Equipos de Respuesta a Incidentes de Seguridad Informáticos Sectoriales “CSIRT Sectoriales” que podrán constituirse por los reguladores o fiscalizadores sectoriales, con el objeto de 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.

En cuanto a la relación entre la Agencia Nacional de Ciberseguridad y los CSIRT Sectoriales, asegura, se contemplan deberes de información. Así, la Agencia dará a conocer a cada CSIRT Sectorial los reportes o alarmas de incidentes y los planes de acciones sugeridos para subsanar dichas brechas de ciberseguridad. Del mismo modo, prosigue, cada CSIRT Sectorial deberá avisar a su sector regulado de manera anonimizada los reportes de incidentes de ciberseguridad, vulnerabilidades existentes y de los cursos de acción tomados en cada caso.

A su vez, subraya, 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 y el plan de acción que adoptó en un plazo no superior a 24 horas, prorrogable, por una sola vez por el mismo período, contado desde que se tuvo conocimiento de su ocurrencia.

Menciona que los CSIRT Sectoriales deberán comunicar a más tardar una hora después de haber verificado la existencia de un incidente de ciberseguridad, cuando este ha tenido un impacto significativo en el sistema de una institución que tiene infraestructura de la información calificada como crítica o en la continuidad de un servicio esencial. Clarifica que para estos efectos, se considera que un incidente de ciberseguridad tiene impacto significativo, cuando cumple al menos una de las siguientes condiciones: 1) afecta a una gran cantidad de usuarios; 2) supone la interrupción o mal funcionamiento de larga duración; 3) abarca una extensión geográfica considerable; 4) incide en sistemas de información que contengan datos personales o, 5) repercute, significativamente, en la integridad física, la salud o la vida cotidiana de las personas.

5. Título V

Esta parte de la iniciativa de ley crea y regula el CSIRT de Gobierno y el CSIRT de Defensa, siendo el primero el responsable de la prevención, contención, protección, detección y recuperación de los sistemas y respuesta asociados a instalaciones, redes, sistemas, plataformas, servicios y equipos

físicos y de tecnología de la información del Estado. El segundo, en tanto, perteneciente al Estado Mayor Conjunto del Ministerio de Defensa Nacional, es el órgano responsable de la coordinación y protección de la infraestructura de la información calificada como crítica de dicho sector.

6. Título VI

Conforme a lo prescrito en el mensaje, este título norma la reserva de la información, la que se considerará secreta y de circulación restringida para todos los efectos legales respecto de aquellos antecedentes, datos, informaciones y registros que obren en poder de los CSIRT o de su personal. La obligación de reserva se extiende a todos quienes, sin ser funcionarios de la Agencia Nacional de Ciberseguridad, 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.

Consigna, además, que la Agencia cautelará especialmente la reserva de los secretos o información comercial sensible que llegare a saber en el desempeño de su labor, como también el respeto a los derechos fundamentales de las personas.

Adelanta que las infracciones a las obligaciones dispuestas en este título serán sancionadas en la forma prevista en los artículos 246, 247 o 247 bis, todos del Código Penal, sin perjuicio de la responsabilidad administrativa que procediere.

7. Título VII

El ex Primer Mandatario relata que este título establece las infracciones, las multas y el procedimiento sancionatorio.

8. Título VIII

Crea y regula el Comité Interministerial de Ciberseguridad, encargado de asesorar al Ministro del Interior y Seguridad Pública en materias de ciberseguridad relevantes para el funcionamiento de los órganos de la Administración del Estado y de servicios esenciales en los términos de esta iniciativa.

Acota que el referido Comité será presidido por el Subsecretario de Interior y estará integrado por diversos subsecretarios de Estado, además del Director General de la Agencia Nacional de Inteligencia y de Ciberseguridad y de un experto de notable conocimiento en la materia.

Plantea que los funcionarios que estén en conocimiento de información reservada que sea atingente a los fines del Comité podrán compartirla para su análisis, y que no se podrá levantar acta mientras se

encuentre en tal condición. Su revelación será sancionada de conformidad al delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.

9. Título IX

Anuncia que este título modifica el estatuto Orgánico del Ministerio de Defensa Nacional

10. Título X

Contiene las disposiciones transitorias.

Para concluir, el ex Primer Mandatario reafirma su convicción en cuanto a que esta proposición legal será un medio efectivo para modernizar el país y brindar mayor seguridad en el ciberespacio a las personas e instituciones públicas y privadas, permitiendo conectar Chile al mundo digital y avanzar con solidez hacia el desarrollo, además de enfrentar con visión de Estado los desafíos del futuro.

- - -

ASPECTOS CENTRALES DEL DEBATE

La era digital ha generado cambios significativos a nivel mundial y nacional, los que se han incrementado durante la pandemia provocada por el COVID-19.

Chile destaca como uno de los países con mayor crecimiento en uniones fijas a fibra óptica. Actualmente, el 83% de los habitantes tiene acceso a internet y se registran más de 26 millones de conexiones a la red informática descentralizada mediante smartphones, lo que representa un 136% de la población total.

El Estado, por su parte, también ha avanzado en su transformación digital, luego de la publicación de la ley Nº 21.180, el año 2019, lo que ha permitido que, hoy, el 74% de los trámites de la administración central esté disponible en línea.

Si bien los avances indicados han traído múltiples beneficios para el país, también suponen nuevos riesgos y amenazas para la seguridad de la gente y de las instituciones. De hecho, el año 2021, Chile recibió cuatro veces más ataques cibernéticos que en 2020, llegando a las 9.400.000.000. Ello, porque el mayor número de superficie incrementa las posibilidades de accesos indebidos.

En el último tiempo, diversos e importantes organismos han sido objeto de incidentes cibernéticos; entre ellos figuran el Banco Central, la plataforma virtual de Carabineros de Chile, el Servicio Nacional del Consumidor, el Estado Mayor Conjunto y el Poder Judicial.

Estas amenazas han sido posible porque el crecimiento exponencial en conectividad no ha ido acompañado de las medidas de seguridad cibernética requeridas y porque los antivirus han devenido en mecanismos obsoletos.

Una de las herramientas existentes es la Política Nacional de Ciberseguridad, del año 2017, que fija los lineamientos para el resguardo de la seguridad de las personas y de sus derechos, por medio del establecimiento de cinco objetivos estratégicos y un conjunto de medidas para lograr un ciberespacio libre, abierto, seguro y resiliente. Entre estas últimas se encuentra la elaboración y presentación al Congreso Nacional de un proyecto de ley sobre ciberseguridad que consolide la institucionalidad y regule la gestión de incidentes de seguridad informática en el país.

De esta manera, en el marco referido, surge esta iniciativa legal que apunta a 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.

Si bien el vertiginoso desarrollo de la sociedad digital conlleva un mayor riesgo de vulnerabilidad en todas las estructuras, especial atención debe ponerse en aquellos sectores estratégicos que poseen infraestructura crítica de la información.

La Comisión dedicó ocho sesiones al estudio de esta proposición legal, recibiendo en audiencia a representantes del Ejecutivo; a las Fuerzas de Orden y Seguridad Pública; a exsubsecretarios de Telecomunicaciones; a académicos expertos en la materia y a agentes de diversas asociaciones vinculadas a la ciberseguridad.

Durante su análisis, miembros de esta instancia legislativa coincidieron en que el proyecto debatido es urgente y relevante para el país, destacando entre sus fortalezas las siguientes:

1) Crea una nueva institucionalidad; coordina acciones y estandariza la regulación, lo que es indispensable y permite adecuar la legislación chilena;

2) Define y establece con claridad la infraestructura crítica de información, así como los principios, responsabilidades y deberes para quienes la poseen;

3) Consagra las instituciones y sectores que tienen servicios esenciales;

4) Fija facultades regulatorias y fiscalizadoras, con atribuciones específicas, generando un Registro Nacional de Incidentes;

5) Contempla infracciones, multas y un procedimiento sancionatorio;

6) Brinda la posibilidad de lograr coherencia sistémica regulatoria entre las diversas normas vinculadas a la materia;

7) Reconoce legalmente unidades que ya existen por decreto en el aparato del Estado, como el Comité Interministerial de Ciberseguridad y el CSIRT del Ministerio del Interior y Seguridad Pública, y

8) Resguarda la seguridad de las personas en el espacio virtual.

Las falencias advertidas, en tanto, fueron los que se expresan a continuación:

1) Naturaleza jurídica del órgano encargado de la ciberseguridad. En este punto, se estimó esencial erradicar posibles problemas de vinculación con las Secretarías de Estado, particularmente con el Ministerio de Defensa Nacional, cuyas competencias dicen relación con todo la seguridad nacional y la soberanía del país;

2) Funciones conferidas a la Agencia Nacional de Ciberseguridad y a su Director Nacional, toda vez que conforme al texto del mensaje, aparece como una institución con atribuciones menores, carente de otras esenciales, como las de coordinación, especialmente respecto del sector privado;

3) Estatuto laboral al que quedarán sometidos los funcionarios del órgano encargado de la ciberseguridad. La contratación de hackers y otras personas talentosas dentro del servicio señalado serán fundamentales para el éxito de su labor, además de impedir su reclusión por bandas criminales. Por ello, se hizo ver la necesidad de considerar un sistema de contratación más flexible que el previsto en el Estatuto Administrativo;

4) Sujeción del cargo de Director Nacional de la Agencia Nacional de Ciberseguridad al Sistema de Alta Dirección Pública. Algunos parlamentarios opinaron que éste debía ser de exclusiva confianza del Presidente de la República;

5) Delimitación de la calidad de la infraestructura crítica. El texto presentado a tramitación dispone que el Ministerio del Interior y Seguridad Pública será el encargado de señalar aquellos sectores o instituciones que la poseen. En algunos países -como Estados Unidos de América y Uruguay- el asunto queda al alero del Ministerio de Defensa Nacional, en atención a que los ataques no solo pueden provenir de hechos internos, sino también externos, razón que amerita su participación.

Adicionalmente, se alertó que el proyecto prescribe que cada dos años el Ministerio del Interior y Seguridad Pública establecerá las infraestructuras críticas, lo que implicará dejar sin protección a otras nuevas que pudieran crearse en el tiempo intermedio.

Asimismo, se previno que no solo hay infraestructuras críticas, sino también procesos de tal carácter que merecen ser protegidos, ejemplo de ellos es el acto eleccionario del pasado 4 de septiembre.

6) Omisión en señalar cuál es el primer organismo competente para enfrentar los ataques. Al respecto, los legisladores se mostraron proclives a que este llamado recaiga en la institución afectada, dado que la ciberseguridad sobrepasa la capacidad de administración del Estado;

7) No se reconoce a las catástrofes naturales como amenazas a la seguridad digital;

8) Ausencia de medidas que eviten conflictos y aseguren una relación armónica entre la Agencia Nacional de Inteligencia y la Agencia Nacional de Ciberseguridad;

9) No se definen grados de alerta, lo que resulta fundamental para orientar los esfuerzos;

10) No se abordan los hackeos neurocognitivos y las operaciones sicológicas en las redes sociales;

11) No se contemplan atribuciones para los CSIRT vinculadas a la ciberinteligencia, dificultándoles la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoyan la toma de decisiones;

12) No se prevén mecanismos para asegurar que este texto legal esté en sintonía con la futura ley que fortalece y moderniza el sistema de inteligencia del Estado;

13) No existe referencia a la ley N° 21.113, que declara el mes de octubre como el de la ciberseguridad;

14) El CSIRT Nacional no es calificado como un órgano supraministerial, lo que le permitiría tener la capacidad de ver qué está pasando en todo el Estado y de determinar cómo este y los privados -que gestionan el 85% de la infraestructura crítica nacional- pueden colaborar;

15) La denominación “CSIRT Nacional” da a entender que este equipo será el encargado de resolver incidentes de ciberseguridad, en circunstancias que no será así;

16) No se advierten mecanismos que permitan la incorporación de nuevos talentos ni tampoco de aquellos que incrementen las capacidades de las personas y su retención, pieza clave para prevenir y enfrentar ciberataques, y

17) Los recursos previstos para esta iniciativa de ley no están a la altura de lo requerido.

- - -

DISCUSIÓN EN GENERAL [1]

A.- Presentación del proyecto de ley por parte de la exministra del Interior y Seguridad Pública, señora Izquia Siches y del exsubsecretario de Defensa, señor Fernando Ayala, y debate preliminar en la Comisión.

Al iniciar el análisis de la iniciativa legal, la Comisión recibió en audiencia a **la exministra del Interior y Seguridad Pública, señora Izkia Siches**, quien puso de relieve que, en los últimos ocho años, Chile ha avanzado significativamente en el campo de la transformación digital. En efecto, subrayó que la mayoría de los habitantes utiliza tecnologías relacionadas con internet y que cada vez más ciudadanos pueden desenvolverse en ese ambiente.

Proporcionando mayores antecedentes, expresó que el 83% de los chilenos tiene acceso a la aludida red informática. Al respecto, connotó que en 2017 dicha cifra alcanzaba solo el 70% de la población. Pese a ello, prosiguió,

---

[1] A continuación, figura el link de cada una de las sesiones, transmitidas por TV Senado, que la Comisión dedicó al estudio del proyecto:
1.- Sesión 5 de julio de 2022 (Ministerio del Interior y Seguridad Pública): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-07-04/152710.html
2.- Sesión 12 de julio de 2022 (Carabineros de Chile y PDI): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-07-11/173507.html
3.- Sesión 9 de agosto de 2022 (señores Huichalaf y Atton): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-08-08/153420.html
4.- Sesión 16 de agosto de 2022 (Subsecretario de Telecomunicaciones): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-08-16/081841.html
5.- Sesión 30 de agosto de 2022 (Cámara Chilena de Infraestructura Digital y señor Jijena): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-08-30/081100.html
6.- Sesión 6 de septiembre de 2022 (señora Garrido y señores González y Reyes): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-09-06/110856.html
7.- Sesión 13 de septiembre de 2022 (señores Morales y Covarrubias): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-09-13/110927.html
8.- Sesión 28 de septiembre de 2022 (votación en general): https://tv.senado.cl/tvsenado/comisiones/permanentes/defensa/comision-de-defensa-nacional/2022-09-28/083409.html

un número relevante de personas aún no cuenta con esta herramienta o mantiene conexiones de inferior calidad.

Por otro lado, comunicó que el 67,48% de los hogares posee internet fija, siendo hoy las preferidas las líneas de alta velocidad. En 2017, advirtió, únicamente el 28,9% de las viviendas disponía de esta herramienta.

Destacó que, en la actualidad, se registran más de 26 millones de conexiones a la red informática descentralizada mediante smartphones -en su gran mayoría de tecnología 4G-, lo que representa un 136% de la población total.

Asimismo, resaltó que más de 13 millones de personas ya tienen Clave Única, y que el 74% de los trámites de la administración central del Estado está disponible en línea.

Sin embargo, alertó que los avances generan nuevos riesgos y amenazas para la seguridad de la gente y de las instituciones, además de incrementar la dependencia y vulnerabilidad frente a incidentes informáticos. De hecho, lamentó, el año 2021, Chile recibió cuatro veces más ataques cibernéticos que en 2020.

Para ilustrar el número de este tipo de acciones en América Latina y, particularmente, en Chile, exhibió el cuadro siguiente:

Siguiendo con su exposición, sentenció que el programa de Gobierno del Presidente, señor Gabriel Boric, propone profundizar y desarrollar aún más el proceso de transformación digital, mediante un ambicioso plan que contempla a internet como un servicio básico; la reducción de brechas sociales en su acceso de calidad; la mejor protección de los derechos digitales de las personas; el incremento de los niveles de madurez de la ciberseguridad del país, y el fortalecimiento de las capacidades de ciberdefensa.

Para lograr estos objetivos, pormenorizó, el Ejecutivo continuará con la implementación de la Política Nacional de Ciberseguridad -elaborada durante la Administración de la ex Presidenta de la República, señora Michelle Bachelet-que fue el resultado de un intenso diálogo público-privado. En este punto, dijo que, durante meses, el Comité Interministerial de Ciberseguridad recibió en audiencia a representantes de servicios públicos; de organizaciones

gremiales y de la sociedad civil, además de académicos y expertos nacionales e internacionales.

Explicó que el año 2017, luego de dos años de trabajo, se aprobó este primer instrumento de Estado que fija los lineamientos políticos para el resguardo de la seguridad de las personas y de sus derechos, por medio del establecimiento de cinco objetivos estratégicos y un conjunto de medidas para lograr un ciberespacio libre, abierto, seguro y resiliente.

Recordó que durante el Gobierno del ex Presidente, señor Sebastián Piñera, en tanto, la Política Nacional de Ciberseguridad fue confirmada, avanzándose en su implementación y en el cumplimiento de las medidas de corto y mediano plazo.

Durante esta Administración, anunció, se dará inicio a su evaluación y actualización para el período 2022-2026, en base a un proceso abierto y participativo.

En el mismo orden de consideraciones, reiteró que la finalidad de la política citada consiste en promover un ciberespacio libre, abierto, seguro y resiliente.

En relación con los objetivos estratégicos previstos para dicha herramienta al año 2022, expuso lo siguiente:

Apuntó que para asesorar al Primer Mandatario en el análisis e implementación de la Política Nacional de Ciberseguridad y otras medidas asociadas, se creó el Comité Interministerial sobre Ciberseguridad, órgano presidido por el Subsecretario del Interior e integrado, además, por los Subsecretarios de Defensa, de Hacienda, de Economía, de Energía, de Relaciones Exteriores, de Minería, de la Secretaría General de la Presidencia, de Telecomunicaciones y de Justicia; las Intendencias; las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función

administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, las municipalidades y las empresas públicas creadas por ley. Asimismo, indicó, el sector privado se integra en la medida que pertenezca a áreas estratégicas, o se haya establecido un convenio de colaboración público-privado.

Declaró que la Política Nacional referida contiene un conjunto de medidas de corto y mediano plazo que han sido implementadas con éxito por los últimos dos Gobiernos. Entre ellas, especificó, destacan las de orden legislativo, por un lado, y administrativas y técnicas, por otro.

Sostuvo que entre las primeras se encuentran las que se señalan a continuación:

1) Suscripción y aprobación del Convenio de Budapest sobre Ciberdelincuencia, acuerdo internacional para combatir los delitos informáticos mediante el establecimiento de una legislación penal y procedimientos comunes entre los Estado Parte.

2) 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.

3) Ley Nº 21.113, que declara el mes de octubre como el de la ciberseguridad.

4) Proyecto de ley, en segundo trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07).

Acerca de las medidas administrativas y técnicas, enunció las siguientes:

1) Establecimiento de requisitos actualizados en materia de ciberseguridad para los sectores económicos regulados, como el de las telecomunicaciones, el financiero y las instituciones de seguridad social, donde se han dictado instrucciones, normas técnicas y resoluciones sobre ciberseguridad en los últimos años;

2) Fortalecimiento de las capacidades para la investigación y análisis forense de los delitos informáticos, mediante la creación de la Jefatura Nacional de Cibercrimen de la Policía de Investigaciones y las mejoras procesales contenidas en la ley N° 21.459;

3) Incorporación en la Encuesta Nacional Urbana de Seguridad Ciudadana de preguntas específicas sobre ciberdelitos, que ha evidenciado el incremento constante de este tipo de crímenes en los últimos años, e

4) Implementación de una plataforma para la notificación e información sobre incidentes de ciberseguridad, que ahora es administrada por el CSIRT de Gobierno.

Luego, planteó que la Política Nacional de Ciberseguridad contempla, como medida de corto plazo, la elaboración y presentación al Congreso Nacional de un proyecto de ley sobre ciberseguridad que consolide la institucionalidad y regule la gestión de incidentes de seguridad informática en el país. En efecto, explicó que la aludida herramienta dispone que Chile necesita un modelo que se haga cargo de las funciones y atribuciones esenciales, tales como la gestión de episodios de ciberseguridad; la coordinación interinstitucional; la función normativa técnica; la asesoría general al Gobierno, y la implementación y evaluación de dicha política, entre otras.

Juzgó que el sistema de gobernanza debe llevarse a cabo en atención a los requerimientos del país y al nivel de desarrollo digital, y debe ser coherente y complementario a otras iniciativas, como la transformación digital.

En cumplimiento de la mencionada medida de la Política Nacional de Ciberseguridad, remarcó que el ex Presidente de la República, señor Sebastián Piñera, envió a tramitación, al finalizar su mandato, la propuesta legal en estudio.

Formulando algunos comentarios iniciales a su respecto, afirmó que la Administración comparte la necesidad de disponer de un modelo de gobernanza a nivel central en este ámbito. Acotó que la experiencia de otras naciones, con mayor o similar nivel de desarrollo al de Chile, evidencia que la ciberseguridad de un país precisa una institucionalidad especializada.

Estimó que dicho modelo debe construirse sobre tres pilares esenciales:

1) Normas, políticas y obligaciones de ciberseguridad tanto para el sector público como para el privado;

2) Capacidades operacionales, y

3) Fortalecimiento de derechos y de la cultura digital.

Con todo, adelantó que el Gobierno evalúa la posibilidad de que la institucionalidad se materialice en un servicio público y no en una Agencia -como se sugiere en el texto en debate-, contemplando un enfoque de protección de derechos, que centralice la labor de las tres columnas fundamentales, además de incorporar las funciones que la Política Nacional de Ciberseguridad considera trascendentes.

Calificó como crucial que la nueva gobernanza establezca estándares y obligaciones de seguridad digital tanto al sector público como al privado, y que la protección de las personas y sus derechos sean el centro de toda acción en esta área.

Hizo hincapié en que próximamente, y a partir de los resultados que arroje el trabajo del Comité Interministerial de Ciberseguridad -espacio de coordinación interinstitucional del Estado en materia de ciberseguridad-, el Ejecutivo formulará indicaciones a esta iniciativa de ley con el objeto de fortalecerla.

Para concluir, relevó dos hitos significativos vinculados al asunto objeto de debate: la constitución de una mesa de trabajo público -privada sobre ciberseguridad en la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado, y la inclusión del derecho a la seguridad informática en el artículo 88 del borrador de nueva Constitución, que será sometido a plebiscito el próximo 4 de septiembre.

A continuación, la Comisión escuchó al **exsubsecretario de Defensa, señor Fernando Ayala**, quien reiteró que la ciberseguridad es una materia radicada en el Ministerio del Interior y Seguridad Pública, razón por la cual la Cartera que representa adhiere a los planteamientos realizados por la exsecretaria de Estado que le precedió en el uso de la palabra.

No obstante, reconoció que el tema es de suma importancia a nivel mundial, reflejándolo así la reciente creación en Australia del Ministerio de Ciberseguridad y el ataque ocurrido en Costa Rica, en el mes de mayo de 2022, a pocos días de haber asumido su nuevo Presidente de la República, hecho que motivó la declaración de estado de emergencia.

Deteniéndose en los comentarios vertidos por el expersonero de Gobierno, **el Honorable Senador señor Huenchumilla** le solicitó que, en una próxima sesión, el Ministerio de Defensa Nacional emita su opinión respecto del proyecto en discusión. Detalló que su análisis por parte de esta Comisión así lo justifica. Además, prosiguió, ello permitirá a la Sala del Senado tener una visión sistémica de esta iniciativa de ley.

A su turno, **el Honorable Senador señor Macaya** juzgó que la propuesta legal es urgente y relevante para el país. Además, estimó que existe consenso a este respecto por parte del Ejecutivo y del Congreso Nacional, pese a las legítimas diferencias en ciertos aspectos, como la protección de datos personales.

Su Señoría consultó los tiempos que el Gobierno contempla para su tramitación.

El Honorable Senador señor Araya anunció que, habida consideración de la trascendencia de esta iniciativa legal, la respaldaría. Connotó que el país avanzó significativamente en transformación digital tras la pandemia provocada por el COVID-19; sin embargo, lamentó, la legislación nacional no tiene las herramientas imprescindibles para dar certeza y tranquilidad a los ciudadanos en torno a que habrá un correcto funcionamiento del mundo tecnológico.

Formulando algunos comentarios acerca del proyecto, subrayó que resulta fundamental revisar las funciones conferidas al órgano encargado de la ciberseguridad, más allá de si se opta por un servicio público o por una agencia nacional. Destacó que esta última, conforme al texto del mensaje, aparece como una institución más bien decorativa, con atribuciones menores, carente de otras esenciales, como las de coordinación, especialmente respecto del sector privado, siendo este el caso de la banca.

En sintonía con lo planteado, preguntó a los integrantes del Ejecutivo si existe la intención de reforzar las facultades del Director Nacional de la Agencia de Ciberseguridad. Su Señoría fue tajante en demandar mayores potestades para dicha figura.

Posteriormente, expresó su preocupación por el estatuto laboral al que quedarán sometidos los funcionarios del órgano encargado de la ciberseguridad. Así, fue enfático en sostener que dicho organismo requeriría de personas con grandes conocimientos en cibernética -e incluso de hackers, como ocurre en la experiencia comparada-, que suelen no cumplir con el perfil tradicional de quienes se desempeñan en la Administración Pública. Avizoró que muchos no podrán ingresar si se aplican las normas del Estatuto Administrativo. Por ello, exhortó a prever un sistema de contratación más flexible.

Siguiendo con el examen de la institucionalidad, discrepó de la propuesta efectuada por el Gobierno anterior, en orden a que el cargo de Director Nacional de la Agencia Nacional de Ciberseguridad quede sujeto al Sistema de Alta Dirección Pública. Por el contrario, opinó, debe ser de exclusiva confianza del Presidente de la República, sin perjuicio de establecer ciertos requisitos. Luego, consultó la opinión del Ejecutivo.

A su turno, **el Honorable Senador señor Saavedra** puso de relieve que una de las consecuencias de la pandemia provocada por el COVID-19 fue motivar el uso intensivo de las tecnologías y, como corolario, la inmersión del país en la revolución digital. No obstante, advirtió que este nuevo escenario obliga al legislador a dictar un cuerpo normativo que esté a la altura de aquel, que brinde seguridad y evite catástrofes.

También adujo que la regulación que se adopte deberá abarcar tanto al sector público como al privado, y que supondrá la implementación de políticas públicas que trasciendan a los diversos Gobiernos. Además, sentenció que será fundamental tener a la vista la experiencia comparada.

Fijando su atención en la discusión sobre el órgano encargado de la ciberseguridad -una agencia nacional o un servicio público-, **el Honorable Senador señor Galilea** manifestó que al momento de adoptar la decisión hay que tener presente ciertos aspectos, como son la dependencia y la jerarquía de las instituciones dentro del Estado.

En este contexto, declaró que la creación de un Ministerio de Ciberseguridad, verbigracia, como ocurrió recientemente en Australia, posibilita una relación directa con otras Carteras de Estado. Especificó que algo parecido podría suceder en el caso de escoger la figura del texto elaborado por el ex Presidente de la República. Por el contrario, continuó, si se prefiere la segunda opción -un servicio dependiente de alguna Secretaría de Estado- se ocasionarían problemas en la vinculación, por ejemplo, con el Ministerio de Defensa Nacional, una de cuyas competencias dice relación con todo aquello que pueda afectar la seguridad nacional y la soberanía del país.

Una discusión similar, recordó, se originó con motivo de la iniciativa de ley que crea la Subsecretaría de Recursos Hídricos en el Ministerio de

Obras Públicas y una nueva institucionalidad nacional de recursos hídricos, y modifica los cuerpos legales que indica (Boletín N° 14.446-09). Puntualizó que algunos se inclinan por una Agencia Nacional del Agua en lugar de la figura señalada. Sin embargo, connotó que esta última erradica conflictos con otros Ministerios, como el del Medio Ambiente o el de Agricultura.

En un orden distinto de ideas, alertó que las funciones de la Agencia Nacional de Ciberseguridad refieren, principalmente, a aspectos normativos y de supervisión, mas no queda clara la extensión de su facultad sancionatoria. Tampoco, remarcó, se observan con claridad sus atribuciones en materia de investigación.

Finalmente, notó que según el informe financiero que acompaña la proposición de ley, los recursos previstos no están a la altura de lo requerido.

El Honorable Senador señor Huenchumilla, deteniéndose en la intervención de la exministra del Interior y Seguridad Pública, mostró su preocupación ante el número de ataques cibernéticos en América Latina y, especialmente, en Chile.

Observó que al recaer la discusión sobre algo intangible, puede ser difícil de comprender. Se trata, prosiguió, de la seguridad en el ciberespacio, que abarca tanto al mundo público como al privado. Ejemplo de este último, ilustró, es el sector bancario, área fundamental para el funcionamiento de la economía y de los particulares, cuyos datos personales podrían verse vulnerados.

En cuanto al riesgo al que se encuentran expuestas las instituciones públicas, especial inquietud expresó acerca de las Fuerzas Armadas y de los organismos dedicados a obtener información fundamentándose en la seguridad nacional.

Sentenció que la legislación deberá poner atención en la institucionalidad ofrecida, de modo que sea capaz de anticiparse a eventuales incidentes de ciberseguridad. Adicionó que el Estado, en su conjunto, debe evitar posibles ataques, para lo cual la coordinación entre diversos sectores es esencial. Además, juzgó, se precisa fortalecer los servicios de inteligencia.

Seguidamente, coincidió con la prevención formulada por el Honorable Senador señor Araya, en relación con el régimen aplicable a los funcionarios de la Agencia Nacional de Ciberseguridad.

Respondiendo las inquietudes planteadas por los legisladores, **la exministra del Interior y Seguridad Pública, señora Izkia Siches**, compartió el diagnóstico de los integrantes de la Comisión, declarando que Chile enfrenta una nueva dimensión que requiere un abordaje legislativo veloz y una adecuada institucionalidad.

Reiteró que convocaría prontamente al Comité Interministerial de Ciberseguridad para estudiar detalladamente el proyecto de ley, particularmente, la naturaleza jurídica del órgano encargado de la

ciberseguridad -con las fortalezas y debilidades de cada opción- y el financiamiento correspondiente.

Todo lo anterior, adelantó, podría motivar la presentación de indicaciones por parte del Ejecutivo.

Para concluir, anunció que Su Excelencia el Presidente de la República daría urgencia al despacho de esta proposición de ley.

El exsubsecretario de Defensa Nacional, señor Fernando Ayala, enfatizó que si bien la ciberseguridad es un tema de futuro, Chile está atrasado en la materia. Recordó que recientemente el Banco Central fue objeto de un ciberataque -que se tradujo en la sustracción de US $150.000-, previniendo que incidentes como este podrían replicarse en Codelco o en otras empresas públicas, acarreando grandes perjuicios económicos.

Añadió que si bien el país ha avanzado en cobertura de internet de manera significativa, aún existen sectores de la sociedad que no han podido acceder al servicio, y otros que solo han logrado uno de mala calidad.

En virtud de lo expuesto, juzgó que el tema objeto de debate precisa ser analizado con profundidad y prioridad, en pos de todos los habitantes.

Luego, **el Honorable Senador señor Galilea** recomendó solicitar a la Biblioteca del Congreso Nacional un informe de la experiencia comparada para organizar la institucionalidad en torno a la ciberseguridad.

El Honorable Senador señor Saavedra acotó que el país está ad portas de un cambio estructural, ya que se debate un proyecto de ley que crea el Ministerio de Seguridad Pública (Boletín N° 14.614-07). **Su Señoría** planteó que en dicha Cartera de Estado debiera alojarse el órgano a cargo de la ciberseguridad.

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

1) Exposición de Carabineros de Chile.

El General Subdirector de Carabineros de Chile, General Inspector, señor Esteban Díaz, contextualizando la importancia de la iniciativa de ley, comunicó que, en las últimas veinticuatro horas, el Centro de Seguridad de la Información de la institución que integra registró 941.000 intentos de sabotaje, lo que evidencia las múltiples acciones tendientes a afectar su ciberseguridad. La cifra, dijo, deja al descubierto la necesidad de avanzar en la dirección prevista en el proyecto.

Con todo, recordó que los ataques han impactado tanto a entidades públicas como privadas, destacando aquella dirigida en contra del Banco Estado, que perjudicó a más de 7.000.000 de personas.

Los daños referidos, connotó, no solo provienen de hackers, sino también de empresas -que tienen vínculos con el crimen organizado- dedicadas a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos. Insistió en que es esencial una arquitectura institucional capaz de prevenir y de hacer frente a tales agresiones. No obstante, aclaró que se requiere una gobernanza general en materia de ciberseguridad, y otra específica para el área de defensa.

Continuando con su intervención, llamó a tener en consideración que los antivirus se han transformado en mecanismos obsoletos, toda vez que, actualmente, existen diversas formas de ingresar a los registros que contienen los datos de las diferentes entidades.

A la luz de lo señalado, juzgó que establecer un marco jurídico para el desarrollo de la ciberseguridad, tanto en su dimensión operativa como regulatoria, ampliará y fortalecerá el trabajo preventivo y la formación de una cultura pública, pasos fundamentales para que los órganos del Estado posean herramientas de defensa ante este tipo de atentados.

Añadió que la nueva dimensión de la seguridad exige la capacitación y el entrenamiento del personal de Carabineros de Chile, para que esté alerta ante eventuales ataques.

Luego, dio a conocer los principales ilícitos informáticos en Chile, a saber: el acceso indebido a la información (9,8%); el espionaje (25,5%); la difusión de información (4,9%), y el sabotaje (59,8%). Especificó que, entre los años 2019 y 2021, acumularon un total de 184 casos policiales.

Notó que en tres de las cinco figuras delictuales mencionadas se observa un incremento significativo en el periodo referido. Detalló que el espionaje informático aumentó en 313%, mientras que la difusión de información y el sabotaje, en un 100%.

Adicionalmente, expresó que los principales lugares afectados por los ciberdelitos corresponden a domicilios particulares (56,5%); otros servicios privados (23,9%), industria o empresas (8,2%), entidades bancarias (7,6%), e instituciones públicas (3,8%).

Relató que, durante el año 2019, la plataforma virtual de Carabineros de Chile fue víctima de acceso ilegal, hecho que permitió la obtención de gran parte de la información contenida en los registros institucionales. Aseguró que, después de un proceso investigativo, se ubicó a los responsables, siguiéndose, hoy en día, un proceso penal en su contra.

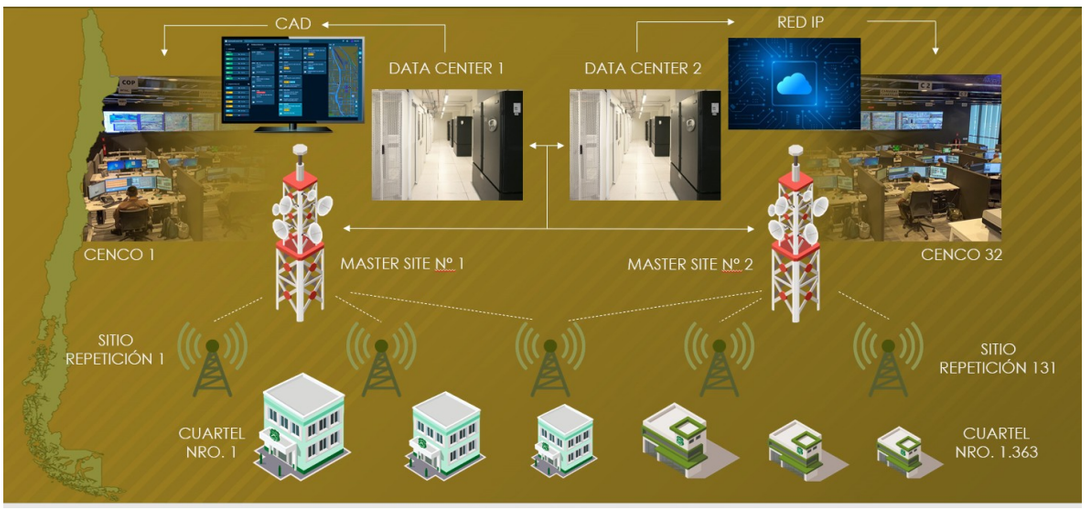
De todo lo expuesto, subrayó, se desprende la trascendencia de un marco legislativo como el de la iniciativa de ley.

Adentrándose en el análisis de la proposición legal, opinó que consagra importantes principios, como el de cooperación con la autoridad; el de responsabilidad; el de protección integral; el de confidencialidad de los sistemas de información; el de integridad de estos últimos; el de disponibilidad; el de control de daños, y el de especialidad en la sanción.

Por otro lado, puso de manifiesto que la propuesta en estudio establece preceptos claros relativos a cómo se determinan los sectores que poseen infraestructura crítica de la información y las obligaciones derivadas.

En línea con lo anterior, relató que Carabineros de Chile cuenta con un sistema de seguridad de la información y se encuentra adscrito al CSIRT del Ministerio del Interior y Seguridad Pública. En consecuencia, continuó, en la aludida Cartera de Estado está radicado el control de esta institución ante posibles ataques. Con todo, anunció que, en la actualidad, se discute permanentemente quién es el primer llamado a defender la organización-Carabineros de Chile o el equipo de respuesta a incidentes de seguridad informática de la Secretaría de Estado mencionada-. Este aspecto relevante, estimó, tampoco se desprende con claridad de la lectura del texto presentado a tramitación, cuestión que el respectivo reglamento debería precisar.

Dando a conocer la infraestructura crítica del organismo policial, acompañó el gráfico siguiente:



Los sistemas depositarios de la información de Carabineros de Chile, expuso, son fundamentales. De hecho, arguyó, en ellos convergen todas las plataformas de la institución, como la consulta de antecedentes policiales; el manejo de las centrales de comunicaciones; la conducción de vehículos policiales; la información desde los cuarteles fronterizos hacia las unidades operativas, y el manejo, dirección y control de las acciones que se realizan a lo largo del territorio.

Resaltó que las repetidoras que se observan, en tanto, son propias de la policía uniformada y merecen especial cuidado, toda vez que, además de ser esenciales para ella, también los son para otros organismos, como Onemi, Bomberos, Directemar y el SAMU. A mayor abundamiento, declaró que fueron significativas después del terremoto del año 2010, así como también para los diferentes eventos naturales que ha debido sortear el país en los últimos años.

Siguiendo con el análisis del proyecto de ley, elogió que prescriba con exactitud los deberes generales de las instituciones que poseen

infraestructura crítica de la información, así como los específicos de algunas de ellas y sus facultades normativas.

Adicionalmente, alabó la creación de la Agencia Nacional de Ciberseguridad. Sin embargo, aconsejó especificar su naturaleza jurídica. A este respecto, recomendó que, en caso de optarse por un servicio público, sus funcionarios no queden adscritos al Estatuto Administrativo, puesto que dificultaría la contratación de hackers y de otros especialistas capaces de enfrentar los ataques. En este contexto, se mostró partidario de la figura de la agencia, diseño que, además, permite alianzas con otras entidades.

Fijando su atención en las atribuciones del órgano aludido precedentemente, previno que no se le confiere la posibilidad de investigar las agresiones de ciberseguridad, lo que resulta fundamental para una correcta estrategia de defensa.

En un orden distinto de consideraciones, estuvo conteste con la creación del Registro Nacional de Incidentes de Ciberseguridad, puesto que dicho instrumento acumulará las experiencias vividas; prevendrá agresiones y aportará las soluciones pertinentes.

En relación con el Consejo Técnico de la Agencia Nacional de Ciberseguridad, propuso que estén representados en él ciertos servicios básicos, como las empresas de agua, luz e internet, entre otras.

A continuación, apreció el establecimiento del Equipo Nacional de Respuesta a Incidentes de Seguridad Informática -CSIRT Nacional-, así como el CSIRT del sector público, correspondientes a los de Gobierno y Defensa. Indicó que, pese a que estos órganos operan en la actualidad, aún no está claro cómo responden ante ciertos eventos. Sobre el particular, postuló que la regulación debiera señalar cuál es el competente en cada caso, según el tipo de infraestructura, datos y consecuencias, entre otros factores. Planteó que tal precisión cobraría especial valor, por ejemplo, en los ataques a la plataforma Comisaría Virtual, cuyo uso aumenta exponencialmente.

Haciendo ver la solidez de la recomendación formulada, recordó que el sistema nombrado cobró un rol fundamental durante el primer año de la pandemia provocada por el COVID-19, evitando el traslado de las personas a los cuarteles policiales para la obtención de permisos, además de atochamientos y gastos materiales. Agregó que los trámites efectuados en dicho periodo ascendieron a 756.000.000, alcanzándose un máximo de 2.400.000 en un día.

El uso del referido portal, aseveró, se ha ampliado en el último tiempo, denunciándose directamente en él los hurtos, el maltrato animal y los daños a la propiedad privada. Adicionalmente, prosiguió, prontamente se incluirán las acusaciones por violencia intrafamiliar y algunas que están en evaluación, como el abandono de hogar; el no pago de pensión de alimentos; la pérdida de documentos y de teléfono móvil, y los reclamos por el actuar policial. En definitiva, reiteró, la Comisaría Virtual es un ícono del buen funcionamiento de la entidad policial.

Para concluir, ofreció la colaboración de la institución en la tramitación de esta iniciativa, especialmente en el aporte de datos que sean indispensables para legislar.

El Honorable Senador señor Pugh señaló que Carabineros de Chile, al igual que otros organismos, es víctima de ataques cibernéticos, cuyo origen puede ser diverso.

El espacio virtual, resaltó, conecta todo el mundo, traspasando fronteras. Por consiguiente, constató, los incidentes pueden provenir de distintas latitudes y no solo del mismo país. Además, consignó, pueden emanar incluso de órganos estatales. Por esta razón, es primordial tener una ley marco que defina la forma de operar ante estos eventos, concluyó.

Refiriéndose al organismo competente para enfrentar los ataques, se mostró proclive a que el primer llamado a este cometido sea la institución afectada, haciendo ver que la ciberseguridad sobrepasa la capacidad de administración del Estado. Opinó que hacerlo de manera colectiva es complejo, ya que supone una entidad capaz de gestionar atentados en contra de todas las organizaciones.

En lo que atañe a las disposiciones aplicables a los funcionarios de la Agencia Nacional de Ciberseguridad, coincidió con el General Subdirector de Carabineros acerca de la conveniencia de flexibilizar su régimen de contratación. Pormenorizó que los hackers y otras personas talentosas dentro del servicio señalado serán fundamentales para el éxito de su labor, además de impedir su reclusión por bandas criminales.

Compartió, asimismo, la apreciación relativa a que el proyecto tiene falencias en materia de investigación de los incidentes de ciberseguridad. No obstante, enunció que la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado trabaja en la generación de una red de indagación.

También llamó a reflexionar sobre la importancia de propagar la cultura de la ciberseguridad, puesto que los individuos constituyen la primera línea de defensa. Por este motivo, ahondó, en el caso de la institución recibida en audiencia, cada funcionario que opera un sistema debe ser capaz de reaccionar ante este tipo de eventos y de instruir a sus colegas.

A modo de fortalecer la proposición de ley, sugirió tener a la vista el modelo de integración existente en España. Puntualizó que dicho país creo el Centro Nacional de Protección de Infraestructuras Críticas -CNPIC-, cuya dotación asciende a 54 personas, distribuyéndose en partes iguales entre funcionarios de la Guardia Civil -equivalente a Carabineros de Chile- y de la Policía Nacional -semejante a la Policía de Investigaciones. La composición, recalcó, apunta a balancear el peso de ambas y a lograr una adecuada organización.

Por último, afirmó que el Presidente del aludido país, el año en curso, externalizó el Centro de Operaciones de Ciberseguridad para utilizar las competencias de la industria local, alcanzando una integración completa.

El Honorable Senador señor Huenchumilla preguntó cuál es el propósito que motiva la comisión de ataques cibernéticos a Carabineros de Chile.

Su Señoría advirtió que tales atentados suelen perseguir la obtención de dinero, como ocurre en el caso de las agresiones en contra de los bancos. Otras veces, prosiguió, buscan acceder a datos personales.

En línea con lo expuesto, adujo que la situación de la institución invitada apuntaría en esa última dirección, o a desestabilizarla. Con todo, sostuvo que el primer objetivo podría obtenerse por medio de sabotajes a compañías mundiales.

Atendiendo la interrogante formulada por el Presidente de la Comisión, **el General Subdirector de Carabineros de Chile, General Inspector, señor Esteban Díaz**, fue enfático en manifestar que los atentados cibernéticos al organismo que representa persiguen tres grandes objetivos:

1) Demostrar a otros hackers mayor capacidad.

2) Apropiarse de datos. En este punto, dio cuenta de que Carabineros de Chile maneja la información de los detenidos que son puestos a disposición del Ministerio Público. Sin ellos, resaltó, no es posible su formalización y se torna imposible la labor de los fiscales, lo que generaría un gran daño al sistema.

3) Adquirir antecedentes del personal que ha participado en investigaciones o en actividades de control del orden público. Indicó que las acciones aludidas les permiten conocer la identidad de familiares, su domicilio y vehículos, todo lo cual facilita ataques en su contra. Afirmó que esta última hipótesis es la que motiva mayor preocupación.

El Honorable Senador señor Saavedra connotó que la ciberseguridad debe ser una pieza fundamental en la institucionalidad y en la legislación, ya que la digitalización abarca diversos sectores y se expande cada día más. De este modo, razonó, una agresión virtual al Metro de Santiago o a los vuelos nacionales sería catastrófica para la seguridad de los chilenos.

En sintonía con lo expresado, planteó que el Estado debe adoptar medidas para evitar estos incidentes. Por ello, aspiró a una estructura que garantice una mirada y control generales, sin perjuicio de vigilancias específicas. Tal modelo, adelantó, facultaría reunir en un solo lugar los medios de que el país dispone para asegurar el bienestar de la población.

El General Subdirector de Carabineros de Chile, General Inspector, señor Esteban Díaz, abocándose a los comentarios realizados por el legislador que le antecedió en el uso de la palabra, destacó que las policías, habitualmente, están coordinadas entre sí, como también con sus pares internacionales.

A reglón seguido, sentenció que la experiencia demuestra que los actos que atentan contra la ciberseguridad suelen provenir de empresas

diseñadas para tomar posesión de determinados sistemas. Una vez que lo hacen, puntualizó, la institución afectada solo tiene dos alternativas: pagar por la liberación o denunciar para que intervenga algún organismo estatal que logre poner término a la agresión. Explicó que, en la actualidad, cuando ello ocurre, no es posible conocer qué acciones se han adoptado para resolver el problema.

El Honorable Senador señor Macaya preguntó qué porcentaje de los ataques cometidos termina en persecución penal. Vislumbró que una cifra menor llega a esa etapa.

Acto seguido, consultó si Carabineros de Chile contempla alguna forma de coordinación adicional con la Policía de Investigaciones de Chile.

Al respecto, **el General Subdirector de Carabineros de Chile, General Inspector, señor Esteban Díaz**, contestó que los datos proporcionados al inicio de su exposición solo dicen relación con las denuncias por ellos recibidas y cuya investigación está en manos de la Fiscalía. Sin embargo, aclaró, hay estadísticas que maneja la PDI y otras el Ministerio Público. La cifra consolidada, concluyó, la posee esta última institución.

Al finalizar, postuló que, si bien el Registro de Incidentes de Ciberseguridad es preponderante, también es fundamental asegurar la investigación, de modo de conocer mayores antecedentes para la defensa y prevención de agresiones a la ciberseguridad.

2) Exposición de la Policía de Investigaciones de Chile.

El Jefe Nacional de Gestión Estratégica de la Policía de Investigaciones, Prefecto, señor Erick Menay, valoró la iniciativa de ley, expresando que mejorará la ciberseguridad, además de crear la institucionalidad y regular algunos asuntos urgentes, como la determinación de la infraestructura crítica de la información.

Alertó que el mundo es volátil, incierto, complejo y ambiguo, y que la globalización acelera este fenómeno, puesto que, junto a los beneficios, conlleva riesgos y amenazas, que aumentan en áreas vulnerables como el espacio virtual. Sostuvo que los ataques que mayor preocupación provocan son aquellos que recaen en la defensa.

En el último tiempo, enfatizó, producto del incremento de la transformación digital, el número de delitos cibernéticos se expandió de manera significativa. Adicionó que particular cuidado existe cuando las amenazas tienen ribetes transnacionales, principalmente, vinculadas al crimen organizado.

Refiriéndose a la organización policial que integra, recordó que su función primordial radica en la investigación de los delitos; sin embargo, declaró, también participa en otras instancias, como aquellas que permiten mejorar la seguridad en el espacio virtual. En efecto, dio cuenta de que la PDI, consciente de la relevancia de la materia, trabaja en consolidar internamente

una institucionalidad para hacer frente a los riesgos y amenazas, no solo desde la perspectiva del cibercrimen, sino también desde una interna, a fin de mantener resilientes los sistemas de información.

En sintonía con lo manifestado, subrayó que la entidad, desde el año 2000, tiene una unidad especializada para investigar los delitos informáticos.

Acotó que las brigadas investigadoras del cibercrimen constituyen una respuesta frente al creciente desarrollo de dichos delitos, y a la conveniencia de tener unidades dedicadas a la investigación y a la solución de los problemas que enfrenta la ciudadanía en el ciberespacio.

Por otro lado, consignó que se estableció, el año 2019, el Centro Nacional de Ciberseguridad, vinculado con el CSIRT de Gobierno. Especificó que su labor consiste en responder a incidentes críticos; colaborar y asesorar a la PDI en este tipo de materias, y difundir alertas preventivas.

Comentó que desde su creación se ha capacitado a los funcionarios que trabajan en asuntos relacionados con el cibercrimen y la ciberseguridad, y a los demás de la institución. También, enunció, dicta instructivos sobre la materia.

A continuación, hizo hincapié en que la información que posee la PDI reúne las características para ser calificada como infraestructura crítica. En este sentido, planteó que cobra especial relevancia la relativa al control migratorio; aquella referida a investigaciones criminales complejas y la que versa sobre el sistema de inteligencia del Estado. Fijando su atención en esta última, remarcó que su vulneración podría incidir en la seguridad de las personas.

Continuando con su intervención, sostuvo que, de acuerdo a datos de Fortinet -una de las empresas líderes en ciberseguridad- en Chile, el año 2021, hubo más de 9.400.000.000 intentos de ciberataques, cifra que cuadriplica aquella del 2020. Adicionó que, conforme a los antecedentes de la PDI, en tanto, el año 2021 se registraron 28.000 eventos maliciosos; 1.500 de los cuales iban dirigidos en contra de la institución referida.

En relación con las razones que se esconden detrás de los ataques, estimó que muchos buscan la obtención de recompensas económicas; otros la validación frente a hackers y, algunos, simplemente, dañar y desestabilizar.

En ese contexto, previno que resulta indispensable brindar a los ciudadanos seguridad en el ciberespacio, permitiéndoles el normal desarrollo de sus actividades personales y sociales. Sin embargo, hizo presente que se requiere coordinación, pues de lo contrario no es posible evitar ni enfrentar este tipo de amenazas.

Por último, reveló la voluntad de su institución en orden a cooperar en la tramitación de esta iniciativa, poniendo a disposición de esta instancia legislativa la experiencia acumulada a lo largo de dos décadas, en pos de una adecuada ley marco de ciberseguridad.

El Honorable Senador señor Araya, centrando su atención en la exposición del General Subdirector de Carabineros, observó que una de los planteamientos realizados a la exministra del Interior y Seguridad Pública, señora Izkia Siches, en una sesión anterior, radicó en la naturaleza jurídica de la Agencia Nacional de Ciberseguridad y en el régimen laboral aplicable a sus funcionarios. Reiteró que su sujeción al Estatuto Administrativo sería un obstáculo para que personas con conocimiento y experiencia en el ámbito informático decidan desempeñarse en ella.

En relación a la intervención del Jefe Nacional de Gestión Estratégica de la PDI, en tanto, aseguró que la persecución penal de los delitos cibernéticos seguirá en manos de dicha entidad, y que al nuevo servicio le corresponderán atribuciones diferentes.

Seguidamente, quiso saber su parecer respecto a la estructura propuesta en la iniciativa de ley para la Agencia Nacional de Ciberseguridad, así como las funciones encomendadas. A mayor abundamiento, consultó si está a la altura de lo que se requiere hoy en día. En este punto, llamó a tener en cuenta que la mayor cantidad de incidentes que repercuten en la vida de los ciudadanos se produce en el sector privado. Tal es el caso, detalló, del comercio electrónico.

A la luz de lo expuesto, preguntó si la composición del Consejo Técnico de la Agencia Nacional de Ciberseguridad asegura horizontalidad en el trabajo, para una adecuada política de ciberseguridad para todos los actores.

Respondiendo la interrogante del legislador que le precedió en el uso de la palabra, **el Jefe Nacional de Gestión Estratégica de la Policía de Investigaciones, Prefecto, señor Erick Menay**, insistió en que la entidad que representa celebra esta propuesta legal que persigue prevenir, contener, resolver y dar respuesta a incidentes de ciberseguridad, generando la institucionalidad y la normativa imprescindibles. Reiteró que en la elaboración de los reglamentos a que alude el proyecto de ley, la PDI puede colaborar con su conocimiento y experiencia en la materia.

A su turno, **el General Subdirector de Carabineros de Chile, General Inspector, señor Esteban Díaz**, puso de relieve que la conformación del Comité Interministerial de Ciberseguridad incluye, dentro de sus integrantes, al Subsecretario del Interior, lo que supone la colaboración de la PDI y de Carabineros de Chile.

Acto seguido, afirmó que el marco sugerido en la iniciativa legal es un avance en comparación al existente. Al respecto, adujo que el modelo actual carece de integración y colaboración, piezas clave para dar solución a los problemas de ciberseguridad.

El Honorable Senador señor Pugh destacó el rol de la Academia Nacional de Estudios Políticos y Estratégicos (Anepe) en la producción de conocimiento y en la capacitación a diversos funcionarios del Estado, siendo este el caso del Prefecto Menay.

Celebró que la Jefatura Nacional de Cibercrimen, en tanto, esté a cargo del Prefecto Luis Silva, quien se encuentra cursando un curso de formación dictado por el Instituto de Ciberseguridad, ubicado en la ciudad de León, en España.

Al igual que ellos, apuntó, se requiere que personas altamente preparadas trabajen para el Estado y tengan redes de contacto internacionales. Más aún, profundizó, si se tiene a la vista que recientemente se aprobó el segundo protocolo adicional a la Convención de Budapest, instrumento que permite a las policías coordinarse mundialmente tanto con el sector público como el privado. En este punto, acotó que son las empresas las que tienen la capacidad de entregar datos para perseguir adecuadamente el cibercrimen.

Fijando su atención en la legislación comparada, recordó que España creó, como parte de su estrategia de seguridad y de defensa, el foro Nacional de Ciberseguridad, e informó que en un sentido similar trabaja la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado.

En otro orden de ideas, dijo que recientemente se publicó la ley N° 21.459, que establece normas sobre delitos informáticos, lo que lo ha llevado a Chile a ser un país líder en la materia. No obstante, recalcó que es fundamental seguir avanzando en esa senda, previniendo ataques orquestados que se dirigen a desestabilizar las democracias y a destruir el Estado de derecho. Para ello, argumentó, es preciso fomentar la cultura de ciberseguridad. Sobre el particular, afirmó que la ley N° 21.113, que declara octubre como el mes nacional de la ciberseguridad, fomenta el desarrollo de actividades relacionadas en dicho periodo. A este respecto, consultó a los representantes de las policías qué ejercicios han ejecutado en el marco del cuerpo normativo recién individualizado.

Para finalizar, preguntó qué porcentaje de incidentes provienen desde direcciones del protocolo de internet del extranjero.

En relación con las interrogantes planteadas por el parlamentario que le antecedió en el uso de la palabra, **el Jefe Nacional de Gestión Estratégica de la Policía de Investigaciones, Prefecto, señor Erick Menay**, respondió que la institución que integra creó recientemente la Jefatura de Coordinación Internacional, a fin de dar mayor relevancia a esa área del quehacer de la entidad. Adicionalmente, anunció, forma parte de la Organización International de Policía Criminal, Interpol, conformada por 195 países.

A su turno, **el General Subdirector de Carabineros de Chile, General Inspector, señor Esteban Díaz**, atendiendo la consulta del Honorable Senador, fue tajante en señalar que el número de agresiones diarias es tan elevado que los equipos competentes limitan su labor en prevenirlos, contenerlos y resolverlos. En paralelo, agregó, hacen la denuncia correspondiente al Ministerio Público, para que este órgano investigue los hechos.

Enseguida, comentó que la Universidad de Santiago de Chile imparte un programa especial de ciberseguridad, en el cual se han formado muchos de sus funcionarios, de modo de dotarlos de las herramientas imprescindibles para hacer frente a estos ataques. A lo anterior, indicó, se suman otras formas de capacitación de la institución y la contratación de especialistas.

A mayor abundamiento, informó que existe un equipo especial, dentro del Departamento O.S.9, Investigación de Organizaciones Criminales, de Carabineros, que patrulla durante las veinticuatro horas del día el espacio virtual, detectando posibles hackeos, además de ventas de drogas y de armas, y contrabando de mercancías, entre otros ilícitos.

3) Exposición del ex Subsecretario de Telecomunicaciones, señor Pedro Huichalaf**.**

El señor Pedro Huichalaf advirtió que el proyecto de ley aborda dos aspectos: ciberseguridad, por un lado, e infraestructura crítica, por otro.

Enseguida, se detuvo en las fortalezas de la iniciativa legal. Al respecto, juzgó que ellas son las siguientes:

1) Crea una nueva institucionalidad; coordina acciones y estandariza la regulación, lo que es indispensable y permite adecuar la legislación chilena;

2) Define y establece con claridad la infraestructura crítica de información, así como los principios, responsabilidades y deberes para quienes la poseen. En efecto, admitió que no solo se identifica aquella, sino que, además, se determina la forma en que operará y las sanciones que se derivarán en caso de incumplimiento;

3) Consagra las instituciones y sectores que tienen servicios esenciales, hasta hoy inexistente en el ordenamiento jurídico, con lo cual resulta igual la ciberseguridad de las pymes a la de un sistema nacional de transmisión eléctrica. Esta propuesta legal, explicó, eleva los estándares para unos y deja a los demás sujetos a las reglas generales;

4) Fija facultades regulatorias y fiscalizadoras, con atribuciones específicas, generando un Registro Nacional de Incidentes. Remarcando la importancia de este último instrumento, recordó que en materia de seguridad digital un aspecto esencial es la información;

5) Contempla infracciones, multas y un procedimiento sancionatorio, junto con instituir una agravante especial.

Su principal debilidad, en tanto, estimó, radica en la delimitación de la calidad de la infraestructura crítica. Sobre el particular, connotó que el texto en tramitación dispone que el Ministerio del Interior y Seguridad Pública será el encargado de señalar aquellos sectores o instituciones que la poseen. Consideró que la primera interrogante que surge de dicha decisión es por qué esta facultad corresponderá a esta Cartera de Estado. Asimismo, postuló,

surgen dudas respecto a qué ocurrirá en caso de crearse el Ministerio de Seguridad Pública.

Informó que, en algunos países -como Estados Unidos de América y Uruguay- el asunto queda al alero del Ministerio de Defensa Nacional. En este punto, manifestó que es dable preguntarse cuál será el rol de esta última Secretaría de Estado en Chile. A mayor abundamiento, hizo hincapié en que los ataques no solo pueden provenir de hechos internos, sino también externos, razón que amerita su participación, sin perjuicio de resguardar la debida coordinación entre ambos organismos.

Continuando con su intervención, advirtió que la proposición de ley analizada no precisa cuáles son los sectores críticos, sino que encomienda tal determinación a un reglamento. Notó que, en el caso de EE.UU., la Agencia de Ciberseguridad e Infraestructura define cuáles son y los clasifica en 16 sistemas de vital importancia.

Adicionalmente, criticó, el proyecto prescribe que cada dos años el Ministerio del Interior y Seguridad Pública establecerá las infraestructuras críticas, lo que implicará dejar sin protección a otras nuevas que pudieran crearse en el tiempo intermedio. En atención a lo expuesto, sugirió incorporar medidas de flexibilización para casos como el referido.

Adentrándose en lo que denominó las amenazas de la iniciativa legal, subrayó que la primera es el debilitamiento institucional. Justificando su aseveración, observó que son múltiples los actores que se interrelacionan, como la Agencia Nacional de Ciberseguridad, los CSIRT sectoriales, el CSIRT de Gobierno, el CSIRT de Defensa y el Comité Interministerial de Ciberseguridad, lo que obligará a tener una mirada coordinada.

En sintonía con lo señalado, consignó que actualmente diversos decretos contienen normativa de ciberseguridad, tal como ocurre en las áreas bancaria, de telecomunicaciones y de casinos.

Por otro lado, destacó que los reguladores sectoriales definirán las infracciones de ciberseguridad y, en caso de no hacerlo, corresponderá a la Agencia Nacional de Ciberseguridad tal función, arriesgando posibles faltas de concordancia en la materia.

También llamó a tener en cuenta que las principales amenazas a la seguridad digital provienen de las naciones extranjeras, del crimen organizado, del espionaje y de las catástrofes naturales, no recogiéndose estas últimas en el texto. Al respecto, apuntó que en la ley general de telecomunicaciones existe una regulación de infraestructura crítica para este sector, pero solo respecto de las antenas, dejando fuera, por ejemplo, la fibra óptica.

Otros riesgos, prosiguió, son la vulnerabilidad de los softwares-muchos de los cuales ya no tienen soporte técnico-; la infraestructura deficiente -toda vez que no hay un estándar de instalación ni resguardos adecuados para ella-, y las guerras híbridas, además de las causas sin especificar.

Centrando su atención en las oportunidades que ofrece el proyecto, sentenció que brinda la posibilidad de lograr coherencia sistémica regulatoria entre las diversas normas vinculadas a la materia, y que son las que siguen:

1) Ley de delitos informáticos. Apuntó que este texto normativo solo considera la mirada del delincuente, mas no establece la obligación de las empresas atacadas de custodiar la información;

2) Proyecto de ley sobre protección de datos personales (Boletín N° 11.092-07);

3) Reglamento de infraestructura de telecomunicaciones;

4) Política Nacional de Ciberseguridad y la de Ciberdefensa. Recordó que en virtud de esta última se otorgó a las Fuerzas Armadas la facultad de declarar la guerra a otro Estado en caso de ataque digital;

5) Proyecto de modernización del Estado;

6) Iniciativa para reconocer el acceso a internet como un servicio público de telecomunicaciones (Boletín N° 11.632-15), y

7) Nueva Constitución. Sin embargo, adelantó, el borrador propuesto a la ciudadanía no incorpora la creación de una entidad encargada de la ciberseguridad.

Realizando algunas sugerencias de enmiendas a la iniciativa legal, exhibió las siguientes:

• Incorporar un sistema flexible de determinación de infraestructura crítica;

• Establecer exigencias de estándares ISO, así como capacitación en ciberseguridad a funcionarios y trabajadores estratégicos, además de certificados de obsolescencia tecnológica en instalaciones de infraestructura y en sistemas informáticos;

• Contemplar obligaciones de corrección, actualización o medidas de respuestas ante avisos de vulnerabilidades;

• Unificar criterios en materia de infracciones y multas;

• Perfeccionar el procedimiento sancionatorio, definiendo quién realiza los cargos y quien resuelve y sanciona, sin perjuicio de introducir el trámite de apelación de las penas;

• Reincorporar la figura del hacker ético, para contribuir a la identificación de vulnerabilidades y promover la formación de capital humano;

• Exigir la presencia de un oficial de seguridad que sea la contraparte de la institución o empresa con infraestructura crítica, y

• Otorgar la facultad a la Agencia Nacional de Ciberseguridad de declarar estado de emergencia ante ciberataques y facultar el trabajo conjunto con entidades afectadas en casos graves.

Aseguró que esas modificaciones permitirán tener un entorno seguro y resiliente.

Deteniéndose en la interrupción del servicio de telecomunicaciones ocurrida el día 8 de agosto de 2022, indicó que a las 19:30 horas se reportó la caída de internet fijo y móvil de Movistar, sumándose posteriormente la de WOM y VTR. Agregó que a las 20:10 horas, la Subsecretaría de Telecomunicaciones tomó contacto con las empresas referidas, comunicándoles que si el corte excedía las seis horas, los clientes tendrían derecho a ser compensados. Notó que solo dos horas después de ocurridos los hechos, a las 21:30 horas, Movistar informó “intermitencias” desde la Región de Valparaíso al norte, asegurando que ella obedecía a imponderables externos, sin especificar las razones. Finalmente, relató, a las 23:15 horas la citada compañía dio a conocer el restablecimiento de sus operaciones.

Destacó que tal como se aprecia en el evento previamente descrito, la regulación no contempla mecanismos de transparencia para los usuarios ni para el Estado, desconociéndose si hubo un ciberataque o los motivos que desencadenaron la falta de comunicación. Además, lamentó, no hay un organismo que se haga responsable de hechos como el citado.

4) Exposición del ex Subsecretario de Telecomunicaciones, señor Jorge Atton.

El señor Jorge Atton coincidió con el invitado que le precedió en el uso de la palabra, en cuanto a que el proyecto de ley amerita enmiendas para estar a la altura de lo requerido.

Sentando algunos principios básicos en la materia, hizo hincapié en que los esfuerzos en ciberseguridad deben reflejar la naturaleza del espacio a proteger, el que no posee fronteras y es de alcance global. Además, agregó, las normas deben estar basadas en la gestión de riesgos y el foco en identificar qué requiere ser resguardado, por qué, de qué y cómo.

Asimismo, postuló, es indispensable balancear el intercambio de información con la protección de la privacidad. Hoy, constató, existe reticencia a compartir los antecedentes de ciberincidentes, ante el temor de afectar la reputación o las ganancias económicas, o de dañar la imagen del país o la defensa nacional.

También enfatizó que las mejoras prácticas en ciberseguridad deben adaptarse rápidamente a los constantes cambios y a las nuevas tecnologías que emergen diariamente. Por ello, remarcó, las normas que

emanen de este proyecto de ley deben ser flexibles. En este punto, advirtió que tecnologías-como la 5G- no se recogen en la iniciativa en estudio.

Otro principio básico, prosiguió, es que debe emplearse un enfoque multisectorial para la definición de estándares, políticas y mejores prácticas.

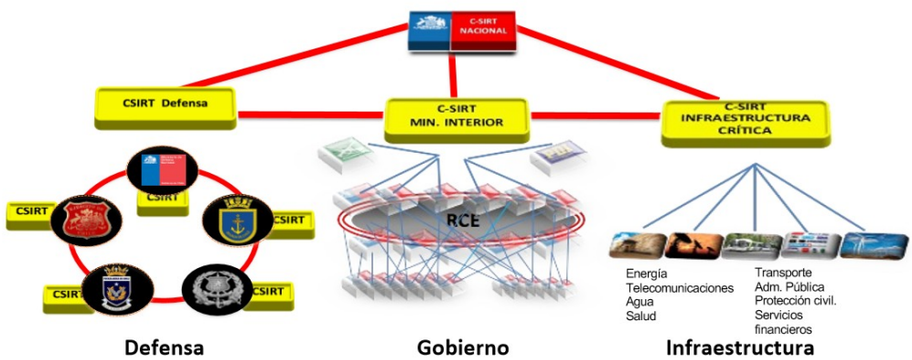
A continuación, juzgó que el país ha avanzado en innovación y modernización digital; sin embargo, ha descuidado los mecanismos de ciberseguridad. Estos últimos, alertó, deben evolucionar a la par de las primeras, a fin de resguardar la infraestructura crítica, las transacciones, los procesos y las bases de datos, entre otros.

Siguiendo con su intervención, recordó que la Política Nacional de Ciberseguridad, establecida el año 2017, fijó los lineamientos del Estado hasta el año 2022 para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente, a través de acciones que permitan identificar y gestionar los riesgos. Dicho instrumento, especificó, consagra cinco ejes estratégicos, a saber: 1) infraestructura; 2) legislación; 3) difusión; 4) colaboración internacional, y 5) desarrollo de la industria de ciberseguridad.

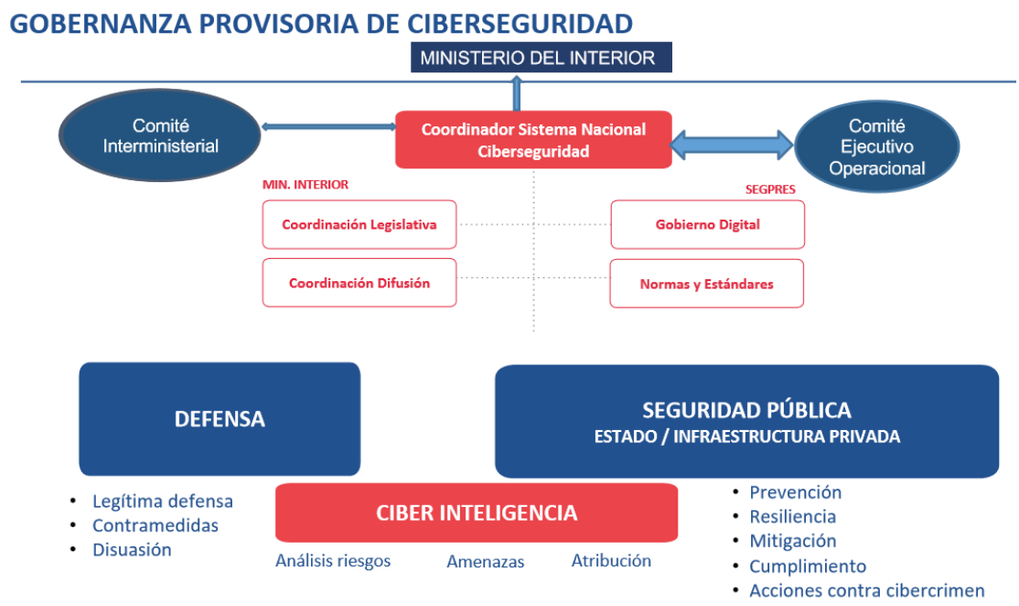
De la citada política, indicó, solo ha surgido la ley de delitos informáticos. A la luz de lo expuesto, estimó que su actualización debe llevarse a cabo en forma paralela con los avances pendientes, a fin de no retrasar aún más al país.

Refiriéndose a la gobernanza, observó que la proposición legal no define una estructura clara sobre el particular. Consignó que, conforme a lo planteado en la Política Nacional de Ciberseguridad del año 2017, debía existir un CSIRT Nacional, además de otro para Defensa, uno para el Gobierno y otro para la infraestructura crítica de los sectores más importantes, tal como se aprecia en el gráfico que sigue:

Protección, monitoreo y gestión de crisis (PNCS)



Declaró que el año 2018, se propuso una gobernanza provisoria de ciberseguridad en tanto no entre en vigencia la Ley Marco de Ciberseguridad, que es la que se ve en la lámina siguiente:



Seguidamente, dio a conocer que las metas a lograr en el periodo de transición hacia el referido cuerpo normativo, en lo que respecta a la actualización de decretos de conectividad y ciberseguridad del Estado, eran las que siguen:

1) Incorporar estándares de seguridad informática a las redes de telecomunicaciones;

2) Contemplar nuevos modelos de ciberseguridad en las instituciones del Estado y actualizar su red de conectividad;

3) Dictar un instructivo presidencial sobre gobernanza transitoria y normas mínimas de seguridad digital para el Estado;

4) Incluir exigencias de ciberseguridad a proveedores del Estado, y

5) Establecer coordinación y mecanismos de intercambio de experiencias y de información con gobiernos y entidades internacionales.

La segunda y la última, notó, solo se han cumplido de manera parcial, mientras que en lo que concierne a la cuarta no se ha hecho nada aún.

En cuanto a las metas vinculadas a los centros de infraestructura crítica, señaló que fueron las que se indican:

1) Implementación del Centro de Respuesta a Incidencias Informáticas y de Ciberseguridad en el sector público (Transportes, Salud y Minería, entre otros). Al respecto, comentó, solo se ha implementado el CSIRT de Gobierno (Medidas N º 6 y N° 9 de la Política Nacional de Ciberseguridad), mientras que en las demás áreas no se observa avances;

2) Creación y puesta en marcha de centros de respuesta ante emergencias informáticas en el sector privado (financiero, telecomunicaciones y energía). Alertó que nada se ha hecho al respecto;

3) Implementación de Centros de Respuesta ante Incidentes Informáticos en divisiones de servicios básicos, financieros o de retail más relevantes. En ello, criticó, tampoco ha habido avances.

4) Capacitación y difusión de buenas prácticas en los organismos del Estado, incentivando campañas de información y difusión en las áreas más sensibles para la población al poseer el resguardo y cuidado de su información personal. Acá, remarcó, los progresos han sido escasos.

En relación con los avances de la agenda legislativa vinculada a la ciberseguridad, formulada el año 2018, relató que su estado es el que se señala a continuación:

1) Ley General de Bancos: aprobada. Sin embargo, no se incorporaron exigencias de ciberseguridad del mercado financiero, sino solo una normativa sectorial para la Comisión del Mercado Financiero;

2) Proyecto de ley sobre protección de datos personales (Boletín N° 11.092-07): en tramitación. Connotó que la protección de estos antecedentes es una medida clave;

3) Ley de delitos informáticos: aprobada. Acotó que la tipifica nuevos ilícitos, avanzando en el cumplimiento del Convenio de Budapest. Además, perfecciona lo concerniente a la prueba;

4) Ley Marco de Ciberseguridad: en tramitación. Hizo hincapié en que este cuerpo legal es fundamental para tener definiciones y responsabilidades sobre la materia, además de crear centros de respuesta ante incidencias informáticas en el sector público y en el privado;

5) Proyecto de ley que modifica la ley N° 18.168, General de Telecomunicaciones, en materia de individualización y registro de datos de los usuarios de servicios de telefonía en la modalidad de prepago (Boletín N° 12.042-15): pendiente. Adelantó que traerá beneficios aparejados a la prevención del delito, disminución del fraude en portabilidad y minimización los ilícitos de ciberseguridad, y

6) Ley de Infraestructura Crítica para Sistemas de Información: pendiente, pero asociada a esta iniciativa de ley. Posibilitará la definición de las instituciones públicas y empresas privadas estratégicas para los sistemas de información y su regulación.

Adentrándose en el análisis de la propuesta legal, anheló su perfeccionamiento, especialmente en lo que respecta a su alcance y estructura. Además, opinó que tiene muchos aspectos indefinidos, y que no hay coherencia con las atribuciones de las distintas áreas sectoriales.

Por otra parte, observó que no quedan claras la gobernanza ni las atribuciones de la Agencia Nacional de Ciberseguridad y su coordinación con el Ministerio de Defensa Nacional.

Finalmente, sentenció, no resuelve el modelo de definición de las infraestructuras críticas para los sistemas de información, y no considera el efecto de la tecnología 5G ni el impacto de internet.

Fijando su atención en la presentación realizada el pasado 6 de julio de 2022 por la exministra del Interior y Seguridad Pública, señora Izkia Siches, sobre este proyecto de ley ante la Comisión, celebró la aseveración relativa a que la ciberseguridad es una política de Estado reafirmada en los tres últimos gobiernos.

Asimismo, valoró la incorporación de requisitos en materia de seguridad informática para los sectores económicos regulados, como el de las telecomunicaciones, el financiero y las instituciones de seguridad social, donde se han dictado instrucciones, normas técnicas y resoluciones en los últimos años (Medida Nº 7 de la Política Nacional de Ciberseguridad). Alabó, también, el fortalecimiento de las capacidades para la investigación y el análisis forense de los delitos informáticos (Medida Nº 15 de la Política Nacional de Ciberseguridad).

Con todo, en lo que concierne a la idea de actualizar la aludida política para el período 2022-2026 a través de un proceso abierto y participativo, discrepó de ella, en atención al retraso del país. De avanzar en esa senda, especificó, podría seguirse el mal ejemplo de la Agenda Digital, la que varía en cada gobierno. A mayor abundamiento, recordó que el proceso llevado a cabo el año 2017 fue abierto y participativo.

Para concluir, concordó en la necesidad de ingresar indicaciones que fortalezcan el proyecto -a fin de progresar en su discusión-, superando las debilidades del texto, a partir del trabajo del Comité Interministerial de Ciberseguridad, espacio de coordinación interinstitucional del Estado en el área.

A continuación, **el Honorable Senador señor Araya** señaló que una de las dudas que deja esta proposición de ley es la naturaleza jurídica que debe tener el órgano encargado de la ciberseguridad, esto es, si debe ser un servicio público o una agencia.

Por otro lado, arguyó que el Director Nacional de la Agencia Nacional de Ciberseguridad no debe ser nombrado por el Sistema de Alta Dirección Pública -como lo propone el texto en estudio-, sino ser un cargo de la exclusiva confianza del Presidente de la República, sin perjuicio del establecimiento de ciertos requisitos.

En relación con estos temas, demandó conocer la opinión de los invitados.

Atendiendo las consultas del legislador, **el señor Jorge Atton** respondió que la naturaleza jurídica del organismo citado es un asunto muy discutido en la experiencia comparada.

Comentó que el modelo sugerido en el proyecto es similar al previsto en Israel. Llamó a analizar el sistema de ciberseguridad de Australia, Estado que posee una gobernanza similar a la chilena, y el de Estonia, país que fue víctima de ataques cibernéticos por parte de Rusia, afectando considerablemente sus sistemas de información, lo que lo obligó a dictar una ley de ciberseguridad que es de las más destacadas a nivel internacional y contempla directrices, obligaciones y coordinación entre las diversas entidades involucradas. Con todo, previno que cualquiera que sea la decisión, el régimen debe estar inspirado por la flexibilidad, dado el dinamismo de la materia regulada.

A su vez, **el señor Pedro Huichalaf** coincidió en la importancia de tener a la vista los modelos de ciberseguridad más destacados del mundo a la hora de determinar la gobernanza.

Pormenorizó que la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado ha motivado la conformación de diversas mesas de trabajo destinadas a lograr coordinación entre distintos actores, tanto del mundo público como privado, en seguridad digital.

En otro orden de ideas, lamentó la ausencia de representantes del Ejecutivo en la sesión en curso y durante toda la tramitación de la iniciativa de ley. Ahondando en sus planteamientos, reiteró que dada la trascendencia del proyecto objeto de análisis, debe ser impulsado por el referido Poder del Estado.

En efecto, alertó que, pese al tiempo transcurrido desde la instalación del Gobierno, aún no hay un coordinador de ciberseguridad que lidere la iniciativa y vele por su avance con celeridad y con una visión común.

Deteniéndose en el último comentario vertido por el expositor que le precedió en el uso de la palabra, **el señor Jorge Atton** informó que, recientemente, se incorporó al Ministerio del Interior y Seguridad Pública el señor Daniel Álvarez, quien ha dedicado gran parte de su vida profesional a temas de ciberseguridad, y será el que coordinará y dirigirá este proceso. Adelantó que el nombrado experto conoce las fortalezas y debilidades de esta propuesta legal, lo que posibilitará perfeccionarla a través de las indicaciones correspondientes.

5) Exposición del Subsecretario de Telecomunicaciones, señor Claudia Araya.

El Subsecretario de Telecomunicaciones, señor Claudio Araya, hizo ver a los miembros de la Comisión la especial atención que debiera ponerse en la composición de los órganos contemplados en la iniciativa de ley, a fin de no generar burocracia. Particular consideración, acotó, debe haber

respecto a la integración del Consejo Técnico de la Agencia Nacional de Ciberseguridad, así como en la del Comité Interministerial de Ciberseguridad.

Otro aspecto relevante, juzgó, es el relativo a la determinación de la infraestructura crítica de la información.

En línea con lo sostenido, sentenció que la Subsecretaría que encabeza tiene mucho que aportar en materia de redes de telecomunicaciones, las que son fundamentales para que los servicios digitales operen adecuadamente. A mayor abundamiento, recordó que los ataques cibernéticos se concretan a través de ellas y, en consecuencia, deben catalogarse como un activo esencial y resguardarse.

Hoy en día, previno, la industria es reacia a tomar acciones sobre el particular. En parte, adujo, porque la legislación existente -ley N° 20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet- inhibe a inspeccionar direcciones del protocolo de internet o a tomar medidas de filtrado de contenido.

El Honorable Senador señor Huenchumilla consultó al Personero de Gobierno la opinión de la Cartera de Estado por él representada acerca de la proposición legal analizada.

Atendiendo la inquietud del Presidente de la Comisión, **el Subsecretario de Telecomunicaciones, señor Claudio Araya**, insistió en la necesidad de analizar pormenorizadamente la composición de los organismos comprendidos en el proyecto de ley.

A su vez, **el Honorable Senador señor Araya** puso de relieve que el largo tiempo que transcurre desde que el ente regulador toma conocimiento de la caída del servicio de internet de una empresa hasta que esta logra reestablecer sus operaciones, da cuenta de que el modelo existente es anacrónico. Así, resaltó, quedó al descubierto la semana pasada con lo ocurrido con Movistar.

En consecuencia, preguntó cuáles debieran ser las facultades de la Agencia Nacional de Ciberseguridad para cumplir cabalmente su cometido, especialmente ante casos como el citado, para evitar que se repitan.

El Subsecretario de Telecomunicaciones, señor Claudio Araya, contestó que, conforme a lo dispuesto en el decreto N° 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, la facultad de declarar una infraestructura de la información como crítica corresponde a las empresas. Esto, subrayó, se ha transformado en una gran valla, toda vez que las compañías actúan en función de la cantidad de abonados afectados. Sin embargo, advirtió, estos eventos suelen trascender a los particulares. Así, ejemplificó, quedó de manifiesto con la caída de Entel hace algunas semanas, la que repercutió en el quehacer del Servicio de Registro Civil e Identificación.

En virtud de lo indicado, calificó como una función indispensable de la Agencia Nacional de Ciberseguridad definir cuáles son los sectores o instituciones que poseen activos digitales esenciales.

6) Exposición de la Cámara Chilena de Infraestructura Digital.

La Directora Ejecutiva de la Cámara Chilena de Infraestructura Digital, señora Corina Gómez, puso de relieve, en primer término, que la iniciativa de ley objeto de análisis reviste suma importancia para el mercado de las telecomunicaciones, los socios de la entidad que representa y los consumidores.

Argumentó que la organización que dirige es una alianza público privada -que incluye a doce empresas del rubro aludido-, dedicada al despliegue de infraestructura pasiva; es decir, a la construcción de antenas, redes de fibra óptica, pequeños puntos de acceso móvil y centros de procesamiento de datos, entre otros. En definitiva, precisó, su quehacer está en los medios, servicios e instalaciones habilitantes para las comunicaciones a distancia.

Informó que a la Cámara Chilena de Infraestructura Digital se suman, también, municipalidades, como la de Renca y la de Licantén; el Gobernador de la Región de Magallanes y de la Antártica Chilena, y dos institutos profesionales, Inacap e Infocap.

El propósito de su asociación gremial, en tanto, reveló, radica en disminuir la desigualdad tecnológica y habilitar las instalaciones para el despliegue de la comunicación a distancia.

Enfatizó que la proposición legal en estudio es de gran interés para la entidad que integra, atendida la cantidad de transacciones que sus consumidores efectúan. En este sector, connotó, las operaciones que se hacen en dos horas equivalen a las que se llevan a cabo en 36 horas en el comercio minorista y en la banca.

Proporcionando algunos datos del mercado de las comunicaciones a distancia, subrayó que, actualmente, el país se encuentra en un escenario de digitalización total. De hecho, destacó, existen 26 millones de conexiones móviles, cifra superior al número de habitantes. Además, prosiguió, el 67,48 % de los hogares tiene internet fija.

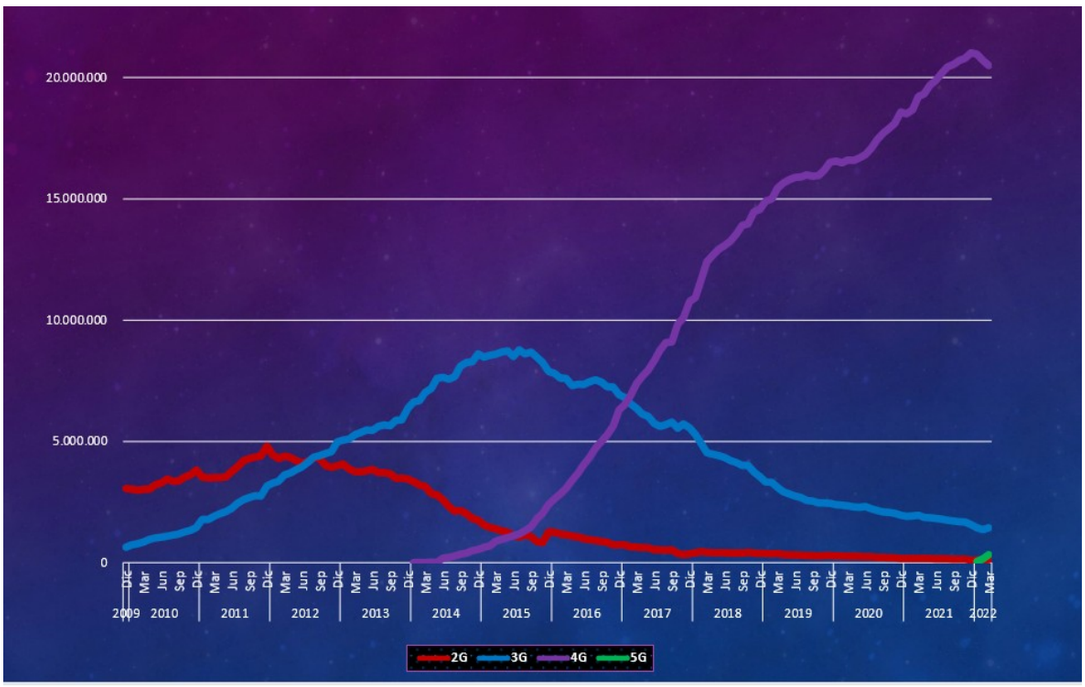
En sintonía con lo expuesto, resaltó que la Organización para la Cooperación y el Desarrollo Económicos posiciona a Chile como uno de los Estados con mayor crecimiento en materia de uniones fijas a fibra óptica, lo que permite que las personas puedan tener una mejor conectividad y menor latencia.

Adicionalmente, dio a conocer que el ranking mundial de velocidades de internet, realizado por la empresa Ookla, ubica al país en el segundo puesto de la banda ancha fija más veloz y el primero en la OCDE, superando en este ámbito a Estados Unidos y a Canadá.

Los antecedentes proporcionados, hizo hincapié, dan cuenta de un mundo globalizado, en donde el tráfico de información es relevante, siendo las

redes de telecomunicaciones las encargadas de suministrarla a los consumidores finales.

Ilustrando el avance de la tecnología 4G desde el 2014 a la fecha, exhibió el gráfico que sigue:



A continuación, manifestó que, conforme a lo publicado recientemente por el Observatorio Iberoamericano de la Ciencia, la Tecnología y la Sociedad (OCTS), Chile lidera el ranking en la región en este tipo de servicios, al ser el Estado con mejor conectividad. Esto evidencia, acotó, que ella, la infraestructura digital y el acceso a internet son asuntos estratégicos para el país y, por lo tanto, las leyes vinculadas también tienen este carácter.

Notó que el avance de la tecnología 5G, a abril del año en curso, ha significado más de 545.000 conexiones, lo que ha supuesto un progreso para la agricultura y la telemedicina, entre otras áreas.

Centrando su atención en la iniciativa de ley, apuntó que es necesaria para Chile, toda vez que llevará a una gobernanza de ciberseguridad. Además, prosiguió, elevará los estándares nacionales, al crear la institucionalidad sobre el particular; reconocerá legalmente unidades que ya existen por decreto en el aparato del Estado, como el Comité Interministerial de Ciberseguridad y el CSIRT del Ministerio del Interior y Seguridad Pública; resguardará la seguridad de las personas en el espacio virtual, y definirá a las infraestructuras críticas de la información.

Sin perjuicio de las fortalezas indicadas, juzgó ineludible advertir, también, las oportunidades de perfeccionamiento. La primera, especificó, radica en evaluar la conveniencia de la Agencia Nacional de Ciberseguridad como el órgano idóneo para enfrentar los desafíos y reportar los mejores resultados.

En el mismo orden de ideas, declaró que una de las dudas a resolver es la gobernanza y las atribuciones de dicha entidad, y cómo se coordinará con la Cartera de Defensa Nacional y con el Ministerio del Interior y Seguridad Pública.

Otro aspecto a perfeccionar, continuó, dice relación con la dependencia o autonomía de la Agencia Nacional de Ciberseguridad, toda vez que el texto en debate nada prescribe al respecto.

Asimismo, alertó que dentro de las funciones del organismo aludido se contempla la de prestar asesoría técnica a instituciones públicas y privadas afectadas por un incidente de ciberseguridad. Opinó que tal decisión lleva a cuestionarse si este órgano será un actor más del mercado; es decir, una empresa de ciberseguridad. De ser así, observó, debiera especificarse la imparcialidad que tendrá al momento de brindar este tipo de prestación.

Siguiendo con el análisis de la proposición de ley, planteó que el artículo 2° define un servicio esencial como todo aquel respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción de su infraestructura de la información pueda afectar gravemente, de modo general, el normal desarrollo y bienestar de la población. Estimó que atribuir un significado tan amplio a dicha locución posibilita que cualquiera pueda ser calificado como tal.

Fijando su atención en el artículo 4° de la iniciativa legal, expuso que la determinación de una infraestructura como crítica colisiona con aquella prevista en el decreto supremo N° 60, de 2021, del Ministerio de Transportes y Telecomunicaciones. Este último cuerpo normativo, explicó, la define como aquellos sistemas de comunicación a distancia cuya interrupción, destrucción, corte o fallo generaría un serio impacto en la seguridad de la población afectada, adicionando que, para estos efectos, será aquella que sea declarada como tal conforme al artículo 24 del reglamento.

Postuló que, sin lugar a dudas, las redes de telecomunicaciones son activos esenciales para el funcionamiento de la sociedad, puesto que su suspensión podría llegar a paralizar la vida de los habitantes de un país. En efecto, aseveró, existen al menos cuatro sectores que requieren de ellas para su normal funcionamiento, tal como se aprecia en la lámina que sigue:

Luego, reveló que muchos de los asociados de la Cámara Chilena de Infraestructura Digital experimentan el robo de cables de fibra óptica. Comentó que, entre enero y julio de 2022, ha habido más de 7.216 de estos actos de vandalismo en la Región Metropolitana, afectando, principalmente, a los servicios fijos y móviles, mediante su interrupción.

Agregó que diariamente el sector de telecomunicaciones vive más de 60 ilícitos solo en la Capital, lo que genera preocupación en la organización. Arguyó que cifras parecidas se constatan en las regiones del Libertador Bernardo O´Higgins y en la de Valparaíso.

En atención a lo señalado, recordó que el artículo 16 del texto objeto de examen contempla la creación del Registro Nacional de Incidentes de Ciberseguridad. Al respecto, llamó a tener una mirada más aguda sobre la cantidad de reportes que tendrá que recibir este padrón.

Por otra parte, afirmó que sería conveniente que el Ministerio Público tenga acceso al citado inventario, a fin de poseer los insumos para la persecución de estos ilícitos. En este punto, hizo presente que hoy se recurre al delito de daños a la propiedad o a los bienes nacionales de uso público, en circunstancias que existe una figura penal específica en el artículo 36 B de la ley general de telecomunicaciones, la que impone penas más gravosas a quienes incurren en esas conductas. Por ello, insistió, se requiere entregar los mecanismos idóneos a la Fiscalía para que pueda formalizar correctamente.

Acto seguido, relató que la Cámara Chilena de Infraestructura Digital forma parte de la Alianza por el Cifrado en América Latina y el Caribe, organización conformada por más de 35 entidades del ecosistema digital que velan por los derechos y las políticas públicas de esta índole.

Puso de manifiesto que el cifrado de extremo a extremo es una tecnología fundamental para la seguridad y privacidad en dicho ambiente, así como también para el respeto, promoción y garantía de los derechos humanos y el desarrollo económico, sostenible e inclusivo.

Para concluir, observó que la institución aludida, tras conocer esta iniciativa de ley, sugirió que, dentro de los principios rectores del artículo 3°, se incluya al de cifrado de extremo a extremo, para que las comunicaciones

tengan tal carácter desde su envío hasta su recepción por el destinatario, de manera que nadie pueda acceder a ellas ni interferir en su tránsito.

El Honorable Senador señor Pugh enfatizó que esta iniciativa de ley protegerá la infraestructura crítica de la información, la que el 99% del tiempo está en los cables de fibra óptica que conducen los datos.

En virtud de lo indicado, compartió la preocupación de la entidad recibida en audiencia respecto a la destrucción de los aludidos bienes. Remarcó que constituye un daño a activos que son esenciales para el funcionamiento de la sociedad y de la economía, y produce efectos que pueden llegar a ser mortales.

En relación con la dependencia de la Agencia Nacional de Ciberseguridad, opinó que debe ser un organismo capaz de coordinar todas las actividades. En este contexto, concordó con la idea de un ente de nivel superior, de modo de determinar la atribución de los ataques y, consecuentemente, de responder correctamente.

Acerca de la carta de la Alianza por el Cifrado en Latinoamérica y el Caribe, reconoció que muchas aplicaciones -entre ellas WhatsApp- se encuentran cifradas. Sin embargo, juzgó que es imprescindible que las policías, debidamente autorizadas en ciertos procedimientos, tengan la facultad para intervenir las comunicaciones con la finalidad de probar el hecho delictual.

En sintonía con lo expuesto, connotó que Chile es el primer país en América Latina en actualizar su ley de delitos informáticos y en incorporar el Convenio de Budapest, que permite perseguir el cibercrimen trasnacional con 66 naciones. Subrayó que el segundo protocolo de este tratado habilita a los órganos mencionados para intercambiar evidencia y solicitarla a las compañías. Ello, adujo, porque para saber qué está ocurriendo se requiere el apoyo de las empresas.

A la luz de lo expresado, preguntó a la expositora su parecer respecto a la posibilidad de que las policías, en los casos aludidos, accedan a las comunicaciones cifradas.

Para terminar, recordó que en el plebiscito del próximo 4 de septiembre se empleará infraestructura crítica de la información -llamando a protegerla-, a fin de evitar experiencias como el reciente secuestro de datos del Servicio Nacional del Consumidor.

Atendiendo la consulta del legislador que le precedió en el uso de la palabra, **la Directora Ejecutiva de la Cámara Chilena de Infraestructura Digital, señora Corina Gómez**, aseguró que la asociación gremial que representa siempre ha acatado la legislación nacional y que así también lo hará en caso de dictarse una normativa como la planteada. No obstante, hizo ver que la protección de la información y de los datos personales son sustanciales para el ejercicio de los derechos fundamentales y para el libre acceso al ecosistema digital y al ciberespacio.

A su turno, **el Honorable Senador señor Huenchumilla** recordó que, conforme a la tramitación dispuesta por la Sala del Senado, la propuesta legal debe ser estudiada, en general, primeramente, por esta Comisión, la que lo hará desde la óptica de la Defensa Nacional, y, posteriormente, por la de Seguridad Pública, la que la examinará a la luz de la seguridad interior del Estado.

Comunicó que la segunda instancia legislativa citada está analizando, en particular, el proyecto de ley que crea el Ministerio de Seguridad Pública (Boletín N° 14.614-07). Añadió que, oportunamente, se coordinarán ambas iniciativas.

Para finalizar, solicitó a la Directora Ejecutiva de la Cámara Chilena de Infraestructura Digital hacer llegar a esta Comisión mayores antecedentes respecto a los tipos penales aludidos con ocasión de los hechos de vandalismo relatados.

7) Exposición del profesor de Derecho Informático de la Pontificia Universidad Católica de Valparaíso, señor Renato Jijena.

El profesor de Derecho Informático de la Pontificia Universidad Católica de Valparaíso, señor Renato Jijena, juzgó, en primer término, que, quizás, esta proposición de ley debiera ser revisada también por la Comisión de Constitución, Legislación, Justicia y Reglamento, toda vez que contiene algunos aspectos que impactan en materia de derechos fundamentales.

Posteriormente, consignó que el proyecto en estudio tiene dos piedras basales: la ciberseguridad, por un lado, y la infraestructura crítica, por otro.

En términos generales, respaldó la iniciativa de ley. Justificando su posición, puntualizó que está bien estructurada; es completa; propone una legislación moderna; actualiza algunos conceptos, y sus objetivos generales y principios rectores, a priori, parecen bien definidos. Con todo, prosiguió, ello no obsta a la necesidad de depurar algunos de sus aspectos, especialmente los que se repiten, como el concepto de ciberespacio.

Alertó que tal expresión está contenida en la Política Nacional de Ciberseguridad, y que el texto en discusión la reformula. En consecuencia, llamó a revisarlo.

Continuando con el desarrollo de su exposición, puso de relieve que el estado de conectividad de Chile en el contexto del ciberespacio vía redes -y en especial mediante internet- es muy alto y se incrementa a diario, lo que inevitablemente se traduce en riesgos, vulnerabilidades e incidentes de ciberseguridad. Así, especificó, se observa, por ejemplo, en el caso del Servicio Nacional del Consumidor.

En la medida en que hay más servidores y conectividad susceptibles de atentados, mayor será el número de accesos indebidos, lamentó. Esta realidad obliga a adoptar medidas de prevención y a que exista un órgano ad

hoc para tal propósito. Al respecto, consideró que la Agencia Nacional de Ciberseguridad será un significativo aporte. Sin perjuicio de ello, advirtió la utilidad de revisar algunas de sus atribuciones, como la fijación unilateral de estándares mínimos de ciberseguridad para los órganos de la Administración del Estado.

Centrándose en el ámbito de aplicación de esta ley marco, sostuvo que abre la puerta a un posible conflicto, dado que ya existe un concepto legal sobre el particular, a menos que ambos sean complementarios. En efecto, planteó que el decreto supremo N° 533, de 2015, del Ministerio del Interior y Seguridad Pública, entiende por ciberseguridad a una condición en el ciberespacio, que se caracteriza por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, a los componentes lógicos de la información y a las interacciones que se verifican en él, debiendo tener en cuenta las políticas y técnicas para lograr esa condición. Por su lado, acotó, el artículo 2°, N° 4, de esta iniciativa, pone otros énfasis y alude a las acciones para el estudio y el manejo de las amenazas y los riesgos y a la prevención, mitigación y respuesta frente a los eventos que afecten a los activos informáticos y de servicios.

Lo dicho, hizo hincapié, no es algo menor, porque, al momento de fijar los alcances de la aplicación de esta ley, será clave y podría conducir a su judicialización.

En lo que atañe a los principios rectores, los compartió y calificó de idóneos. Algunos, puntualizó, son generales y obvios, como el de responsabilidad, y están en el mundo público y en el privado. Aseveró que en este último sector hay áreas que ya lo contemplan; así, verbigracia, ocurre en el caso de la banca, en donde la Comisión del Mercado Financiero tiene grandes exigencias en la materia. A ello, continuó, se suman textos estandarizados, como ciertas normas ISO.

Sin embargo, anunció, se formulan otros, cuyo alcance deberá ser interpretado según la lex artis y los estándares conocidos de ciberseguridad, como el de protección integral, el de confidencialidad, el de disponibilidad y el de integridad de los sistemas informáticos. Así, por ejemplo, ocurre al aludirse copulativamente a la determinación de los riesgos potenciales que puedan afectar a los sistemas, servidores y redes y -para su protección- a la aplicación de las medidas técnicas, organizativas y de gestión apropiadas, bajo el paraguas de la protección integral. Lo anterior, adelantó, puede acarrear conflictos, por lo que es recomendable un mayor desarrollo en el texto legal.

En cuanto a los objetivos generales, señaló que la propuesta legal declara los cuatro siguientes, que, a priori, el articulado operativiza en forma correcta:

a) 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 estos y los particulares;

b) Disponer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad;

c) Contemplar 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, e

d) Incluir mecanismos de control, supervisión y de responsabilidad por la infracción de la normativa.

Apuntó que un aspecto que parece muy trascendente es el que dice relación con los derechos fundamentales. En este punto, observó que a la Agencia Nacional de Ciberseguridad se le mandata para cautelar, especialmente, la reserva de los secretos y de la información comercial sensible de que conozca -esto es, su confidencialidad-, así como el respeto a los derechos fundamentales del artículo 19, N° 4, de la Constitución Política de la República. Estos últimos, explicó, son dos, diversos y autónomos, siendo el más amplio la protección de datos personales, correspondientes a aquellos que identifican o hacen identificable a una persona natural y, el más restrictivo, la vida privada o privacidad.

Por consiguiente, **el señor Jijena** valoró que la iniciativa de ley contemple como un deber explícito de la entidad referida respetar la reserva de los antecedentes de las personas.

Para terminar, fijó su atención en el Título VII, referido a las infracciones y sanciones. Sobre el particular, previno que, al margen de los montos de las multas, los elementos a considerar para fijarlas -en una primera lectura- aparecen muy genéricos, reflejándose ello, por ejemplo, en la ponderación relativa a si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones. En atención a tal advertencia, estimó conveniente que, a nivel legal, se fijen criterios de determinación más rígidos y exigentes.

El Honorable Senador señor Pugh remarcó que todas las acciones a desarrollar en el ciberespacio deben ser reguladas. Especificó que piezas esenciales en él son la identidad digital y los derechos de las personas, como la libertad de expresión. Aclaró que este tipo de derechos no corresponde a las máquinas.

Por otro lado, afirmó que los ataques suelen provenir de bandas criminales que trabajan con inteligencia artificial. Agregó que los accesos indebidos se incrementarán en la medida en que aumenten las conexiones, dado que la amplitud de la superficie supone también la de incidentes. Resaltó que la tecnología 5G implicará billones de dispositivos vinculados que proporcionan información, todos los cuales merecen protección.

En el mismo orden de ideas, notó que Chile ingresa a una velocidad increíble a la dimensión digital; en efecto, es el país que tiene la mayor cantidad de conexiones, pese a lo cual aún no posee una legislación sobre ciberseguridad. En consecuencia, hizo un llamado a precaver los riesgos que implica la apertura a tal dimensión, y destacó que esta es la primera normativa en donde quedará establecido qué significa este nuevo espacio.

Estimó también importante otros cuerpos legales que sostienen a este proyecto; entre ellos, la iniciativa sobre protección de datos personales (Boletín N° 11.092-07).

Adicionalmente, dijo que es esencial que la futura ley responda a las transformaciones digitales venideras. Actualmente, recordó, se está pasando del internet 2D al 3D, en donde ocurrirán interacciones desconocidas.

En lo que atañe al modelo más adecuado a implementar, recomendó revisar la experiencia comparada. Con todo, afirmó que el país tiene recursos financieros para el desarrollo de la ciberseguridad, toda vez que existe un crédito del Banco Interamericano de Desarrollo para ello.

Siguiendo con su intervención, anheló el resguardo no solo del sector público, sino también del privado. A mayor abundamiento, aspiró a que los proveedores de servicios del Estado cuenten con sus propios centros de respuesta ante incidentes, y que haya un gran coordinador nacional. Informó que España, en enero del año en curso, creó el Centro de Operaciones de Ciberseguridad, que abarca al mundo físico y al digital, e indicó que medidas como la expuesta son esenciales en escenarios de guerras híbridas, como la que vive Ucrania.

A su vez, **el Honorable Senador señor Huenchumilla** solicitó al invitado profundizar en el breve análisis constitucional efectuado al aludir al artículo 19, N° 4, de la Carta Fundamental.

Abocándose a los requerimientos del Presidente de la Comisión, **el profesor de Derecho Informático de la Pontificia Universidad Católica de Valparaíso, señor Renato Jijena**, explicó que una pregunta clave a tener en consideración es cuáles son las responsabilidades que se pueden generar y cómo afectan los bienes jurídicos fundamentales.

Relató que el debate tecnológico está estrechamente vinculado a la confidencialidad. Aclaró que esta es distinta a la privacidad y a la protección de datos. Así, especificó que aquella es un atributo de los sistemas, servidores, redes y bases, entre otros, y que para ello hay obligaciones de secreto y existe el decreto supremo N° 83, del Ministerio Secretaría General de la Presidencia, promulgado en 2004 y publicado en 2005, norma técnica del sistema de ciberseguridad y gestión de la información.

Detalló que una de las atribuciones de la Agencia Nacional de Ciberseguridad se relaciona con el respecto de las garantías constitucionales a las que alude el artículo 19, N° 4, de la Constitución Política de la República, particularmente con la protección de antecedentes personales de los individuos. Notó que, si bien está consagrada en el Texto Supremo, no ha sido objeto de una construcción robusta a nivel legal.

Consideró que el proyecto, al otorgar facultades a la Agencia Nacional de Ciberseguridad, debe analizar bien cuáles serán las que poseerá en materia de fiscalización, evitando transformarla en una entidad de protección de datos que entre en conflicto con la existente.

En definitiva, prosiguió, es indispensable desarrollar más las facultades de control que tendrá en el caso de que los antecedentes referidos sean vulnerados por un incidente de ciberseguridad como, por ejemplo, si se filtraran las bases de información de salud de los ciudadanos, pues el texto solo lo aborda tangencialmente.

El Honorable Senador señor Macaya puso de relieve que la proposición legal en estudio es de suma importancia para el país. Por ello, lamentó la ausencia del Ejecutivo en su tramitación. A mayor abundamiento, expresó que, conforme a nuestro ordenamiento jurídico, es un órgano colegislador.

Adicionalmente, destacó que la Agencia Nacional de Ciberseguridad será una institución pública y, en consecuencia, el Ministerio del Interior y Seguridad Pública y el de Defensa Nacional debieran seguir de cerca su estudio.

En línea con lo expuesto, solicitó al Presidente de la Comisión comunicarse con las Secretarias de Estado aludidas, manifestándoles la preocupación ante el abandono de este proyecto de ley. Además, requirió que les solicitara informar qué medidas adoptarán para perfeccionarlo.

El Honorable Senador señor Saavedra pidió claridad sobre la naturaleza jurídica de la Agencia Nacional de Ciberseguridad, como también respecto a qué ministerios quedará vinculada.

Por otro lado, anheló saber quién, a su vez, controlará a esta entidad, con la finalidad de garantizar que Chile no será vulnerado por países más desarrollados.

Poe último, hizo ver que las investigaciones realizadas por las instituciones de educación superior pueden servir como un camino de independencia tecnológica y para proteger la ciberseguridad del Estado, razón por la cual llamó a tenerlas a la vista.

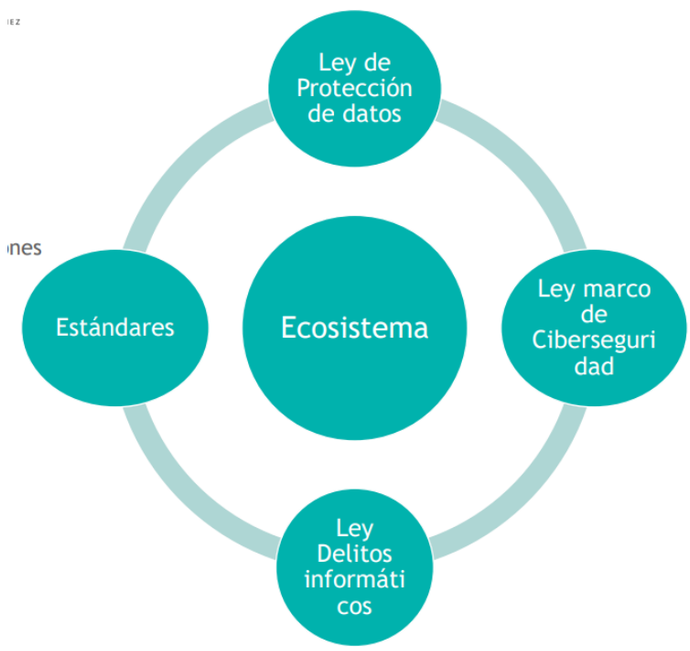
8) Exposición de la Académica de la Universidad Adolfo Ibáñez, señora Romina Garrido.

La académica de la Universidad Adolfo Ibáñez, señora Romina Garrido, afirmó que la necesidad de hablar de seguridad en el espacio virtual surge del incremento de las relaciones humanas en dicho lugar. En efecto, resaltó que este ha devenido en un sitio de interacción, en donde las personas adquieren servicios, realizan compras y ventas, desarrollan relaciones sociales y estudian.

Puso de relieve que, en un contexto de aumento de las capacidades de producción, recolección y tratamiento de datos digitales, la ciberseguridad juega un rol fundamental para la protección de la información. A las razones señaladas, recordó, se suma el hecho que el Estado se ha volcado a ser digital, luego de la entrada en vigencia de la ley N° 21.180. De esta manera, insistió,

aquella se torna un elemento básico para llevar adelante el referido proceso, así como el ejercicio de los derechos de los individuos en este nuevo mundo.

Consignó que la Política Nacional de Ciberseguridad del año 2017, que fija una hoja de ruta hasta el 2022, plantea un ecosistema normativo para recorrer la ruta trazada. Dentro de los compromisos asumidos en el escenario citado, acotó, se encuentra la ley de protección de datos -en tramitación en la Cámara de Diputados (Boletín N° 11.092-07)-; la fijación de estándares para ciertos sectores fundamentales de la sociedad, como el bancario, el de las telecomunicaciones, el de las pensiones, el eléctrico y el de la seguridad social; la ley de delitos informáticos, y la ley marco de ciberseguridad, tal como se aprecia en el gráfico que sigue:

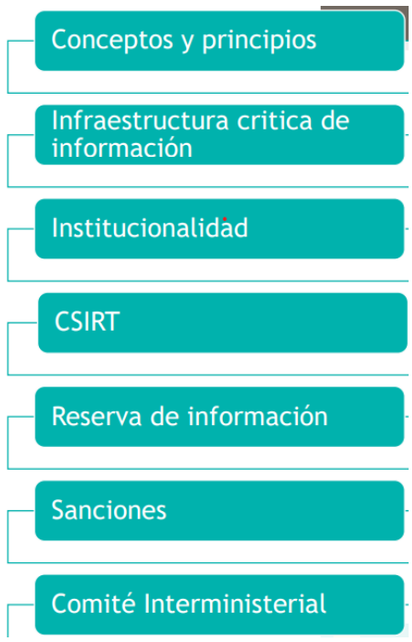


Así, observó, esta propuesta legal cumple con uno de los compromisos asumidos en el instrumento indicado, y aborda en un solo texto normativo la gobernanza de la ciberseguridad, por un lado, y la infraestructura crítica de la información, por otro.

Declaró que los objetivos de esta iniciativa de ley consisten en sentar las bases de la institucionalidad de la seguridad virtual, los principios rectores y los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de esta naturaleza, y establecer las atribuciones y obligaciones de los órganos del Estado, así como de las instituciones privadas que posean infraestructura de la información calificada como crítica.

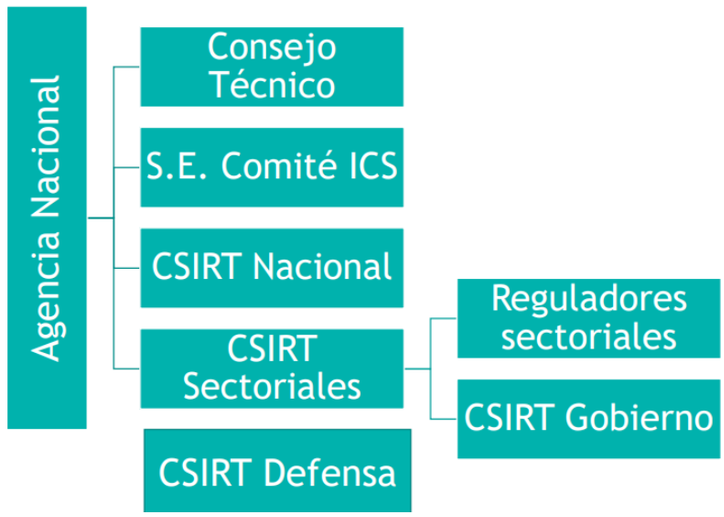
En sintonía con lo expuesto, llamó a tener en cuenta que si bien en la actualidad existe un modelo de gobernanza provisorio, se requiere uno de carácter permanente, capaz de fijar las exigencias básicas para la coordinación de todos los actores participantes.

Adentrándose en el análisis de la proposición de ley, comentó que ella presenta la siguiente estructura:



Puso de manifiesto que, a diferencia de los textos legales de la experiencia comparada, este define la expresión ciberseguridad, concepto en evolución. Al respecto, especificó que se entiende por ella 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. Celebró en este punto la iniciativa aludida, mas llamó a revisar su descripción para evitar ser presa de ella.

Exhibiendo un esquema del proyecto en estudio, sostuvo que su columna vertebral está constituida por la Agencia Nacional de Ciberseguridad y los órganos que se indican a continuación:



Relató que, en un primer momento, el citado organismo rector será una entidad dependiente del Ministerio del Interior y Seguridad Pública. A futuro, consideró, debiera alojarse en el nuevo Ministerio de Seguridad Pública.

Fijando su atención en las funciones previstas para la Agencia Nacional de Ciberseguridad, informó las siguientes:

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

2) Coordinar el ecosistema de actores;

3) Dictar la normativa técnica;

4) Administrar el Registro Nacional de Incidentes de Ciberseguridad;

5) Regular y fiscalizar al Estado y a los privados que posean infraestructura de la información calificada como crítica y que no estén sometidos a una competencia específica. Al respecto, juzgó esencial expresar con mayor precisión a quién corresponderá llevar a cabo tales acciones, dado que el texto en debate no señala si tal función corresponderá a Superintendencias, Subsecretarías o al Sernac, y

6) Cursar las sanciones y llevar los procedimientos sancionatorios. Tal labor, puntualizó, corresponde al Director.

Establecido lo anterior, enfatizó que contar con una Agencia Nacional de Ciberseguridad es una necesidad urgente, toda vez que será la institucionalidad coordinadora del ecosistema de seguridad virtual. Añadió que la entidad mencionada es más que un mero organismo técnico. En efecto, subrayó, es una institución de gestión, análisis, de generación de cultura, de colaboración y quien tendrá una mirada estratégica. Ella, descartó, no es centro de respuesta ante incidentes, y deberá coordinarse con la Agencia de Protección de Datos.

Seguidamente, hizo un llamado a revisar su estructura funcional, su dependencia y la relación con otros entes públicos, particularmente en lo que refiere a sus capacidades regulatorias.

Deteniéndose en los CSIRT sectoriales, afirmó que muestran un gran avance. Con todo, manifestó la conveniencia de precisar quiénes cumplirán dicha función.

Aseveró que los órganos referidos constituyen la formalización de una estructura existente. En este punto, recordó que actualmente hay entidades de esta naturaleza con normativa propia. No obstante, alertó, se observa un alto grado de dispersión, requiriéndose la coordinación de la Agencia Nacional de Ciberseguridad.

Adicionalmente, estimó que la cadena de reportes es compleja y que falta claridad en las obligaciones que deben cumplir las instituciones reguladas, debiendo especificarse a quién y cómo comunicar. Ello, justificó, porque compartir información es una pieza clave.

Por otro lado, planteó que es indispensable que los CSIRT sectoriales estén coordinados con el CSIRT Nacional.

Siguiendo con el análisis de la proposición legal, se detuvo en las infraestructuras críticas de la información. Puntualizó que el proyecto las define como 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.

Previno que por servicios esenciales, en tanto, se comprende a todos aquellos cuya afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción de su infraestructura de la información pueda afectar gravemente: a) La vida o integridad física de las personas; b) La provisión de servicios sanitarios, energéticos o de telecomunicaciones; c) El normal funcionamiento de obras públicas fiscales y medios de transporte; d) La generalidad de usuarios o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que facultan la transacción de dinero o valores y, e) de modo general, el normal desarrollo y bienestar de la población.

Respecto al procedimiento para efectuar tal calificación, connotó que, conforme a lo dispuesto en el artículo 4° de la iniciativa de ley, el Ministerio del Interior y Seguridad Pública requerirá, cada dos años, al Consejo Técnico de la Agencia Nacional de Ciberseguridad un informe que detalle cuáles son los sectores o instituciones que la poseen. Valoró tal mecanismo, en atención a la flexibilidad que proporciona.

Sin embargo, instó a revisar los factores que permiten concluir que en un área o institución existe infraestructura de la información que deba calificarse como crítica, dada su amplitud.

Continuando con su atención puesta en la misma materia, apuntó que la propuesta de ley contempla deberes generales para quienes las posean. Ellos, acotó, consisten en aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas e informativas 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.

Adicionó que las obligaciones específicas para el sector público y privado, en tanto, radican en la gestión de riesgos y en la forma de hacer su seguimiento, ejercicios continuos de revisión, simulacros y en la adopción de medidas de seguridad para reducir los impactos y los daños que pudieran

ocasionar los incidentes de ciberseguridad. Remarcó que el incumplimiento de estas constituye una infracción a la ley.

Asimismo, develó la oportunidad para precisar adecuadamente el rol del Consejo Técnico y de la Agencia Nacional de Ciberseguridad en la definición de las infraestructuras críticas de la información. Ello, argumentó, porque la propuesta indica que el primer organismo citado elaborará un informe exponiendo cuáles son las secciones o instituciones que las poseen, pero es el Ministerio del Interior y Seguridad Pública quien decide. En consecuencia, criticó, no se confiere un rol al primero.

Expresó que hay algunas ambigüedades que es imprescindible precisar, especialmente respecto a las responsabilidades derivadas de tal calificación. Sobre el particular, notó que el texto en tramitación presume que el hecho de determinar que un sector las tiene conlleva que las instituciones que lo conforman también.

En relación con el deber de comunicar previsto en la propuesta legal, sentenció que es una pieza clave para el funcionamiento del sistema. En este punto, hizo ver también algunos ajustes a realizar. Ahondando en su afirmación, explicó que por un lado hay un deber de información de la Agencia Nacional de Ciberseguridad al ecosistema de las alarmas de incidentes y uno desde lo sectorial hacia las infraestructuras críticas de la información. Pero, además, observó, hay uno desde los CSIRT Sectoriales hacia la Agencia cuando los incidentes tienen un impacto significativo.

En resumen, constató, la imposición mencionada se traduce en lo siguiente:

1) La Agencia informa a los CSIRT sectoriales alarmas de incidentes;

2) Los sectoriales, a las entidades de la administración y órganos regulados de su sector;

3) Las infraestructuras críticas de la información deben reportar a su CSIRT sectorial;

4) Los CSIRT sectoriales también deben comunicar a la Agencia incidentes de impacto significativo.

Planteó que las referencias a la Agencia Nacional de Ciberseguridad debieran hacerse al CSIRT Nacional.

Adicionalmente, expuso que si bien el deber de informar se encuentra dentro del régimen sancionatorio, no se entiende qué es lo que se castiga.

Formulando algunas conclusiones a su intervención, enfatizó que la iniciativa de ley avanza en una línea correcta, pero propone una estructura diversificada.

Opinó que un diseño descentralizado permite crear una mirada especializada en los sectores, evaluando impactos, culturas organizativas y generando estrategias que, sin duda, pueden converger con una coordinación eficaz.

En lo que atañe a la Agencia Nacional de Ciberseguridad, connotó la necesidad de delimitar sus funciones y alivianar su burocrática estructura. Al respecto, juzgó que algunas de las instituciones de la gobernanza transitoria no son indispensables, como el Comité Interministerial de Ciberseguridad.

Sugirió, además, revisar los criterios para las infraestructuras críticas de la información, como también los de reportes de incidencias.

Para concluir, hizo hincapié en que la protección del ciberespacio es vital para el bienestar de la población y para el funcionamiento de la sociedad, y remarcó que Chile está al debe en esta materia que constituye un componente de la seguridad pública.

El Honorable Senador señor Pugh advirtió que la exposición de la académica de la Universidad Adolfo Ibáñez hace reflexionar respecto a la utilidad de posicionar la Agencia Nacional de Ciberseguridad en un ecosistema de seguridad y dentro del futuro Ministerio de Seguridad Pública.

Agregó que al interior de la referida Cartera quedarán alojadas distintas entidades, entre ellas aquella cuya creación se propone en esta iniciativa de ley y la Agencia Nacional de Inteligencia.

En atención a lo indicado, llamó a evitar posibles conflictos entre ambas, asegurando una relación armónica. Justificando su posición, destacó que el proyecto de ley que fortalece y moderniza el sistema de inteligencia del Estado, contenido en el Boletín N° 12.234-02, considera también la evaluación de las infraestructuras críticas.

Por otro lado, previno que el mencionado ecosistema tiene diversos niveles. En ese contexto, subrayó que el CSIRT Nacional debiera ser un órgano supraministerial, a fin de tener la capacidad de ver qué está pasando en todo el Estado y de determinar cómo este y los privados -que gestionan el 85% de la infraestructura crítica nacional- pueden colaborar.

En línea con lo anterior, reiteró que España, en enero del año en curso, creó el Centro de Operaciones de Ciberseguridad, instancia que se ubica en un grado superior al de las Secretarías de Estado para coordinar todo lo que ocurre.

Recomendó también tener a la vista la experiencia española en lo que a los reportes respecta. Puntualizó que, en esta área, dicho país trabaja con sondas, las que ven las conexiones que están ocurriendo con los servidores, las que al detectar algo extraño, informan de inmediato. De esta manera, constató, el proceso aludido está automatizado, garantizando reacciones rápidas.

Siguiendo con su atención puesta en el CSIRT Nacional, instó a sustituir su denominación. La de hoy, acotó, da a entender que este equipo será el encargado de resolver incidentes de ciberseguridad, en circunstancias que no será así.

En el mismo orden de ideas, calificó como esencial que el órgano nombrado tenga la capacidad de determinar la atribución de los ataques.

Finalmente, solicitó a la invitada, de ser posible, remitir a la Comisión un documento en el que se expongan con mayor precisión aquellos aspectos que pudieran generar problemas de coordinación.

9) Exposición del Académico de la Universidad del Desarrollo, señor Juan Pablo González.

El académico de la Universidad del Desarrollo, señor Juan Pablo González, alabó la iniciativa de ley en estudio, toda vez que hará posible contar con una gobernanza definitiva en ciberseguridad. Recordó que actualmente Chile tiene una transitoria, liderada por el Ministerio del Interior y Seguridad Pública, en donde se aloja CSIRT Nacional. Además, agregó, el país posee un Comité Interministerial de Ciberseguridad, instancia presidida por el Subsecretario del ramo.

Sostuvo que, en paralelo, existe la Política Nacional de Ciberdefensa, la que fija una hoja de ruta para abordar la seguridad informática hasta el año 2022. Sin perjuicio de ello, notó, en la práctica, diversos sectores han dictado su normativa y se requiere homogeneizar la regulación.

Reveló que el CSIRT existente ha realizado enormes esfuerzos no solo en las materias propias de este tipo de entidad técnica -el manejo de incidentes informáticos, la promoción de buenas prácticas para su detección y la generación de entrenamiento a los diversos órganos de la Administración del Estado-, sino que también participa en la dictación de políticas públicas, leyes y reglamentos, lo que es propio de la labor de una autoridad especializada.

No obstante, estimó que el rol asumido debiera quedar radicado en la Agencia Nacional de Ciberseguridad, con el objeto de que pueda coordinar, colaborar y dar pie al diálogo de los diversos sectores involucrados en el área.

En sintonía con lo expresado, aseveró que un elemento esencial de cualquier autoridad de ciberseguridad es generar puentes entre el área pública, la privada y la academia, fomentando la cooperación y la confianza.

Como lo ha reconocido la experiencia internacional, prosiguió, la existencia del CSIRT Nacional otorga múltiples beneficios para aumentar la madurez de los órganos de la Administración del Estado como de aquellos sectores críticos.

Connotó que el proyecto de ley es ambicioso en la generación de diversos equipos de respuesta a incidentes de seguridad informática; a saber:

el CSIRT Nacional; el de Gobierno; el de Defensa y los sectoriales, llamando a la especialización. También, añadió, crea dos CSIRT dentro de la Agencia.

Ahondando en el punto anterior, consideró conveniente explicar con claridad cuál será la relación del CSIRT Nacional y el de Gobierno. Ello, adujo, con el propósito de alivianar la carga burocrática; de crear políticas que puedan ajustarse a la realidad del país y de tener una visión respecto a cómo resolver los problemas de seguridad informática, tanto interna como externamente.

Continuando con el examen de la proposición legal, celebró la obligación de reportar incidentes desde el regulado al CSIRT sectorial correspondiente dentro del plazo de 24 horas. Al respecto, llamó a tener presente que la experiencia ha demostrado que tiempos tan breves acarrean inconvenientes a las áreas reguladas. Por lo anterior, manifestó la importancia de comprender las características y los niveles de madurez de cada sector.

Adicionó que el CSIRT Sectorial tiene, a su vez, la misión de comunicar al CSIRT Nacional en el lapso de una hora en caso de impactos significativos. Cuando ellos ocurren, acotó, poniendo en riesgo a todo el país, se requiere una visión más amplia, ya sea desde la Agencia Nacional de Ciberseguridad o desde la defensa.

Abocándose al análisis de la determinación de una infraestructura como crítica de la información, enfatizó que no es algo baladí. En efecto, profundizó, un sector de esta naturaleza implica una carga regulatoria adicional en cuanto a la inversión en recursos técnicos y monetarios.

En ese contexto, juzgó que los criterios que establece el proyecto para arribar a tal conclusión deben ser revisados, asegurando que la criticidad no sea la regla general, como pareciera desprenderse.

Proporcionando antecedentes de la legislación comparada, informó que la normativa española (Ley Nº 8/2011) tiene como factores para calificar un sector como crítico: 1) el número de personas afectadas; 2) el impacto económico; 3) la repercusión medioambiental, degradación en el lugar y sus alrededores y, 4) el efecto público y social, por la incidencia en la confianza de la población de la Administraciones Pública, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales. Todos ellos, remarcó, permiten garantizar su excepcionalidad, evitando sobrecargar regulatoriamente a las secciones que por su nivel de madurez no están en condiciones de asumir tantas obligaciones. Sin embargo, enunció, a medida que avance la ciberseguridad en el país, se pueden incluir nuevas áreas.

Por otro lado, observó que la propuesta legal no contiene mención alguna relativa al sistema de impugnación de la declaración de criticidad. Tampoco, alertó, aplica supletoriamente la ley Nº 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

En lo que respecta al régimen sancionatorio del proyecto de ley, consignó que el Título VII establece infracciones y penas asociadas al incumplimiento de las obligaciones establecidas en el cuerpo normativo.

Pormenorizó que entre las vulneraciones se encuentran el retardo o entrega fuera de plazo de la información requerida; negarla injustificadamente; la entrega maliciosa de datos falsos o manifiestamente erróneos, o quebrantar los deberes para aquellas entidades declaradas como críticas.

Las multas que pueden imponerse, en tanto, comunicó, van en un rango entre las 10 a 20.000 UTM, y existe una agravante especial cuando se configure algún ataque al sistema o a la data informática en aquella infraestructura crítica.

Sin embargo, lamentó, la proposición en estudio no establece una vacancia legal para la aplicación de sanciones, lo que podría resolverse mediante una marcha blanca, incorporando, por ejemplo, un plazo de 6 meses o de 1 año desde publicación de la ley.

Además, reveló, el proyecto nada dispone sobre la existencia de recursos ante la decisión del Director la Agencia de sancionar a una organización privada declarada como crítica.

Asimismo, mostró que el texto analizado hace un uso excesivo de la potestad reglamentaria. A mayor abundamiento, especificó que prescribe en diversos artículos que el Ministerio del Interior y Seguridad Pública establecerá los detalles en un cuerpo normativo de esta naturaleza.

Pormenorizó que las materias que serán desarrolladas de la forma indicada son nueve. En consecuencia, solicitó examinar cuáles ameritan ser reguladas así, evitando postergar la plena operatividad de la Agencia Nacional de Ciberseguridad y, por consiguiente, retrasando el objetivo perseguido.

Para concluir, sentenció que la iniciativa de ley constituye un enorme avance al crear una estructura permanente en materia de ciberseguridad, posibilitando entenderla no solo como un componente técnico sino también con una visión multidisciplinaria, desde una perspectiva estratégica y de cultura. Sin perjuicio de ello, reiteró la necesidad de perfeccionar algunos aspectos.

10) Exposición del experto internacional en seguridad cibernética, señor Israel Reyes.

El experto internacional en seguridad cibernética, señor Israel Reyes, alabó la iniciativa de ley objeto de análisis, su estructura y la regulación propuesta.

En sintonía con lo manifestado, celebró la idea de incorporar algunas definiciones básicas y los principios que iluminarán el texto normativo. Asimismo, valoró el establecimiento de factores que determinarán cuándo una infraestructura de la información posee el carácter de crítica y las obligaciones que se derivarán de tal calificación.

A la luz de lo señalado, constató que el foco del proyecto radica en los posibles ataques a los activos que son esenciales para el funcionamiento de una sociedad y de una economía. Con todo, advirtió que no se abordan los hackeos neurocognitivos y las operaciones sicológicas en las redes sociales. A mayor abundamiento, sentenció que si bien se crea la Agencia Nacional de Ciberseguridad, no hay referencia alguna a ellos.

Haciendo ver la importancia de regularlas, recordó diversos ataques cibernéticos, como el provocado recientemente por Rusia a Ucrania; el sufrido por Estonia, y el de Georgia el año 2008, entre otros.

Deteniéndose en la experiencia estadounidense, manifestó que la Ley de Decencia en las Comunicaciones exime de responsabilidad a los dueños de las plataformas digitales por el contenido publicado en ellas, pese a que este puede socavar la credibilidad de un gobierno y de las instituciones, llevando a una situación de ingobernabilidad e, incluso, de guerra civil.

En atención a la realidad expuesta, recomendó incluir en la iniciativa de ley un título que norme la actividad de los trolls y de los bots, sometiéndolos a la legislación nacional.

En línea con lo planteado, explicó que la gobernanza y la seguridad en el ciberespacio tiene dos aristas: los ataques a la infraestructura crítica de la información, que se dirigen en contra de la confidencialidad, integridad y disponibilidad de los sistemas de la Nación, por un lado, y aquellos que suponen una guerra sicológica o de desinformación.

En el mismo orden de consideraciones, consignó que los proveedores de redes sociales debieran ser calificados como infraestructura crítica de la información, atendida la gran cantidad de datos personales que almacenan.

Indicó que, si bien el proyecto de ley precisa los deberes específicos que pesan sobre quienes la poseen, no demanda la capacitación continua ni auditorias independientes. Sobre el particular, fue tajante en sostener que resulta fundamental obligarlos a someterse a estas últimas, a fin de evaluar el riesgo y la probabilidad que existe en caso de ataque de desinformación en una red social en contra del gobierno o en contra de sistemas esenciales.

Fijando su atención en el Título VIII de la propuesta de ley, apreció la creación del Comité Interministerial de Ciberseguridad, pues aseguró que uno de los aspectos que suele fallar en la legislación comparada es la comunicación entre Secretarías de Estado.

En lo que respecta al Título III, celebró la decisión de asignar a la Agencia Nacional de Ciberseguridad la calidad de órgano asesor del Presidente de la República en materia de seguridad informática. Sin embargo, estimó imprescindible también que cumpla tal función con el Ministerio de Defensa Nacional en aras de la seguridad del Estado.

Seguidamente, valoró la creación del Equipo Nacional de Respuesta ante Incidentes de Ciberseguridad, organismo encargado de coordinar los CSIRT sectoriales, como asimismo el CSIRT de Gobierno y el de Defensa. No obstante, juzgó importante aclarar cuál es la línea que divide los aspectos de seguridad nacional y los de seguridad interna.

El Honorable Senador señor Pugh subrayó que la ciberseguridad es un concepto amplio que va más allá de los ataques a infraestructuras críticas. En efecto, concordó, abarca también la protección de los datos personales y la interoperabilidad.

Puso de manifiesto que, tal como lo como lo señala la Política Nacional de Ciberseguridad, es necesario contar con un cuerpo legislativo que resguarde los actos digitales del Estado, las personas naturales y jurídicas y los dispositivos conectados a la red, lo que supone una arquitectura digital robusta y resiliente.

Su Señoría recordó que en la Cámara de Diputados se encuentra radicada la iniciativa de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletines N°s 11.144-07 y 11.092-07, refundidos). Ambas proposiciones legales, remarcó, permitirán enfrentar el desafío de la seguridad informática.

Adicionó que, desde el punto de vista de la defensa, resulta esencial preservar al país de los ataques externos, particularmente de aquellos de índole estatal. Una experiencia tal, relató, ocurrió recientemente con la agresión de Rusia a Ucrania, en donde, simultáneamente, el primer país aludido desplegó sus capacidades militares y cibernéticas.

En consecuencia, hizo ver la importancia de perfeccionar la iniciativa de ley en los términos propuestos por el experto en ciberseguridad, de manera de saber quién está detrás de las agresiones y de las campañas de desinformación, como lo hace el modelo español.

Por otro lado, señaló que no solo hay infraestructura crítica, sino también procesos de tal carácter que merecen ser protegidos; este es el caso, ejemplificó, del acto eleccionario del pasado 4 de septiembre.

A reglón seguido, observó que la propuesta legal no define los grados de alerta, lo que resulta fundamental para orientar los esfuerzos.

Adicionalmente, llamó a tener en cuenta que las Fuerzas Armadas tienen capacidades no solo físicas, sino también en el ciberespacio. Estas últimas, consideró, deben coordinarse, por medio de un centro nacional de carácter supraministerial, para poder determinar quién está detrás de los ataques. A mayor abundamiento, relevó que si estos provienen de un actor estatal no se está en presencia de una mera amenaza, sino una declaración de guerra.

Afirmó que enfrentar las campañas de desinformación protegerá la democracia del país en la era de la inteligencia artificial. En este punto, connotó

que la libertad de expresión es un derecho humano, y no uno que corresponda a los bots, trolls, avatar u otros.

Prosiguiendo con sus planteamientos, resaltó que Chile es un referente en materia digital, por ser el Estado con más conectividad móvil de Latinoamérica y el que posee la mayor velocidad de fibra óptica, la que, además, tiene un gran despliegue. Sin embargo, lamentó, tal expansión no ha ido acompañada del desarrollo de ciberseguridad, arriesgándose los activos nacionales y a las personas.

En línea con lo anterior, postuló que la Agencia Nacional de Ciberseguridad será el motor para generar una cultura de protección en el ciber espacio.

Advirtió, por otra parte, que el proyecto en estudio no contiene referencia a ley N° 21.113, que declara el mes de octubre como el de la ciberseguridad, de la ciberseguridad, dando cuenta de la desconexión existente en cuanto al desafío a enfrentar.

Por último, observó que en materia de defensa deberán levantarse las infraestructuras críticas de la información más importantes, esto es, aquellas en donde exista una mayor probabilidad de ocurrencia de un hecho con gran impacto.

El Honorable Senador señor Huenchumilla consultó si el problema descansa en las nuevas tecnologías o en las noticias falsas emitidas a sabiendas de su falta de veracidad. Añadió que las mentiras también pueden expresarse por otros medios, pero su alcance es limitado. Estas herramientas, en tanto, posibilitan una extensión considerable, provocando riesgos en servicios esenciales y en la gobernabilidad, entre otros.

Apuntó que la respuesta a su interrogante determinará dónde poner el énfasis en esta iniciativa de ley.

Finalmente, hizo ver que el sector defensa y el de seguridad pública tienen grandes desafíos en este nuevo escenario tecnológico que no solo trae beneficios, sino también peligros.

El Honorable Senador señor Pugh deteniéndose en la intervención del Presidente de la Comisión, aclaró que el problema no radica en los medios, sino en su utilización para fines inadecuados. Asimismo, agregó que las noticias falsas no generan mayores inconvenientes, a menos que supongan campañas de desinformación y haya una organización detrás que busque desestabilizar.

Arguyó que hacer frente a estas amenazas requiere talento; vale decir, de personas preparadas, las que no necesariamente están en las Fuerzas Armadas. Por consiguiente, la figura de cibersoldados -reservas activas que se desempeñan en el sector privado y que puedan apoyar al personal castrense cuando se requiera- sería de gran utilidad.

A la medida anterior, estimó, podrían sumarse los incentivos adecuados para evitar que el capital humano capacitado de las Fuerzas Armadas salga de ellas.

11) Exposición del Coordinador de Ciberseguridad en Sistemas Eléctricos del Comité Chileno del Consejo Internacional de Grandes Redes Eléctricas, señor Eduardo Morales.

El Coordinador de Ciberseguridad en Sistemas Eléctricos del Comité Chileno del Consejo Internacional de Grandes Redes Eléctricas, señor Eduardo Morales, dio inicio a su exposición resaltando dos conceptos esenciales vinculados a la proposición de ley: infraestructuras críticas y ciberespacio. En relación con el primero de ellos, aseguró que si bien no hay una definición sobre el particular, al revisar aquellas dadas por la Comisión Europea o por la Agencia de Ciberseguridad y Seguridad de la Infraestructura -en adelante CISA-, se observan ciertas características comunes; a saber, son servicios esenciales; tienen carácter estratégico para la sociedad y la economía del país; son interoperables y dependientes entre ellas; viven en el plano físico y en el virtual, y poseen un alto impacto para la seguridad de la Nación y de las personas, como también para la estabilidad económica.

Apuntó que si se pudieran graficar, ellas serían los pilares de una ciudad, tal como se aprecia a continuación:

En lo que atañe a la voz “ciberespacio”, afirmó que hasta hace algunos años, era algo heterogéneo y abstracto. Sin embargo, hoy está adecuadamente definida a nivel internacional. Así, ahondó, en la Cumbre de la OTAN del año 2016, fue calificada como un nuevo dominio de las operaciones, al lado de los de tierra, mar, aire y espacio.

Luego, advirtió, el hecho de que las infraestructuras críticas estén conectadas con este último hace que la dependencia entre lo físico y lo virtual

sea aún más importante. De esta manera, subrayó, no es posible separar las infraestructuras físicas de las de la información, siendo ambas críticas.

Destacó que pese a que en el ciberespacio se generan muchas oportunidades, su existencia aumenta también los riesgos y amenazas, toda vez que crece la superficie de ataque.

Por otro lado, puso de relieve que son las interacciones humanas las que abren las puertas al espacio virtual, que está conformado por la infraestructura física, la lógica y todas las interrelaciones entre las personas.

Planteó que lo anterior conduce a hablar de los sistemas cibernéticos y ciberfísicos, los que tienen tres características importantes: conjugan el control, la computación y la comunicación.

Dando ejemplos del segundo modelo aludido, recordó que está presente en las líneas 3 y 6 del Metro de Santiago, en donde los vagones que transitan por ellas no tienen conductor y funcionan de forma remota. Lo mismo ocurre en materia eléctrica y en las telecomunicaciones, afirmó.

Alertó que este cambio de paradigma implicará que los datos -o flujos de información- lleguen a ser más importantes que los flujos de energía para los operadores. No obstante, previno, también lo serán para los hackers.

En sintonía con lo expresado, consignó que conforme a lo señalado por Data Management Association -DAMA por sus siglas en inglés-, un dato ubicado en un contexto da lugar a información. Si a ella se añade inteligencia, se obtiene conocimiento y si a este se le suma buena estrategia, se crea poder. Este último, insistió, beneficiará a los países, al generar ciudades inteligentes, pero también atraerá a ciberactivistas. En consecuencia, sin resguardo adecuado en la legislación, los ataques se incrementarán, alertó.

Con todo, remarcó que las ciberamenazas son uno de los tantos riesgos de las infraestructuras críticas, existiendo también las pandemias, los terremotos, los actos terroristas y el cambio climático, entre otros.

Continuando con el desarrollo de su exposición, informó que el plan de protección Nacional de Infraestructuras Críticas de Estados Unidos, considera una gobernanza enfocada en la gestión y en los indicadores clave de rendimiento, asegurando la medición periódica del desempeño y nivel de madurez de cada uno de los sectores críticos.

Sostuvo que la CISA es un instrumento fundamental en dicho ámbito, cuya misión consiste en lograr que los activos que son esenciales para el funcionamiento de una sociedad y una economía sean más resilientes.

Deteniéndose en la evolución de las capacidades de defensa para la infraestructura crítica, enunció que hay guías y modelos sobre el particular. Precisó que la gran mayoría se centra en dar visibilidad de lo que tienen. Así, especificó, ocurre con las sanitarias, el sector eléctrico y el de transportes, y un nivel de madurez superior posibilitaría tener capacidad de respuesta, permitiendo atender de forma rápida y temprana los ciberataques.

En atención a lo expuesto, celebró la iniciativa de ley analizada, especialmente su intención de poner el acento en la conformación de un CSIRT Nacional y de equipos de respuesta a incidentes de seguridad informática sectoriales. No obstante, señaló que el texto en tramitación no contempla atribuciones para los CSIRT vinculadas a la ciberinteligencia, dificultándoles la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoyan la toma de decisiones.

Lo dicho, lamentó, da cuenta de que no se consideran las herramientas para adelantarse a los imprevistos, evitar ataques y adoptar acciones de forma rápida.

En cuanto a la determinación de los sectores que poseen infraestructura crítica de la información, dio a conocer que la Submesa de Operadores de Servicios Esenciales ha propuesto los siguientes:

Ellos, estimó, debieran ser las áreas a ponderar en el proyecto de ley. Sin embargo, postuló que tal como se observa en la lámina acompañada, hay tres que son de suma importancia, atendido su alto nivel de interdependencia con otras infraestructuras críticas: el de energía, el de las telecomunicaciones y el de las aguas. Por consiguiente, sugirió que una vez entrada en vigencia la ley, estas sean las tres primeras cuya protección se refuerce.

Justificando la exclusión del sector defensa, sostuvo que la mesa de trabajo aludida ha adoptado un modelo similar al previsto en la normativa española, conforme a la cual las infraestructuras críticas de las Fuerzas Armadas y de la Policía se rigen por sus propias normativas.

Enseguida, exhibió los avances realizados por el grupo de trabajo citado en cuanto a definiciones:

Basado en la Ley Española: Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se toman como definiciones los siguientes términos:

- **Servicio esencial:** El servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, para organismos públicos y privados.

- **Sector estratégico:** Cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Se definen los siguientes sectores estratégicos:

1. Energía
2. Telecomunicaciones
3. Aguas
4. Salud
5. Financiero
6. Transporte
7. Industria Crítica
8. Alimentación
9. Educación
10. Administración Pública
11. Industria Química
12. Espacio
13. Instalaciones de Investigación
14. Instalaciones Comerciales
15. Organizaciones Tecnológicas

Subsector estratégico: Cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados.

Infraestructuras críticas: Son las infraestructuras compuestas por las instalaciones físicas, redes, sistemas y equipos físicos y de tecnología de la información (TI), y/o sistemas y redes en el ámbito de: Tecnologías de Operación (TO), y/o Sistemas de Control Industrial y/o dispositivos del Internet de las Cosas (IoT), sobre las que descansa el funcionamiento de los servicios esenciales, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Zona crítica: Aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas (públicas o privadas) radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías de Orden y Seguridad.

Criterios de criticidad: los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.
2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.
3. El impacto medioambiental, degradación en el lugar y sus alrededores.
4. El impacto público, reputacional y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

- **Análisis de riesgos:** el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

- **Interdependencias:** los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, nacional o internacional.

- **Protección de infraestructuras críticas:** el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

- **Información sensible sobre protección de infraestructuras críticas:** los datos específicos sobre infraestructuras críticas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.

- **Operadores críticos:** las entidades u organismos, denominados también como Operadores de Servicios Esenciales, responsables de las inversiones o del funcionamiento diario de las infraestructuras críticas, tanto públicas como privadas.

Organizaciones Tecnológicas: las empresas que dan soporte y gestión tercerizada a las infraestructuras críticas a nivel de sus sistemas y redes de tecnología de la información y/o sistemas y redes en el ámbito de: Tecnologías de Operación (TO), Sistemas de Control Industrial y/ dispositivos del Internet de las Cosas (IoT). ***(Estos proveedores no son responsables de la seguridad del servicio esencial pero si deben alertar, informar y reportar de manera oportuna a lo que establezca la ley, ante cualquier amenaza de ciberincidente, lo cuál implica que deben tener un sistema robusto de alerta temprana ante ciberincidentes de ciberseguridad)***

Nivel de Seguridad: Definido en un Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

Catálogo Nacional de Infraestructuras Críticas: la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras críticas existentes en el territorio nacional.

Centrando su atención en la gobernanza prevista en la iniciativa de ley, propuso que la Agencia Nacional de Ciberseguridad, a futuro, se enfoque en lo estratégico y táctico, dimensión que incluye la planificación, la elaboración de normas y la fiscalización en el cumplimiento de las exigencias. Adicionó que el Equipo Nacional de Respuesta a Incidentes de Seguridad, en tanto, debiera pasar a ser un gran centro de protección de infraestructura crítica en lo operativo, preocupado de la cooperación y de la coordinación con los CSIRT sectoriales.

El Honorable Senador señor Pugh expresó que grupos organizados son capaces de actuar de forma sistemática, produciendo ataques contra los Estados, los que pueden resultar muy destructivos. Añadió que los de índole externo deben preocupar de sobremanera al país y que en ellos el Ministerio de Defensa Nacional debe tener un rol fundamental.

Seguidamente, celebró que el invitado citara el modelo de ciberdefensa de infraestructuras críticas de Mandiant, el que, puntualizó, considera tres niveles: 1) Monitoreo de lo que ocurre; 2) Capacidad de respuesta, y 3) Amenazas. Para este último, resaltó, es fundamental la inteligencia con análisis de datos.

En sintonía con lo expuesto, concordó con el expositor acerca de la ausencia de capacidades relacionadas con la ciberinteligencia en la Agencia Nacional de Ciberseguridad.

A mayor abundamiento, postuló que el referido sistema debe tener una orientación clara respecto a cómo lograr ese objetivo y delimitar las áreas en dónde puede hacerse inteligencia abierta y dónde estará la inteligencia dura. Esta última, acotó, no está dentro del ámbito de competencias de la Agencia Nacional de Ciberseguridad.

A la luz de lo indicado, manifestó la necesidad de velar por que este texto legal esté en sintonía con la nueva ley que fortalece y moderniza el sistema de inteligencia del Estado, correspondiente al Boletín N° 12.234-02.

Para concluir su intervención y en base a lo planteado, consultó al invitado hasta dónde debiera extenderse la función de ciberinteligencia de la Agencia Nacional de Ciberseguridad. Asimismo, preguntó cómo ha sido la coordinación de las capacidades de inteligencia de los Estados.

El Presidente de la Comisión, Honorable Senador señor Huenchumilla, pidió aclarar si la referencia al ciberespacio dice relación con algo físico o meramente metafísico. Profundizando en su inquietud, preguntó si en el caso de un ciberataque a una transferencia electrónica, este se produce en un aparato o en el espacio.

El Coordinador de Ciberseguridad en Sistemas Eléctricos del Comité Chileno del Consejo Internacional de Grandes Redes Eléctricas, señor Eduardo Morales, fue enfático en sostener que, actualmente, el ser humano vive a la vez en dos planos, en el físico y en el virtual. Esa realidad, previno, se acrecienta día a día y llevará al metaverso. Advirtió que algo similar ocurre con la dualidad de la materia, la que algunas veces se comporta como partícula y otras como onda.

Anunció que de este nuevo escenario surgirán importantes discusiones éticas y morales.

Luego, en relación a la consulta del **Honorable Senador señor Pugh,** puso de relieve que las agencias de ciberseguridad de los países desarrollados aplican inteligencia artificial en la ciberinteligencia, ayudando a los equipos de respuesta de incidentes a anticiparse a las acciones de los hackers. Agregó que estos últimos también están utilizando herramientas de tal naturaleza para operar.

Señaló que, si bien el Estado Mayor Conjunto tiene un centro de ciberdefensa, carece de plataformas como la aludida, herramientas esenciales en el presente.

Calificó como indispensable contar con especialistas en la materia y con programas de inteligencia artificial, toda vez que ello posibilitará no solo que los equipos de respuesta puedan apoyar a los CSIRT sectoriales, sino también llegar a transformarse en un polo de desarrollo económico.

Finalmente, reiteró que la Agencia Nacional de Ciberseguridad debe jugar un rol estratégico y táctico, dejando lo operativo al CSIRT Nacional.

12) Exposición del Presidente de la Fundación País Digital, señor Pelayo Covarrubias

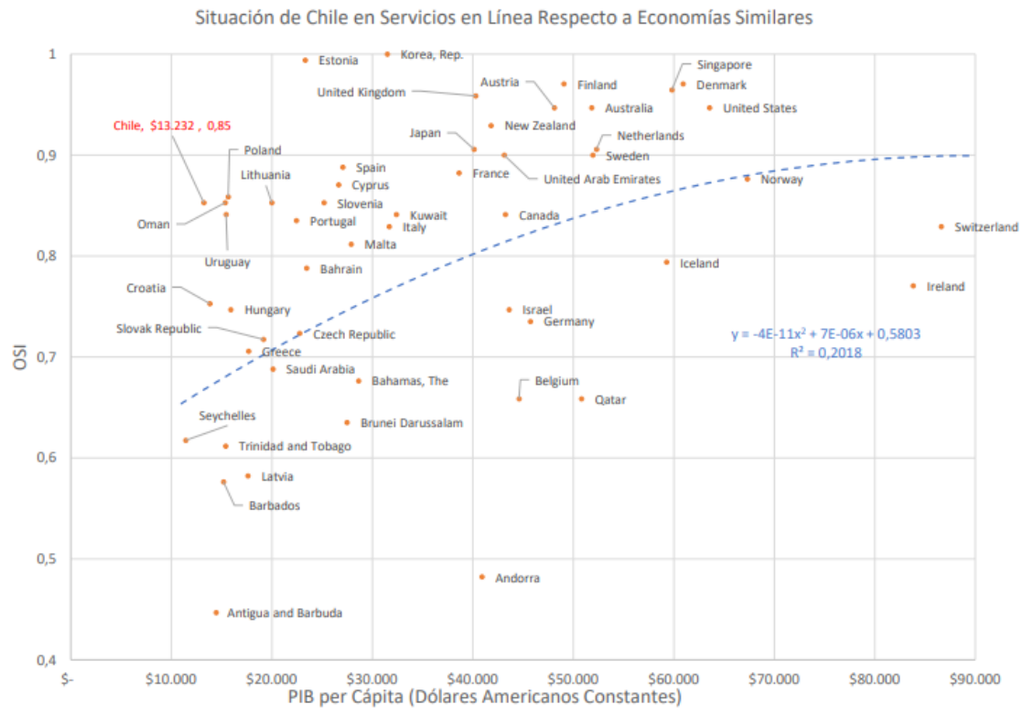
El Presidente de la Fundación País Digital, señor Pelayo Covarrubias, enfatizó que la dualidad mencionada por el invitado anterior en la que viven los seres humanos, ha llevado a acuñar la expresión “figital”.

A continuación, se detuvo en la situación cibernética del país. Al respecto, resaltó que, a partir de la ley de transformación digital, Chile ha experimentado un cambio fundamental. En efecto, recordó que más del 80% de los trámites están digitalizados y que se espera que dicha cifra llegue al 100% en 2025. Además, subrayó que durante la pandemia provocada por el COVID-19, el uso de las tecnologías se aceleró aún más.

Esta realidad, connotó, se refleja también en el nivel de inversión del país en los proyectos tecnológicos. Así, destacó, Chile es líder en Latinoamérica en el área; sin embargo, relevó, la ciberseguridad ha sido rezagada hasta el momento.

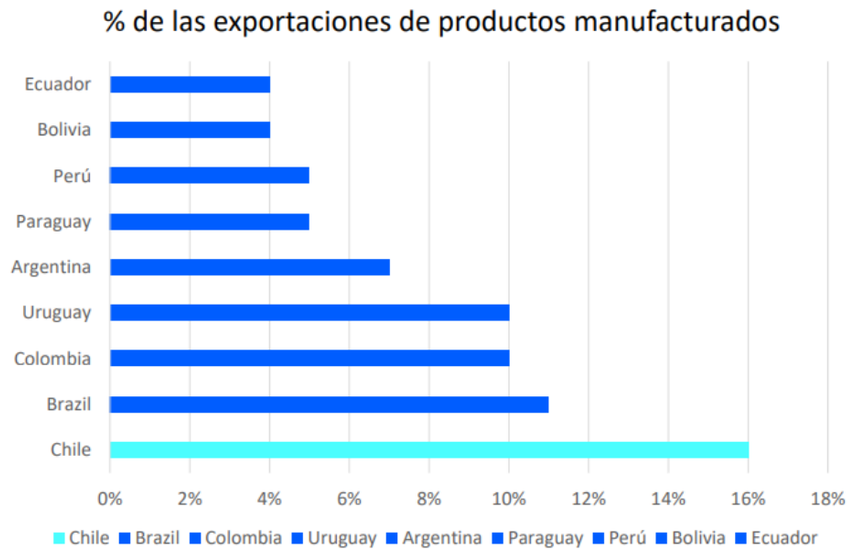
Siguiendo con el desarrollo de su exposición, evidenció que Chile ha tenido grandes avances en materia de Gobierno Digital en los últimos años, transformándose en uno de los Estados líderes de la región.

Añadió que en el índice de servicios en línea (OSI), Chile se encuentra por encima del promedio y relativamente cerca al nivel de países europeos, como se aprecia en el gráfico siguiente:



Por otra parte, apuntó que en el país más del 74% de los hogares están conectados a banda ancha y que se llega a 100% de movilidad a nivel de teléfonos. Puntualizó que el 50% de las viviendas se conecta a través de fibra óptica, lo que implica mayor rapidez y un adecuado precio.

Luego, planteó que la matriz digital chilena permite exportar productos a todo el mundo. En efecto, profundizó, a nivel latinoamericano, es el país que envía más productos de alta tecnología a Sudamérica. De ello, relató, da cuenta el gráfico siguiente:



Con todo, constató, la pregunta que surge luego de la realidad expuesta es cómo seguir creciendo. Sobre el particular, comentó que la fundación que preside ha propuesto el plan “País Digital 2025”, el que considera cinco temas: 1) Fomento de la economía; 2) Transformación digital del Estado; 3) Entorno digital; 4) Conectividad digital, y 5) Competencias y habilidades digitales.

Centrando su atención en la iniciativa de ley en estudio, expresó que apunta en la dirección correcta y constituye un gran avance en relación con lo que existe en la actualidad.

Consideró, sin embargo, fundamental aprovechar las oportunidades que brinda esta iniciativa legal en orden a incorporar la cultura digital, así como las habilidades, datos y tecnologías en los servicios públicos y privados. Afirmó que lo anterior es una pieza fundamental, toda vez que hará posible dar pasos significativos en educación.

Analizando la gobernanza prevista en el proyecto de ley, manifestó la necesidad de que sea considerada como un tema país. El texto presentado a tramitación, lamentó, solo contempla una parcial, al aludir a los CSIRT sectoriales, al de Defensa y la Agencia Nacional de Ciberseguridad. A mayor abundamiento, opinó que el problema de la ciberseguridad es amplio y que separarlo sectorialmente ocasionaría problemas de coordinación. Si la ley no une lo público con lo privado, no funcionará, previno.

Fijando su atención en infraestructura crítica, sugirió crear tanto una infraestructura física como digital, que incorpore la identidad digital; la interoperabilidad; las prácticas de la privacidad; el control; la ciberseguridad de los principios digitales; la ética, y la confianza.

Estimó importante también tener en cuenta los derechos y la libertad en los espacios digitales, así como la protección, la seguridad, la educación y el trabajo de las empresas en este mundo.

En otro orden de ideas, instó a pensar en un liderazgo flexible y adaptativo, producto del crecimiento que está teniendo lo digital en el país. Añadió que su acelerado crecimiento exige incorporar nuevos talentos, incrementar las capacidades de las personas y retenerlas.

Advirtió que si se observa la experiencia internacional, es posible concluir que otros países no solo están educando sino también conservando las habilidades, toda vez que es indispensable para el mundo privado y para la coordinación con lo público.

Por otro lado, llamó a fomentar la inversión en infraestructuras físicas y digitales, acotando que esta última es la que requiere mayor atención.

Remarcó que las nuevas formas de trabajo incidirán en los estándares digitales y en la capacidad de innovación, aspectos muy relacionados al proyecto.

Para concluir, insistió en la idea de establecer un modelo de ciberseguridad colaborativo entre el mundo público y el privado, tal como lo hace el sistema español y el americano.

El Honorable Senador señor Pugh coincidió con el señor Covarrubias en que el país ha sido débil en la generación y retención de talentos, apreciándose tal realidad, de manera muy evidente, en las Fuerzas Armadas. Adujo que la razón principal que motiva la fuga del personal capacitado radica en las enormes diferencias de remuneraciones que ofrece el mundo castrense con aquellas que brinda el sector privado para expertos en el área de ciberseguridad. Lo anterior, repercute en la defensa del Estado ante ciberataques, observó.

Adicionó que sin los recursos humanos imprescindibles, el país siempre estará en desventaja y limitándose a reaccionar ante amenazas.

En este contexto, solicitó al invitado su opinión respecto a la posibilidad de que exista talento nacional compartido entre el mundo de la defensa y el privado. Connotó que conforme a las tecnologías existentes y al hecho que los expertos en la materia son escasos, ambas organizaciones pueden estar en red y activar sus cibersoldados.

El Presidente de la Comisión, Honorable Senador señor Huenchumilla, consultó cuál es el rol que cumple la Fundación País Digital.

El Presidente de la Fundación País Digital, señor Pelayo Covarrubias, explicó que la institución que encabeza trabaja, hace más de veinte años, en fomentar una cultura digital en Chile, articulando la construcción de alianzas y la realización de proyectos público-privados, además de la generación de contenidos que aporten al debate en el ámbito de la economía digital y el desarrollo del país de cara a la cuarta revolución industrial.

Esta entidad, anunció, se ha impuesto metas en distintos ámbitos del quehacer nacional: lo público, lo educacional y la salud, entre otros, priorizando la conectividad y la infraestructura.

Pormenorizó que la referida fundación está compuesta por treinta empresas, las que conforman sus diversas bases. La primera de ellas, detalló, la integran las compañías de telecomunicaciones, como Entel, Telefónica, Claro, Wom y VTR. La segunda, aquellas que empujan y permiten mostrar la economía digital, como NTT e IBM. La tercera, las empresas proveedoras de servicios y que movilizan el ecosistema, como Samsung, Microsoft, y Google. La cuarta, finalmente, son las que utilizan esta importante herramienta, como Caja de Los Andes, Copeuch y Banco de Chile, entre otras.

Aseveró que lo largo del tiempo han impulsado diversos proyectos que han ido estimulando al país. Así, en el ámbito del Gobierno, ejemplificó, se ha apoyado en la modernización del Estado y transformación digital. En el área de la educación, han contribuido con más de 2.500 establecimientos en programación y desarrollo de habilidades digitales. En materia de infraestructura, han aportado en la conectividad de las localidades rezagadas; mientras que en salud han creado iniciativas para ir avanzando en el modelo de atención Hospital Digital.

Sobre la consulta planteada por el **Honorable Senador señor Pugh,** fue tajante en sostener que la formación de habilidades y talentos es esencial. Aseguró que, lamentablemente, Chile está muy atrasado en este aspecto en comparación con los demás países de la Organización para la Cooperación y el Desarrollo Económicos.

Reconoció que las Fuerzas Armadas tienen un rol fundamental en ello, mas alertó que necesitarán la ayuda de los privados también, dado que no tienen los conocimientos requeridos. Lo anterior, prosiguió, dará paso a un gran desafío: el mundo particular deberá formar al de la defensa y este, posteriormente, deberá salir a educar a los primeros. Por consiguiente, instó a evaluar un proyecto que posibilite una formación país.

En sintonía con lo expuesto, pidió considerar que si bien algunas universidades ofrecen programas relacionados con la ciberseguridad, su demanda es baja, requiriéndose, en consecuencia, un cambio cultural que acelere el proceso educacional, para lo cual, enunció, la fundación que representa posee un plan.

Por último, sostuvo que una de las debilidades de la proposición de ley radica en la separación de los CSIRT sectoriales del de Defensa y de la Agencia Nacional de Ciberseguridad. Ahondando en su afirmación, señaló que la seguridad informática es un tema que involucra a todos. Verbigracia, abundó, podría existir una adecuada regulación de la defensa nacional y recibir ataques en otras áreas, como las redes eléctricas o las de gas.

C.-Votación en general

- Puesto en votación el proyecto de ley, en general, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Araya, Huenchumilla, Macaya, Pugh y Saavedra.

- - -

TEXTO DEL PROYECTO

En mérito de los acuerdos precedentemente expuestos, la Comisión de Defensa Nacional tiene el honor de proponer a la Sala la aprobación, en general, del siguiente proyecto de ley:

- - -

PROYECTO DE LEY:

"TÍTULO I
Disposiciones generales

Artículo 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los mecanismos de control, supervisión y de responsabilidad por la infracción de la normativa.

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

1. Agencia: La Agencia Nacional de Ciberseguridad.

2. Ciberataque: Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. Servicios esenciales: Todo servicio respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción de su infraestructura de la información pueda afectar gravemente:

a) La vida o integridad física de las personas;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TÍTULO II
De la determinación de Infraestructura Crítica de la Información

Párrafo 1°
Determinación de la infraestructura crítica de la información

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 5. Deberes generales. Será obligación de los órganos del Estado y de las instituciones privadas que posean infraestructura de la información calificada como crítica, aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los

riesgos, así como contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad e integridad del servicio prestado, de conformidad a lo prescrito en esta ley.

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

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

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

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

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

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

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

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

TÍTULO III
De la Agencia Nacional de Ciberseguridad

Párrafo 1°
Objeto, naturaleza y atribuciones

Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad y regular y fiscalizar las acciones de los órganos de la Administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o fiscalizador sectorial, y que posea infraestructura de la información calificada como crítica, según los preceptos de esta ley. Se relacionará con el Presidente de la República por intermedio del Ministerio del Interior y Seguridad Pública.

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

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

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

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

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

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

e) Administrar el Registro Nacional de Incidentes de Ciberseguridad.

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

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

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

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

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

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

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

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

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

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

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

Párrafo 2°
Dirección, organización y patrimonio

Artículo 10. Dirección de la Agencia. La dirección y administración superior de la Agencia estará a cargo de un Director Nacional, quien será el jefe superior del Servicio, tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta Dirección Pública establecidas en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.

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

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

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

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

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

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

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

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

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

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

b) Los recursos otorgados por leyes generales o especiales;

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

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

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

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

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

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

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

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

Párrafo 3°
Registro Nacional de Incidentes de Ciberseguridad

Artículo 16. Del Registro Nacional de Incidentes de Ciberseguridad. Créase el Registro Nacional de Incidentes de Ciberseguridad, el que será administrado por la Agencia Nacional de Ciberseguridad y tendrá el carácter de reservado, por exigirlo el debido cumplimiento de las funciones de la Agencia, el debido resguardo de los derechos de las personas y la seguridad de la nación. En este registro se ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. Sobre la base de este registro se podrán realizar las respetivas investigaciones por parte de la Agencia, así como comunicar las alertas a los CSIRT Sectoriales, a los órganos del Estado señalados en el inciso final del artículo 4º y a las instituciones privadas que posean infraestructura de la información calificada como crítica, que corresponda al caso.

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

Párrafo 4°
Consejo Técnico de la Agencia Nacional de Ciberseguridad

Artículo 17. Consejo Técnico de la Agencia Nacional de Ciberseguridad. Créase el Consejo Técnico de la Agencia Nacional de Ciberseguridad, en adelante el “Consejo”, que tendrá como objeto asesorar y apoyar técnicamente a la Agencia en el análisis y revisión periódica de las políticas públicas propias de su ámbito de competencia, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad y, proponer posibles medidas para abordarlas.

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

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

Artículo 18. Funciones del Consejo. Corresponderá al Consejo:

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

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

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

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

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

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

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

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

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

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

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

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

a) Expiración del plazo por el que fue designado.

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

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

d) Fallecimiento.

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

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

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

i. Inasistencia injustificada a dos sesiones consecutivas.

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

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

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

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

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

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

a) Responder ante incidentes de ciberseguridad o ciberataque que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información relativos a instituciones privadas no sometidas a la supervigilancia de un regulador o fiscalizador sectorial y que posean infraestructura de la información calificada como crítica, de conformidad a lo prescrito en esta ley.

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

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

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

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

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

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

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

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

j) Generar y difundir información mediante campañas públicas y prestar asesoría técnica general a personas naturales o jurídicas, que no se encuentran reguladas por esta ley, que estén o se hayan visto afectadas por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o hayan afectado el funcionamiento de su operación.

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

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

Artículo 23. CSIRT Sectoriales. Los reguladores o fiscalizadores sectoriales podrán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad dar respuesta a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de sus respectivos sectores regulados.

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

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

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

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

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

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

e) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos de la Administración de Estado de su sector y de las instituciones reguladas cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.

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

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

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

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

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

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

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

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

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

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

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

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

a) Afecta a una gran cantidad de usuarios.

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

c) Afecta a una extensión geográfica considerable.

d) Afecta sistemas de información que contengan datos personales.

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

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

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

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

El procedimiento específico para notificar un incidente de ciberseguridad, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad serán establecidos en el reglamento de la presente ley.

TÍTULO V
De los CSIRT del sector público

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

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

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

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

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

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

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

Sus funciones principales serán las siguientes:

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

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

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

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

Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de los CSIRT, sean el CSIRT Nacional, de Gobierno, Defensa o los CSIRT Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales órganos de la Administración del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

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

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

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de riesgos y los registros previstos en el artículo 6º, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

Adicionalmente, serán considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad;

ii. Los planes de continuidad operacional y planes ante desastres;

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

iv. Los reportes de incidentes de ciberseguridad.

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

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

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

TÍTULO VII
De las infracciones y sanciones

Artículo 33. De las infracciones. Serán consideradas infracciones para efectos de esta ley:

a) Retardar o entregar fuera del plazo señalado la información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;

b) Negar injustificadamente información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;

c) Entregar maliciosamente información falsa o manifiestamente errónea, e;

d) Incumplir los deberes previstos en el párrafo 2° del Título II.

Podrán imponerse, a beneficio fiscal, multas entre 10 y 20.000 Unidades Tributarias Mensuales, de conformidad a la gravedad de la infracción. Para determinar la cuantía de la multa, se entenderá por:

a) Faltas gravísimas: aquellas señaladas en los literales b) y c) del inciso precedente. En este caso, la multa será de hasta a 20.000 Unidades Tributarias Mensuales.

b) Faltas graves: aquellas señaladas en el literal a) del inciso precedente. En este caso, la multa será de hasta 10.000 Unidades Tributarias Mensuales.

c) Faltas leves: aquellas obligaciones señaladas en esta ley cuyo incumplimiento negligente o injustificado no tenga señalada una sanción especial, caso en el que la multa será de 10 a 5.000 Unidades Tributarias Mensuales.

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

Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.

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

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

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

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

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

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

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

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

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

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

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

TÍTULO VIII
Del Comité Interministerial de Ciberseguridad

Artículo 36. Comité Interministerial de Ciberseguridad. Créase el Comité Interministerial de Ciberseguridad, en adelante el Comité, cuya función será asesorar al Ministro del Interior y Seguridad Pública en materias de ciberseguridad relevantes para el funcionamiento de los órganos de la Administración del Estado y de servicios esenciales.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 39. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios que estén en conocimiento de información reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición.

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

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

TÍTULO IX
De las modificaciones a otros cuerpos legales

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

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

TÍTULO X
Disposiciones transitorias

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

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

En el ejercicio de esta facultad, el Presidente de la República deberá dictar todas las normas necesarias para la adecuada estructuración y operación de la planta de personal que fije, así como el número de cargos para cada planta, los requisitos específicos para el ingreso y promoción de dichos

cargos, sus denominaciones y niveles jerárquicos para efectos de la aplicación de lo dispuesto en el Título VI de la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica, y en el artículo 8º del decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda. Igualmente, fijará su sistema de remuneraciones y las normas necesarias para la fijación de las remuneraciones variables, en su aplicación transitoria.

Además, podrá establecer las normas para el encasillamiento del personal en la planta que fije, las que podrá incluir a los funcionarios que se traspasen desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.

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

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

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

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

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

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

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

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

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

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

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

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

Artículo Segundo Transitorio.- El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº 19.882, podrá nombrar, a partir de la publicación de la presente ley, al primer Director de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública. En el acto de nombramiento, el Presidente de la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese solo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal.

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

capítulos, programas, ítems, asignaciones y glosas presupuestarias que sean pertinentes.

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

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

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

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

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

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

- - -

ACORDADO

Acordado en sesiones celebradas **los siguientes días de 2022: 5 de julio**, con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Rodrigo Galilea Vial (en reemplazo del Honorable Senador señor Kenneth Pugh Olavarría), Javier Macaya Danús, y Gastón Saavedra Chandía; **12 de julio,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Javier Macaya Danús, Kenneth Pugh Olavarría y Gastón Saavedra Chandía; **9 de agosto,** con asistencia de los Honorables Senadores señores Pedro Araya Guerrero (Presidente Accidental), Rodrigo Galilea Vial (en reemplazo del Honorable Senador señor Kenneth Pugh Olavarría) y Gastón Saavedra Chandía; **16 de agosto,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Javier Macaya Danús y Gastón Saavedra Chandía; **30 de agosto,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Javier Macaya Danús, Kenneth Pugh Olavarría y Gastón Saavedra Chandía; **6 de septiembre,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Kenneth Pugh Olavarría y Gastón Saavedra Chandía; **13 de septiembre,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Kenneth Pugh Olavarría y Gastón Saavedra Chandía, **y 28 de septiembre,** con asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo (Presidente), Pedro Araya Guerrero, Javier Macaya Danús, Kenneth Pugh Olavarría y Gastón Saavedra Chandía.

Valparaíso, a 29 de septiembre de 2022.


MILENA KARELOVIC RÍOS
Abogada Secretaria

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE DEFENSA NACIONAL, 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. OBJETIVOS DEL PROYECTO PROPUESTO POR LA COMISIÓN: establecer la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, formar una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

II. ACUERDOS: aprobado en general por unanimidad (5X0).

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

IV. NORMAS DE QUÓRUM ESPECIAL:
A. Normas orgánicas constitucionales, según el artículo 38 de la Constitución Política de la República, en relación con el artículo 66, inciso segundo, del mismo Texto Supremo:
- Artículos 8; 9 letras a), b), d), h), l) y m); 10; 13; 17; 22; 23; 24 letra b); 27; 28; 34; 36; 37; 38 y 41, permanentes.
- Artículos segundo; quinto y sexto de las disposiciones transitorias.

B. Normas de quórum calificado, de conformidad al artículo 8°, inciso segundo, y 66, inciso tercero, ambos de la Carta Fundamental:
- Artículos 16; 29; 30; 31 y 39, permanentes.

V. URGENCIA: no tiene.

VI. ORIGEN E 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: primer informe, en general.

X. NORMAS QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: 1.- Ley N° 20.424, estatuto orgánico del Ministerio de Defensa Nacional; 2.- Ley N° 21.180, sobre transformación digital del Estado; 3.- Ley N° 19.882, que regula nueva política de personal a los funcionarios públicos que indica; 4.- Decreto con fuerza de ley N° 29, del Ministerio de Hacienda, promulgado en 2004 y publicado en 2005, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.834, sobre Estatuto Administrativo; 5.-Ley N° 19.628, sobre protección de la vida privada; 6.- Ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia; 7.-

Decreto con fuerza de ley N° 1, del Ministerio Secretaría General de la Presidencia, promulgado en 2000 y publicado en 2001, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado; 8.- Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; 9.- Ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses; 10.- Código Penal; 11.- Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest); 12.- Ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; 13.- Ley N° 21.113, que declara el mes de octubre como el de la ciberseguridad; 14.- Ley N° 18.168, general de telecomunicaciones; 15.- Decreto N° 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad; 16.- Instructivo Presidencial 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad; 17.- Decreto N° 3, de 2018, del Ministerio de Defensa Nacional, que aprueba la Política de Ciberdefensa; 18.- Ley N° 21.130, que moderniza la legislación bancaria; 19.- Ley N° 20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet; 20.- Decreto N° 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, reglamento para la interoperación y difusión de mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones; 21.- Decreto supremo N° 83, 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, y 22.- Artículo 19, número 4°. de la Constitución Política de la República.

Valparaíso, a 29 de septiembre de 2022.

ÍNDICE