Nº 216/SEC/23

Valparaíso, 26 de abril de 2023.

A S.E. el Presidente de la Honorable Cámara de Diputados

Tengo a honra comunicar a Vuestra Excelencia que, con motivo del Mensaje, informes y antecedentes que se adjuntan, el Senado ha dado su aprobación al proyecto de ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, correspondiente al Boletín N° 14.847-06:

PROYECTO DE LEY:

"TÍTULO I
Disposiciones generales

Artículo 1°. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para los efectos de esta ley, se entenderá por Administración del Estado a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad Pública y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. Los órganos autónomos constitucionales se

ajustarán a las disposiciones de esta ley que así lo señalen. No se aplicarán las disposiciones de esta ley a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12. Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir,

detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

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

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

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

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

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

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

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

20. Operadores de importancia vital: institución pública o privada, identificada como tal por la Agencia de conformidad con esta ley, por prestar algún servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, que depende de las redes y sistemas informáticos, y cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.

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

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

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

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

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

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

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

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

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

2. Principio de confidencialidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos deberá ser conocida y accedida exclusivamente por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.

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

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

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

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

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

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

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

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

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

TÍTULO II
Obligaciones de ciberseguridad

Párrafo 1°
Servicios esenciales y operadores de importancia vital

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

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

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

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

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

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

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

a) La cantidad de usuarios potencialmente afectados;

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

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

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

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

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

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

h) El daño reputacional que pueda ocasionarse.

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

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

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

Párrafo 2°

Obligaciones de ciberseguridad

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

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

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

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

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

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

Artículo 6°. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales. Todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital deberán:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 propio, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

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

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

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

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

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

a) Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.

b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

o) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los Ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.

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

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

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

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

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

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

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

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

x) Coordinar anualmente durante el mes de octubre, un ejercicio nacional de comprobación de capacidades de ciberseguridad, en cumplimiento

de la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad.

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

Párrafo 2°

Dirección, organización y patrimonio

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

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

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

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

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

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

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

f) Delegar atribuciones o facultades específicas en los funcionarios y funcionarias que indique;

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

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

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

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

b) Los recursos otorgados por leyes generales o especiales;

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

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

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

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

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

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

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

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

Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con fuerza de ley N° 29, promulgado el año 2004 y publicado el año 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

Asimismo, el personal estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle por los actos realizados en el ejercicio de sus funciones. La responsabilidad disciplinaria del personal de la Agencia por los actos realizados en el ejercicio de sus funciones podrá hacerse efectiva por la autoridad respectiva, de acuerdo al procedimiento establecido en

el Título V “De la Responsabilidad Administrativa” del decreto con fuerza de ley N° 29, promulgado el año 2004 y publicado el año 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

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

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

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

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

Un reglamento expedido por el Ministerio encargado de la seguridad pública determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 1, promulgado el año 2000 y publicado el año 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

La Agencia deberá cumplir con las normas establecidas en el decreto ley N° 1.263, promulgado y publicado el año 1975, de Administración Financiera del Estado.

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

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

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

En todo caso, quedarán exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañan personalmente al funcionario o funcionaria, o que se refieran a la administración de su patrimonio. El desempeño de

funciones en la Agencia será de dedicación exclusiva y será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley. No obstante, será compatible con cargos docentes en instituciones públicas o privadas reconocidas por el Estado hasta un máximo de doce horas semanales, para lo cual deberá prolongar su jornada a fin de compensar las horas durante las cuales no haya podido desempeñar su cargo.

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

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

Párrafo 3°

Consejo Multisectorial sobre Ciberseguridad

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

El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por

el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, quienes permanecerán en su cargo durante seis años, renovándose en tríos cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.

Los integrantes del Consejo estarán obligados a presentar una declaración de intereses y patrimonio, en conformidad a lo dispuesto por la ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses, y estarán afectos al principio de abstención contenido en el artículo 12 de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

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

El Consejo sesionará todas las veces que sea necesario para el cumplimiento de sus funciones. La Agencia prestará el apoyo técnico y administrativo indispensable para el adecuado funcionamiento del Consejo.

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

Artículo 18. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro sesiones consecutivas.

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

El consejero respecto del cual se verificare alguna de las causales de cesación referidas anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.

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

Si quedare vacante el cargo de consejero deberá procederse al nombramiento de uno nuevo, de conformidad con el procedimiento establecido en

esta ley. El consejero nombrado en reemplazo durará en el cargo sólo por el tiempo que falte para completar el período del consejero reemplazado.

Párrafo 4°
Red de Conectividad Segura del Estado

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

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

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

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

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

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

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

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

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

e) Supervisar incidentes a escala nacional.

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

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

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

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

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

TÍTULO IV

Otras instituciones intervinientes

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

Los CSIRT Sectoriales tendrán las siguientes funciones:

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

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

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

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

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

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

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

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

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

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

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

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

Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las instancias de coordinación entre la Agencia y las autoridades sectoriales y sus respectivos CSIRT.

Artículo 22. Facultades especiales. Las autoridades sectoriales podrán dictar las normas de carácter general y las normas técnicas que

consideren necesarias para la ciberseguridad de las instituciones de su sector, de conformidad con la regulación respectiva, las que deberán ser sometidas a aprobación previa de la Agencia, quien deberá pronunciarse en el plazo de treinta días hábiles.

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

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

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

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

a) El número de personas afectadas.

b) La duración del incidente.

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

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

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

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

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

Estos centros serán los únicos habilitados para certificar que un determinado ente cumple con los estándares y normas de seguridad que se exijan

para la prestación de servicios al Estado, y el desarrollo de los sistemas y programas informáticos que sean utilizados por las instituciones públicas.

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

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

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

TÍTULO V

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

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

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

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

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

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

b) Asumir el rol de coordinador y enlace entre la Agencia y su CSIRT Nacional con los CSIRT Institucionales de la Defensa Nacional, asegurando la cooperación, colaboración e intercambio de información pertinente que fortalezca la ciberseguridad.

c) Establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y del Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.

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

Artículo 27. De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. En el sector de la defensa nacional se constituirán Equipos de Respuesta a Incidentes de Seguridad Informática

Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales de la Defensa Nacional, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional.

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

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

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

TÍTULO VI

De la reserva de información en el sector público en materia de ciberseguridad

Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter

aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

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

Los funcionarios y funcionarias de la Agencia y del CSIRT Nacional, de Defensa o de los Sectoriales que hubieren tomado conocimiento de los antecedentes a que se refiere el inciso primero, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 6°, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

Adicionalmente, serán considerada como información secreta o reservada, la siguiente:

i. Las matrices de riesgos de ciberseguridad;

ii. Los planes de continuidad operacional y planes ante desastres, y

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

Artículo 30. Extensión de la obligación de reserva. La obligación de guardar secreto regirá, además, para aquellos que, sin ser funcionarios o funcionarias de la Agencia, tomaren conocimiento de las solicitudes para la ejecución de

procedimientos especiales de obtención de información de los antecedentes que las justifiquen y de las resoluciones judiciales que se dicten al efecto.

Artículo 31. Deber de reserva de la Agencia. La Agencia cautelará especialmente la reserva de los secretos o información comercial sensible que llegare a conocer en el desempeño de su labor, como también el respeto a los derechos fundamentales de las personas, particularmente el respeto y resguardo del derecho a la vida privada y el derecho a la protección de datos personales.

Artículo 32. Sanciones. La infracción a las obligaciones dispuestas en el presente Título, serán sancionadas en la forma prevista en los artículos 246, 247 o 247 bis, todos del Código Penal, según corresponda. Lo anterior es sin perjuicio de la responsabilidad administrativa que procediere.

TÍTULO VII
De las infracciones y sanciones

Artículo 33. De las infracciones. Las sanciones a las infracciones de la presente ley cometidas por instituciones privadas serán las siguientes:

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

b) Las infracciones graves serán sancionadas con multa de 1.001 a 5.000 unidades tributarias mensuales. En caso de que el infractor sea un

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

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

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

Se consideran infracciones graves las siguientes:

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

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

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

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

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

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

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

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

La multa será fijada teniendo en consideración si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del riesgo, la gravedad de los efectos de los ataques, la reiteración en la infracción dentro del plazo de tres años contado desde el momento en que se produjo el incidente y la capacidad económica del infractor.

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

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

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

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

a) El procedimiento sancionatorio será instruido por la Agencia.

b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Junto con la apertura del expediente, la Agencia deberá designar un funcionario o una funcionaria responsable de la instrucción del procedimiento, que recibirá el nombre de instructor o instructora. En el evento de que producto de una

denuncia se iniciare un procedimiento administrativo sancionador, el denunciante tendrá la calidad de interesado, para todos los efectos legales.

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

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

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

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

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

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

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

j) Cumplidos los trámites señalados en los literales anteriores, el instructor o instructora emitirá, dentro de diez días hábiles, un dictamen en el cual propondrá la absolución o la sanción que a su juicio corresponda aplicar. Dicho dictamen deberá contener la individualización del o de los infractores; la relación de los hechos investigados y la forma como se ha llegado a comprobarlos, y la proposición al Director o Directora de las sanciones que estimare procedente aplicar o de la absolución de uno o más de los infractores.

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

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

m) La resolución que establezca la infracción a la normativa sobre ciberseguridad y aplique la sanción correspondiente deberá ser fundada. Esta resolución deberá indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia que resuelve el procedimiento por infracción de ley será reclamable mediante recurso de reposición que se podrá

interponer en el plazo de cinco días hábiles contados desde la notificación, el que deberá ser resuelto por el Director o Directora dentro del plazo de treinta días hábiles.

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

Artículo 35. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

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

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

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

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

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

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

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

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

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

Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente.

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

Las infracciones a los principios y obligaciones contenidos en los artículos 21 y 29 serán sancionadas con multa de veinte por ciento a cincuenta por

ciento de la remuneración mensual del jefe superior del organismo público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza del incidente y el número de personas afectadas, si las hubiere. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor.

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

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

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

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

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

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

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

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

Artículo 38. Agravante especial. Si como consecuencia de la perpetración de un delito resultare afectada gravemente la continuidad operativa de un operador de importancia vital, se impondrá la pena que corresponda, aumentada en un grado.

Lo mismo se observará cuando el delito consistiere en la alteración o supresión de los datos informáticos relevantes del operador de importancia vital o en la obstaculización del acceso o la alteración perjudicial del funcionamiento de su sistema informático.

TÍTULO VIII
Del Comité Interministerial de Ciberseguridad

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

En el ejercicio de sus funciones, el Comité deberá:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios o funcionarias de la Administración del Estado u otras autoridades públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.

Artículo 41. De la Secretaría Ejecutiva. El Comité contará con una Secretaría Ejecutiva radicada en la Agencia, la que prestará el apoyo técnico, administrativo y de contenidos para el desarrollo de las reuniones del Comité.

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

Artículo 42. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios o funcionarias que estén en conocimiento de información reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición.

La revelación de la información será sancionada de conformidad al delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.

Artículo 43. Del reglamento. Un reglamento expedido por el Ministerio encargado de la seguridad pública fijará las normas de funcionamiento del Comité.

Título IX
Órganos autónomos constitucionales

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

Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios y funcionarias, en relación a las infracciones a esta ley que se produzcan y, del mismo modo, les corresponderá ejercer

las demás funciones y adoptar las decisiones que esta ley encomienda a la Agencia, para fines de dar cumplimiento a lo previsto en este artículo.

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

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

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

TÍTULO X
De las modificaciones a otros cuerpos legales

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

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

Artículo 46. Introdúcense las siguientes enmiendas en la ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest:

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

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

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

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

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

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

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

2. Derógase el artículo 16.

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

“h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.”.

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

DISPOSICIONES TRANSITORIAS

Artículo primero. Entrada en vigencia y personal. Facúltase al Presidente de la República para que en el plazo de un año de publicada en el Diario Oficial la presente ley, establezca mediante uno o más decretos con fuerza de ley expedidos a través del Ministerio del Interior y Seguridad Pública, los que también deberán ser suscritos por el Ministro de Hacienda, las normas necesarias para regular las siguientes materias:

1. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

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

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

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

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

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

La individualización del personal traspasado conforme al párrafo anterior, se realizará a través de decretos expedidos bajo la fórmula “Por orden del Presidente de la República”, por intermedio del Ministerio del Interior y Seguridad Pública.

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

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

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

Artículo segundo. El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº 19.882, podrá nombrar, a partir de la publicación de la presente ley, al primer Director o Directora de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública. En el acto de nombramiento, el Presidente

de la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director o Directora, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director o Directora se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese sólo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal.

Artículo tercero. El Presidente de la República, por decreto supremo expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia Nacional de Ciberseguridad y podrá modificar el presupuesto del Ministerio del Interior y Seguridad Pública. Para los efectos anteriores podrá crear, suprimir o modificar las partidas, capítulos, programas, ítems, asignaciones y glosas presupuestarias que sean pertinentes.

Artículo cuarto. Dentro del plazo de ciento ochenta días posteriores a la publicación de la ley, el Ministerio del Interior y Seguridad Pública deberá expedir los reglamentos señalados en esta ley.

Artículo quinto. En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás organismos del Estado reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de éstos, de conformidad a lo dispuesto en el artículo 21, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.

Artículo sexto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los

miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 16, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período:

a) Tres consejeros durarán en sus cargos un plazo de tres años.

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

Artículo séptimo. El mayor gasto fiscal que represente la aplicación de la presente ley durante su primer año presupuestario de vigencia se financiará con cargo al presupuesto el Ministerio del Interior y Seguridad Pública. No obstante lo anterior, el Ministerio de Hacienda con cargo a la partida presupuestaria Tesoro Público podrá suplementar dicho presupuesto en la parte del gasto que no pudiere financiar con esos recursos. Para los años siguientes, se financiará de acuerdo con lo determinen las respectivas Leyes de Presupuestos del Sector Público.

Artículo octavo. Sobre los servicios esenciales. Hasta que no se dicten los respectivos decretos señalados en el artículo 4° de la ley, serán calificados como servicios esenciales para los efectos de esta ley, los servicios públicos de telecomunicaciones, incluyendo los servicios de transmisión de datos; los servicios de generación, transmisión y distribución eléctrica; los servicios sanitarios y de suministro de agua potable, excluyendo los servicios sanitarios rurales; los servicios bancarios y financieros; las prestaciones de salud, incluyendo cualquier institución pública o privada que realice tratamiento de datos personales de salud, salvo aquellos prestados por municipios o corporaciones municipales; los órganos de la Administración del Estado, excluyendo a las municipalidades y gobernaciones provinciales y regionales; el Poder Judicial, y el Poder Legislativo. La Agencia identificará, mediante resolución exenta, los operadores de importancia vital que quedarán sujetos a las obligaciones establecidas en el artículo 6° de esta ley.”.

- - -

Hago presente a Su Excelencia que este proyecto de ley fue aprobado, en general, por 38 votos favorables de un total de 47 senadores en ejercicio.

En particular, las normas de rango orgánico constitucional del proyecto de ley fueron votadas conforme al siguiente detalle:

- Los artículos 1°, inciso segundo; 4°, inciso final; 8°; 9°, letras a), b), c), d), e), i), m), n), ñ), v) y x); 10; 13; 14; 16, inciso tercero; 20, con excepción de su letra g); 21; 25; 26; 34; 35; 36; 37; 39; 40; 41; 44 y 45, permanentes, y los artículos segundo; quinto; sexto y octavo, transitorios, fueron aprobados por 37 votos a favor.

- El artículo 20, letra g), fue aprobado por 38 votos.

Por su parte, los artículos 29; 30; 31 y 42, fueron aprobados por 37 votos a favor, por tratarse de normas de quórum calificado.

En todos los casos, respecto de un total de 48 senadores en ejercicio, dándose cumplimiento a lo dispuesto en el inciso segundo del artículo 66 de la Constitución Política de la República.

- - -

Dios guarde a Vuestra Excelencia.

JUAN ANTONIO COLOMA CORREA
Presidente del Senado

RAÚL GUZMÁN URIBE
Secretario General del Senado