rrp/mrb
S.115ª/371ª

Oficio Nº 19.033

VALPARAÍSO, 12 de diciembre de 2023

A S.E. EL
PRESIDENTE
DEL
H. SENADO

La Cámara de Diputados, en sesión de esta fecha, ha dado su aprobación al proyecto de ley de ese H. Senado, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, correspondiente al boletín Nº 14.847-06, con las siguientes enmiendas:

**Artículo 1°**

**Inciso primero**

Ha sustituido el vocablo “privadas” por la frase “determinadas en el artículo 4°”.

**Inciso segundo**

Lo ha reemplazado por los siguientes incisos segundo y tercero, nuevos:

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

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

**Inciso tercero**

Lo ha suprimido.

**Artículo 2º**

**Número 5**

Lo ha eliminado.

**Número 6**

Ha pasado a ser número 5, reemplazado por el siguiente:

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

**Números 7 y 8**

Los ha suprimido.

**Números 9, 10, 11 y 12**

Han pasado a ser números 6, 7, 8 y 9, respectivamente, sin enmiendas.

**Números 13 y 14**

Lo ha eliminado.

**Número 15**

Ha pasado a ser número 10, eliminándose la expresión “o no-repudio”.

**Número 16**

Ha pasado a ser número 11, sin modificaciones.

**Números 17, 18, 19 y 20**

Los ha suprimido.

**Números 21, 22 y 23**

Han pasado a ser números 12, 13 y 14, respectivamente, sin enmiendas.

**Números 24, 25 y 26**

Los ha eliminado.

**Número 27**

Ha pasado a ser número 15, sin enmiendas.

**Artículo 3º**

Lo ha reemplazado por el siguiente:

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

1. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, y adoptar las medidas necesarias para evitar la escalada del ciberataque o del incidente de

ciberseguridad y su posible propagación a otros sistemas informáticos.

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

3. Principio de coordinación: de conformidad a lo dispuesto por el inciso segundo del artículo 5º de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fija el fuerza de ley Nº1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones.

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

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

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

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

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

**Artículo 4º**

Lo ha sustituido por el que sigue:

“Artículo 4°. Ámbito de aplicación. La presente ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los incisos segundo y tercero de este

artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5 y 6.

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

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

Dicha calificación deberá someterse al proceso de consulta pública y se regirá por las disposiciones de la ley Nº 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en este artículo, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 8°.”.

*****

**Artículos 5º y 6º, nuevos**

Ha incorporado, a continuación del artículo 4º, los siguientes artículos 5º y 6º, nuevos:

“Artículo 5º. Operadores de Importancia Vital. La Agencia establecerá mediante resolución dictada por el Director o la Directora Nacional, según se establece en el artículo siguiente, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

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

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

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

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

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

Artículo 6º. Procedimiento de calificación de los operadores de importancia vital. Al menos cada tres años, la Agencia deberá revisar y actualizar la

calificación de operadores de importancia vital mediante una resolución dictada por el Director o la Directora Nacional.

Para los efectos del inciso anterior, la Agencia requerirá informe fundado a los organismos públicos con competencia sectorial para que se pronuncien sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital. Dichos informes deberán evacuarse en la forma prescrita en el artículo 37 bis de la ley Nº 19.880.

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

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

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

En contra de la resolución que se dicte podrán deducirse aquellos recursos a que se refiere la ley N° 19.880, sin perjuicio de la facultad de ejercer el recurso establecido en el artículo 46 de la presente ley.

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

*****

**Artículo 5º**

Ha pasado a ser artículo 7º, con la siguiente redacción:

“Artículo 7°. Deberes generales. Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares

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

Para efectos de emitir las medidas de seguridad a que se refiere el inciso primero, la Agencia deberá observar lo prescrito en el artículo 25, según corresponda. Dichos protocolos y estándares deberán someterse a consulta pública, en la misma forma y plazo señalados en el inciso tercero del artículo 6. La medida deberá publicarse junto con el informe en que se justifique el rechazo o modificación de las observaciones que correspondan.

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

**Artículo 6º**

Ha pasado a ser artículo 8º, reemplazado por el siguiente:

“Artículo 8º. Deberes específicos de los operadores de importancia vital. Todos los operadores de importancia vital deberán:

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

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

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

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en conformidad al artículo 28, y someterse a revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

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

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

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

f) Contar con las certificaciones que señala el artículo 28.

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

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

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

**Artículo 7º**

Ha pasado a ser artículo 9º, sustituido por el siguiente:

“Artículo 9. Deber de reportar. Todas las instituciones públicas y privadas señaladas en el artículo 4° tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27, tan pronto les sea posible y conforme al siguiente esquema:

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

b) Dentro del plazo máximo de setenta y dos horas, una actualización de la información contemplada en la letra a), que incluya una evaluación

inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles.

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

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

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

ii. El tipo de amenaza o causa principal que probablemente haya causado el incidente.

iii. Las medidas de mitigación aplicadas y en curso.

iv. Si procede, las repercusiones transfronterizas del incidente.

d) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal c), éste se reemplazará por un informe sobre la situación en ese momento. El informe final deberá ser presentado en el plazo de quince días corridos contado desde que se haya gestionado el incidente.

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

Los operadores de importancia vital deberán, además, informar al CSIRT Nacional su plan de acción, tan pronto lo hubieren adoptado. El plazo para la adopción de un plan de acción en ningún caso podrá ser superior a siete días corridos contados desde que se tuvo conocimiento de la ocurrencia del incidente.

En el caso de los organismos del Estado, para el cumplimiento del deber establecido en este artículo, los jefes de servicio deberán exigir a los proveedores de servicios de tecnologías de la información que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado, y siempre que tenga por objeto prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad, y garantizar a su vez que se respete la posible naturaleza delicada de la información compartida. Con el objeto de cumplir con lo anterior, los contratos de prestación de servicios no podrán contener ninguna cláusula que pueda restringir o dificultar de cualquier modo la comunicación de información sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo. En caso de existir la obligación de notificar a más de una autoridad, la Agencia en conjunto con las autoridades involucradas, y conforme lo dispuesto en el artículo 24, procurará poner a disposición de los obligados un sistema de ventanilla única que permita notificarlas simultáneamente.

Un reglamento expedido por el ministerio encargado de la Seguridad Pública regulará el contenido de las diversas clases de reportes señalados en este artículo.”.

**Artículo 8º**

Ha pasado a ser artículo 10, con las siguientes enmiendas:

**Inciso segundo**

Lo ha suprimido.

**Incisos tercero, cuarto y quinto**

Han pasado a ser incisos segundo, tercero y cuarto, respectivamente, sin modificaciones.

**Artículo 9º**

Ha pasado a ser artículo 11, reemplazado por el siguiente:

“Artículo 11. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones:

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

b) Dictar los protocolos y estándares que señala el artículo 7; las instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley; y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos.

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

d) Coordinar y supervisar al CSIRT Nacional y a los demás pertenecientes a la Administración del Estado, y requerir de éstos la información que sea necesaria para el cumplimiento de sus fines.

e) Establecer una coordinación con el CSIRT de la Defensa Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de

ciberseguridad o vulnerabilidades, y respecto a las materias que serán objeto de intercambio de información.

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

g) Calificar, mediante resolución fundada y en la forma prevista en los artículos 4, 5 y 6 a los servicios esenciales y a los operadores de importancia vital.

h) Requerir a las entidades obligadas por la presente ley que hayan visto afectados sus servicios por un incidente de ciberseguridad o ciberataque, que entreguen a los potenciales afectados información veraz, suficiente y oportuna sobre su ocurrencia, conforme lo dispuesto en el literal g) del artículo 8º.

i) Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.

j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4º acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Para lo anterior, podrá requerir la entrega del registro de actividades de las redes y sistemas informáticos que

permitan comprender detalladamente los incidentes de ciberseguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, y deberá especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior incluya datos personales, éstos deberán ser anonimizados, siempre que ello sea posible sin entorpecer la gestión de incidentes. En cualquier caso, los datos personales sólo podrán ser tratados con estricto cumplimiento de lo dispuesto en la ley 19.628, sobre Protección de la Vida Privada, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

Con todo, para efectos de lo dispuesto en esta ley no se considerará la dirección IP como un dato personal.

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido a través de la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad con lo establecido en el reglamento. Una vez notificado, el requerido deberá proporcionar todas las facilidades de acceso que sean necesarias. En el caso de que el requerido sea una institución privada de las señaladas en el artículo 4º, podrá oponerse. Formulada la oposición la Agencia solo podrá acceder previa autorización judicial conforme lo dispuesto en

los párrafos siguientes y no procederá el reclamo establecido en el artículo 46.

Corresponderá a un ministro de la Corte de Apelaciones de Santiago conocer del requerimiento. Anualmente, el Presidente de la Corte de Apelaciones de Santiago deberá designar, por sorteo, a dos de sus miembros para cumplir esta labor. Si ninguno de los ministros estuviere en funciones, corresponderá otorgar la autorización al Presidente de la Corte o a quien lo subrogue. La autorización deberá solicitarse por escrito y fundarse en hechos específicos que justifiquen la necesidad del requerimiento. Para tales efectos todos los días y horas se entenderán hábiles.

La resolución que autorice o deniegue el acceso a las redes y sistemas deberá dictarse previa audiencia, la que tendrá lugar en el más breve plazo, y en la que se escuchará a las partes.

En contra de la resolución que dicte el Ministro de Corte procederá el recurso de apelación ante la Corte de Apelaciones de Santiago. Dicha Corte podrá resolver la apelación en cuenta sin más trámite. Los autos se agregarán de manera extraordinaria y con preferencia a la tabla del día siguiente; pero si éste fuere inhábil, deberá el tribunal funcionar extraordinariamente para el solo conocimiento del recurso. Si producto de la interposición de recusaciones o implicancias no hubiere tribunal, los autos serán conocidos el día siguiente, según las reglas precedentes.

En caso de que se requiriera la restricción del acceso o uso de redes o sistemas informáticos se estará a lo dispuesto en este literal.

No obstante, la Agencia deberá actuar conjuntamente con la autoridad sectorial correspondiente.

El procedimiento dispuesto en los párrafos precedentes también será aplicable a los requerimientos de acceso a redes y sistemas informáticos a que se refiere en el inciso tercero del literal ñ) del presente artículo.

l) Cooperar con organismos públicos e instituciones privadas, en materias propias de su competencia, sin perjuicio de las atribuciones de otros organismos del Estado.

La Agencia servirá de punto de contacto con las autoridades nacionales de ciberseguridad extranjeras o sus homólogos y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad con lo previsto en el inciso primero del artículo 2º de la ley N° 21.080, que modifica diversos cuerpos legales con el objeto de modernizar el Ministerio de Relaciones Exteriores.

m) Prestar, cuando sus recursos humanos, técnicos y financieros así lo permitan, asesoría técnica a los organismos del Estado e instituciones privadas afectados por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o afectado el funcionamiento de su operación. En estos casos deberá cautelar siempre

los deberes de reserva de información que esta ley le impone, así como los consagrados en la ley N° 19.628.

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

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

Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones, e instruir de manera particular auditorías por sí o mediante terceros autorizados y análisis de seguridad basados en criterios de evaluación de riesgos objetivos, los cuales deberán ser equitativos, transparentes y no discriminatorios. La entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8°. Adicionalmente, podrá citar a declarar, respecto de

hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

Para el ejercicio de esta atribución podrá establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes e informaciones referidos en los párrafos precedentes.

o) Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley respecto de sus disposiciones y reglamentos y de las instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, en los términos señalados en el literal n), entre otros, a los representantes legales, administradores, asesores y dependientes de la institución de que se trate, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver el procedimiento sancionatorio. La declaración podrá

tomarse presencialmente o por otros medios que aseguren su integridad y fidelidad.

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

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

r) Informar al CSIRT de la Defensa Nacional y a los CSIRT de los organismos de la Administración del Estado los reportes o alarmas de incidentes de ciberseguridad y de vulnerabilidades existentes, conocidas o detectadas en su sector que considere relevantes. Al respecto podrá sugerir determinados planes de acción.

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

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

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

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

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

x) Administrar la Red de Conectividad Segura del Estado.

y) Coordinar anualmente, durante el mes de octubre, un ejercicio nacional de comprobación de capacidades de ciberseguridad, en cumplimiento de la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad.

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

**Artículo 10**

Ha pasado a ser artículo 12, sin modificaciones.

*****

**Artículo 13, nuevo**

Ha introducido, a continuación, el siguiente artículo 13, nuevo:

“Artículo 13 Subdirección. Existirá un Subdirector o Subdirectora Nacional de la Agencia, quien dependerá del Director o Directora Nacional y lo subrogará, en caso de ausencia o impedimento. Además ejercerá las funciones de los literales ñ) y o) del artículo 11. Para ello contará con la atribución de instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios a cargo, determinar las sanciones e imponerlas.

El Subdirector o Subdirectora Nacional de la Agencia, estará afecto al Sistema de Alta Dirección Pública establecido en la ley N° 19.882, como cargo de segundo nivel jerárquico.”.

*****

**Artículo 11**

Ha pasado a ser artículo 14, enmendado de la siguiente manera:

**Letra f)**

Ha reemplazado el punto y coma por la expresión “, y”.

**Letra g)**

La ha suprimido.

**Letra h)**

Ha pasado a ser letra g), sin enmiendas.

**Artículos 12, 13, 14 y 15**

Han pasado a ser artículos 15, 16, 17 y 18, respectivamente, sin enmiendas.

*****

**Artículo 19, nuevo**

Ha introducido, a continuación del artículo 15, que ha pasado a ser artículo 18, el siguiente artículo 19, nuevo:

"Artículo 19. Notificación responsable de vulnerabilidades. No serán aplicables las obligaciones previstas en el artículo 175 del Código Procesal Penal ni en el literal k) del artículo 61 del Estatuto Administrativo, a los trabajadores de la Agencia respecto de la información que reciban por parte de las personas que les notifiquen vulnerabilidades de ciberseguridad. La Agencia deberá mantener en secreto la notificación, sus antecedentes y la identidad de quien la realice. La identidad de la persona que

notifique vulnerabilidades sólo podrá ser revelada con su consentimiento expreso.”.

*****

**Artículo 16**

Ha pasado a ser artículo 20, enmendado como sigue:

**Inciso segundo**

Ha intercalado, entre las frases “sociedad civil,” y “quienes permanecerán en su cargo durante”, la siguiente: “cuyo objeto o razón social se refiera a materias de esta ley,”.

**Artículos 17, 18 y 19**

Han pasado a ser artículos 21, 22 y 23, respectivamente, sin modificaciones.

**Artículo 20**

Ha pasado a ser artículo 24, modificado del modo siguiente:

**Letra b)**

- Ha reemplazado la palabra “Sectoriales” por la frase “que pertenezcan a organismos de la Administración del Estado”.

- Ha eliminado la frase “por parte de los CSIRT Sectoriales”.

- Ha agregado el siguiente párrafo segundo:

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

**Letra d)**

Ha sustituido la palabra “Sectoriales” por la frase “que pertenezcan a organismos de la Administración del Estado”.

**TÍTULO IV**

**Epígrafe**

Lo ha reemplazado por el siguiente:

“TÍTULO IV
Coordinación regulatoria y otras disposiciones”

**Artículos 21 y 22**

Los ha suprimido.

*****

**Artículos 25 y 26, nuevos**

Ha contemplado, a continuación, los siguientes artículos 25 y 26, nuevos:

“Artículo 25. Coordinación regulatoria. Cuando la Agencia deba dictar protocolos, estándares técnicos o instrucciones de carácter general en el ejercicio de sus funciones, y éstos tengan efectos en las áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectivas entre ambas autoridades.

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

Cuando una autoridad sectorial, en el ejercicio de las atribuciones establecidas en sus leyes orgánicas, deba emitir actos administrativos de

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

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

Artículo 26. Normativa Sectorial. Las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y siguiendo lo dispuesto en el artículo anterior, cuando corresponda.

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

Cuando las normas o instrucciones emitidas por una autoridad sectorial establezcan obligaciones para un sector a fin de prevenir incidentes de ciberseguridad, que tengan, al menos, efectos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la Agencia, prevalecerán las disposiciones de la autoridad sectorial. Esto no afectará los deberes de coordinación establecidos en el artículo 25 ni la aplicación de las normas de la presente ley. No obstante, si las normas o instrucciones de una autoridad sectorial no cubren a todas las entidades de un sector o solo se aplican a una parte de sus supervisados, los protocolos, normas o instrucciones de la Agencia seguirán siendo plenamente aplicables a las entidades no exceptuadas en los términos indicado en este inciso.

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

*****

**Artículo 23**

Ha pasado a ser artículo 27, con la siguiente enmienda:

**Inciso segundo**

Ha sustituido el vocablo “Sectoriales” por la frase “que pertenezcan a los organismos de la Administración del Estado”.

**Artículo 24**

Ha pasado a ser artículo 28, con la siguiente redacción:

“Artículo 28. Centros de Certificación. Los operadores de importancia vital deberán obtener las certificaciones de ciberseguridad que señala esta ley y las que determine la Agencia mediante reglamento. Para estos efectos, solo los organismos que sean parte del registro de entidades certificadoras autorizadas a cargo de la Agencia estarán habilitadas para emitir certificaciones válidas que esta ley exija. Para formar parte de este registro bastará acreditar el cumplimiento de los requisitos que establezca el reglamento, y para mantenerse cumplir con los requisitos referidos.

La Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre

ciberseguridad mediante resolución fundada de su Director o Directora.”.

**Artículos 25, 26 y 27**

Han pasado a ser artículos 29, 30 y 31, sin modificaciones.

**Artículo 28**

Ha pasado a ser artículo 32, intercalándose, entre la expresión “la seguridad y la defensa nacional” y el punto y aparte, la frase “, conforme a lo que determine el reglamento”.

**Artículo 29**

Ha pasado a ser artículo 33, con las siguientes modificaciones:

**Incisos primero**

Ha reemplazado la expresión “Sectoriales,” por la frase “que pertenezcan a organismos de la Administración del Estado”.

**Inciso tercero**

Ha reemplazado la palabra “Sectoriales” por la frase “que pertenezcan a organismos de la Administración del Estado”.

**Inciso cuarto**

Ha reemplazado la referencia al “artículo 6º” por otra al “artículo 8º”.

**Artículo 30**

Ha pasado a ser artículo 34, sin enmiendas.

**Artículo 31**

Ha pasado a ser artículo 35, sustituido por el siguiente:

“Artículo 35. Deber de reserva de la Agencia. La Agencia deberá mantener y cautelar la reserva de la información que llegue a conocer en el desempeño de sus funciones, cuando ella tenga tal calidad en virtud de una norma legal o porque requerida por ella, le sea entregada bajo tal calidad. Asimismo, deberá procurar el respeto a los derechos fundamentales de las personas, particularmente el respeto y resguardo del derecho a la vida privada y del derecho a la protección de datos personales.

Sin perjuicio de lo anterior, no se incumple el deber de reserva en aquellos casos en que la Agencia o el CSIRT Nacional, en cumplimiento de sus funciones, deba difundir antecedentes que se encuentren sujetos a reserva, siempre que ello permita gestionar, prevenir o contener un incidente de ciberseguridad.”.

**Artículo 32**

Ha pasado a ser artículo 36, sin modificaciones.

*****

**Artículos 37, 38 y 39 nuevos**

Ha incorporado, a continuación, los siguientes artículos 37, 38 y 39, nuevos:

“Artículo 37. Competencia de la autoridad sectorial. La autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones según lo establece la normativa sobre ciberseguridad que hubiere dictado y cuyos efectos sean al menos equivalentes al de la normativa dictada por la Agencia, conforme lo dispuesto en el artículo 26. Para este efecto, las sanciones y procedimientos sancionatorios serán los que correspondan a la autoridad sectorial de conformidad a su normativa. Fuera de dichos casos, corresponderá a la Agencia fiscalizar, conocer y sancionar las infracciones así como ejecutar las sanciones a la presente ley, sin perjuicio de la facultad de los organismos de la Administración del Estado de poner en conocimiento del organismo competente las infracciones a la norma de que tomaren conocimiento.

Artículo 38. Infracciones. Las infracciones a las obligaciones que esta ley prescribe a los sujetos obligados por ella se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad.

2. Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima.

3. Cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

Se considerarán infracciones graves las siguientes:

1. No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad.

2. No haber implementado los estándares particulares de ciberseguridad.

3. Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad.

4. Entregar a la Agencia información manifiestamente falsa o errónea.

5. Incumplir la obligación de reportar establecida en el artículo 9.

6. Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial.

7. La reincidencia en una misma infracción leve dentro de un año.

Se considerarán infracciones gravísimas las siguientes:

1. Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad.

2. Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo.

3. No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo.

4. La reincidencia en una infracción grave dentro de un año.

Artículo 39. De las infracciones de los Operadores de Importancia Vital. Sin perjuicio de lo prescrito en el artículo precedente, los Operadores de Importancia Vital podrán ser sancionados por infringir las disposiciones del artículo 8º. Las infracciones de dichas disposiciones por estos operadores se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. No mantener el registro de las acciones de seguridad que señala la letra b).

2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala el literal d).

3. No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone el literal g).

4. No designar un delegado de ciberseguridad, según dispone la letra i).

5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c).

6. No contar con las certificaciones que exija la ley, de acuerdo con el literal f).

Se considerarán infracciones graves las siguientes:

1. No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere el literal a).

2. No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c).

3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g).

4. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e).

5. La reincidencia en una misma infracción leve dentro del periodo de un año.

Se considerarán infracciones gravísimas las siguientes:

1. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e), cuando éste posea un impacto significativo.

2. La reincidencia en una misma infracción grave dentro del periodo de un año.”.

*****

**Artículo 33**

Ha pasado a ser artículo 40, sustituido por el siguiente:

“Artículo 40. De las sanciones. La infracción a los preceptos de esta ley conlleva la imposición de una multa a beneficio fiscal, de acuerdo con la siguiente escala:

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales, o hasta 10.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales, o hasta 20.000 unidades

tributarias mensuales si se trata de un operador de importancia vital.

3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales, o hasta 40.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

Para la fijación de la multa se tendrá en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de tres años contado desde el momento en que se produjo el incidente, el tamaño y la capacidad económica del infractor.

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

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

Las infracciones previstas en esta ley prescribirán a los tres años de cometidas, plazo que se

interrumpirá con la notificación de la formulación de cargos por los hechos constitutivos de ellas.”.

*****

**Artículo 41, nuevo**

Ha incorporado, a continuación del artículo 33, que ha pasado a ser artículo 40, el siguiente artículo 41, nuevo:

“Artículo 41. Procedimiento simplificado. Tratándose de la formulación de cargos por infracciones calificadas como leves en conformidad al artículo 38, la Agencia estará facultada para proponer de manera inmediata la sanción a aplicar. Dicha sanción quedará firme si el presunto infractor opta por allanarse a los cargos formulados en su contra. En caso contrario, si el presunto infractor decide rechazar la imputación y presentar descargos, se procederá conforme a lo indicado en el artículo 40.”.

*****

**Artículo 34**

Ha pasado a ser artículo 42, con la siguiente redacción:

“Artículo 42. Procedimiento administrativo sancionador. El procedimiento administrativo se regirá por lo prescrito en la ley Nº 19.880, que establece bases de los procedimientos administrativos que rigen

los actos de los organismos de la Administración del Estado, sin perjuicio de las siguientes disposiciones:

a) Toda sanción deberá fundarse en un procedimiento que se iniciará con la formulación precisa y fundada de los cargos y contendrá la descripción de los hechos en los que se fundamentan y de la forma en que éstos constan en la investigación, la indicación de la razón porque se consideran una infracción a la normativa, con especificación de la o las normas que se estimen infringidas y el presunto responsable de la infracción. Además, se designará al funcionario a cargo de la instrucción del procedimiento. Se fijará un plazo para la formulación de descargos que no podrá ser inferior a quince ni superior a treinta días. Las notificaciones del procedimiento deberán realizarse a la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad con el reglamento.

b) En los descargos deberán señalarse todas las circunstancias o antecedentes de hecho y de derecho que eximan o atenúen la presunta responsabilidad de la persona objeto de cargos, así como los que nieguen la efectiva ocurrencia de los hechos, o que demuestren que éstos no constituyen infracción. Todo ello, sin perjuicio de otras presentaciones o antecedentes posteriores que se hagan valer en el curso del procedimiento sancionatorio con el mismo objetivo. Asimismo, deberán solicitarse las diligencias probatorias que correspondieren.

c) Vencido el plazo para formular descargos, se abrirá un término probatorio por un plazo no inferior a diez ni superior a veinte días, según la naturaleza y complejidad del asunto. Dicho plazo podrá prorrogarse por una sola vez y hasta por un máximo de quince días. Se podrá rendir prueba mediante cualquier medio admisible en derecho, la que se apreciará de acuerdo con las reglas de la sana crítica.

d) Excepcionalmente, se realizarán las diligencias que, decretadas de oficio o a petición de parte, se estimen estrictamente necesarias para la resolución del asunto. Las diligencias podrán solicitarse dentro de los cinco días siguientes al vencimiento del término probatorio.

e) Una vez transcurrido el plazo mencionado en el literal previo, el procedimiento deberá concluir. El instructor del procedimiento emitirá un informe en el cual incluirá un análisis detallado de todas las defensas, alegatos y pruebas presentadas durante el procedimiento sancionatorio a partir del cual se determinará si se ha infringido la normativa vigente y si procede la imposición de la sanción respectiva o la absolución de los cargos. El informe deberá emitirse dentro del plazo de quince días.

f) Una vez recibido el informe del instructor del procedimiento, corresponderá al Subdirector de la Agencia resolver los procesos sancionatorios en el plazo de quince días, para lo cual dictará resolución fundada en la que absolverá al

infractor o le aplicará sanción, en su caso. La resolución del Subdirector deberá incluir el mismo contenido que el informe señalado en el literal precedente.”.

*****

**Artículos 43, 44 y 45, nuevos**

Ha introducido, a continuación, los siguientes artículos 43, 44 y 45, nuevos:

“Artículo 43. De los recursos. En contra de la resolución del Subdirector mediante la cual se concluye el procedimiento administrativo procederán los recursos que establezca la ley Nº 19.880. El recurso deberá resolverse dentro del plazo de quince días. La interposición del recurso suspenderá el plazo para reclamar de ilegalidad, siempre que se trate de materias por las cuales procede dicho recurso.

Artículo 44. Forma de pago de las multas. Las multas deberán pagarse dentro de los diez días siguientes contados desde que el acto administrativo que las impone quede firme. Vencido ese plazo, la resolución que establezca la sanción tendrá mérito ejecutivo y se hará exigible por la Tesorería General de la República. Para su cobro se aplicará lo dispuesto en el inciso segundo del artículo 35 del decreto ley N° 1.263, de 1975, orgánico de Administración Financiera del Estado.

El pago de toda multa deberá ser acreditado ante la Agencia dentro de los diez días siguientes a la fecha en que debió ser pagada.

El retardo en el pago de estas multas devengará los intereses y reajustes establecidos en el artículo 53 del Código Tributario.

Artículo 45. Pronto pago. El sancionado que no interponga recurso alguno podrá, dentro de los cinco días siguientes a que le sea notificada la resolución del Subdirector que le impone la sanción, pagar directamente en la Tesorería General de la República. En este caso, el monto de la multa será reducido en el veinticinco por ciento. Una vez ejercido este derecho, se entenderán renunciado todos los recursos.

Lo dicho en este artículo no será aplicable para el caso previsto en el artículo anterior.”.

*****

**Artículo 35**

Ha pasado a ser artículo 46, con las siguientes modificaciones:

**Encabezamiento**

Ha incorporado, a continuación de la expresión “resolución impugnada,” la siguiente frase: “los que deberán computarse de acuerdo con el artículo 25 de la ley N° 19.880,”.

**Letra b)**

Ha sustituido los vocablos “le produzca” por “pueda ocasionar”.

**Letra h)**

Ha reemplazado la frase “no procederá recurso alguno” por “se podrá recurrir ante la Corte Suprema, dentro del plazo de diez días hábiles, la que resolverá en cuenta”.

**Artículo 36**

Ha pasado a ser artículo 47, enmendado de la manera que sigue:

**Inciso primero**

- Ha reemplazado la expresión “organismo público”, la primera vez que aparece, por la frase “organismo de la administración del Estado”.

- Ha sustituido la frase “de un organismo público” por “del organismo de la administración del Estado”.

- Ha sustituido la frase “los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente” por “lo establecido en esta ley”.

**Inciso segundo**

Ha sustituido el vocablo “someterse” por “adoptar”.

**Incisos tercero, cuarto, quinto, sexto, séptimo y octavo**

Los ha suprimido.

**Artículo 37 y 38**

Los ha eliminado

**TÍTULO VIII**

**Epígrafe**

Ha sustituido en su denominación la preposición “de” por “sobre”.

**Artículo 39**

Ha pasado a ser artículo 48, con las siguientes modificaciones:

**Inciso segundo**

**Letras d) y e)**

Las ha suprimido.

**Letras f) y g)**

Han pasado a ser letras d) y e), respectivamente, sin enmiendas.

**Artículos 40, 41, 42 y 43**

Han pasado a ser artículos 49, 50, 51 y 52, respectivamente, sin modificaciones.

**Artículo 44**

Ha pasado a ser artículo 53, reemplazado por el siguiente:

"Artículo 53. Regímenes especiales. El Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral y el Consejo Nacional de Televisión deberán adoptar las medidas de seguridad de sus redes y sistemas informáticos que sean pertinentes. Para estos efectos, la Corte Suprema, el respectivo jefe de servicio o los órganos colegiados que ejerzan dicha función, podrán dictar la normativa que sea conveniente a tales efectos, y considerar en su formulación las recomendaciones que efectúe la Agencia.

Las instituciones y órganos señalados en este artículo no estarán sujetos en modo alguno a la regulación, fiscalización o supervigilancia de la Agencia; sin perjuicio de que deberán convenir mecanismos de reporte de incidentes de ciberseguridad y de coordinación y cooperación para la respuesta a incidentes de ciberseguridad.

Asimismo, si el órgano autónomo constitucional revistiera el carácter de autoridad sectorial, deberá considerársele para los efectos de los artículos 6, 25 y 26.".

**Artículo 45**

Ha pasado a ser artículo 54, sin enmiendas.

**Artículo 46**

Ha pasado a ser artículo 55, enmendado del siguiente modo:

**Número 1**

Lo ha reemplazado por el siguiente:

“1. Agrégase en el artículo 2° el siguiente inciso final, nuevo:

“No será objeto de sanción penal por haber incurrido en los hechos tipificados en el inciso primero, el que habiendo accedido a un sistema informático cuyo responsable tenga domicilio en Chile, lo hiciera cumpliendo con las siguientes condiciones:

1. Que se encuentre inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad.

2. Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia.

3. Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado.

4. Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información

contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni habrá utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos.

5. Que no haya divulgado públicamente la información relativa a la potencial vulnerabilidad.

6. Que se trate de un acceso a un sistema informático de los organismos de la administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático.

7. Que haya dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.”.

**Artículos 47 y 48**

Lo ha suprimido.

**DISPOSICIONES TRANSITORIAS**

**Artículo primero**

*****

**Número 2, nuevo**

Ha incorporado, a continuación del número 1, el siguiente número 2, nuevo:

"2. Determinar un periodo para la vigencia de las normas establecidas por la presente ley, el que no podrá ser inferior a seis meses desde su publicación.".

*****

**Números 2, 3, 4, 5 y 6**

Han pasado a ser números 3, 4, 5, 6 y 7, respectivamente, sin modificaciones.

**Artículo segundo**

**Inciso primero**

Ha agregado, a continuación del punto y aparte, que pasa a ser punto y seguido, la siguiente oración: "El primer Director o Directora de la Agencia Nacional de Ciberseguridad no podrá participar del primer proceso de selección por Alta Dirección Pública para la provisión de su cargo.".

**Artículo quinto**

Lo ha eliminado.

**Artículos sexto y séptimo**

Han pasado a ser artículos quinto y sexto, respectivamente, sin enmiendas.

**Artículo octavo**

Lo ha suprimido.

*****

Hago presente a V.E. que los artículos 1° inciso segundo; 10; 12; 11 letras a), b), c), d), e), i), k) párrafos segundo y cuarto, n), ñ), o); w) e y); 16; 17; 20 inciso tercero; 24, con excepción de su letra g); 29; 30; 46; 47; 48; 49; 50; 53 y 54, permanentes, y los artículos segundo y quinto transitorios, del texto del proyecto de ley despachado por la Cámara de Diputados, fueron aprobados, en general y en particular, por 131 votos a favor, respecto de un total de 154 diputadas y diputados en ejercicio, dándose así cumplimiento a lo dispuesto en el inciso segundo del artículo 66 de la Constitución Política de la República, por tratarse de normas de rango orgánico constitucional.

Por su parte, los artículos 19; 21 inciso primero; 33; 34; 35 y 51, permanentes, del texto del proyecto de ley despachado por la Cámara de Diputados, fueron aprobados, en general y en particular, por 131 votos a favor, de un total de 154 diputadas y diputados en ejercicio, dándose cumplimiento de esta manera a lo dispuesto en el inciso segundo del artículo 66 de la Constitución Política de la República, por tratarse de normas de quórum calificado.

Lo que tengo a honra decir a V.E., en respuesta a vuestro oficio Nº 216/SEC/23, de 26 de abril de 2023.

Acompaño la totalidad de los antecedentes.

Dios guarde a V.E.

RICARDO CIFUENTES LILLO
Presidente de la Cámara de Diputados

MIGUEL LANDEROS PERKIĆ
Secretario General de la Cámara de Diputados