Cariola Díez
Pérez-Cotapos

PROYECTO DE LEY

"Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información"

BOLETÍN 14847-06

Proyecto de Ley "Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información", boletín 14847-06

- **Versión aprobada por el Senado el 12 de diciembre de 2023**
- **Equipo Tecnología, Privacidad y Medios. Cariola Díez Pérez-Cotapos Abogados**

El pasado 12 de diciembre de 2023 el Senado despachó el proyecto de Ley que "Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información", boletín 14847-06. Así, esta iniciativa tiene pendiente únicamente su revisión por el Tribunal Constitucional, tras la cual quedará en condiciones de ser promulgada y publicada en el diario oficial como ley.

A continuación, puede encontrar la versión actual del proyecto de Ley, , enriquecida con concordancias internas y un índice para facilitar su lectura.

Índice

TÍTULO I Disposiciones generales 4
Artículo 1°. Objeto. 4
Artículo 2°. Definiciones. 4
Artículo 3°. Principios rectores. 5
TÍTULO II Obligaciones de ciberseguridad 6
Párrafo 1° Servicios esenciales y operadores de importancia vital 6
Artículo 4°. Ámbito de aplicación. 6
Artículo 5. Operadores de Importancia Vital. 7
Artículo 6. Procedimiento de calificación de los operadores de importancia vital. 7
Párrafo 2° Obligaciones de ciberseguridad 7
Artículo 7°. Deberes generales. 8
Artículo 8º. Deberes específicos de los operadores de importancia vital. 8
Artículo 9°. Deber de reportar. 9
TÍTULO III De la Agencia Nacional de Ciberseguridad 10
Párrafo 1° Objeto, naturaleza y atribuciones 10
Artículo 10. Agencia Nacional de Ciberseguridad. 10
Artículo 11. Atribuciones. 10
Párrafo 2° Dirección, organización y patrimonio 13
Artículo 12. Dirección de la Agencia. 13
Artículo 13 Subdirección 14
Artículo 14. Atribuciones del Director o Directora Nacional. 14
Artículo 15. Del patrimonio de la Agencia. 14
Artículo 16. Nombramiento de autoridades. 15
Artículo 17. Del personal de la Agencia. 15
Artículo 18. Prohibiciones e inhabilidades. 16
Artículo 19. Notificación responsable de vulnerabilidades. 16
Párrafo 3° Consejo Multisectorial sobre Ciberseguridad 16
Artículo 20. Consejo Multisectorial sobre Ciberseguridad. 16

Artículo 21. Funcionamiento del Consejo. 17
Artículo 22. De las causales de cesación 17
Párrafo 4° Red de Conectividad Segura del Estado 17
Artículo 23. Red de Conectividad Segura del Estado. 17
Párrafo 5° Equipo Nacional de Respuesta a Incidentes de Seguridad Informática 18
Artículo 24. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. 18
TÍTULO IV Coordinación regulatoria y otras disposiciones 19
Artículo 25. Coordinación regulatoria. 19
Artículo 26. Normativa Sectorial 19
Artículo 27. Incidentes de efecto significativo. 19
Artículo 28. Centros de Certificación. 20
TÍTULO V Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional 20
Artículo 29. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. 20
Artículo 30. De las funciones del CSIRT de la Defensa Nacional. 20
Artículo 31. De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional 21
Artículo 32. Deber de reporte al CSIRT de la Defensa Nacional 21
TÍTULO VI De la reserva de información en el sector público en materia de ciberseguridad 21
Artículo 33. De la reserva de información. 21
Artículo 34. Extensión de la obligación de reserva 22
Artículo 35. Deber de reserva de la Agencia. 22
Artículo 36. Sanciones. 22
TÍTULO VII De las infracciones y sanciones. 22
Artículo 37. Competencia de la autoridad sectorial. 22
Artículo 38. Infracciones. 22
Artículo 39. De las infracciones de los Operadores de Importancia Vital. 23
Artículo 40. De las sanciones. 24
Artículo 41. Procedimiento simplificado. 24
Artículo 42. Procedimiento administrativo sancionador. 24
Artículo 43. De los recursos. 25
Artículo 44. Forma de pago de las multas. 25
Artículo 45. Pronto pago. 25
Artículo 46. Procedimiento de reclamación judicial. 25
Artículo 47. Responsabilidad administrativa del jefe superior del organismo de la administración del Estado 26
TÍTULO VIII Del Comité Interministerial sobre Ciberseguridad 26
Artículo 48. Comité Interministerial sobre Ciberseguridad. 26
Artículo 49. De los integrantes del Comité. 27
Artículo 50. De la Secretaría Ejecutiva. 27
Artículo 51. De la información reservada. 27
Artículo 52. Del reglamento. 27

Título IX Órganos autónomos constitucionales 27
Artículo 53. Regímenes especiales. 27
TÍTULO X De las modificaciones a otros cuerpos legales 28
Artículo 54. 28
Artículo 55. 28
DISPOSICIONES TRANSITORIAS.....29
Artículo primero. Entrada en vigencia y personal. 29
Artículo segundo.....29
Artículo tercero. 30
Artículo cuarto.....30
Artículo quinto.....30
Artículo sexto.....30

PROYECTO DE LEY:

TÍTULO I Disposiciones generales

Artículo 1°. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

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

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

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

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

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

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

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

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

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

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

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

9. Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

10. Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

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

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

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

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

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

Artículo 3°. Principios rectores.

Para alcanzar los objetivos de esta ley se deberán observar los siguientes principios:

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

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

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

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

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

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

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

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

TÍTULO II Obligaciones de ciberseguridad

Párrafo 1° Servicios esenciales y operadores de importancia vital

Artículo 4°. Ámbito de aplicación. La presente ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los incisos segundo y tercero de este artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos *5* y *6* de esta ley.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Párrafo 2° Obligaciones de ciberseguridad

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

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

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

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

Artículo 8º. Deberes específicos de los operadores de importancia vital.

Todos los operadores de importancia vital deberán:

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

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

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

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

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

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

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

f) Contar con las certificaciones que señale el artículo 28 de la presente ley.

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

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

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

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

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

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

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

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

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

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

iii) las medidas de mitigación aplicadas y en curso;

iv) si procede, las repercusiones transfronterizas del incidente;

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

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

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

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

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

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

TÍTULO III De la Agencia Nacional de Ciberseguridad

Párrafo 1° Objeto, naturaleza y atribuciones

Artículo 10. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido a través de la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad con lo establecido en el reglamento. Una vez notificado, el requerido deberá proporcionar todas las facilidades de acceso que sean necesarias. En caso de que el requerido sea una institución privada de las señaladas en el artículo 4º, podrá oponerse. Formulada la oposición la Agencia solo podrá acceder previa autorización judicial conforme lo dispuesto en los párrafos siguientes y no procederá el reclamo establecido en el artículo 46.

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

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

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

En caso de que se requiriera la restricción del acceso o uso de redes o sistemas informáticos se estará a lo dispuesto en este literal. No obstante, la Agencia deberá actuar conjuntamente con la autoridad sectorial correspondiente.

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

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

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

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

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

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

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

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

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8°. Adicionalmente, podrá citar a declarar, respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a

declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

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

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

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

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

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

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

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

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

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

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

x) Administrar la Red de Conectividad Segura del Estado.

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

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

Párrafo 2° Dirección, organización y patrimonio

Artículo 12. Dirección de la Agencia. La dirección y administración superior de la Agencia estará a cargo de un Director o Directora Nacional, quien será el jefe superior del Servicio,

tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta Dirección Pública establecidas en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.

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

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

Artículo 14. Atribuciones del Director o Directora Nacional. Corresponderá especialmente al Director o Directora Nacional:

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

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

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

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

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

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

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

Artículo 15. Del patrimonio de la Agencia. El patrimonio de la Agencia estará constituido por:

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

b) Los recursos otorgados por leyes generales o especiales;

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

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

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

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

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

Artículo 16. Nombramiento de autoridades. La Agencia estará afecta al Sistema de Alta Dirección Pública establecido en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica, hasta el segundo nivel jerárquico.

Artículo 17. Del personal de la Agencia. El personal de la Agencia se regirá por las normas del Código del Trabajo.

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

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

Asimismo, el personal estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle por los actos realizados en el ejercicio de sus funciones. La responsabilidad disciplinaria del personal de la Agencia por los actos realizados en el ejercicio de sus funciones podrá hacerse efectiva por la autoridad respectiva, de acuerdo al procedimiento establecido en el Título V "De la Responsabilidad Administrativa" del decreto con fuerza de ley N° 29, promulgado el año 2004 y publicado el año 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

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

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

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

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

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

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

Artículo 18. Prohibiciones e inhabilidades. Prohíbese al personal de la Agencia prestar por sí o a través de otras personas naturales o jurídicas, servicios personales a personas o a entidades sometidas a la fiscalización de la Agencia, o a los directivos, jefes o empleados de ellas, sean éstas públicas o privadas.

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

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

En todo caso, quedarán exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañan personalmente al funcionario o funcionaria, o que se refieran a la administración de su patrimonio. El desempeño de funciones en la Agencia será de dedicación exclusiva y será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley. No obstante, será compatible con cargos docentes en instituciones públicas o privadas reconocidas por el Estado hasta un máximo de doce horas semanales, para lo cual deberá prolongar su jornada a fin de compensar las horas durante las cuales no haya podido desempeñar su cargo.

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

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

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

Párrafo 3° Consejo Multisectorial sobre Ciberseguridad

Artículo 20. Consejo Multisectorial sobre Ciberseguridad. Créase el Consejo Multisectorial sobre Ciberseguridad, en adelante el Consejo, de carácter consultivo y que tendrá por función asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódica de la situación de ciberseguridad del país, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad, y proponer medidas para abordarlas.

El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, cuyo objeto o razón social se refiera a materias de esta ley, quienes permanecerán en su cargo durante seis años, renovándose en tríos cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.

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

Artículo 21. Funcionamiento del Consejo. El Consejo sesionará, a lo menos, cuatro veces al año; sus recomendaciones serán de carácter público y deberán recoger la diversidad de opiniones existentes en él cuando no haya unanimidad respecto de las mismas. Excepcionalmente y mediante decisión fundada, el Director o Directora podrá decretar secreta o reservada una parte o toda una sesión del Consejo, de lo cual se deberá dejar constancia en el acta respectiva. En este caso, se aplicará lo dispuesto en el artículo 51.

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

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

Artículo 22. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro sesiones consecutivas.

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

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

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

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

Párrafo 4° Red de Conectividad Segura del Estado

Artículo 23. Red de Conectividad Segura del Estado. Créase la Red de Conectividad Segura del Estado, en adelante RCSE, que proveerá servicios de interconexión y

conectividad a internet a los organismos de la Administración del Estado señalados en el artículo 1° de la presente ley.

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

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

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

Artículo 24. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. Créase dentro de la Agencia Nacional de Ciberseguridad el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, en adelante "CSIRT Nacional", el que tendrá las siguientes funciones:

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

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

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

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

d) Prestar colaboración o asesoría técnica a los CSIRT que pertenezcan a organismos de la Administración del Estado en la implementación de políticas y acciones relativas a ciberseguridad.

e) Supervisar incidentes a escala nacional.

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

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

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

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

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

TÍTULO IV Coordinación regulatoria y otras disposiciones

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

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

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

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

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

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

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

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

Artículo 27. Incidentes de efecto significativo. Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un

servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales. Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:

a) El número de personas afectadas.

b) La duración del incidente.

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

Los CSIRT que pertenezcan a los organismos de la Administración del Estado tendrán la obligación de tomar las providencias necesarias para apoyar en el restablecimiento del servicio afectado, bajo la coordinación del CSIRT Nacional.

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

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

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

La Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.

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

Artículo 29. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. Créase el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional, en adelante CSIRT de la Defensa Nacional, dependiente del Ministerio de Defensa Nacional, como el organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del mencionado Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional.

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

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

Artículo 30. De las funciones del CSIRT de la Defensa Nacional. Las funciones principales del CSIRT de la Defensa Nacional serán las siguientes:

a) Conducir y asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de

las redes de información, los servicios esenciales y operadores vitales para la defensa nacional. Para ello, estará a cargo de la coordinación y será enlace entre los diferentes CSIRT Institucionales de la Defensa Nacional.

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

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

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

Artículo 31. De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. En el sector de la defensa nacional se constituirán Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales de la Defensa Nacional, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional.

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

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

Artículo 32. Deber de reporte al CSIRT de la Defensa Nacional. Todas las instituciones de la defensa nacional deberán reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos al CSIRT de la Defensa Nacional. El CSIRT de la Defensa Nacional reportará a la Agencia todos los incidentes identificados cuando no se ponga en riesgo la seguridad y la defensa nacional, conforme a lo que determine el reglamento.

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

Artículo 33. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o que pertenezcan a organismos de la Administración del Estado o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

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

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

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 8°, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

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

i. Las matrices de riesgos de ciberseguridad;

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

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

Artículo 34. Extensión de la obligación de reserva. La obligación de guardar secreto regirá, además, para aquellos que, sin ser funcionarios o funcionarias de la Agencia, tomaren conocimiento de las solicitudes para la ejecución de procedimientos especiales de obtención de información de los antecedentes que las justifiquen y de las resoluciones judiciales que se dicten al efecto.

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

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

Artículo 36. Sanciones. La infracción a las obligaciones dispuestas en el presente Título, serán sancionadas en la forma prevista en los artículos 246, 247 o 247 bis, todos del Código Penal, según corresponda. Lo anterior es sin perjuicio de la responsabilidad administrativa que procediere.

TÍTULO VII De las infracciones y sanciones.

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

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

Se considerarán infracciones leves las siguientes:

1. Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima; y
3. Cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

Se considerarán infracciones graves las siguientes:

1. No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad;
2. No haber implementado los estándares particulares de ciberseguridad;
3. Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad;
4. Entregar a la Agencia de información manifiestamente falsa o errónea.
5. Incumplir la obligación de reportar establecida en el artículo 9;
6. Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial; y
7. La reincidencia en una misma infracción leve dentro de un año.

Se considerarán infracciones gravísimas las siguientes:

1. Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo;
3. No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo; y
4. La reincidencia en una infracción grave dentro de un año.

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

Se considerarán infracciones leves las siguientes:

1. No mantener el registro de las acciones de seguridad que señala la letra b);
2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala el literal d);
3. No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone el literal g);
4. No designar un delegado de ciberseguridad, según dispone la letra i);
5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c); y
6. No contar con las certificaciones que exija la ley, de acuerdo al literal f).

Se considerarán infracciones graves las siguientes:

1. No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere el literal a);
2. No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c);
3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g);
4. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e); y
5. La reincidencia en una misma infracción leve dentro del periodo de un año.

Se considerarán infracciones gravísimas las siguientes:

1. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e), cuando este posea un impacto significativo; y
2. La reincidencia en una misma infracción grave dentro del periodo de un año.

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

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales; o con hasta 10.000 unidades tributarias mensuales si se tratare de un operador de importancia vital;
2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales; o con hasta 20.000 unidades tributarias mensuales si se tratare de un operador de importancia vital; y
3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales; o con hasta 40.000 unidades tributarias mensuales si se tratare de un operador de importancia vital.

La multa será fijada teniendo en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño y la capacidad económica del infractor.

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

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

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

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

Artículo 42. Procedimiento administrativo sancionador. El procedimiento administrativo se regirá por lo prescrito por la ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los organismos de la Administración del Estado, sin perjuicio de las siguientes disposiciones:

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

b) En los descargos deberán señalarse todas las circunstancias o antecedentes de hecho y de derecho que eximan o atenúen la presunta responsabilidad de la persona objeto de cargos, así como aquellas que nieguen la efectiva ocurrencia de los hechos, o que demuestren

que éstos no constituyen infracción. Todo ello, sin perjuicio de otras presentaciones o antecedentes posteriores que se hagan valer en el curso del procedimiento sancionatorio con el mismo objetivo. Asimismo, deberán solicitarse las diligencias probatorias que correspondieren.

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

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

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

f) Una vez recibido el informe del instructor del procedimiento, corresponderá al Subdirector de la Agencia resolver los procesos sancionatorios en el plazo de quince días, dictando al efecto resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. La resolución del Subdirector deberá incluir el mismo contenido que el informe señalado en el literal precedente.

Artículo 43. De los recursos. En contra de la resolución del Subdirector mediante la cual se concluye el procedimiento administrativo procederán los recursos que establezca la ley Nº19.880. El recurso deberá resolverse dentro del plazo de quince días. La interposición del recurso suspenderá el plazo para reclamar de ilegalidad, siempre que se trate de materias por las cuales procede dicho recurso.

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

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

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

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

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

Artículo 46. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, los que deberán computarse de acuerdo al artículo 25 de la ley N°19.880, según las siguientes reglas:

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

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

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

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

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

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

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

h) Contra la resolución de la Corte de Apelaciones se podrá apelar ante la Corte Suprema, dentro del plazo de diez días hábiles, la que resolverá en cuenta.

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

Artículo 47. Responsabilidad administrativa del jefe superior del organismo de la administración del Estado. El jefe superior del organismo de la administración del Estado deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a lo establecido en esta ley.

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

TÍTULO VIII Del Comité Interministerial sobre Ciberseguridad

Artículo 48. Comité Interministerial sobre Ciberseguridad. Créase el Comité Interministerial sobre Ciberseguridad, en adelante el Comité, que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país.

En el ejercicio de sus funciones, el Comité deberá:

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

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

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

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

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

Artículo 49. De los integrantes del Comité. El Comité estará integrado por los siguientes miembros permanentes:

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

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

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

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

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

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

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

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

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

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

Artículo 50. De la Secretaría Ejecutiva. El Comité contará con una Secretaría Ejecutiva radicada en la Agencia, la que prestará el apoyo técnico, administrativo y de contenidos para el desarrollo de las reuniones del Comité.

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

Artículo 51. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios o funcionarias que estén en conocimiento de información reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición.

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

Artículo 52. Del reglamento. Un reglamento expedido por el Ministerio encargado de la seguridad pública fijará las normas de funcionamiento del Comité.

Título IX Órganos autónomos constitucionales

Artículo 53. Regímenes especiales. El Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral y el Consejo Nacional de Televisión deberán adoptar las medidas de seguridad de sus redes y

sistemas informáticos que sean pertinentes. Para estos efectos, la Corte Suprema, el respectivo jefe de servicio o los órganos colegiados que ejerzan dicha función, podrán dictar la normativa que sea conveniente a tales efectos, pudiendo considerar en su formulación las recomendaciones que efectúe la Agencia.

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

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

TÍTULO X De las modificaciones a otros cuerpos legales

Artículo 54. Incorpórase, en el artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, la siguiente letra k), nueva:

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

Artículo 55. Introdúcense las siguientes enmiendas en la ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest:

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

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

1) Encontrarse inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad;

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

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

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

5) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad;

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

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

2. Derógase el artículo 16.

DISPOSICIONES TRANSITORIAS

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

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

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

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

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

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

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

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

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

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

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

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

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

la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director o Directora, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director o Directora se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese sólo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal. El primer Director de la Agencia Nacional de Ciberseguridad no podrá participar del primer proceso de selección por Alta Dirección Pública para la provisión de su cargo.

Con todo, conforme a este artículo no podrá ser nombrado en el cargo de Director o Directora de la Agencia, quien hubiere ejercido el cargo de Coordinador Nacional de Ciberseguridad, dependiente del. Ministerio del Interior y Seguridad Pública, los tres años previos a la publicación de esta ley en el Diario Oficial.

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

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

Artículo quinto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 20, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período:

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

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

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

Cariola Díez
Pérez-Cotapos

CONTACTOS

Rodrigo Lavados

Socio, líder de proyectos de telecomunicaciones y gestión de activos intangibles.

Eduardo Vilches

Asociado senior, líder de proyectos de ciberseguridad y contratación tecnológica.

Gabriel Pensa

Asociado senior, líder de proyectos de datos personales y ética publicitaria.