**BOLETÍN Nº 14.847-06**

**INDICACIONES**

**22.11.22**

**INDICACIONES FORMULADAS DURANTE LA DISCUSIÓN EN GENERAL DEL PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL,**

**QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN**

**1.-** Del Honorable Senador señor Insulza, para reemplazar, todas las veces que aparece en el texto, la frase “incidentes de ciberseguridad” por la expresión “incidentes de ciberseguridad o ciberataques”.

**2.-** Del Honorable Senador señor Insulza, para sustituir, todas las veces que aparece en el texto, la frase “sistema informático” por “red o sistema de información”.

**TÍTULO I**

**ARTÍCULO 1**

**3.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

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

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

**4.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”; y la expresión “órganos del Estado” por “organismos de la Administración del Estado”.

**ARTÍCULO 2**

**Número 1**

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

**Número 2**

**6.-** Del Honorable Senador señor Insulza, para reemplazar el numeral 2, por el siguiente:

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

**7.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para agregar entre la palabra “soportan” y el punto final, la siguiente frase: “y/o que se vean afectados eléctrica o mecánicamente”.

**Número 3**

**8.-** Del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

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

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

**9.-** De Su Excelencia el Presidente de la República, para suprimir la frase “que abarcan los dominios físico, virtual y cognitivo”.

**Número 4**

**10.-** Del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

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

**Número 5**

**11.-** Del Honorable Senador señor Insulza, para reemplazarlo por el siguiente

“5. Equipo de respuesta a incidentes de seguridad informática o CSIRT: Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.”.

**12.-** De Su Excelencia el Presidente de la República, para sustituir la expresión “coadyuvando asimismo” por la palabra “ayudando”.

**Número 6**

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

**14.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

**Número 7**

**15.-** Del Honorable Senador señor Insulza, para reemplazar la frase “Gestión de incidente de ciberseguridad” por su plural “Gestión de incidentes de ciberseguridad”.

**16.-** De Su Excelencia el Presidente de la República, para suprimir la frase “en la medida de lo posible”.

**Número 8**

**17.-** Del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

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

**Número 9**

**18.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

**19.-** Del Honorable Senador señor Van Rysselberghe, para eliminar la palabra “instalaciones”.

**20.-** Del Honorable Senador señor Van Rysselberghe, para sustituir la frase “, y servicios y equipos físicos y de tecnología de la información”, por la siguiente expresión: “y servicios”.

**Número 10**

**21.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el que sigue:

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

**22.-** Del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

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

**Número 11**

**23.-** De Su Excelencia el Presidente de la República, para consultar, en su lugar, el siguiente:

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

**Número 12**

**24.-** Del Honorable Senador señor Insulza, para reemplazarlo por el que sigue:

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

**Número 13**

**25.-** Del Honorable Senador señor Insulza, para sustituirlo por el siguiente:

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

**Número 14**

**26.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

**Número 15**

**27.-** De Su Excelencia el Presidente de la República, para sustituirlo por el que sigue:

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

**Número 16**

**28.-** Del Honorable Senador señor Insulza, para reemplazarlo por el siguiente:

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

**°°°°°**

Números nuevos

**29.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para incorporar los siguientes números, nuevos:

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

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

…. Auditorías de Seguridad: Procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad y Riesgo de la Información y Ciberseguridad – SGSRI.

…. Ciberhigiene: Conducta personal responsable referida a la actitud de cautela que debe tener un usuario al conectarse a los sistemas informáticos, incluyendo el cuidado de las claves personales, el visitar sitios dudosos y conexiones en redes abiertas, establecer nexos con desconocidos a través de las redes sociales, o compartir información a través de medios extraíbles.

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

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

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

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

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

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

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

**°°°°°**

**°°°°°**

Números nuevos

**30.-** Del Honorable Senador señor Pugh, para consultar los siguientes números nuevos:

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

…. Operador de Servicios Esenciales – OSE: Entidad pública o privada que se identifique considerando los factores establecidos en la presente ley.”.

**°°°°°**

**ARTÍCULO 3**

**Número 1**

**31.-** Del Honorable Senador señor Van Rysselberghe, para sustituir la expresión “ofrece u opera” por “desarrolla, ofrece u opera”.

**Número 3**

**32.-** Del Honorable Senador señor Insulza, para reemplazar la frase “los datos, conectividad y sistemas deberán ser exclusivamente accedidos” por “la información almacenada o transmitida por redes y sistemas de información deberán ser conocidas y accedidas exclusivamente”.

**Número 4**

**33.-** Del Honorable Senador señor Insulza, para sustituir la frase “los datos y elementos de configuración de un sistema” por “la información almacenada o transmitida por redes y sistemas de información, incluida la configuración de estos,”.

**Número 5**

**34.-** Del Honorable Senador señor Insulza, para reemplazar la frase “los datos, conectividad y sistemas” por “la información almacenada o transmitida por redes y sistemas de información, y las redes y sistemas de información”.

**Número 6**

**35.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

**36.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos del Estado” por “organismos del Estado”.

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

**Número 7**

**38.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

**Número 8**

**39.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

**40.-** Del Honorable Senador señor Van Rysselberghe, para sustituirlo por el que sigue:

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

**°°°°°**

Número nuevo

**41.-** De Su Excelencia el Presidente de la República, para incorporar el siguiente número, nuevo, consultado como número 9:

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

**°°°°°**

**°°°°°**

Número nuevo

**42.-** Del Honorable Senador señor Insulza, para consultar el siguiente número 9, nuevo:

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

**°°°°°**

**°°°°°**

Números nuevos

**43.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para incorporar los siguientes números, nuevos:

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

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

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

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

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

**°°°°°**

**TÍTULO II**

**44.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para suprimirlo.

**EPÍGRAFE**

**45.-** De Su Excelencia el Presidente de la República, para sustituir su denominación por la siguiente:

“TÍTULO II

Obligaciones de ciberseguridad”.

**PÁRRAFO 1°**

**EPÍGRAFE**

**46.-** De Su Excelencia el Presidente de la República, para reemplazar su denominación por la siguiente:

“Párrafo 1°

Servicios esenciales y operadores de importancia vital”.

**ARTÍCULO 4**

**47.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

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

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

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

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

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

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

a) La cantidad de usuarios potencialmente afectados;

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

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

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

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

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

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

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

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

**Inciso primero**

**48.-** Del Honorable Senador señor Van Rysselberghe, para reemplazar la expresión “al Consejo Técnico de”, por la vocal “a”.

**Letra b)**

**49.-** Del Honorable Senador señor Insulza, para sustituir la frase “del sistema informático, red o sistema de información” por “red o sistema de información”.

**Inciso final**

**50.-** Del Honorable Senador señor Insulza, para suprimirlo.

**PÁRRAFO 2°**

**EPÍGRAFE**

**51.-** De Su Excelencia el Presidente de la República, para sustituir su denominación por la siguiente:

“Párrafo 2°

Obligaciones de ciberseguridad”.

**ARTÍCULO 5**

**52.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

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

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

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

**53.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos del Estado” por “organismos del Estado”.

**54.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para reemplazar la frase “físicas e informativas”, por la siguiente: “físicas, informativas y de trazabilidad”.

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

**ARTÍCULO 6**

**DENOMINACIÓN**

**56.-** De Su Excelencia el Presidente de la República, para reemplazarla por la siguiente:

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

**ENCABEZAMIENTO**

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

**58.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos del Estado” por “organismos del Estado”.

**Letra a)**

**59.-** De Su Excelencia el Presidente de la República, para sustituir la voz “permanente”, por la palabra “continuo”.

**60.-** Del Honorable Senador señor Insulza, para suprimir la frase “y cuáles de ellos facilitan la ocurrencia de incidentes de ciberseguridad.”

**61.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “determinar la gravedad” por la frase “estimar tanto la probabilidad como el impacto”.

**Letra c)**

**62.-** De Su Excelencia el Presidente de la República, para agregar, a continuación de la expresión “ciberseguridad”, la frase “certificados por un Centro de Certificación Acreditado o por la Agencia, según sea el caso”.

**63.-** De Su Excelencia el Presidente de la República, para sustituir la frase “periódicamente, a lo menos una vez al año”, por la siguiente: “y certificados periódicamente”.

**Letra e)**

**64.-** De Su Excelencia el Presidente de la República, para intercalar, entre las voces “Adoptar” y “las medidas”, la expresión “de forma oportuna y expedita”.

**°°°°°**

Letra nueva

**65.-** De Su Excelencia el Presidente de la República, para agregar la siguiente letra, nueva, contemplada como letra g):

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

**°°°°°**

**°°°°°**

Letra nueva

**66.-** De Su Excelencia el Presidente de la República, para incorporar la siguiente letra, nueva, consultada como letra h):

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

**°°°°°**

**°°°°°**

Letra nueva

**67.-** De Su Excelencia el Presidente de la República, para agregar una letra, nueva, consultada como letra i):

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

**°°°°°**

**°°°°°**

Inciso nuevo

**68.-** De Su Excelencia el Presidente de la República, para agregar el siguiente inciso segundo, nuevo:

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

**°°°°°**

**ARTÍCULO 7**

**69.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

La obligación de reportar debe cumplirse en un plazo inferior a 3 horas contadas desde que se tuvo conocimiento del evento respectivo. Este plazo podrá ser prorrogado por una sola vez y con la sola finalidad de recabar mayores detalles, siempre que la prórroga sea solicitada dentro del plazo original de tres horas.

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

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

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

**TÍTULO III**

**PÁRRAFO 1°**

**ARTÍCULO 8**

**70.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

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

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

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

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

**Inciso primero**

**71.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”.

**ARTÍCULO 9**

**Letra a)**

**72.-** De Su Excelencia el Presidente de la República, para reemplazarla por la que sigue:

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

**Letra b)**

**73.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente:

“b) Dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.”.

**74.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”.

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

**Letra c)**

**76.-** De Su Excelencia el Presidente de la República, para reemplazarla por la que se señala a continuación:

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

**77.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para sustituir la frase “al Ministro del Interior y Seguridad Pública”, por la siguiente: “a los Ministros del Interior y Seguridad Pública, y de Transportes y Telecomunicaciones”.

**Letra d)**

**78.-** De Su Excelencia el Presidente de la República, para consultar, en su lugar, la siguiente:

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

**79.-** Del Honorable Senador señor Van Rysselberghe, para eliminar el siguiente texto: “a los CSIRT Sectoriales y a aquellos que pertenezcan a órganos del Estado señalados en el inciso final del artículo 4º, a instituciones privadas y”.

**80.-** Del Honorable Senador señor Insulza, para reemplazar en la expresión “órganos del Estado” por “organismos de la Administración del Estado”.

**°°°°°**

Letra nueva

**81.-** De Su Excelencia el Presidente de la República, para intercalar la siguiente letra e), nueva, ajustándose el orden correlativo de las letras subsiguientes:

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

**°°°°°**

**Letra e)**

**82.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente, consultada como letra f):

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

**Letra f)**

**83.-** De Su Excelencia el Presidente de la República, para reemplazarla por la siguiente, contemplada como letra g):

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

**Letra g)**

**84.-** De Su Excelencia el Presidente de la República, para sustituirla por la que sigue, consultada como letra h):

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

**85.-** Del Honorable Senador señor Van Rysselberghe, para reemplazar la frase “de los CSIRT Sectoriales y del”, por la voz “al”.

**Letra h)**

**86.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente, consultada como letra i):

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

**Letra i)**

**87.-** De Su Excelencia el Presidente de la República, para reemplazarla por la que sigue, consultada como letra j):

“j) Requerir a los órganos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sea necesaria para el cumplimiento de sus fines, incluyendo el acceso a sistemas y redes informáticas, observando de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N°19.628.”.

**88.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos del Estado” por “organismos del Estado”.

**Letra j)**

**89.-** De Su Excelencia el Presidente de la República, para reemplazarla por la que sigue, consultada como letra k):

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

**Letra k)**

**90.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente, contemplada como letra l):

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

**91.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos del Estado” por “organismos del Estado”.

**Letra l)**

**92.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente, contemplada como letra m):

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

**93.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para reemplazarla por la siguiente:

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

**Letra m)**

**94.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente, consultada como letra n):

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

**Letra n)**

**95.-** De Su Excelencia el Presidente de la República, para reemplazarla por la siguiente, considerada como letra ñ):

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

**96.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para sustituirla por la siguiente:

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

**Letra o)**

**97.-** De Su Excelencia el Presidente de la República, para reemplazarla por la siguiente:

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

**98.-** Del Honorable Senador señor Van Rysselberghe, para sustituirla por la siguiente:

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

**°°°°°**

Letras nuevas

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

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

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

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

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

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

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

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

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

**°°°°°**

**°°°°°**

Letra nueva

**100.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para intercalar la siguiente letra p), nueva, pasando la actual letra p) a ser letra q):

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

**°°°°°**

**°°°°°**

Letras nuevas

**101.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para agregar las siguientes letras, nuevas:

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

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

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

**°°°°°**

**PÁRRAFO 2°**

**ARTÍCULO 11**

**Letra f)**

**102.-** De Su Excelencia el Presidente de la República, para reemplazar la expresión “funcionarios de las plantas directiva, profesional o técnica de la Agencia, y” por “los funcionarios que indique, e”.

**Letra g)**

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

**104.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos de la Administración del Estado” por “organismos de la Administración del Estado”.

°°°°°

Letra nueva

**105.-** De Su Excelencia el Presidente de la República, para incorporar la siguiente letra h), nueva:

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

°°°°°

**ARTÍCULO 13**

**106.-** De Su Excelencia el Presidente de la República, para intercalar, a continuación de la voz “indica”, la expresión “hasta el segundo nivel jerárquico”.

**ARTÍCULO 14**

**107.-** De Su Excelencia el Presidente de la República, para sustituirlo por el que sigue:

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

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

Asimismo, el personal estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle por los actos realizados en el ejercicio de sus funciones.

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

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

La Agencia no podrá celebrar contratos de trabajo estableciendo el pago de indemnizaciones por causas distintas a las indicadas en los artículos 161, 162 y 163 del Código del Trabajo, y en caso alguno se podrá alterar el monto que entregue la base de cálculo dispuesta en dichas normas.

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

La Agencia deberá cumplir con las normas establecidas en el decreto ley N° 1.263, de 1975, sobre administración financiera del Estado.”.

**108.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para reemplazar la expresión “Estatuto Administrativo” por “Código del Trabajo”.

**ARTÍCULO 15**

**109.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente:

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

El personal de la Agencia no podrá intervenir, en razón de sus funciones, en asuntos en que tenga interés él o ella, su cónyuge, su conveniente civil, sus parientes consanguíneos del 1° a 4° 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 quedan exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañen personalmente al funcionario o que se refieran a la administración de su patrimonio. Además, será compatible con los cargos docentes hasta un máximo de doce horas semanales.

Igualmente queda exceptuada la atención no remunerada prestada a sociedades de beneficencia, instituciones de carácter benéfico y, en general, a instituciones sin fines de lucro.

Con todo, para que operen estas excepciones, será necesario obtener autorización previa y expresa del jefe superior del servicio.”.

**PÁRRAFO 3°**

**EPÍGRAFE**

**110.-** De Su Excelencia el Presidente de la República, para reemplazar su denominación por la siguiente:

“Párrafo 3°

Consejo Multisectorial sobre Ciberseguridad”.

**ARTÍCULO 16**

**111.-** De Su Excelencia el Presidente de la República, para suprimirlo.

**Inciso primero**

**112.-** Del Honorable Senador señor Van Rysselberghe, para eliminar la frase “a los CSIRT Sectoriales,”.

**113.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos del Estado señalados en el inciso final del artículo 4º y a las” por “organismos del Estado e”.

**PÁRRAFO 4°**

**114.-** Del Honorable Senador señor Van Rysselberghe, para eliminarlo, junto con los artículos 17, 18, 19, 20 y 21, que lo integran.

**EPÍGRAFE**

**115.-** De Su Excelencia el Presidente de la República, para suprimirlo, pasando el actual Párrafo 5° a ser Párrafo 4° y así sucesivamente.

**ARTÍCULO 17**

**116.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como artículo 16:

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

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

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

**ARTÍCULO 18**

**117.-** De Su Excelencia el Presidente de la República, para suprimirlo.

**ARTÍCULO 19**

**118.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, consultado como artículo 17:

“Artículo 17. Funcionamiento del Consejo. El Consejo sesionará al menos cuatro veces al año, sus recomendaciones serán de carácter público y deberán recoger la diversidad de opiniones existentes en el Consejo, en caso de no existir unanimidad respecto de las mismas.

El Consejo sesionará todas las veces que sea necesario para el cumplimiento de sus funciones. La Agencia prestará el apoyo técnico y administrativo que sea necesario 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 20**

**119.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, contemplado como artículo 18:

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

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro sesiones consecutivas.

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

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

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

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

**ARTÍCULO 21**

**120.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, consultado como artículo 19:

“Artículo 19. Red de Conectividad Segura del Estado. Créase la Red de Conectividad Segura del Estado (RCSE), que proveerá servicios de interconexión y conectividad a Internet a los órganos de la Administración del Estado señalados en el artículo 1 de la presente ley.

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

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

**PÁRRAFO 5°**

**ARTÍCULO 22**

**Letra a)**

**121.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente:

“a) Responder ante ciberataques o incidentes de ciberseguridad, cuando éstos sean de impacto significativo.”.

**Letra b)**

**122.-** Del Honorable Senador señor Van Rysselberghe, para eliminarla.

**123.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente:

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

**Letra d)**

**124.-** Del Honorable Senador señor Van Rysselberghe, para suprimirla.

**Letra e)**

**125.-** Del Honorable Senador señor Van Rysselberghe, para eliminarla.

**126.-** De Su Excelencia el Presidente de la República, para reemplazarla por la siguiente:

“e) Supervisar incidentes a escala nacional.”.

**Letra f)**

**127.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente:

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

**Letra g)**

**128.-** De Su Excelencia el Presidente de la República, para eliminar el siguiente texto: “, con la finalidad de procurar que los órganos del Estado e instituciones privadas que posean infraestructura de la información calificada como crítica cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques”.

**129.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos del Estado” por “organismos del Estado”.

**Letra h)**

**130.-** Del Honorable Senador señor Van Rysselberghe, para suprimirla.

**131.-** De Su Excelencia el Presidente de la República, para reemplazar la expresión “a los CSIRT Sectoriales, dentro del ámbito de su competencia,”, por la siguiente: “a las instituciones afectadas y/o a los CSIRT correspondientes”.

**Letra i)**

**132.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente:

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

**133.-** Del Honorable Senador señor Van Rysselberghe, para suprimir la frase “, conjuntamente con uno o más CSIRT Sectoriales,”.

**134.-** Del Honorable Senador señor Insulza, para reemplazar las dos veces en que aparece la expresión “órganos del Estado”, por “organismos del Estado”.

**Letra j)**

**135.-** De Su Excelencia el Presidente de la República, para sustituirla por la siguiente:

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

**Letra k)**

**136.-** De Su Excelencia el Presidente de la República, para eliminarla.

**137.-** Del Honorable Senador señor Van Rysselberghe, para reemplazar la expresión “los otros CSIRT Sectoriales, de Gobierno y Defensa” por “los reguladores o fiscalizadores sectoriales”.

**TÍTULO IV**

**138.-** Del Honorable Senador señor Van Rysselberghe, para suprimirlo, junto con los artículos 23, 24, 25 y 26, que lo integran.

**EPÍGRAFE**

**139.-** De Su Excelencia el Presidente de la República, para reemplazar su denominación por la siguiente:

“TÍTULO IV

Otras instituciones intervinientes”.

**ARTÍCULO 23**

**140.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como artículo 21:

“Artículo 21. CSIRT Sectoriales. Las autoridades sectoriales deberán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad dar respuesta a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de las instituciones privadas.

Las funciones de los CSIRT Sectoriales serán determinadas por la Agencia, y en su actuación quedarán sujetos a su coordinación e instrucción.

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

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

**ARTÍCULO 24**

**141.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como artículo 22:

“Artículo 22. Facultades especiales. Las autoridades sectoriales podrán dictar las normas de carácter general y las normas técnicas que consideren necesarias para la ciberseguridad de las instituciones de su sector, de conformidad con la regulación sectorial respectiva, las que deberán ser sometidas a aprobación previa de la Agencia, quien deberá pronunciarse en el plazo de 30 días hábiles.

Asimismo, las autoridades sectoriales deberán dictar las instrucciones, circulares y órdenes que sean necesarias para la implementación de los protocolos y estándares técnicos establecidos por la Agencia. Con todo, si las autoridades sectoriales dictan normas generales sobre gestión de riesgos, que estén basadas en estándares internacionales e incluyan elementos relativos a ciberseguridad, podrán mantener dichos elementos.

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

**Letra b)**

**142.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos del Estado” por “organismos del Estado”.

**ARTÍCULO 25**

**143.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, considerado como artículo 23:

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

a) El número de personas afectadas.

b) La duración del incidente.

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

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

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

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

**ARTÍCULO 26**

**144.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como artículo 24:

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

Estos centros serán los únicos habilitados para certificar que un determinado ente cumple con los estándares y normas de seguridad que se exijan para la prestación de servicios al Estado, y el desarrollo de los sistemas y programas informáticos que sean utilizados por las instituciones públicas.

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

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

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

**°°°°°**

Título nuevo

**145.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para incorporar el siguiente Título, nuevo, consultado como Título V:

“Título V

De la Infraestructura Crítica de la Información

Párrafo 1°

De la calificación de la infraestructura de la información como crítica

Artículo …. La calificación de la infraestructura como crítica, será realizada por la Agencia Nacional de Ciberseguridad, en forma interagencial con los organismos que correspondan, debiendo efectuarse en un plazo inicial de 12 meses, un primer catastro de infraestructura crítica de la información.

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

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

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

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

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

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

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

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

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

e) El impacto que tenga sobre la economía de una comunidad, provincia o región a causa de la disrupción de los sistemas informáticos o de telecomunicaciones.

f) El daño reputacional que pueda ocasionarse por la vulnerabilidad en la infraestructura de la información, produciendo afectación de actividades o generando desconfianza respecto a su disponibilidad.

Transcurridos los 12 meses dispuestos para el catastro inicial, el Ministerio del Interior y Seguridad Pública, mediante la dictación de un decreto supremo bajo la fórmula “Por orden del Presidente de la República”, determinará aquellos sectores o instituciones que constituyen servicios esenciales y poseen infraestructura crítica de la información. Se entenderá que por el hecho de determinar que un sector posee infraestructura crítica de la información, las instituciones que conformen ese sector también poseerán infraestructura crítica de la información.

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

Artículo …. Los Directorios de empresas que posean infraestructura crítica de la información en los términos de los incisos anteriores, deberán acreditar que al menos uno de sus directores posea:

a) Certificación o título en ciberseguridad, o

b) Conocimientos, habilidades u otros antecedentes profesionales en ciberseguridad, tales como: áreas de política y gobierno de seguridad, gestión de riesgos, evaluación de seguridad, evaluación de control, arquitectura e ingeniería de seguridad, operaciones de seguridad, manejo de incidentes o planificación de continuidad comercial.

Artículo …. El catastro de Infraestructuras Críticas de la Información se actualizará anualmente, incluyendo a los criterios, los incidentes e impactos que se hayan registrado entre cada actualización, y remitirá su informe al Ministerio respectivo para su vigencia y aplicación.

Asimismo, se mantendrá un listado actualizado de todos los Directores de Informática de las empresas e instituciones calificadas como Infraestructura Crítica, y sus datos de contacto.

La Agencia Nacional de Ciberseguridad tendrá facultades de regulación sobre los organismos que posean infraestructura crítica, pudiendo establecer, entre otros, los contenidos mínimos de los Sistemas de Gestión de la Seguridad y Riesgo de la Información – SGSRI de los regulados, controlando que los mismos se encuentren correctamente auditados por entidades externas debidamente habilitadas para tal efecto por la Agencia.

Párrafo 2°

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

Artículo …. Deberes generales. Será obligación de los órganos del Estado y de las instituciones privadas que posean infraestructura de la información calificada como crítica, aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas, informativas y de trazabilidad necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos, así como contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad e integridad del servicio prestado, de conformidad a lo prescrito en esta ley. Se prohíbe a dichos órganos e instituciones, realizar pagos de cualquier tipo por rescate ante ataques de secuestro de datos o ransomware, así como de equipos o de dispositivos.

Artículo …. Deberes específicos. Los órganos del Estado, las municipalidades, las entidades fiscales autónomas, las empresas del Estado o aquellas en las que el Fisco tenga intervención por aportes de capital, y las instituciones privadas cuya infraestructura de la información sea calificada como crítica, deberán:

a) Implementar un Sistema de Gestión de la Seguridad y Riesgo de la Información – SGSRI, permanente y actualizado regularmente, cada 180 días a lo menos, con el fin de determinar aquellos que pueden afectar la seguridad de las redes, sistemas informáticos y datos, cuáles afectarían la continuidad operacional del servicio y cuáles de ellos facilitan la ocurrencia de incidentes de ciberseguridad. Dicho sistema deberá contar con la capacidad de determinar la gravedad de las consecuencias de un incidente de ciberseguridad.

EL SGSRI debe además considerar el entorno operacional de la o las instalaciones, tales como las vulnerabilidades físicas a las que puede estar expuesta la información producto de acciones de la naturaleza, actos vandálicos que interrumpan comunicaciones, vulnerabilidad física y otros.

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

c) Establecer un plan de capacitación y actualización del personal en las tecnologías en uso, así como planes de inducción y procedimientos de administración del cambio al introducir modificaciones o actualizaciones relevantes de los sistemas.

d) Elaborar e implementar planes de continuidad operacional y ciberseguridad. Dichos planes deberán ser actualizados periódicamente, a lo menos cada 180 días, o cada vez que sean actualizados los sistemas o procesos. Los planes de ciberseguridad deberán contemplar los protocolos de acción inmediata frente a incidentes de ciberseguridad, y de la forma de comunicar la ocurrencia de estos.

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

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

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

**°°°°°**

**TÍTULO V**

**146.-** Del Honorable Senador señor Van Rysselberghe, para suprimirlo, junto con los artículos 27 y 28, que lo integran.

**EPÍGRAFE**

**147.-** De Su Excelencia el Presidente de la República, para reemplazar su denominación por la siguiente:

“TÍTULO V

Del Equipo de Respuesta a incidentes de seguridad informática de la Defensa Nacional”.

**ARTÍCULO 27**

**148.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, contemplado como artículo 25:

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

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

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

**Letra a)**

**149.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

**ARTÍCULO 28**

**150.-** De Su Excelencia el Presidente de la República, para sustituirlo por el siguiente, consultado como artículo 26:

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

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

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

c) Establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y 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 nuevo

**151.-** De Su Excelencia el Presidente de la República, para incorporar el siguiente artículo, nuevo, consultado como artículo 27:

“Artículo 27. De los Equipos de Respuesta a incidentes de seguridad informática institucionales de la Defensa Nacional. En el sector de la Defensa Nacional se constituirán Equipos de Respuesta a incidentes de seguridad informática institucionales de la Defensa Nacional, en adelante “CSIRT institucionales de la Defensa Nacional”, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la Defensa Nacional.

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

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

**°°°°°**

**°°°°°**

Artículo nuevo

**152.-** De Su Excelencia el Presidente de la República, para agregar el siguiente artículo, nuevo, consultado como artículo 28:

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

**°°°°°**

**TÍTULO VI**

**ARTÍCULO 29**

**Inciso primero**

**153.-** Del Honorable Senador señor Van Rysselberghe, para reemplazar la frase “los CSIRT, sean el CSIRT Nacional, de Gobierno, Defensa o los CSIRT Sectoriales”, por la siguiente: “la Agencial Nacional de Ciberseguridad”.

**154.-** De Su Excelencia el Presidente de la República, para suprimir la expresión “de Gobierno,”.

**155.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

**Inciso segundo**

**156.-** De Su Excelencia el Presidente de la República, para intercalar, entre las palabras “autorización” y “su”, el vocablo “de”.

**Inciso tercero**

**157.-** Del Honorable Senador señor Van Rysselberghe, para sustituir la frase “CSIRT, sean del CSIRT Nacional, de Gobierno, Defensa o de los CSIRT Sectoriales,” por “la Agencia Nacional de Ciberseguridad”.

**158.-** De Su Excelencia el Presidente de la República, para suprimir la expresión “de Gobierno,”.

**TÍTULO VII**

**ARTÍCULO 33**

**159.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

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

b) Las infracciones graves serán sancionadas con multa de 1.001 a 5.000 unidades tributarias mensuales. En caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 10.000 unidades tributarias mensuales.

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

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

Se consideran infracciones graves, las siguientes:

a) Retardar o entregar fuera de plazo la información a la autoridad u órgano de la Administración del Estado habilitado por ley para requerirla.

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

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

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

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

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

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

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

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

Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.”.

**160.-** Del Honorable Senador señor Insulza, para sustituirlo por el que sigue:

“Artículo 33. De las infracciones. Serán consideradas infracciones leves para efectos de esta ley, las siguientes:

a) Retardar o entregar fuera del plazo señalado la información a la autoridad u órgano del Estado habilitado para requerirla.

b) Incumplir el plazo previsto en el artículo 25, para efectos de reportar incidentes.

c) Incumplir los deberes generales previstos en el artículo 5.

Serán consideradas infracciones graves para efectos de esta ley, las siguientes:

a) Negar injustificadamente información a la autoridad u órgano del Estado habilitado para requerirla.

b) Incumplir los deberes específicos previstos en el artículo 6.

Serán consideradas infracciones gravísimas para efectos de esta ley, las siguientes:

a) Entregar información falsa o manifiestamente errónea.

b) Incumplir el deber de reportar previsto en el artículo 25.

Podrán imponerse, a beneficio fiscal, multas entre 10 y 20.000 Unidades Tributarias Mensuales, de conformidad a la gravedad de la infracción y a la siguiente escala:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 10 a 5.000 Unidades Tributarias Mensuales.

b) Las infracciones graves serán sancionadas con multa de hasta 10.000 Unidades Tributarias Mensuales.

c) Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 Unidades Tributarias Mensuales.

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

Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.

Las infracciones cometidas por funcionarios del Estado se regirán por su respectivo estatuto sancionatorio.”.

**Inciso primero**

**Letra a)**

**161.-** Del Honorable Senador señor Van Rysselberghe, para eliminar la expresión “Retardar o”.

**Letra b)**

**162.-** Del Honorable Senador señor Van Rysselberghe, para suprimir la palabra “injustificadamente”.

**ARTÍCULO 34**

**163.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

“Artículo 34. Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan las instituciones privadas por incumplimiento o vulneración de los principios y obligaciones establecidas en esta ley y la aplicación de las sanciones correspondientes se sujetará a las siguientes reglas especiales:

a) El procedimiento sancionatorio será instruido por la Agencia.

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

c) La Agencia deberá presentar una formulación de cargos en contra de la institución privada, la que señalará una descripción clara y precisa de los hechos que se estimen constitutivos de infracción y la fecha de su verificación, así como los principios, obligaciones, protocolos, estándares técnicos, instrucciones generales y particulares eventualmente infringidos por la institución privada, la disposición que establece la infracción, la sanción y cualquier otro antecedente que sirva para sustentar la formulación.

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

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

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

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

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

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

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

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

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

m) La resolución que establezca el incumplimiento o vulneración a los principios y obligaciones de esta ley y aplique la sanción correspondiente deberá ser fundada. Esta resolución debe indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia que resuelve el procedimiento por infracción de ley será reclamable mediante recurso de reposición que se podrá interponer en el plazo de 5 días hábiles contados desde la notificación, el que deberá ser resuelto por el Director dentro del plazo de 30 días hábiles.

n) El procedimiento administrativo de infracción de ley no podrá superar los seis meses. Cuando hayan transcurrido más de seis meses desde la fecha de la certificación indicada en la letra b) de este artículo sin que la Agencia haya resuelto la reclamación, la institución privada podrá presentar un reclamo de ilegalidad en los términos previstos en el siguiente artículo.”.

**°°°°°**

Artículos nuevos

**164.-** De Su Excelencia el Presidente de la República, para incorporar los siguientes artículos, nuevos, consultados como artículos 35, 36 y 37, pasando el actual artículo 35 a ser artículo 38 y así sucesivamente:

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

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

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

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

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

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

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

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

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

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

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

Las infracciones a los principios y obligaciones contenidos en los artículos 21 y 29 serán sancionadas con multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del órgano público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza del incidente y el número de personas afectadas, si las hubiere. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor.

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

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

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

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

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

Artículo 37. Responsabilidad del funcionario infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios del órgano público, la Contraloría General de la República, a petición de la Agencia, iniciará una investigación sumaria para determinar las responsabilidades de dichos funcionarios o lo hará en el procedimiento administrativo ya iniciado, en su caso. Las sanciones a los funcionarios infractores serán determinadas de conformidad a lo dispuesto en el Estatuto Administrativo.

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

**°°°°°**

**ARTÍCULO 35**

**165.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, consultado como artículo 38:

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

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

**TÍTULO VIII**

**166.-** Del Honorable Senador señor Van Rysselberghe, para suprimirlo, junto con los artículos 36, 37, 38, 39 y 40, que lo integran.

**ARTÍCULO 36**

**167.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como artículo 39:

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

En el ejercicio de sus funciones, el Comité deberá:

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

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

c) Coordinar la implementación de la política nacional de ciberseguridad.

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

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

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

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

**168.-** Del Honorable Senador señor Insulza, para sustituir la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

**ARTÍCULO 37**

**169.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como artículo 40:

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

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

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

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

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

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

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

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

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

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

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

**Inciso final**

**170.-** Del Honorable Senador señor Insulza, para sustituir la expresión “funcionarios de la Administración del Estado” por “funcionarios del Estado”.

**ARTÍCULO 38**

(consultado por el Ejecutivo como artículo 41)

**Inciso segundo**

**171.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

**ARTÍCULO 40**

(contemplado por el Ejecutivo como artículo 43)

**172.-** De Su Excelencia el Presidente de la República, para sustituir la expresión “Ministerio del Interior y Seguridad Pública” por “Ministerio encargado de la seguridad pública”.

**°°°°°**

Título nuevo

**173.-** De Su Excelencia el Presidente de la República, para incorporar el siguiente Título IX, nuevo, pasando el actual Título IX a ser Título X y así sucesivamente:

“Título IX

Órganos autónomos constitucionales”.

**°°°°°**

**°°°°°**

Artículo nuevo

**174.-** De Su Excelencia el Presidente de la República, para consultar el siguiente artículo 44, nuevo, pasando el actual artículo 41 a ser artículo 45:

“Artículo 44. Regímenes especiales. Corresponde a las autoridades superiores de los órganos internos del Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral y el Consejo Nacional de Televisión adoptar las medidas especiales de ciberseguridad señaladas en el artículo 6 de la presente ley, debiendo dictar para ello las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidas en esta ley, pudiendo requerir para ello la asistencia técnica de la Agencia Nacional de Ciberseguridad.

Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios, en relación a las infracciones a esta ley que se produzcan.

Las instituciones y organismos señalados en este artículo no estarán sujetas a la regulación, fiscalización o supervigilancia de la Agencia.”.

**°°°°°**

**°°°°°**

Artículo nuevo

**175.-** Del Honorable Senador señor Insulza, para agregar el siguiente artículo, nuevo:

“Artículo…. Derecho general al cifrado. Toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio de este derecho.”.

**°°°°°**

**TÍTULO IX**

**176.-** Del Honorable Senador señor Van Rysselberghe, para eliminarlo, junto con el artículo 41, que lo integra.

**ARTÍCULO 41**

**177.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente, contemplado como artículo 45:

“Artículo 45. Incorpórese, 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.”.”.

**°°°°°**

Artículos nuevos

**178.-** De Su Excelencia el Presidente de la República, para agregar los siguientes artículos, nuevos, consultados como artículos 46, 47 y 48:

“Artículo 46. Modificaciones a la ley N° 21.459 sobre delitos informáticos.

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

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

“No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que reporte inmediatamente al responsable de las redes o sistemas informáticos afectados y a la Agencia Nacional de Ciberseguridad el acceso y las vulnerabilidades de seguridad detectadas en su investigación.”.

2.- Derógase el artículo 16.

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

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

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

**°°°°°**

**TÍTULO X**

**DISPOSICIONES TRANSITORIAS**

**ARTÍCULO PRIMERO TRANSITORIO**

**179.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

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

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

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

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

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

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

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

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

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

5. Determinar la estructura de la Agencia y su dotación máxima de personal.

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

**ARTÍCULO SEGUNDO TRANSITORIO**

**180.-** De los Honorables Senadores señor Pugh, señora Órdenes, y señores Macaya y Ossandón, para sustituir la expresión “un año”, por la siguiente frase: “dieciocho meses, prorrogables por necesidades del servicio,”.

**ARTÍCULO QUINTO TRANSITORIO**

**181.-** Del Honorable Senador señor Van Rysselberghe, para eliminarlo.

**182.-** Del Honorable Senador señor Insulza, para reemplazar la expresión “órganos de la Administración del Estado” por “organismos del Estado”.

**ARTÍCULO SEXTO TRANSITORIO**

**183.-** Del Honorable Senador señor Van Rysselberghe, para suprimirlo.

**184.-** De Su Excelencia el Presidente de la República, para reemplazarlo por el siguiente:

“Artículo sexto transitorio.- Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 16, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período:

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

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

**°°°°°**

Artículo transitorio nuevo

**185.-** De Su Excelencia el Presidente de la República, para incorporar el siguiente artículo octavo transitorio, nuevo:

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

**°°°°°**

- - -