PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL, QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN
BOLETÍN Nº 14.847-06

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	PROYECTO DE LEY: "TÍTULO I Disposiciones generales **Artículo 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y**	**ARTÍCULO 1** Reemplazarlo por el siguiente: "Artículo 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos 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	**PROYECTO DE LEY:** "TÍTULO I Disposiciones generales **Artículo 1. Objeto. La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos 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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los mecanismos de control, supervisión y de responsabilidad por la infracción de la normativa.	deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.	**del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.**
		Para los efectos de esta ley, se entenderá por Administración del Estado a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, 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 este tenga participación accionaria superior al	**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 este tenga participación**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital. La institucionalidad de la ciberseguridad velará por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias, que comprende la adopción de las medidas necesarias e idóneas para garantizar la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan sus redes y sistemas informáticos, incluyendo las herramientas de cifrado.”. **(Unanimidad 7x0. Indicación número 3, y artículo 121, inciso final, del Reglamento del Senado).**	**accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.** **La institucionalidad de la ciberseguridad velará por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias, que comprende la adopción de las medidas necesarias e idóneas para garantizar la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan sus redes y sistemas informáticos, incluyendo las herramientas de cifrado.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ARTÍCULO 2 Sustituirlo por el que se señala a continuación:	
	Artículo 2. Definiciones. Para efectos de esta ley se entenderá por: **1. Agencia: La Agencia Nacional de Ciberseguridad.** **2. Ciberataque: Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.** **3. Ciberespacio: Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las**	"Artículo 2. Definiciones. Para efectos de esta ley se entenderá por: 1. Activo informático: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización. 2. Agencia: la Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI. 3. Auditorías de seguridad: procesos de control destinados a revisar el	**Artículo 2. Definiciones. Para efectos de esta ley se entenderá por:** **1. Activo informático: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.** **2. Agencia: la Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI.** **3. Auditorías de seguridad: procesos de control destinados a revisar el cumplimiento de las**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo y las interacciones sociales que se verifican en su interior. **Las infraestructuras tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores, estaciones, sistemas radiantes, nodos, conductores, entre otros.** **Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red.** **4. Ciberseguridad: el conjunto de acciones destinadas al estudio y manejo de las amenazas y riesgos de incidentes de ciberseguridad; a la prevención, mitigación y**	cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información. 4. Autenticación: propiedad de la información que da cuenta de su origen legítimo.	**políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.** **4. Autenticación: propiedad de la información que da cuenta de su origen legítimo.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	respuesta frente a estos, así como para reducir sus efectos y el daño causado, antes, durante y después de su ocurrencia, respecto de los activos informáticos y de servicios.		
	5. Equipo de respuesta a incidentes de seguridad informática o CSIRT: Centros conformados por especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, y que actúan según procedimientos y políticas predefinidas, coadyuvando asimismo a mitigar sus efectos.	5. Autoridad sectorial: aquellos servicios públicos que cuentan con facultades regulatorias, fiscalizadoras y eventualmente sancionatorias respecto de sus regulados.	**5. Autoridad sectorial: aquellos servicios públicos que cuentan con facultades regulatorias, fiscalizadoras y eventualmente sancionatorias respecto de sus regulados.**
	6. Estándares Mínimos de Ciberseguridad: Corresponden al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad, dictados por la Agencia o por el regulador sectorial competente, los cuales deben ser cumplidos por los órganos de la Administración del Estado y por quienes posean infraestructura de la información	6. Ciberataque: un incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, exfiltrar, hacer uso o acceder de manera no autorizada a un activo de información, y en el que puedan verse afectados también activos físicos de forma eléctrica o	**6. Ciberataque: un incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, exfiltrar, hacer uso o acceder de manera no autorizada a un activo de información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	calificada como crítica. **7. Gestión de incidente de Ciberseguridad: Conjunto ordenado de acciones enfocadas a prevenir en la medida de lo posible la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.** **8. Incidente de ciberseguridad: Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos a través sistemas de telecomunicaciones y su infraestructura, que puedan afectar al normal funcionamiento**	mecánica. 7. Ciberespacio: ambiente formado por la interconexión e interrelación compleja entre las redes y sistemas informáticos, los componentes lógicos de la información, los datos almacenados, procesados o transmitidos, y las interacciones sociales que ocurren en aquel. Los componentes lógicos de la información son los diferentes programas computacionales que permiten el funcionamiento, administración y uso de la red. 8. Ciberhigiene o higiene digital: conjunto de prácticas habituales de las personas para mejorar la gestión segura de datos y proteger redes y sistemas informáticos, que incluyen, entre otros, el cuidado de claves de acceso, la gestión de vulnerabilidades y la actualización de programas y aplicaciones.	**7. Ciberespacio: ambiente formado por la interconexión e interrelación compleja entre las redes y sistemas informáticos, los componentes lógicos de la información, los datos almacenados, procesados o transmitidos, y las interacciones sociales que ocurren en aquel.** **Los componentes lógicos de la información son los diferentes programas computacionales que permiten el funcionamiento, administración y uso de la red.** **8. Ciberhigiene o higiene digital: conjunto de prácticas habituales de las personas para mejorar la gestión segura de datos y proteger redes y sistemas informáticos, que incluyen, entre otros, el cuidado de claves de acceso, la gestión de vulnerabilidades y la actualización de programas y aplicaciones.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	de los mismos.		
	9. Infraestructura Crítica de la Información: corresponde a aquellas instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción puede tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.	9. Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.	**9. Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.**
	10. Red o sistema de información: Medio en virtud del cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí.	10. Confidencialidad: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.	**10. Confidencialidad: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	11. Regulador o fiscalizador sectorial: Son aquellos servicios públicos dentro de cuyas funciones se encuentra la regulación y/o supervigilancia de uno o más sectores regulados. **12. Resiliencia: Capacidad de las redes o sistemas de información para seguir operando pese a estar sometidos a un incidente de ciberseguridad o ciberataque, aunque sea en un estado degradado, debilitado o segmentado; y, también, la capacidad de restaurar con presteza sus funciones esenciales después de un incidente de ciberseguridad o ciberataque, por lo general con un efecto reconocible mínimo.** **13. Riesgo: Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes o sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza**	11. Disponibilidad: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado. 12. Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos. 13. Estándares mínimos de ciberseguridad: corresponde al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad, dictados por la Agencia o por la autoridad sectorial competente de conformidad con la	**11. Disponibilidad: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.** **12. Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.** **13. Estándares mínimos de ciberseguridad: corresponde al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad, dictados por la Agencia o por la autoridad sectorial competente de conformidad con la presente ley.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	que produzca un impacto negativo en éstas. **14. Sector regulado: Sector que representa alguna actividad económica estratégica nacional, que se encuentra sometido a la supervigilancia de un regulador o fiscalizador sectorial.** **15. Servicios esenciales: Todo servicio respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción de su infraestructura de la información pueda afectar gravemente:** **a) La vida o integridad física de las personas;** **b) La provisión de servicios sanitarios, energéticos o de telecomunicaciones;** **c) Al normal funcionamiento de obras públicas fiscales y medios de transporte;**	presente ley. 14. Gestión de incidentes de ciberseguridad: conjunto ordenado de acciones enfocadas a prevenir la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, restaurar los niveles de operación lo antes posible. 15. Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación o no-repudio de los procesos ejecutados o implementados en las redes y sistemas informáticos.	**14. Gestión de incidentes de ciberseguridad: conjunto ordenado de acciones enfocadas a prevenir la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.** **15. Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación o no-repudio de los procesos ejecutados o implementados en las redes y sistemas informáticos.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	d) A la generalidad de usuarios o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que permitan la transacción de dinero o valores; y **e) De modo general, el normal desarrollo y bienestar de la población.** **16. Sistema informático: Todo dispositivo aislado o el conjunto de ellos, interconectados o relacionados entre sí, incluidos sus soportes lógicos, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.** **17. Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.**	16. Integridad: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización. 17. Interagencialidad: coordinación que permite que dos o más agencias o instituciones actúen de forma conjunta, sinérgica y coherente para alcanzar objetivos comunes, imposibles de lograr de forma independiente.	**16. Integridad: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.** **17. Interagencialidad: coordinación que permite que dos o más agencias o instituciones actúen de forma conjunta, sinérgica y coherente para alcanzar objetivos comunes, imposibles de lograr de forma independiente.** **18. Interoperabilidad: capacidad**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		18. Interoperabilidad: capacidad de los sistemas informáticos de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos en tiempo real. 19. No repudio: propiedad de la información que permite probar su origen. 20. Operadores de importancia vital: institución pública o privada, identificada como tal por la Agencia de conformidad con esta ley, por prestar algún servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, que depende de las redes y sistemas informáticos, y cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar.	**de los sistemas informáticos de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos en tiempo real.** **19. No repudio: propiedad de la información que permite probar su origen.** **20. Operadores de importancia vital: institución pública o privada, identificada como tal por la Agencia de conformidad con esta ley, por prestar algún servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, que depende de las redes y sistemas informáticos, y cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar.** **21. Red y sistema informático:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		21. Red y sistema informático: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales. 22. Resiliencia: capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad. 23. Riesgo: posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo. 24. Sector regulado: aquel sector de	**conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.** **22. Resiliencia: capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.** **23. Riesgo: posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.** **24. Sector regulado: aquel sector de la actividad económica que se encuentra sometido a la**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		la actividad económica que se encuentra sometido a la supervigilancia de un órgano público con facultades suficientes para regular, fiscalizar y eventualmente sancionar. 25. Servicios esenciales: todo servicio cuya afectación o interrupción tendría un impacto perturbador en el normal funcionamiento de la defensa nacional, la sociedad o la economía. 26. Sistema de gestión de seguridad de la información: conjunto de políticas, procedimientos, guías técnicas, y las actividades y recursos asociados, gestionados colectivamente por una organización para proteger sus activos de información. 27. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.”.	**supervigilancia de un órgano público con facultades suficientes para regular, fiscalizar y eventualmente sancionar.** **25. Servicios esenciales: todo servicio cuya afectación o interrupción tendría un impacto perturbador en el normal funcionamiento de la defensa nacional, la sociedad o la economía.** **26. Sistema de gestión de seguridad de la información: conjunto de políticas, procedimientos, guías técnicas, y las actividades y recursos asociados, gestionados colectivamente por una organización para proteger sus activos de información.** **27. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Encabezamiento, unanimidad. Artículo 121, inciso final, del Reglamento del Senado). **(Número 1, unanimidad 7x0. Indicación número 28, y artículo 121, inciso final, del Reglamento del Senado).** **(Número 2, unanimidad 9x0. Indicación número 5).** **(Número 3, unanimidad 8x0. Indicación número 29).** **(Número 4, unanimidad 8x0. Indicación número 29).** **(Número 5, unanimidad 7x0. Indicación número 23).** **(Número 6, unanimidad 7x0. Indicaciones números 6 y 7).** **(Número 7, unanimidad 8x0. Indicación número 8).** **(Número 8, unanimidad 8x0. Indicación número 29).** **(Número 9, unanimidad 8x0.**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Indicación número 10). **(Número 10, unanimidad 8x0. Indicación número 29).** **(Número 11, unanimidad 8x0. Indicación número 29).** **(Número 12, unanimidad 8x0. Indicación número 11).** **(Número 13, unanimidad 9x0. Indicación número 13).** **(Número 14, unanimidad 8x0. Indicaciones números 15 y 16).** **(Número 15, unanimidad 8x0. Indicación número 17, y artículo 121, inciso final, del Reglamento del Senado).** **(Número 16, unanimidad 8x0. Indicación número 29).** **(Número 17, unanimidad 8x0. Indicación número 29).** **(Número 18, unanimidad 8x0. Indicación número 29).**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Número 19, unanimidad 8x0. Indicación número 29). **(Número 20, unanimidad 7x0. Indicación número 18, y artículo 121, inciso final, del Reglamento del Senado).** **(Número 21, unanimidad 7x0. Indicación número 22, y artículo 121, inciso final, del Reglamento del Senado).** **(Número 22, unanimidad 7x0. Indicación número 24, y artículo 121, inciso final, del Reglamento del Senado).** **(Número 23, unanimidad 7x0. Indicación número 25).** **(Número 24, unanimidad 7x0. Indicación número 26).** **(Número 25, unanimidad 7x0. Indicación número 27).** **(Número 26, unanimidad 8x0. Indicación número 29).** **(Número 27, unanimidad. Artículo**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		121, inciso final, del Reglamento del Senado).	
		<u>ARTÍCULO 3</u> Reemplazarlo por el que se transcribe:	
	Artículo 3. Principios rectores. En la aplicación de las disposiciones de esta ley se deberán observar los siguientes principios:	"Artículo 3. Principios rectores. En la aplicación de las disposiciones de esta ley se deberán observar los siguientes principios:	**Artículo 3. Principios rectores. En la aplicación de las disposiciones de esta ley se deberán observar los siguientes principios:**
	1. Principio de responsabilidad: aquel en cuya virtud la seguridad de las redes, sistemas y datos es de responsabilidad de aquel que las ofrece u opera, con independencia de la naturaleza pública o privada del organismo.	1 Principio de actualización de programas computacionales: los organismos públicos e instituciones privadas adoptarán las medidas necesarias para la instalación de las actualizaciones de seguridad de los sistemas informáticos que usen o administren, dando prioridad a aquellas que solucionen vulnerabilidades graves.	**1 Principio de actualización de programas computacionales: los organismos públicos e instituciones privadas adoptarán las medidas necesarias para la instalación de las actualizaciones de seguridad de los sistemas informáticos que usen o administren, dando prioridad a aquellas que solucionen vulnerabilidades graves.**
	2. Principio de protección	2. Principio de confidencialidad de	**2. Principio de confidencialidad**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	integral: se deberán determinar los riesgos potenciales que puedan afectar a las redes o sistemas de información y aplicar las medidas organizativas, de gestión y técnicas apropiadas para la protección de los mismos.	los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos deberá ser conocida y accedida exclusivamente por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.	**de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos deberá ser conocida y accedida exclusivamente por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.**
	3. Principio de confidencialidad de los sistemas de información: los datos, conectividad y sistemas deberán ser exclusivamente accedidos por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.	3. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad, todos los organismos del Estado, así como las instituciones privadas, deberán siempre actuar diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.	**3. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad, todos los organismos del Estado, así como las instituciones privadas, deberán siempre actuar diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.**
	4. Principio de integridad de los sistemas informáticos y de la información: los datos y elementos de configuración de un sistema sólo podrán ser modificados por personas autorizadas en el ejercicio de sus	4. Principio de cooperación con la autoridad: los organismos del Estado y los privados deberán cooperar con la autoridad competente para resolver los incidentes de ciberseguridad y, si es necesario, deberán cooperar entre	**4. Principio de cooperación con la autoridad: los organismos del Estado y los privados deberán cooperar con la autoridad competente para resolver los incidentes de ciberseguridad y, si es necesario, deberán cooperar**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	funciones o por sistemas que cuenten con la autorización respectiva.	diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.	**entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.**
	5. Principio de disponibilidad de los sistemas de información: los datos, conectividad y sistemas deben estar accesibles para su uso a demanda.	5. Principio de disponibilidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos, y las redes y sistemas informáticos deberán estar accesibles para su uso a demanda.	**5. Principio de disponibilidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos, y las redes y sistemas informáticos deberán estar accesibles para su uso a demanda.**
	6. Principio de control de daños: los órganos del Estado y aquellas instituciones privadas que posean infraestructura de la información calificada como crítica, en el caso de un incidente de ciberseguridad o de un ciberataque, deben siempre actuar diligentemente y adoptar las medidas necesarias (_) para evitar la escalada del incidente de ciberseguridad o del ciberataque y su posible propagación a otros sistemas informáticos, notificando de igual forma el incidente de ciberseguridad al CSIRT respectivo.	6. Principio de igualdad y no discriminación: todas las personas tienen derecho a participar de un espacio digital seguro y libre de violencia. El Estado desarrollará acciones de prevención, promoción, reparación y garantía de este derecho, otorgando especial protección a mujeres, niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas.	**6. Principio de igualdad y no discriminación: todas las personas tienen derecho a participar de un espacio digital seguro y libre de violencia. El Estado desarrollará acciones de prevención, promoción, reparación y garantía de este derecho, otorgando especial protección a mujeres, niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	7. Principio de cooperación con la autoridad: los órganos de la Administración del Estado y los privados deberán cooperar con la autoridad competente para resolver los incidentes de ciberseguridad, y, si es necesario, deberán cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios. **8. Principio de especialidad en la sanción: en materia sancionatoria, se preferirá la aplicación de la regulación sectorial por sobre la establecida en esta ley.**	7. Principio de integridad de los sistemas informáticos y de la información: la información almacenada o transmitida por redes y sistemas informáticos, incluida la configuración de estos, solo podrá ser modificada por personas autorizadas en el ejercicio de sus funciones o por sistemas que cuenten con la autorización respectiva. 8. Principio de protección integral: se deberán determinar los riesgos potenciales que puedan afectar a las redes y sistemas informáticos y aplicar las medidas organizativas, de gestión y técnicas apropiadas para la protección de los mismos. 9. Principio de responsabilidad: aquel en cuya virtud la seguridad de las redes, sistemas y datos es de responsabilidad de aquel que las provee, ofrece u opera, con independencia de la naturaleza	**7. Principio de integridad de los sistemas informáticos y de la información: la información almacenada o transmitida por redes y sistemas informáticos, incluida la configuración de estos, solo podrá ser modificada por personas autorizadas en el ejercicio de sus funciones o por sistemas que cuenten con la autorización respectiva.** **8. Principio de protección integral: se deberán determinar los riesgos potenciales que puedan afectar a las redes y sistemas informáticos y aplicar las medidas organizativas, de gestión y técnicas apropiadas para la protección de los mismos.** **9. Principio de responsabilidad: aquel en cuya virtud la seguridad de las redes, sistemas y datos es de responsabilidad de aquel que las provee, ofrece u opera, con independencia de la naturaleza pública o privada del organismo.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		pública o privada del organismo. 10. Principio de respuesta responsable: la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización de, o el apoyo a, operaciones ofensivas. 11. Principio del cifrado: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio de este derecho.”. **(Encabezamiento, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).** **(Número 1, unanimidad 9x0, indicación número 43, y 10x0, indicación número 43 bis).** **(Número 2, unanimidad 8x0. Indicación número 32).**	**10. Principio de respuesta responsable: la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización de, o el apoyo a, operaciones ofensivas.** **11. Principio del cifrado: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio de este derecho.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Número 3, unanimidad 9x0. Indicaciones números 35 y 36). **(Número 4, unanimidad 9x0, indicación número 38, y 10x0, indicación número 38 bis).** **(Número 5, unanimidad 8x0. Indicación número 34).** **(Número 6, unanimidad 9x0, indicación número 42, y 10x0, indicación número 42 bis).** **(Número 7, unanimidad 8x0. Indicación número 33).** **(Número 8, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).** **(Número 9, unanimidad 8x0. Indicación número 31).** **(Número 10, unanimidad 9x0. Indicación número 39).** **(Número 11, unanimidad 7x0. Indicación número 175).**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		<u>TÍTULO II</u> Considerar como tal el siguiente: "TÍTULO II Obligaciones de ciberseguridad". **(Unanimidad 7x0. Indicación número 45).** **Párrafo 1°** Contemplar, en su lugar, el que se indica a continuación: "Párrafo 1° Servicios esenciales y operadores de importancia vital".	**TÍTULO II** **Obligaciones de ciberseguridad** **Párrafo 1°** **Servicios esenciales y operadores de importancia vital**
	TÍTULO II **De la determinación de Infraestructura Crítica de la Información** **Párrafo 1°** **Determinación de la infraestructura crítica de la información**		

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Unanimidad 7x0. Indicación número 46).	
		ARTÍCULO 4	
		Reemplazarlo por el que sigue:	
	Artículo 4. Calificación de la infraestructura de la información como crítica. Cada dos años, el Ministerio del Interior y Seguridad Pública requerirá al Consejo Técnico de la Agencia Nacional de Ciberseguridad un informe que detalle cuáles son aquellos sectores o instituciones que posean infraestructura de la información que deba ser calificada como crítica.	"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.	**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.**
	Para determinar si en un sector o institución existe infraestructura de la información que deba calificarse como crítica, se deberán tener en consideración,	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	**A fin de determinar qué servicios resultan esenciales, se deberá atender a la entidad del impacto**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	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;**	mantenimiento de actividades sociales y económicas fundamentales. Los criterios para la identificación de los operadores de importancia vital serán los siguientes: a) Se trata de un operador que presta un servicio calificado como esencial de conformidad con esta ley; b) La prestación de dicho servicio depende de las redes y sistemas informáticos, y c) Un incidente de ciberseguridad tendría un impacto perturbador en la prestación de dicho servicio. Para determinar si el impacto de un incidente de ciberseguridad podría ser perturbador, se deberán tener en consideración, al menos, los siguientes factores: a) La cantidad de usuarios potencialmente afectados;	**cuya afectación o interrupción podría tener en la defensa nacional o en el mantenimiento de actividades sociales y económicas fundamentales.** **Los criterios para la identificación de los operadores de importancia vital serán los siguientes:** **a) Se trata de un operador que presta un servicio calificado como esencial de conformidad con esta ley;** **b) La prestación de dicho servicio depende de las redes y sistemas informáticos, y** **c) Un incidente de ciberseguridad tendría un impacto perturbador en la prestación de dicho servicio.** **Para determinar si el impacto de un incidente de ciberseguridad podría ser perturbador, se deberán tener en consideración, al menos, los siguientes factores:** **a) La cantidad de usuarios potencialmente afectados;**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	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**	b) La interdependencia de otros sectores calificados como servicios esenciales; c) La potencial afectación de la vida, integridad física o salud de las personas; d) La repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales, en la seguridad nacional o en el ejercicio de la soberanía; e) La extensión geográfica que podría verse afectada por un incidente; f) La importancia del operador para el mantenimiento de un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio;	**b) La interdependencia de otros sectores calificados como servicios esenciales;** **c) La potencial afectación de la vida, integridad física o salud de las personas;** **d) La repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales, en la seguridad nacional o en el ejercicio de la soberanía;** **e) La extensión geográfica que podría verse afectada por un incidente;** **f) La importancia del operador para el mantenimiento de un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	funcionamiento del Estado y sus órganos.	g) La afectación relevante del funcionamiento del Estado y sus organismos, y h) El daño reputacional que pueda ocasionarse. La Agencia requerirá a la Agencia Nacional de Inteligencia un informe fundado sobre los servicios que deban calificarse como esenciales e identifique, para cada uno de 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.	**ese servicio;** **g) La afectación relevante del funcionamiento del Estado y sus organismos, y** **h) El daño reputacional que pueda ocasionarse.** **La Agencia requerirá a la Agencia Nacional de Inteligencia un informe fundado sobre los servicios que deban calificarse como esenciales e identifique, para cada uno de 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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
			Defensa Nacional.
		Transcurrido este plazo, con los antecedentes que hubiere recibido, la Agencia propondrá una lista actualizada de servicios esenciales y de operadores de importancia vital al Comité Interministerial de Ciberseguridad para que, dentro del plazo de treinta días, se pronuncie fundadamente, pudiendo aprobar o sugerir las enmiendas que considere necesarias para su aprobación, las que serán comunicadas a la Agencia.	**Transcurrido este plazo, con los antecedentes que hubiere recibido, la Agencia propondrá una lista actualizada de servicios esenciales y de operadores de importancia vital al Comité Interministerial de Ciberseguridad para que, dentro del plazo de treinta días, se pronuncie fundadamente, pudiendo aprobar o sugerir las enmiendas que considere necesarias para su aprobación, las que serán comunicadas a la Agencia.**
	Dentro de los ciento veinte días siguientes a la recepción del informe, el Ministerio del Interior y Seguridad Pública, mediante la dictación de un decreto supremo bajo la fórmula "Por orden del Presidente de la República", determinará aquellos sectores o instituciones que constituyen servicios esenciales y poseen infraestructura crítica de la información. Se entenderá que por el hecho de determinar que un sector posee infraestructura crítica de la información, las instituciones que conformen ese sector también poseerán	Dentro de los treinta días siguientes a la recepción de la decisión del Comité Interministerial de Ciberseguridad, el Ministerio encargado de la seguridad pública, mediante la dictación de un decreto supremo bajo la fórmula "Por orden del Presidente de la República", determinará aquellos servicios que serán considerados esenciales y a los operadores de importancia vital. Este decreto quedará exento del	**Dentro de los treinta días siguientes a la recepción de la decisión del Comité Interministerial de Ciberseguridad, el Ministerio encargado de la seguridad pública, mediante la dictación de un decreto supremo bajo la fórmula "Por orden del Presidente de la República", determinará aquellos servicios que serán considerados esenciales y a los operadores de importancia vital. Este decreto quedará exento del**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	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.**	trámite de toma de razón de la Contraloría General de la República.". **(Unanimidad 7x0. Indicación número 47).**	**trámite de toma de razón de la Contraloría General de la República.**
	Párrafo 2° **De las obligaciones de las instituciones que poseen infraestructura de la información calificada como crítica**	**Párrafo 2°** Contemplar, en su lugar, el que se transcribe a continuación: "Párrafo 2° Obligaciones de ciberseguridad". **(Unanimidad 7x0. Indicación número 51).**	**Párrafo 2°** **Obligaciones de ciberseguridad**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ARTÍCULO 5 Sustituirlo por el que se señala:	
	Artículo 5. Deberes generales. Será obligación de los órganos del Estado y de las instituciones privadas que posean infraestructura de la información calificada como crítica, aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos, así como contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad e integridad del servicio prestado, de conformidad a lo prescrito en esta ley.	"Artículo 5. Deberes generales. Será obligación de los organismos del Estado y de las instituciones privadas aplicar de manera permanente las medidas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso. Asimismo, estas medidas tendrán	**Artículo 5. Deberes generales. Será obligación de los organismos del Estado y de las instituciones privadas aplicar de manera permanente las medidas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.** **Asimismo, estas medidas tendrán**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		por objeto la gestión de riesgos asociados a la ciberseguridad y la contención y mitigación del impacto que los incidentes puedan tener sobre la continuidad operacional, la confidencialidad y la integridad del servicio prestado, de conformidad con lo prescrito en la presente ley. En el caso de los organismos de la Administración del Estado e instituciones privadas que presten servicios esenciales, el cumplimiento de estas obligaciones exige, al menos, la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva, de ser el caso. La Agencia deberá establecer protocolos y estándares diferenciados según el tipo de organización de que se trate y su relación con la prestación de servicios calificados como esenciales, teniendo especialmente	**por objeto la gestión de riesgos asociados a la ciberseguridad y la contención y mitigación del impacto que los incidentes puedan tener sobre la continuidad operacional, la confidencialidad y la integridad del servicio prestado, de conformidad con lo prescrito en la presente ley.** **En el caso de los organismos de la Administración del Estado e instituciones privadas que presten servicios esenciales, el cumplimiento de estas obligaciones exige, al menos, la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva, de ser el caso.** **La Agencia deberá establecer protocolos y estándares diferenciados según el tipo de organización de que se trate y su relación con la prestación de servicios calificados como**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		en consideración las características y necesidades de las pequeñas y medianas empresas, tal como se definen en la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño. Para efectos de emitir los protocolos y estándares a los que se refiere el inciso anterior, la Agencia deberá solicitar informe previo de la autoridad sectorial competente, el que deberá ser evacuado a más tardar dentro el plazo de treinta días hábiles, sin perjuicio de lo dispuesto en el artículo 22 respecto de las instituciones financieras fiscalizadas por la Comisión para el Mercado Financiero. Se prohíbe a los organismos e instituciones señalados en el inciso primero, realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital o ransomware, ya sea que dichos ataques causen la inoperatividad de los sistemas o amenacen con exponer la	**esenciales, teniendo especialmente en consideración las características y necesidades de las pequeñas y medianas empresas, tal como se definen en la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.** **Para efectos de emitir los protocolos y estándares a los que se refiere el inciso anterior, la Agencia deberá solicitar informe previo de la autoridad sectorial competente, el que deberá ser evacuado a más tardar dentro el plazo de treinta días hábiles, sin perjuicio de lo dispuesto en el artículo 22 respecto de las instituciones financieras fiscalizadas por la Comisión para el Mercado Financiero.** **Se prohíbe a los organismos e instituciones señalados en el inciso primero, realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital o ransomware, ya sea que dichos ataques causen la inoperatividad de los sistemas o amenacen con**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		información exfiltrada.”. **(Unanimidad 7x0, indicaciones números 52 y 53; 8x0, indicación número 55, y 10x0, indicación número 55 bis).**	**exponer la información exfiltrada.**
		ARTÍCULO 6 Reemplazarlo por el siguiente:	
	Artículo 6. Deberes específicos. Los órganos del Estado señalados en el inciso final del artículo 4º y las instituciones privadas cuya infraestructura de la información sea calificada como crítica, deberán:	“Artículo 6. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales. Todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital, deberán:	**Artículo 6. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales. Todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital, deberán:**
	a) Implementar un sistema de gestión de riesgo permanente con el fin de determinar aquellos que pueden afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio y cuáles de ellos facilitan	a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio. Dicho	**a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio. Dicho**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	la ocurrencia de incidentes de ciberseguridad. Dicho sistema debe contar con la capacidad de determinar la gravedad de las consecuencias de un incidente de ciberseguridad.	sistema debe contar con la capacidad de estimar tanto la probabilidad como el impacto de las consecuencias de un incidente de ciberseguridad.	**sistema debe contar con la capacidad de estimar tanto la probabilidad como el impacto de las consecuencias de un incidente de ciberseguridad.**
	b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de riesgos, de conformidad a lo que señale el reglamento. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores de los protocolos de ciberseguridad y la aplicación de los mismos, tanto durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad.	b) Mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, de conformidad a lo que señale el reglamento. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores de los protocolos de ciberseguridad y la aplicación de los mismos, tanto durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad.	**b) Mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, de conformidad a lo que señale el reglamento. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores de los protocolos de ciberseguridad y la aplicación de los mismos, tanto durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad.**
	c) Elaborar e implementar planes de continuidad operacional y ciberseguridad. Dichos planes deberán ser actualizados periódicamente, a lo menos una vez al año.	c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, certificados por un centro de certificación acreditado o por la Agencia, según sea el caso. Dichos planes deberán ser	**c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, certificados por un centro de certificación acreditado o por la Agencia, según sea el caso. Dichos planes deberán ser actualizados y**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		actualizados y certificados periódicamente.	**certificados periódicamente.**
	d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos, plataformas y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Sectorial respectivo o al CSIRT Nacional, según correspondiere, en la forma que determine el reglamento.	d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Sectorial respectivo o al CSIRT Nacional, según correspondiere, en la forma que determine el reglamento.	**d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Sectorial respectivo o al CSIRT Nacional, según correspondiere, en la forma que determine el reglamento.**
	e) Adoptar 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.	e) Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.	**e) Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.**
	f) Contar con las certificaciones de los sistemas de gestión y procesos que determine el reglamento.	f) Contar con las certificaciones de los sistemas de gestión y procesos que determine el reglamento.	**f) Contar con las certificaciones de los sistemas de gestión y procesos que determine el reglamento.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		g) Informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes y sistemas informáticos, en los siguientes casos: cuando se vean expuestos datos personales y no exista otra ley que obligue su notificación; o cuando generar conciencia pública sea necesario para evitar un incidente o para gestionar uno que ya hubiera ocurrido. Todo lo anterior, conforme a las instrucciones generales y particulares que al efecto dicte la Agencia. h) Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene. i) Designar un delegado de ciberseguridad, quien será la contraparte de la Agencia y dependerá directamente de la máxima autoridad de la institución a la que pertenece.	**g) Informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes y sistemas informáticos, en los siguientes casos: cuando se vean expuestos datos personales y no exista otra ley que obligue su notificación; o cuando generar conciencia pública sea necesario para evitar un incidente o para gestionar uno que ya hubiera ocurrido. Todo lo anterior, conforme a las instrucciones generales y particulares que al efecto dicte la Agencia.** **h) Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.** **i) Designar un delegado de ciberseguridad, quien será la contraparte de la Agencia y dependerá directamente de la máxima autoridad de la institución a la que pertenece.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Un reglamento expedido por el Ministerio encargado de la seguridad pública identificará los organismos del Estado con competencias específicas sobre servicios esenciales.”. **(Denominación y encabezamiento del artículo: 8x0 y 7x0, respectivamente. Indicaciones número 56, 57 y 58).** **(Letra a), unanimidad 8x0, indicaciones números 59, 60 y 61, y 10x0, indicación número 61 bis).** **(Letra b), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).** **(Letra c), unanimidad 8x0. Indicaciones números 62 y 63).** **(Letra d), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).** **(Letra e), unanimidad 8x0. Indicación número 64).**	**Un reglamento expedido por el Ministerio encargado de la seguridad pública identificará los organismos del Estado con competencias específicas sobre servicios esenciales.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Letra f), unanimidad. Artículo 121, inciso final, del Reglamento del Senado). **(Letra g), unanimidad 8x0. Indicación número 65, y artículo 121, inciso final, del Reglamento del Senado).** **(Letra h), unanimidad 8x0. Indicación número 66).** **(Letra i), unanimidad 8x0. Indicación número 67).** **(Inciso final, unanimidad 8x0. Indicación número 68).**	
	Artículo 7. Facultades normativas. Los reguladores o fiscalizadores sectoriales podrán dictar instrucciones, circulares, órdenes, normas de carácter general y las normas técnicas que sean necesarias para establecer	**ARTÍCULO 7** Considerar como tal el que sigue: "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	**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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	los estándares particulares de ciberseguridad respecto de sus regulados o fiscalizados, de conformidad a la regulación sectorial respectiva, las que deberán considerar, a lo menos, los estándares establecidos por la Agencia Nacional de Ciberseguridad.	instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley. La obligación de reportar deberá cumplirse en un plazo inferior a tres horas contadas desde que se tuvo conocimiento del evento respectivo. La entidad informante podrá solicitar la prórroga de dicho plazo por una sola vez y mientras se encuentre este vigente, con la sola finalidad de recabar mayores antecedentes. Adicionalmente, todos los operadores de servicios esenciales, sean de importancia vital o no, deberán informar al CSIRT Nacional su plan de acción tan pronto lo hubieren adoptado. El plazo para la adopción de un plan de acción en	**hubiere eximido expresamente en sus instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley.** **La obligación de reportar deberá cumplirse en un plazo inferior a tres horas contadas desde que se tuvo conocimiento del evento respectivo. La entidad informante podrá solicitar la prórroga de dicho plazo por una sola vez y mientras se encuentre este vigente, con la sola finalidad de recabar mayores antecedentes.** **Adicionalmente, todos los operadores de servicios esenciales, sean de importancia vital o no, deberán informar al CSIRT Nacional su plan de acción tan pronto lo hubieren adoptado. El plazo para la adopción de un plan de acción en ningún caso**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ningún caso podrá ser superior a siete días corridos, de ocurrido alguno de los hechos a que refiere el inciso primero. Para el cumplimiento del deber establecido en este artículo, los jefes de servicio deberán exigir a los proveedores de servicios de tecnologías de la información, que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado. Con el objeto de cumplir con lo anterior, deberán eliminar cualquier restricción, especialmente las contractuales, que pudiera dificultar la comunicación de información sobre amenazas entre el Gobierno y el sector privado. La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo.”.	**podrá ser superior a siete días corridos, de ocurrido alguno de los hechos a que refiere el inciso primero.** **Para el cumplimiento del deber establecido en este artículo, los jefes de servicio deberán exigir a los proveedores de servicios de tecnologías de la información, que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado. Con el objeto de cumplir con lo anterior, deberán eliminar cualquier restricción, especialmente las contractuales, que pudiera dificultar la comunicación de información sobre amenazas entre el Gobierno y el sector privado.** **La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Unanimidad 8x0. Indicación número 69, y artículo 121, inciso final, del Reglamento del Senado).	
	TÍTULO III De la Agencia Nacional de Ciberseguridad Párrafo 1° Objeto, naturaleza y atribuciones **Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses**	**<u>ARTÍCULO 8</u>** 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,	TÍTULO III De la Agencia Nacional de Ciberseguridad Párrafo 1° Objeto, naturaleza y atribuciones **Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad y regular y fiscalizar las acciones de los órganos de la Administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o fiscalizador sectorial, y que posea infraestructura de la información calificada como crítica, según los preceptos de esta ley. Se relacionará con el Presidente de la República por intermedio del Ministerio del Interior y Seguridad Pública.	coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.	**nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.**
		La Agencia deberá regular, fiscalizar y sancionar las acciones de los organismos de la Administración del Estado y de las instituciones privadas en materia de ciberseguridad, incluida la facultad de impartir instrucciones generales y particulares. En el ejercicio de sus funciones, la Agencia deberá siempre velar por la coherencia normativa, buscando que sus acciones se inserten de manera	**La Agencia deberá regular, fiscalizar y sancionar las acciones de los organismos de la Administración del Estado y de las instituciones privadas en materia de ciberseguridad, incluida la facultad de impartir instrucciones generales y particulares.** **En el ejercicio de sus funciones, la Agencia deberá siempre velar por la coherencia normativa,**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		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.”. **(Unanimidad 8x0. Indicaciones números 70 y 71).**	**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.**
	La Agencia tendrá domicilio en la ciudad de Santiago, sin perjuicio de contar con oficinas en otras localidades o regiones del país.		
		ARTÍCULO 9 Sustituirlo por el que se transcribe a continuación:	
	Artículo 9. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones: **a) Asesorar al Presidente de la República, en el análisis y**	“Artículo 9. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones: a) Asesorar al Presidente de la República en la elaboración y	**Artículo 9. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones:** **a) Asesorar al Presidente de la República en la elaboración y**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	definiciones de la política nacional de ciberseguridad, así como los planes y programas de acción específicos para su ejecución y cumplimiento, así como en temas relativos a estrategias de avance en su implementación.	aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.	**aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.**
	b) Dictar normas técnicas de carácter general y los estándares mínimos de ciberseguridad e impartir instrucciones particulares para los órganos de la Administración del Estado y para los privados cuya infraestructura de la información sea calificada como crítica y no se encuentren sometidos a la regulación o fiscalización de un regulador o fiscalizador sectorial, según corresponda.	b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.	**b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.**
	c) Proponer al Ministro del Interior y Seguridad Pública las normas legales y reglamentarias que se requieran para asegurar el acceso libre y seguro al ciberespacio así como aquellas que estén dentro del marco de su competencia.	c) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad; los protocolos y estándares técnicos, y las instrucciones generales y	**c) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad; los protocolos y estándares técnicos, y las**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		particulares que dicte al efecto.	**instrucciones generales y particulares que dicte al efecto.**
	d) Coordinar a los CSIRT Sectoriales y a aquellos que pertenezcan a órganos del Estado señalados en el inciso final del artículo 4º, a instituciones privadas y al CSIRT Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades.	d) Coordinar y supervisar a los CSIRT Sectoriales existentes; a aquellos que pertenezcan a organismos de la Administración del Estado; a instituciones privadas y al CSIRT Nacional, en la forma que establece esta ley.	**d) Coordinar y supervisar a los CSIRT Sectoriales existentes; a aquellos que pertenezcan a organismos de la Administración del Estado; a instituciones privadas y al CSIRT Nacional, en la forma que establece esta ley.**
		e) Establecer una coordinación con el CSIRT de la Defensa Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, así como respecto a las materias que serán objeto de intercambio de información.	**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.**
	e) Administrar el Registro Nacional de Incidentes de Ciberseguridad.	f) Crear y administrar un Registro Nacional de Incidentes de Ciberseguridad.	**f) Crear y administrar un Registro Nacional de Incidentes de Ciberseguridad.**
	f) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de	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.	**g) Elaborar y actualizar la lista de servicios esenciales y operadores de importancia vital, en la forma**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	ciberseguridad. **g) Requerir de los CSIRT Sectoriales y del CSIRT Nacional la información que sea necesaria para el cumplimiento de sus fines y que sea de responsabilidad de estas instituciones.** **h) Diseñar e implementar planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.** **i) Suscribir convenios con órganos del Estado e instituciones privadas destinados a facilitar la colaboración y la transferencia de información que permita el cumplimiento de los fines de la Agencia.**	h) Requerir de los CSIRT Sectoriales la información que sea necesaria para el cumplimiento de sus fines y que se encuentre en posesión de estas instituciones. i) Diseñar e implementar, en coordinación con el Ministerio de Educación, cuando corresponda, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad. j) Requerir a los organismos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sea necesario para el cumplimiento de sus fines, incluyendo el acceso a redes y sistemas informáticos, observando de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N° 19.628.	**prevista en el artículo 4 de la presente ley.** **h) Requerir de los CSIRT Sectoriales la información que sea necesaria para el cumplimiento de sus fines y que se encuentre en posesión de estas instituciones.** **i) Diseñar e implementar, en coordinación con el Ministerio de Educación, cuando corresponda, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.** **j) Requerir a los organismos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sea necesario para el cumplimiento de sus fines, incluyendo el acceso a redes y sistemas informáticos, observando de manera estricta el**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	j) Cooperar con organismos públicos, instituciones privadas y organismos internacionales, en materias propias de su competencia, en coordinación con el Ministerio de Relaciones Exteriores, cuando corresponda.	k) 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.	**deber de reserva que esta ley impone, así como los consagrados por la ley N° 19.628.** **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.**
	k) Prestar asesoría técnica a los órganos del Estado e instituciones privadas cuya infraestructura de la información haya sido calificada como crítica, que estén o se hayan visto afectados por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o haya afectado el funcionamiento de su operación, cautelando siempre los deberes de reserva de información que esta ley le impone, así como los consagrados por la ley N° 19.628.	l) 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.	**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.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	l) Colaborar y coordinar con organismos de Inteligencia, para enfrentar amenazas que puedan afectar a la infraestructura crítica de información e implementar acciones preventivas.	m) Coordinar y colaborar interagencialmente con los organismos integrantes del Sistema de Inteligencia del Estado en la identificación de amenazas y la gestión de incidentes o ciberataques que puedan representar un riesgo para la seguridad nacional.	**m) Coordinar y colaborar interagencialmente con los organismos integrantes del Sistema de Inteligencia del Estado en la identificación de amenazas y la gestión de incidentes o ciberataques que puedan representar un riesgo para la seguridad nacional.**
	m) Fiscalizar y sancionar el cumplimiento de esta ley, sus reglamentos y la normativa técnica que se dicte en conformidad con la presente ley, cuando ello no corresponda a un regulador o fiscalizador sectorial, según corresponda.	n) Fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley. La Agencia contará con todas las facultades que fueren necesarias para el cumplimiento de su función fiscalizadora; entre otras, las de realizar inspecciones, auditorías, análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas informáticos, datos, documentos e información para el desempeño de sus funciones de	**n) Fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley.** **La Agencia contará con todas las facultades que fueren necesarias para el cumplimiento de su función fiscalizadora; entre otras, las de realizar inspecciones, auditorías, análisis de seguridad o evaluar un sistema de gestión de seguridad de la información;**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		supervisión, y citar a declarar a los socios, directores, administradores, representantes, empleados y personas que, a cualquier título, presten o hayan prestado servicios para las personas o entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza, respecto de algún hecho cuyo conocimiento estime necesario para el cumplimiento de sus funciones.	**requerir el acceso a sistemas informáticos, datos, documentos e información para el desempeño de sus funciones de supervisión, y citar a declarar a los socios, directores, administradores, representantes, empleados y personas que, a cualquier título, presten o hayan prestado servicios para las personas o entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza, respecto de algún hecho cuyo conocimiento estime necesario para el cumplimiento de sus funciones.**
	n) Informar a la Agencia Nacional de Inteligencia sobre riesgos e incidentes de ciberseguridad.	ñ) Ordenar la realización de procedimientos sancionatorios a las entidades fiscalizadas, procediendo a sancionar las infracciones e incumplimientos en que incurran las instituciones públicas y privadas respecto de las disposiciones de esta ley, reglamentos, obligaciones e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, entre otros, a los representantes legales, administradores, asesores y dependientes de la institución de	**ñ) Ordenar la realización de procedimientos sancionatorios a las entidades fiscalizadas, procediendo a sancionar las infracciones e incumplimientos en que incurran las instituciones públicas y privadas respecto de las disposiciones de esta ley, reglamentos, obligaciones e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		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.	**fundada, podrá citar a declarar, entre otros, a los representantes legales, administradores, asesores y dependientes de la institución de que se trate, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver el procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones por otros medios que aseguren su integridad y fidelidad.**
	o) Conjuntamente con el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten la investigación, innovación y desarrollo de la industria de ciberseguridad local.	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.	**o) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.**
		p) Realizar el seguimiento y evaluación de las medidas, planes y acciones elaborados en el ejercicio de sus funciones.	**p) Realizar el seguimiento y evaluación de las medidas, planes y acciones elaborados en el**
		q) Informar al CSIRT de la Defensa	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Nacional y a los CSIRT Sectoriales los reportes o alarmas de incidentes de ciberseguridad y de vulnerabilidades existentes, conocidas o detectadas en su sector, que considere relevantes, pudiendo sugerir determinados planes de acción. r) Determinar, conforme al informe técnico que el CSIRT Nacional elabore para estos efectos, las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación. s) Certificar el cumplimiento de los estándares de ciberseguridad correspondientes por parte de los organismos de la Administración del Estado. t) Otorgar y revocar las acreditaciones correspondientes a los centros de certificación, en los casos y bajo las condiciones que establezca esta ley y el reglamento respectivo.	**ejercicio de sus funciones.** **q) Informar al CSIRT de la Defensa Nacional y a los CSIRT Sectoriales los reportes o alarmas de incidentes de ciberseguridad y de vulnerabilidades existentes, conocidas o detectadas en su sector, que considere relevantes, pudiendo sugerir determinados planes de acción.** **r) Determinar, conforme al informe técnico que el CSIRT Nacional elabore para estos efectos, las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación.** **s) Certificar el cumplimiento de los estándares de ciberseguridad correspondientes por parte de los organismos de la Administración del Estado.** **t) Otorgar y revocar las acreditaciones correspondientes a los centros de certificación, en los casos y bajo las condiciones que establezca esta ley y el**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		u) Establecer los estándares que deberán cumplir las instituciones que provean bienes o servicios al Estado, y las normas de seguridad para el desarrollo de los sistemas y programas informáticos que sean utilizados por los organismos del Estado. v) Regular, en coordinación con el Servicio Nacional del Consumidor, estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales disponibles a consumidores finales, cubriendo tanto la publicidad del producto como la obligación de incluir etiquetas en estos, pudiendo consistir en fechas de expiración, indicadores de riesgo, u otros indicadores similares. w) Administrar la Red de Conectividad Segura del Estado (RCSE). x) Coordinar anualmente durante el mes de octubre, un ejercicio nacional de comprobación de	**reglamento respectivo.** **u) Establecer los estándares que deberán cumplir las instituciones que provean bienes o servicios al Estado, y las normas de seguridad para el desarrollo de los sistemas y programas informáticos que sean utilizados por los organismos del Estado.** **v) Regular, en coordinación con el Servicio Nacional del Consumidor, estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales disponibles a consumidores finales, cubriendo tanto la publicidad del producto como la obligación de incluir etiquetas en estos, pudiendo consistir en fechas de expiración, indicadores de riesgo, u otros indicadores similares.** **w) Administrar la Red de Conectividad Segura del Estado (RCSE).** **x) Coordinar anualmente durante**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	p) Realizar todas aquellas otras funciones que las leyes le encomienden especialmente.	capacidades de ciberseguridad, en cumplimiento de la ley N° 21.113. y) Realizar todas aquellas otras funciones que las leyes le encomienden especialmente.”. **(Encabezamiento, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).** **(Letra a), unanimidad 8x0. Indicación número 72).** **(Letra b), unanimidad 8x0. Indicación número 73).** **(Letra c), unanimidad 8x0. Indicación número 76).** **(Letra d), unanimidad 8x0. Indicaciones números 78 y 80).** **(Letra e), unanimidad 8x0. Indicación número 81).** **(Letra f), unanimidad 8x0. Indicación número 82).** **(Letra g), unanimidad 8x0. Indicación número 83).**	**el mes de octubre, un ejercicio nacional de comprobación de capacidades de ciberseguridad, en cumplimiento de la ley N° 21.113.** **y) Realizar todas aquellas otras funciones que las leyes le encomienden especialmente.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		(Letra h), unanimidad 8x0. Indicación número 84). **(Letra i), unanimidad 8x0. Indicación número 86).** **(Letra j), unanimidad 8x0. Indicaciones números 87 y 88).** **(Letra k), unanimidad 8x0. Indicación número 89).** **(Letra l), unanimidad 8x0. Indicación número 90).** **(Letra m), unanimidad 8x0. Indicación número 92).** **(Letra n), unanimidad 10x0. Indicaciones números 94 y 94 bis).** **(Letra ñ), unanimidad 7x0, indicación número 95, y 10x0, indicación número 95 bis).** **(Letra o), unanimidad 7x0. Indicación número 97).** **(Letras p), q), r), s), t), u), v) y w),**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		unanimidad 10x0. Indicación número 99). **(Letra x), unanimidad 10x0. Indicaciones número 101 y 101 bis).** **(Letra y), unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	
	Párrafo 2° Dirección, organización y patrimonio Artículo 10. Dirección de la Agencia. La dirección y administración superior de la Agencia estará a cargo de un Director **(_)** Nacional, quien será el jefe superior del Servicio, tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta Dirección Pública establecidas en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.	**ARTÍCULO 10** Incorporar, a continuación de la expresión “un Director” la locución “o Directora”. **(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	Párrafo 2° Dirección, organización y patrimonio Artículo 10. Dirección de la Agencia. La dirección y administración superior de la Agencia estará a cargo de un Director **o Directora** Nacional, quien será el jefe superior del Servicio, tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta Dirección Pública establecidas en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
			públicos que indica.
		ARTÍCULO 11 **Encabezamiento** Sustituirlo por el siguiente: “Artículo 11. Atribuciones del Director o Directora Nacional. Corresponderá especialmente al Director o Directora Nacional:”. **(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	
	Artículo 11. Atribuciones del Director Nacional. Corresponderá especialmente al Director Nacional:		**Artículo 11. Atribuciones del Director o Directora Nacional. Corresponderá especialmente al Director o Directora Nacional:**
	a) Planificar, organizar, dirigir, coordinar y controlar el funcionamiento de la Agencia;		a) Planificar, organizar, dirigir, coordinar y controlar el funcionamiento de la Agencia;
	b) Establecer oficinas regionales cuando el buen funcionamiento del Servicio así lo exija;		b) Establecer oficinas regionales cuando el buen funcionamiento del Servicio así lo exija;
	c) Dictar las resoluciones y demás actos administrativos necesarios para el buen funcionamiento de la Agencia;		c) Dictar las resoluciones y demás actos administrativos necesarios para el buen funcionamiento de la Agencia;
	d) Dictar, mediante resolución, la		d) Dictar, mediante resolución, la normativa que de acuerdo a esta ley

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	normativa que de acuerdo a esta ley corresponda dictar a la Agencia; e) Ejecutar los actos y celebrar los convenios necesarios para el cumplimiento de los fines de la Agencia. En el ejercicio de esta facultad, podrá libremente administrar, adquirir y enajenar bienes de cualquier naturaleza; f) Delegar atribuciones o facultades específicas en funcionarios de las plantas directiva, profesional o técnica de la Agencia, y g) Instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios a cargo, determinar las	**Letra f)** Reemplazarla por la siguiente: "f) Delegar atribuciones o facultades específicas en los funcionarios y funcionarias que indique;". **(Unanimidad 10x0. Indicación número 102, y artículo 121, inciso final, del Reglamento del Senado).** **Letra g)** Sustituirla por la que sigue: "g) Instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios y funcionarias a cargo y determinar las sanciones e	corresponda dictar a la Agencia; e) Ejecutar los actos y celebrar los convenios necesarios para el cumplimiento de los fines de la Agencia. En el ejercicio de esta facultad, podrá libremente administrar, adquirir y enajenar bienes de cualquier naturaleza; **f) Delegar atribuciones o facultades específicas en los funcionarios y funcionarias que indique;** **g) Instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios y funcionarias a cargo y determinar las sanciones**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	sanciones e imponerlas, respecto de los órganos de la Administración del Estado, en los términos señalados en el artículo 32 y respecto de aquellos privados que posean infraestructura de la información calificada como crítica, que no estén sujetos a un regulador o fiscalizador sectorial específico.	imponerlas, y”. **(Unanimidad 10x0. Indicación número 103, y artículo 121, inciso final, del Reglamento del Senado).** **°°°°°** Luego, incorporar la siguiente letra h), nueva: “h) Ejercer la representación judicial y extrajudicial de la Agencia, sin perjuicio de las atribuciones que pudieran corresponder al Consejo de Defensa del Estado.”. **(Unanimidad 9x0. Indicación número 105).** **°°°°°**	**e imponerlas, y** **h) Ejercer la representación judicial y extrajudicial de la Agencia, sin perjuicio de las atribuciones que pudieran corresponder al Consejo de Defensa del Estado.**
	Artículo 12. Del patrimonio de la Agencia. El patrimonio de la Agencia estará constituido por:		Artículo 12. Del patrimonio de la Agencia. El patrimonio de la Agencia estará constituido por:

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	a) Los recursos que anualmente le asigne la Ley de Presupuestos del Sector Público; b) Los recursos otorgados por leyes generales o especiales; c) Los bienes muebles e inmuebles, corporales e incorporales, que se le transfieran o que adquiera a cualquier título; d) Los frutos, rentas e intereses de sus bienes y servicios. e) Las donaciones que se le hagan, así como las herencias o legados que acepte, lo que deberá hacer con beneficio de inventario. Dichas donaciones y asignaciones hereditarias estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten. Las donaciones no requerirán del trámite de insinuación; f) Los aportes de la cooperación internacional que reciba a cualquier título, en coordinación con el Ministerio de Relaciones Exteriores;		a) Los recursos que anualmente le asigne la Ley de Presupuestos del Sector Público; b) Los recursos otorgados por leyes generales o especiales; c) Los bienes muebles e inmuebles, corporales e incorporales, que se le transfieran o que adquiera a cualquier título; d) Los frutos, rentas e intereses de sus bienes y servicios. e) Las donaciones que se le hagan, así como las herencias o legados que acepte, lo que deberá hacer con beneficio de inventario. Dichas donaciones y asignaciones hereditarias estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten. Las donaciones no requerirán del trámite de insinuación; f) Los aportes de la cooperación internacional que reciba a cualquier título, en coordinación con el Ministerio de Relaciones Exteriores;

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	y g) Los demás aportes que perciba en conformidad a la ley.		y g) Los demás aportes que perciba en conformidad a la ley.
	Artículo 13. Nombramiento de autoridades. La Agencia estará afecta al Sistema de Alta Dirección Pública establecido en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.	**ARTÍCULO 13** Considerar como tal el que se transcribe a continuación: “Artículo 13. Nombramiento de autoridades. La Agencia estará afecta al Sistema de Alta Dirección Pública establecido en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica, hasta el segundo nivel jerárquico.”. **(Unanimidad 10x0. Indicación número 106).**	**Artículo 13. Nombramiento de autoridades. La Agencia estará afecta al Sistema de Alta Dirección Pública establecido en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica, hasta el segundo nivel jerárquico.**
		ARTÍCULO 14 Reemplazarlo por el siguiente:	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Artículo 14.- Del personal de la Agencia. El personal de la Agencia se regirá por las normas del Estatuto Administrativo.	"Artículo 14. Del personal de la Agencia. El personal de la Agencia se regirá por las normas del Código del Trabajo. Con todo, serán aplicables a este personal las normas de probidad contenidas en la ley N° 20.880, sobre Probidad en la Función Pública y Prevención de los Conflictos de Intereses, y las disposiciones del Título III de la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley Nº 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, debiendo dejarse constancia en los contratos respectivos de una cláusula que así lo disponga. Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con fuerza	**Artículo 14. Del personal de la Agencia. El personal de la Agencia se regirá por las normas del Código del Trabajo.** **Con todo, serán aplicables a este personal las normas de probidad contenidas en la ley N° 20.880, sobre Probidad en la Función Pública y Prevención de los Conflictos de Intereses, y las disposiciones del Título III de la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley Nº 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, debiendo dejarse constancia en los contratos respectivos de una cláusula que así lo disponga.** **Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo. Asimismo, el personal estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle por los actos realizados en el ejercicio de sus funciones. La responsabilidad disciplinaria del personal de la Agencia por los actos realizados en el ejercicio de sus funciones podrá hacerse efectiva por la autoridad respectiva, de acuerdo al procedimiento establecido en el título V “De la Responsabilidad Administrativa” del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo. En el caso de cese de funciones de	**fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.** **Asimismo, el personal estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle por los actos realizados en el ejercicio de sus funciones. La responsabilidad disciplinaria del personal de la Agencia por los actos realizados en el ejercicio de sus funciones podrá hacerse efectiva por la autoridad respectiva, de acuerdo al procedimiento establecido en el título V “De la Responsabilidad Administrativa” del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.** **En el caso de cese de funciones de los trabajadores que hubieren**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		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, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo. Para estos efectos, los viáticos se pagarán conforme al decreto con fuerza de ley N° 262, de 1977, del Ministerio de Hacienda, y al decreto supremo N° 1, de 1991, del Ministerio de Hacienda, o el texto	**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, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo. Para estos efectos, los viáticos se pagarán conforme al decreto con fuerza de ley N° 262, de 1977, del Ministerio de Hacienda, y al decreto supremo N° 1, de 1991, del Ministerio de Hacienda, o el**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		que lo reemplace. La Agencia no podrá celebrar contratos de trabajo estableciendo el pago de indemnizaciones por causas distintas a las indicadas en los artículos 161, 162 y 163 del Código del Trabajo, y en caso alguno se podrá alterar el monto que entregue la base de cálculo dispuesta en dichas normas. Para el caso de evaluación deficiente de su desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal. Una resolución dictada por el Director o la Directora de la Agencia, visada por la Dirección de Presupuestos, establecerá en forma anual la estructura de la dotación de trabajadores de la Agencia, indicando el número máximo de trabajadores que podrá ocupar según el régimen de remuneraciones. Un reglamento expedido por el	**texto que lo reemplace.** **La Agencia no podrá celebrar contratos de trabajo estableciendo el pago de indemnizaciones por causas distintas a las indicadas en los artículos 161, 162 y 163 del Código del Trabajo, y en caso alguno se podrá alterar el monto que entregue la base de cálculo dispuesta en dichas normas. Para el caso de evaluación deficiente de su desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal.** **Una resolución dictada por el Director o la Directora de la Agencia, visada por la Dirección de Presupuestos, establecerá en forma anual la estructura de la dotación de trabajadores de la Agencia, indicando el número máximo de trabajadores que podrá ocupar según el régimen de remuneraciones.** **Un reglamento expedido por el ministerio encargado de la seguridad pública, determinará la**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ministerio encargado de la seguridad pública, determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal. La Agencia deberá cumplir con las normas establecidas en el decreto ley N° 1.263, de 1975, de administración financiera del Estado.”. **(Unanimidad 9x0, indicación número 107, y 10x0 indicación número 107 bis).**	**estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.** **La Agencia deberá cumplir con las normas establecidas en el decreto ley N° 1.263, de 1975, de administración financiera del Estado.**
		ARTÍCULO 15	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Sustituirlo por el que sigue:	
	Artículo 15.- De la estructura interna de la Agencia. Un reglamento expedido por el Ministerio del Interior y Seguridad Pública, determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, de 2000, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.	"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.	**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 primero a cuarto grado inclusives, o por afinidad de primero y segundo grado.	**El personal de la Agencia no podrá intervenir, en razón de sus funciones, en asuntos en que tenga interés él o ella, su cónyuge, su conveniente civil, sus parientes consanguíneos del primero a cuarto grado inclusives, o por afinidad de primero y segundo grado.** **Asimismo, les está prohibido**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Asimismo, les está prohibido actuar por sí o a través de sociedades de que formen parte, como lobbistas o gestores de intereses de terceras personas ante cualquier institución sometida a la fiscalización de la Agencia. En todo caso, quedarán exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañan personalmente al funcionario o funcionaria, o que se refieran a la administración de su patrimonio. El desempeño de funciones en la Agencia será de dedicación exclusiva y será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley. No obstante, será compatible con cargos docentes en instituciones públicas o privadas reconocidas por el Estado hasta un	**actuar por sí o a través de sociedades de que formen parte, como lobbistas o gestores de intereses de terceras personas ante cualquier institución sometida a la fiscalización de la Agencia.** **En todo caso, quedarán exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañan personalmente al funcionario o funcionaria, o que se refieran a la administración de su patrimonio. El desempeño de funciones en la Agencia será de dedicación exclusiva y será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley. No obstante, será compatible con cargos docentes en instituciones**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		máximo de doce horas semanales, para lo cual deberá prolongar su jornada para compensar las horas durante las cuales no haya podido desempeñar su cargo. Igualmente, quedará exceptuada la atención no remunerada prestada a sociedades de beneficencia, instituciones de carácter benéfico y, en general, a instituciones sin fines de lucro. Con todo, para que operen estas excepciones, será necesario obtener autorización previa y expresa del jefe superior del servicio. Al personal de la Agencia le serán aplicables los literales a), e), f), g), h), i), j), k), l) y m) del artículo 84 del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto	**públicas o privadas reconocidas por el Estado hasta un máximo de doce horas semanales, para lo cual deberá prolongar su jornada para compensar las horas durante las cuales no haya podido desempeñar su cargo.** **Igualmente, quedará exceptuada la atención no remunerada prestada a sociedades de beneficencia, instituciones de carácter benéfico y, en general, a instituciones sin fines de lucro. Con todo, para que operen estas excepciones, será necesario obtener autorización previa y expresa del jefe superior del servicio.** **Al personal de la Agencia le serán aplicables los literales a), e), f), g), h), i), j), k), l) y m) del artículo 84 del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Administrativo.”. **(Unanimidad 9x0, indicación número 109, y 10x0 indicación número 109 bis).**	
	Párrafo 3° Registro Nacional de Incidentes de Ciberseguridad **Artículo 16. Del Registro Nacional de Incidentes de Ciberseguridad. Créase el Registro Nacional de Incidentes de Ciberseguridad, el que será administrado por la Agencia Nacional de**	**Párrafo 3°(del Título III)** Sustituir su denominación por la que se indica a continuación: “Párrafo 3° Consejo Multisectorial sobre Ciberseguridad”. **(Unanimidad 9x0. Indicación número 110).** **<u>ARTÍCULO 16</u>** Eliminarlo. **(Unanimidad 9x0. Indicación número 111).**	**Párrafo 3°** **Consejo Multisectorial sobre Ciberseguridad**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Ciberseguridad y tendrá el carácter de reservado, por exigirlo el debido cumplimiento de las funciones de la Agencia, el debido resguardo de los derechos de las personas y la seguridad de la nación. En este registro se ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. Sobre la base de este registro se podrán realizar las respetivas investigaciones por parte de la Agencia, así como comunicar las alertas a los CSIRT Sectoriales, a los órganos del Estado señalados en el inciso final del artículo 4º y a las instituciones privadas que posean infraestructura de la información calificada como crítica, que corresponda al caso. **Un reglamento expedido por el Ministerio del Interior y Seguridad Pública contendrá las disposiciones necesarias para regular la forma en que se confeccionará el referido registro, la operación del mismo y toda**		

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	otra norma necesaria para su adecuado funcionamiento.		
	Párrafo 4° Consejo Técnico de la Agencia Nacional de Ciberseguridad	**Párrafo 4°(del Título III)** Suprimirlo en esta parte, para ubicarlo más adelante, antes del artículo 21 que pasa a ser 19, con la denominación que se señalará en su oportunidad. **(Unanimidad 9x0. Indicación número 115).**	
	Artículo 17. Consejo Técnico de la Agencia Nacional de Ciberseguridad. Créase el Consejo Técnico de la Agencia Nacional de Ciberseguridad, en adelante el "Consejo", que tendrá como objeto asesorar y apoyar técnicamente a la Agencia en el	**<u>ARTÍCULO 17</u>** Pasa a ser artículo 16, reemplazado por el que sigue: "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	**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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	análisis y revisión periódica de las políticas públicas propias de su ámbito de competencia, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad y, proponer posibles medidas para abordarlas.	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.	**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 cuatro consejeros designados por el Presidente de la República, mediante decreto supremo expedido a través del Ministerio del Interior y Seguridad Pública, entre personas de destacada labor en el ámbito de la ciberseguridad y/o de políticas públicas vinculadas a la materia, quienes permanecerán en su cargo durante seis años, renovándose en pares cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.	El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, quienes permanecerán en su cargo durante seis años, renovándose en tríos cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.	**El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, quienes permanecerán en su cargo durante seis años, renovándose en tríos cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.**
	Los integrantes del Consejo estarán obligados a presentar una	Los integrantes del Consejo estarán obligados a presentar una	**Los integrantes del Consejo estarán obligados a presentar una**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	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 Nº19.880.	declaración de intereses y patrimonio, en conformidad a lo dispuesto por la ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses, y estarán afectos al principio de abstención contenido en el artículo 12 de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.”. **(Unanimidad 10x0, todo el artículo, salvo la oración final del inciso segundo que fue eliminada por 7 votos en contra y 3 a favor, en segunda votación, de conformidad al artículo 178 del Reglamento del Senado. Indicación número 116, y artículo 121, inciso final, del Reglamento del Senado).**	**declaración de intereses y patrimonio, en conformidad a lo dispuesto por la ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses, y estarán afectos al principio de abstención contenido en el artículo 12 de la ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.**
		ARTÍCULO 18	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Artículo 18. Funciones del Consejo. Corresponderá al Consejo: **a) Asesorar a la Agencia en materias relacionadas con la ciberseguridad y la protección y aseguramiento de la Infraestructura Crítica de la Información;** **b) Elaborar el informe que señala el artículo 4º de esta ley, relativo a la determinación de los sectores o instituciones que posean infraestructura de la información que deba ser calificada como crítica;** **c) Asesorar en la redacción de propuestas de normas técnicas que la Agencia genere, y;** **d) Asesorar a la Agencia en todas aquellas materias que ésta solicite.**	Suprimirlo. **(Unanimidad 10x0. Indicación número 117).**	
		ARTÍCULO 19	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Pasa a ser artículo 17, sustituido por el que sigue:	
	Artículo 19. Funcionamiento del Consejo. El Consejo sólo podrá sesionar con la asistencia de, al menos, tres de sus miembros, previa convocatoria del Director de la Agencia. Sin perjuicio de lo anterior, el Presidente del Consejo estará obligado a convocar a una sesión extraordinaria cuando así lo requieran, por escrito, a lo menos tres de sus miembros. En todo caso, el Consejo podrá autoconvocarse en situaciones urgentes o necesarias conforme a la decisión de la mayoría de sus integrantes. **El Consejo sesionará todas las veces que sea necesario para el cumplimiento oportuno y eficiente de sus funciones, debiendo celebrar sesiones ordinarias a lo menos una vez cada dos meses, con un máximo de doce sesiones pagadas por cada año calendario, y sesiones extraordinarias**	"Artículo 17. Funcionamiento del Consejo. El Consejo sesionará a lo menos cuatro veces al año; sus recomendaciones serán de carácter público, y deberán recoger la diversidad de opiniones existentes en él cuando no haya unanimidad respecto de las mismas. Excepcionalmente y mediante decisión fundada, el Director o Directora podrá decretar secreta o reservada una parte o toda una sesión del Consejo, de lo cual se deberá dejar constancia en el acta respectiva. En este caso, se aplicará lo dispuesto en el artículo 42. El Consejo sesionará todas las veces que sea necesario para el cumplimiento de sus funciones. La Agencia prestará el apoyo técnico y administrativo indispensable para el adecuado funcionamiento del Consejo.	**Artículo 17. Funcionamiento del Consejo. El Consejo sesionará a lo menos cuatro veces al año; sus recomendaciones serán de carácter público, y deberán recoger la diversidad de opiniones existentes en él cuando no haya unanimidad respecto de las mismas. Excepcionalmente y mediante decisión fundada, el Director o Directora podrá decretar secreta o reservada una parte o toda una sesión del Consejo, de lo cual se deberá dejar constancia en el acta respectiva. En este caso, se aplicará lo dispuesto en el artículo 42.** **El Consejo sesionará todas las veces que sea necesario para el cumplimiento de sus funciones. La Agencia prestará el apoyo técnico y administrativo indispensable para el adecuado funcionamiento del Consejo.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	cuando las cite especialmente el Presidente del Consejo, o cuando aquéllas se citen por medio de una autoconvocatoria del Consejo. Podrán celebrarse un máximo de cuatro sesiones extraordinarias pagadas por cada año calendario. **Los acuerdos del Consejo se adoptarán por la mayoría absoluta de los consejeros presentes. El Presidente del Consejo tendrá voto dirimente en caso de empate. De los acuerdos que adopte el Consejo deberá dejarse constancia en el acta de la sesión respectiva. Podrán declararse secretas las actas en que, de conformidad a la ley, se traten materias que afectaren el debido cumplimiento de las funciones de la Agencia, la seguridad de la Nación o el interés nacional.** **Cada uno de los integrantes del Consejo, con excepción de su Presidente, percibirá una dieta de quince unidades de fomento por cada sesión a la que asista, con un tope máximo de doce sesiones**		

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	por año calendario. Esta dieta será compatible con otros ingresos que perciba el consejero. **Un reglamento expedido por el Ministerio del Interior y Seguridad Pública determinará las demás normas necesarias para el correcto funcionamiento del Consejo.**	Un reglamento expedido por el Ministerio encargado de la seguridad pública determinará las demás normas necesarias para el correcto funcionamiento del Consejo.". **(Unanimidad 7x0. Indicación número 118, y artículo 121, inciso final, del Reglamento del Senado).**	**Un reglamento expedido por el Ministerio encargado de la seguridad pública determinará las demás normas necesarias para el correcto funcionamiento del Consejo.**
		ARTÍCULO 20 Pasa a ser artículo 18, reemplazado por el que se transcribe a continuación:	
	Artículo 20. Incompatibilidades de los miembros del Consejo. No podrán ser designados consejeros las personas que desempeñen empleos o comisiones retribuidos con fondos del Fisco, de las	"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.	**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.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	municipalidades, de las entidades fiscales autónomas, semifiscales, de las empresas del Estado o en las que el Fisco tenga aportes de capital, y con toda otra función o comisión de la misma naturaleza. Exceptúese a los empleos docentes y las funciones o comisiones de igual carácter de la enseñanza superior, media o especial.	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	**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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		deberá comunicar de inmediato dicha circunstancia al Consejo, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción. Tan pronto como el Consejo tome conocimiento de que una causal de cesación afecta a un consejero, el referido consejero cesará automáticamente en su cargo. Si quedare vacante el cargo de consejero deberá procederse al nombramiento de uno nuevo de conformidad con el procedimiento establecido en esta ley. El consejero nombrado en reemplazo durará en el cargo solo por el tiempo que falte para completar el período del consejero reemplazado.”. **(Unanimidad 10x0. Indicación número 119).**	**anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.** **Tan pronto como el Consejo tome conocimiento de que una causal de cesación afecta a un consejero, el referido consejero cesará automáticamente en su cargo.** **Si quedare vacante el cargo de consejero deberá procederse al nombramiento de uno nuevo de conformidad con el procedimiento establecido en esta ley. El consejero nombrado en reemplazo durará en el cargo solo por el tiempo que falte para completar el período del consejero reemplazado.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		°°°°° Como se dijo, incorporar luego un párrafo 4°, nuevo, del siguiente tenor: "Párrafo 4° Red de Conectividad Segura del Estado". **(Unanimidad.10x0. Indicación número 119 bis).** °°°°°	**Párrafo 4°** **Red de Conectividad Segura del Estado**
	Artículo 21. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:	**<u>ARTÍCULO 21</u>** Pasa a ser artículo 19, sustituido por el que sigue: "Artículo 19. Red de Conectividad Segura del Estado. Créase la Red de Conectividad Segura del Estado, en adelante RCSE, que proveerá servicios de interconexión y conectividad a Internet a los	**Artículo 19. Red de Conectividad Segura del Estado. Créase la Red de Conectividad Segura del Estado, en adelante RCSE, que proveerá servicios de interconexión y conectividad a**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		organismos de la Administración del Estado señalados en el artículo 1 de la presente ley.	**Internet a los organismos de la Administración del Estado señalados en el artículo 1 de la presente ley.**
	a) Expiración del plazo por el que fue designado. **b) Renuncia voluntaria aceptada por la autoridad que realizó la designación.** **c) Incapacidad física o síquica para el desempeño del cargo.** **d) Fallecimiento.** **e) Sobreviniencia de alguna causal de incompatibilidad de las contempladas en el artículo 19.** **f) Haber sido condenado por delitos que merezcan pena aflictiva por sentencia firme o ejecutoriada.** **g) Falta grave al cumplimiento de**	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 organismos de la Administración del Estado.”. **(Unanimidad 10x0. Indicación número 120).**	**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 organismos de la Administración del Estado.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	las obligaciones como consejero. Para estos efectos, se considerará falta grave: **i. Inasistencia injustificada a dos sesiones consecutivas.** **ii. No guardar la debida reserva respecto de la información recibida en el ejercicio de su cargo que no haya sido divulgada oficialmente.** **El consejero respecto del cual se verificare alguna de las causales de cesación referidas anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción. Con todo, tratándose del ordinal ii) de dicho literal, será necesario, para cursar la remoción, la presentación de la respectiva querella por el delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.**		

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Tan pronto como el Consejo tome conocimiento de que una causal de cesación afecta a un consejero, el referido consejero cesará automáticamente en su cargo. **Si quedare vacante el cargo de consejero deberá procederse al nombramiento de uno nuevo de conformidad con el procedimiento establecido en esta ley. El consejero nombrado en reemplazo durará en el cargo sólo por el tiempo que falte para completar el período del consejero reemplazado.**		
	Párrafo 5° Equipo Nacional de Respuesta a Incidentes de Seguridad Informática Artículo 22. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. Créase dentro de la Agencia Nacional de	**ARTÍCULO 22** Pasa a ser artículo 20, con las siguientes enmiendas: En su encabezamiento, sustituir	Párrafo 5° Equipo Nacional de Respuesta a Incidentes de Seguridad Informática **Artículo 20.** Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. Créase dentro de la Agencia Nacional de

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Ciberseguridad el Equipo Nacional de Respuesta **ante Incidentes** de Seguridad Informática, en adelante "CSIRT Nacional", el que tendrá las siguientes funciones: a) Responder ante incidentes de ciberseguridad o ciberataque que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información relativos a instituciones privadas no sometidas a la supervigilancia de un regulador o fiscalizador sectorial y que posean infraestructura de la información calificada como crítica, de conformidad a lo prescrito en esta ley. b) Coordinar a los CSIRT Sectoriales frente a ataques,	"ante Incidentes" por "a Incidentes". **(Adecuación formal).** **Letra a)** Reemplazarla por la siguiente: "a) Responder ante ciberataques o incidentes de ciberseguridad, cuando estos sean de efecto significativo.". **(Unanimidad 10x0. Indicación número 121).** **Letra b)** Sustituirla por la que sigue: "b) Coordinar a los CSIRT	Ciberseguridad el Equipo Nacional de Respuesta **a Incidentes** de Seguridad Informática, en adelante "CSIRT Nacional", el que tendrá las siguientes funciones: **a) Responder ante ciberataques o incidentes de ciberseguridad, cuando estos sean de efecto significativo.** **b) Coordinar a los CSIRT Sectoriales frente a ciberataques**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	vulnerabilidades, incidentes y brechas de ciberseguridad.	Sectoriales frente a ciberataques o incidentes de ciberseguridad de efecto significativo. La misma coordinación deberá establecer con el CSIRT de la Defensa Nacional. En el ejercicio de esta función, el CSIRT Nacional podrá realizar todas las acciones necesarias para asegurar una respuesta rápida por parte de los CSIRT Sectoriales, incluida la supervisión de las medidas adoptadas por estos.”. **(Unanimidad 10x0. Indicación número 123).**	**o incidentes de ciberseguridad de efecto significativo. La misma coordinación deberá establecer con el CSIRT de la Defensa Nacional. En el ejercicio de esta función, el CSIRT Nacional podrá realizar todas las acciones necesarias para asegurar una respuesta rápida por parte de los CSIRT Sectoriales, incluida la supervisión de las medidas adoptadas por estos.**
	c) Servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes, para el intercambio de información de ciberseguridad, siempre dentro del marco de sus competencias. d) Prestar colaboración o asesoría técnica a los CSIRT Sectoriales en la implementación de políticas y acciones relativas a ciberseguridad.	**Letra e)**	c) Servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes, para el intercambio de información de ciberseguridad, siempre dentro del marco de sus competencias. d) Prestar colaboración o asesoría técnica a los CSIRT Sectoriales en la implementación de políticas y acciones relativas a ciberseguridad.

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	e) Ofrecer soporte a los CSIRT Sectoriales para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.	Considerar como tal la que se señala continuación: “e) Supervisar incidentes a escala nacional.”. **(Unanimidad 10x0. Indicación número 126).**	**e) Supervisar incidentes a escala nacional.**
		Letra f)	
	f) Consolidar y tratar los datos técnicos y antecedentes que describen la ocurrencia de incidentes de ciberseguridad, ciberataques, vulnerabilidades y demás información para efectos de la alimentación del registro previsto en los términos del artículo 16.	Reemplazarla por la que sigue: “f) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.”. **(Unanimidad 10x0. Indicación número 127).**	**f) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.**
		Letra g)	
	g) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos del Estado e instituciones privadas que posean infraestructura de la	Sustituirla por la siguiente: “g) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad.”.	**g) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	información calificada como crítica cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.	**(Mayoría 9x1. Indicación número 128).**	
		Letra h)	
	h) Requerir a los CSIRT Sectoriales, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.	Contemplar en su lugar la que sigue: “h) Requerir a las instituciones afectadas o a los CSIRT correspondientes, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.”. **(Unanimidad 10x0. Indicación número 131).**	**h) Requerir a las instituciones afectadas o a los CSIRT correspondientes, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.**
		Letra i)	
	i) Responder, conjuntamente con uno o más CSIRT Sectoriales, en la gestión de un incidente de ciberseguridad o de un ciberataque, dependiendo de las capacidades y competencias de los órganos del	Reemplazarla por la que se transcribe: “i) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.”.	**i) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Estado que concurren a su gestión, cuando estos puedan ocasionar un impacto significativo en el sector, institución u órgano del Estado, según corresponda. En estos casos, el CSIRT Nacional podrá recomendar, colaborar, compartir información, coordinar y realizar todas las acciones conjuntas necesarias para asegurar una respuesta rápida frente al incidente. Además, podrá supervisar la implementación de medidas de mitigación de corto plazo, e informarse de las medidas de largo plazo adoptadas.	**(Unanimidad 10x0. Indicación número 132).**	
		Letra j)	
	j) Generar y difundir información mediante campañas públicas y prestar asesoría técnica general a personas naturales o jurídicas, que no se encuentran reguladas por esta ley, que estén o se hayan visto afectadas por un incidente de	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	**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.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	ciberseguridad que haya comprometido sus activos informáticos críticos o hayan afectado el funcionamiento de su operación. k) Crear y administrar para el cumplimiento de sus funciones una red electrónica de comunicaciones segura destinada a comunicar y compartir información con los otros CSIRT Sectoriales, de Gobierno y Defensa. El funcionamiento de la red de comunicaciones se establecerá en el reglamento de la presente ley.	de notificación.”. **(Unanimidad 10x0. Indicación número 135).** **Letra k)** Eliminarla. **(Unanimidad 10x0. Indicación número 136).**	
	TÍTULO IV **De los equipos de respuesta a incidentes de seguridad informática sectoriales**	**<u>TÍTULO IV</u>** Reemplazar su denominación, para que quede del siguiente modo: “TÍTULO IV Otras instituciones intervinientes”. **(Unanimidad 10x0. Indicación número 139).**	**TÍTULO IV** **Otras instituciones intervinientes**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ARTÍCULO 23 Pasa a ser artículo 21, sustituido por el siguiente:	
	Artículo 23. CSIRT Sectoriales. Los reguladores o fiscalizadores sectoriales podrán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad dar respuesta a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de sus respectivos sectores regulados.	"Artículo 21. CSIRT Sectoriales. Las autoridades sectoriales deberán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad contribuir al desarrollo de capacidades, confianza y seguridad de las redes y sistemas informáticos y proporcionar asistencia para la gestión de incidentes de ciberseguridad en sus respectivos sectores. Los CSIRT Sectoriales tendrán las siguientes funciones: a) Responder ante ciberataques o incidentes de ciberseguridad, dando prioridad a aquellos que puedan tener efecto significativo.	**Artículo 21. CSIRT Sectoriales. Las autoridades sectoriales deberán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad contribuir al desarrollo de capacidades, confianza y seguridad de las redes y sistemas informáticos y proporcionar asistencia para la gestión de incidentes de ciberseguridad en sus respectivos sectores.** **Los CSIRT Sectoriales tendrán las siguientes funciones:** **a) Responder ante ciberataques o incidentes de ciberseguridad, dando prioridad a aquellos que puedan tener efecto significativo.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		b) Colaborar e interoperar con los otros CSIRT Sectoriales, frente a ciberataques o incidentes de ciberseguridad de efecto significativo, bajo la coordinación y supervisión de la Agencia. c) Establecer relaciones de cooperación e interoperabilidad con los otros CSIRT Sectoriales. d) Supervisar la gestión de incidentes de ciberseguridad que afecten a su sector. e) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación que afecten a su sector. f) Realizar capacitación en materia de ciberseguridad, debiendo para ello seguir las instrucciones que al efecto pudiera dictar la Agencia. g) Requerir a las instituciones de su sector información sobre los incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para	**b) Colaborar e interoperar con los otros CSIRT Sectoriales, frente a ciberataques o incidentes de ciberseguridad de efecto significativo, bajo la coordinación y supervisión de la Agencia.** **c) Establecer relaciones de cooperación e interoperabilidad con los otros CSIRT Sectoriales.** **d) Supervisar la gestión de incidentes de ciberseguridad que afecten a su sector.** **e) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación que afecten a su sector.** **f) Realizar capacitación en materia de ciberseguridad, debiendo para ello seguir las instrucciones que al efecto pudiera dictar la Agencia.** **g) Requerir a las instituciones de su sector información sobre los incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		mitigarlos, la que deberá ser remitida al CSIRT Nacional. La información que se remita deberá excluir datos personales. h) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad, conforme las instrucciones que dicte al efecto la Agencia. i) Poner en conocimiento de la Agencia toda información relevante, en especial aquella referida a incidentes de ciberseguridad de efecto significativo. j) Colaborar con la Agencia en los casos y en la forma que esta lo solicite. En el ejercicio de sus funciones, los CSIRT Sectoriales deberán dar cumplimientos a todas aquellos protocolos y estándares técnicos, instrucciones generales y particulares, que la Agencia pudiera dictar con el objeto de lograr un nivel común de ciberseguridad y	**para mitigarlos, la que deberá ser remitida al CSIRT Nacional. La información que se remita deberá excluir datos personales.** **h) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad, conforme las instrucciones que dicte al efecto la Agencia.** **i) Poner en conocimiento de la Agencia toda información relevante, en especial aquella referida a incidentes de ciberseguridad de efecto significativo.** **j) Colaborar con la Agencia en los casos y en la forma que esta lo solicite.** **En el ejercicio de sus funciones, los CSIRT Sectoriales deberán dar cumplimientos a todas aquellos protocolos y estándares técnicos, instrucciones generales y particulares, que la Agencia pudiera dictar con el objeto de lograr un nivel común de**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		respuestas coordinadas ante la ocurrencia de incidentes de ciberseguridad. En el caso del CSIRT del sector financiero sujeto a la fiscalización de la Comisión para el Mercado Financiero, bastará con dar cumplimiento a los protocolos y estándares técnicos que la Agencia comunique ante la ocurrencia de incidentes de ciberseguridad, salvo en los casos de incidentes que pudieran tener un efecto sistémico en las redes y sistemas informáticos del país. El incumplimiento de las instrucciones que imparta la Agencia para la respuesta coordinada de incidentes acarreará responsabilidad funcionaria de la autoridad o jefatura del CSIRT respectivo, la que podrá ser sancionada conforme lo dispuesto en los artículos 33 y 34.	**ciberseguridad y respuestas coordinadas ante la ocurrencia de incidentes de ciberseguridad. En el caso del CSIRT del sector financiero sujeto a la fiscalización de la Comisión para el Mercado Financiero, bastará con dar cumplimiento a los protocolos y estándares técnicos que la Agencia comunique ante la ocurrencia de incidentes de ciberseguridad, salvo en los casos de incidentes que pudieran tener un efecto sistémico en las redes y sistemas informáticos del país.** **El incumplimiento de las instrucciones que imparta la Agencia para la respuesta coordinada de incidentes acarreará responsabilidad funcionaria de la autoridad o jefatura del CSIRT respectivo, la que podrá ser sancionada conforme lo dispuesto en los artículos 33 y 34.**
	Un reglamento expedido por el Ministerio del Interior y Seguridad Pública establecerá las instancias	Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las instancias de coordinación entre la Agencia y las	**Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	de coordinación entre la Agencia Nacional de Ciberseguridad, los reguladores y fiscalizadores sectoriales, así como de sus respectivos CSIRT, dentro del marco que fija esta ley.	autoridades sectoriales y sus respectivos CSIRT.”. **(Unanimidad 8x0, indicación número 140, y 10x0, indicación número 140 bis).**	**instancias de coordinación entre la Agencia y las autoridades sectoriales y sus respectivos CSIRT.**
	Artículo 24. Funciones de los CSIRT Sectoriales. Corresponderá a los CSIRT Sectoriales:	**<u>ARTÍCULO 24</u>** Pasa a ser artículo 22, consultado con el siguiente texto: “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	**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,**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		regulación respectiva, las que deberán ser sometidas a aprobación previa de la Agencia, quien deberá pronunciarse en el plazo de treinta días hábiles.	**de conformidad con la regulación respectiva, las que deberán ser sometidas a aprobación previa de la Agencia, quien deberá pronunciarse en el plazo de treinta días hábiles.**
	a) Responder ante incidentes de ciberseguridad que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información que afecten a los órganos de la Administración de Estado y de las instituciones privadas de su sector.	Asimismo, las autoridades sectoriales deberán dictar las instrucciones, circulares y órdenes necesarias para la implementación de los protocolos y estándares técnicos establecidos por la Agencia.	**Asimismo, las autoridades sectoriales deberán dictar las instrucciones, circulares y órdenes necesarias para la implementación de los protocolos y estándares técnicos establecidos por la Agencia.**
	b) Coordinar a los equipos CSIRT, o sus equivalentes, de los órganos del Estado y de las instituciones privadas de su sector frente a ataques, vulnerabilidades, incidentes y brechas de ciberseguridad.	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 serán obligatorios para todos los regulados	**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 serán obligatorios para todos los regulados aun cuando la**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	c) Prestar colaboración o asesoría técnica en la implementación de políticas y acciones relativas a ciberseguridad a los CSIRT de las instituciones reguladas. **d) Ofrecer soporte a los CSIRT de las instituciones reguladas para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.** **e) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos de la Administración de Estado de su sector y de las instituciones reguladas cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.** **f) Requerir a los CSIRT de sus instituciones reguladas, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y**	aun cuando la autoridad sectorial omita referirse a ellos. Tratándose de sus instituciones fiscalizadas, la Comisión para el Mercado Financiero podrá establecer las normas de carácter general y técnicas sobre ciberseguridad sin necesidad de solicitar la aprobación de la Agencia, siempre y cuando tengan un alcance distinto a las normas dictadas por ella. En caso de que la Comisión para el Mercado Financiero emita normativa que regule elementos contenidos en normas, protocolos o instrucciones generales dictados por la Agencia, deberá informarle previamente, remitiendo la norma, protocolo o instrucción, con una anticipación de, al menos, treinta días hábiles a su emisión por parte de la Comisión para el Mercado Financiero.”. **(Unanimidad 8x0, indicación número 141, y 10x0, indicación**	**autoridad sectorial omita referirse a ellos.** **Tratándose de sus instituciones fiscalizadas, la Comisión para el Mercado Financiero podrá establecer las normas de carácter general y técnicas sobre ciberseguridad sin necesidad de solicitar la aprobación de la Agencia, siempre y cuando tengan un alcance distinto a las normas dictadas por ella. En caso de que la Comisión para el Mercado Financiero emita normativa que regule elementos contenidos en normas, protocolos o instrucciones generales dictados por la Agencia, deberá informarle previamente, remitiendo la norma, protocolo o instrucción, con una anticipación de, al menos, treinta días hábiles a su emisión por parte de la Comisión para el Mercado Financiero.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	vulnerabilidades encontradas. **g) Generar y difundir información mediante campañas públicas dentro de su sector.** **h) Trabajar conjuntamente con el CSIRT Nacional y con otros sectoriales, cuando corresponda, en la gestión de un incidente de ciberseguridad en los casos y forma previstas en el literal i) del artículo 20 de esta ley.** **i) Informar al CSIRT Nacional, de vulnerabilidades, incidentes de ciberseguridad y ciberataques detectados o reportados en su sector, junto a sus respectivos cursos o planes de acción para subsanarlos.** **j) Prestar asesoría técnica a los órganos de la Administración de Estado de su sector y a sus instituciones reguladas, que estén o se hayan visto afectadas por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o hayan afectado el funcionamiento de su**	**número 141 bis).**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	operación. **k) Difundir las alertas preventivas e informaciones de ciberseguridad emanadas por el CSIRT Nacional a los órganos de la Administración de Estado de su sector y a sus instituciones reguladas.**		
	Artículo 25. Deber general de informar. La Agencia informará a cada CSIRT Sectorial los reportes o alarmas de incidentes de ciberseguridad, vulnerabilidades existentes, conocidas o detectadas, y los planes de acciones sugeridos para subsanar dichas brechas de ciberseguridad.	**ARTÍCULO 25** Pasa a ser artículo 23, reemplazado por el que se transcribe a continuación: "Artículo 23. Incidentes de efecto significativo. Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales. Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:	**Artículo 23. Incidentes de efecto significativo. Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales. Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Cada CSIRT Sectorial informará a los órganos de la Administración de Estado y a las instituciones privadas de su sector que posean infraestructura de la información calificada como crítica sobre vulnerabilidades existentes o detectadas en ella, y elaborará recomendaciones para subsanar dichas brechas de ciberseguridad. **Cada CSIRT Sectorial deberá informar a su sector regulado de manera anonimizada de los reportes de incidentes de ciberseguridad, vulnerabilidades existentes, conocidas o detectadas y de los cursos de acción tomada en cada caso.** **Toda institución que posea infraestructura de la información calificada como crítica tiene la obligación de informar a su respectivo CSIRT los reportes de incidentes de ciberseguridad e informar respecto del plan de acción que adoptó frente a esta**	a) El número de personas afectadas. b) La duración del incidente. c) La extensión geográfica con respecto a la zona afectada por el incidente. Los CSIRT Sectoriales tendrán la obligación de tomar las providencias necesarias para apoyar en el restablecimiento del servicio afectado, bajo la coordinación del CSIRT Nacional. Deberá omitirse en los reportes de incidentes de ciberseguridad todo dato o información personal, conforme a lo dispuesto en el artículo 2°, letra f), de la ley N° 19.628, sobre protección de la vida privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información personal.	**a) El número de personas afectadas.** **b) La duración del incidente.** **c) La extensión geográfica con respecto a la zona afectada por el incidente.** **Los CSIRT Sectoriales tendrán la obligación de tomar las providencias necesarias para apoyar en el restablecimiento del servicio afectado, bajo la coordinación del CSIRT Nacional.** **Deberá omitirse en los reportes de incidentes de ciberseguridad todo dato o información personal, conforme a lo dispuesto en el artículo 2°, letra f), de la ley N° 19.628, sobre protección de la vida privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	en un plazo no superior a 24 horas, prorrogable, por una sola vez por el mismo plazo, contado desde que se tuvo conocimiento de su ocurrencia. Lo anterior se entiende sin perjuicio de la facultad del regulador de solicitar el cumplimento de esta obligación en un plazo menor si lo considera necesario.	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.”. **(Unanimidad 8x0. Indicación número 143).**	**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. Deber especial de información a la Agencia. Los	**<u>ARTÍCULO 26</u>** Pasa a ser artículo 24, sustituido por el siguiente: “Artículo 24. Centros de Certificación Acreditados. Sin perjuicio de las	**Artículo 24. Centros de Certificación Acreditados. Sin**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	CSIRT Sectoriales deberán informar a la Agencia, a más tardar una hora después de haber verificado la existencia de un incidente de ciberseguridad, cuando éste ha tenido un impacto significativo en la seguridad del sistema informático de una institución que posee infraestructura de la información calificada como crítica o en la continuidad de un servicio esencial.	funciones y atribuciones de la Agencia, los únicos organismos autorizados para certificar el cumplimiento de los estándares de ciberseguridad exigidos por la autoridad competente serán aquellos que cuenten con una acreditación vigente otorgada por la Agencia Nacional de Ciberseguridad, de conformidad con lo dispuesto en esta ley y en su reglamento. En el caso de los organismos de la Administración del Estado que estén sujetos a las obligaciones del artículo 6, será la Agencia la encargada de certificar el cumplimiento de dichos estándares.	**perjuicio de las funciones y atribuciones de la Agencia, los únicos organismos autorizados para certificar el cumplimiento de los estándares de ciberseguridad exigidos por la autoridad competente serán aquellos que cuenten con una acreditación vigente otorgada por la Agencia Nacional de Ciberseguridad, de conformidad con lo dispuesto en esta ley y en su reglamento. En el caso de los organismos de la Administración del Estado que estén sujetos a las obligaciones del artículo 6, será la Agencia la encargada de certificar el cumplimiento de dichos estándares.**
	Se considera que un incidente de ciberseguridad tiene impacto significativo si cumple al menos una de las siguientes condiciones:	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.	**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.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	a) Afecta a una gran cantidad de usuarios. **b) La interrupción o mal funcionamiento es de larga duración.** **c) Afecta a una extensión geográfica considerable.** **d) Afecta sistemas de información que contengan datos personales.** **e) Afecta la integridad física, la salud, o la vida cotidiana de las personas, de manera significativa.** **Corresponderá calificar el impacto significativo a los reguladores o fiscalizadores sectoriales o a la Agencia, según corresponda.**	Una vez contratados o comprados los servicios o programas informáticos, será responsabilidad de los jefes de servicio velar por el cumplimiento de dichos estándares y normas. Los organismos públicos en la celebración de sus contratos deberán evaluar de mejor manera y dar preferencia a los productos y servicios calificados con un nivel adecuado de seguridad por un centro certificador. Lo establecido en este artículo no será aplicable a la defensa nacional, sector que no requerirá de la acreditación de la Agencia ni de certificación para prestar servicios a otros organismos del Estado. Asimismo, el responsable por el cumplimiento de los estándares y normas de seguridad del sector defensa será el Estado Mayor Conjunto, del Ministerio de Defensa Nacional.”. **(Unanimidad 7x0. Indicación**	**Una vez contratados o comprados los servicios o programas informáticos, será responsabilidad de los jefes de servicio velar por el cumplimiento de dichos estándares y normas.** **Los organismos públicos en la celebración de sus contratos deberán evaluar de mejor manera y dar preferencia a los productos y servicios calificados con un nivel adecuado de seguridad por un centro certificador.** **Lo establecido en este artículo no será aplicable a la defensa nacional, sector que no requerirá de la acreditación de la Agencia ni de certificación para prestar servicios a otros organismos del Estado. Asimismo, el responsable por el cumplimiento de los estándares y normas de seguridad del sector defensa será el Estado Mayor Conjunto, del Ministerio de Defensa Nacional.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	La obligación de tomar las providencias necesarias para apoyar en el restablecimiento del servicio afectado no deja sin efectos el deber de los CSIRT Sectoriales de notificar a la Agencia de la ocurrencia de un incidente de ciberseguridad en el plazo indicado en el inciso primero. **Deberán omitirse en los reportes de incidentes de ciberseguridad todo dato o información personal, conforme a lo dispuesto en el artículo 2 letra f) de la ley N°19.628 sobre Protección de la Vida Privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información personal.** **El procedimiento específico para notificar un incidente de ciberseguridad, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad serán establecidos en el reglamento de la presente ley.**	**número 144).**	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	TÍTULO V **De los CSIRT del sector público**	**TÍTULO V** Reemplazar su denominación, para que quede del siguiente modo: "TÍTULO V Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional". **(Unanimidad 8x0. Indicación número 147).**	**T** **TÍTULO V** **Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional**
	Artículo 27. Equipo de Respuesta ante Incidentes de Seguridad Informática del Sector Gobierno.	**ARTÍCULO 27** Pasa a ser artículo 25, reemplazado por el que sigue: "Artículo 25. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. Créase el	**Artículo 25. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Créase en la Agencia el Equipo de Respuesta a Incidentes de Seguridad Informática de Gobierno, en adelante CSIRT de Gobierno. El CSIRT de Gobierno para todos los efectos, se clasificará como un CSIRT sectorial, responsable de la prevención, contención, protección, detección, recuperación de los sistemas y respuesta, asociados a instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información del Estado. Tendrá las siguientes funciones principales: **a) Responder ante incidentes de ciberseguridad que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información que afecten a los órganos de la Administración del Estado.**	Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional, en adelante CSIRT de la Defensa Nacional, dependiente del Ministerio de Defensa Nacional, como el organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del mencionado Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional. El CSIRT de la Defensa Nacional dependerá del Estado Mayor Conjunto, del Ministerio de Defensa Nacional.	**Nacional. Créase el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional, en adelante CSIRT de la Defensa Nacional, dependiente del Ministerio de Defensa Nacional, como el organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del mencionado Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional.** **El CSIRT de la Defensa Nacional dependerá del Estado Mayor Conjunto, del Ministerio de Defensa Nacional.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	b) Asegurar la implementación de los protocolos y estándares mínimos de ciberseguridad establecidos por la Agencia, en los órganos de la Administración de Estado. **c) Gestionar los ciberataques, incidentes, y vulnerabilidades detectadas, informando estas situaciones al CSIRT Nacional de acuerdo a las normas que se establezcan para tal efecto.** **d) Difundir las alertas preventivas e informaciones de ciberseguridad emanadas por el CSIRT Nacional a los órganos de la Administración de Estado.**	Para los efectos presupuestarios, el CSIRT a que se refiere este artículo dependerá del Ministerio de Defensa Nacional; se regirá por el reglamento que este Ministerio dicte al efecto y, en lo que le sea aplicable, por la presente ley.". **(Unanimidad 8x0. Indicación número 148).**	**Para los efectos presupuestarios, el CSIRT a que se refiere este artículo dependerá del Ministerio de Defensa Nacional; se regirá por el reglamento que este Ministerio dicte al efecto y, en lo que le sea aplicable, por la presente ley.**
	Artículo 28. Centro Coordinador del Equipo de Respuesta ante	**<u>ARTÍCULO 28</u>** Pasa a ser artículo 26, sustituido por el que se indica: "Artículo 26. De las funciones del CSIRT de la Defensa Nacional. Las	**Artículo 26. De las funciones del CSIRT de la Defensa Nacional.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Incidentes de Seguridad Informáticos del Sector Defensa. Créase el Centro Coordinador del Equipo de Respuesta ante Incidentes Informáticos del Sector Defensa (CCCD o CSIRT Sectorial de Defensa), dependiente del Ministerio de Defensa Nacional, como el organismo dependiente del Comando Conjunto de Ciberdefensa, perteneciente al Estado Mayor Conjunto del Ministerio de Defensa Nacional, responsable de la coordinación y protección de la infraestructura de la información calificada como crítica, a su vez de los recursos digitales del sector Defensa, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la Seguridad Nacional. **Para efectos presupuestarios, dependerá del Ministerio de Defensa Nacional y, en lo que le sea aplicable, se regirá por la presente ley y por la reglamentación que dicte al efecto el Ministerio de Defensa.**	funciones principales del CSIRT de la Defensa Nacional serán las siguientes: a) Conducir y asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de las redes de información, los servicios esenciales y operadores vitales para la defensa nacional. Para ello, estará a cargo de la coordinación y será enlace entre los diferentes CSIRT Institucionales de la Defensa Nacional. b) Asumir el rol de coordinador y enlace entre la Agencia y su CSIRT Nacional con los CSIRT Institucionales de la Defensa Nacional, asegurando la cooperación, colaboración e intercambio de información	**Las funciones principales del CSIRT de la Defensa Nacional serán las siguientes:** **a) Conducir y asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de las redes de información, los servicios esenciales y operadores vitales para la defensa nacional. Para ello, estará a cargo de la coordinación y será enlace entre los diferentes CSIRT Institucionales de la Defensa Nacional.** **b) Asumir el rol de coordinador y enlace entre la Agencia y su CSIRT Nacional con los CSIRT Institucionales de la Defensa Nacional, asegurando la cooperación, colaboración e intercambio de información pertinente que fortalezca la**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		pertinente que fortalezca la ciberseguridad.	**ciberseguridad.**
	Sus funciones principales serán las siguientes:		
	a) Responsable de la coordinación y enlace entre los diferentes CSIRT del sector Defensa (Ejército, Armada, Fuerza Aérea, Estado Mayor Conjunto, Subsecretaría de Defensa, Subsecretaría para las Fuerzas Armadas y otros órganos dependientes de dicho sector), con el objeto de asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de la infraestructura de la información calificada como crítica del sector Defensa.	c) Establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y del Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.	**c) Establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, detección, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y del Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.**
	b) Asumir el rol de coordinador y enlace entre la Agencia y su CSIRT Nacional con el CSIRT Sectorial de Defensa, asegurando la cooperación, colaboración e intercambio de información	d) Prestar colaboración o asesoría técnica en la implementación de las políticas de ciberseguridad nacionales a los CSIRT Institucionales de la Defensa Nacional.”.	**d) Prestar colaboración o asesoría técnica en la implementación de las políticas de ciberseguridad nacionales a los CSIRT Institucionales de la Defensa Nacional.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	pertinente que fortalezca la ciberseguridad. **c) Establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.**	**(Unanimidad 8x0. Indicación número 150).**	
		°°°°° A continuación, incorporar los siguientes artículos 27 y 28, nuevos: “Artículo 27. De los Equipos de	**Artículo 27. De los Equipos de**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. En el sector de la defensa nacional se constituirán Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales de la Defensa Nacional, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional. Se podrán constituir CSIRT Institucionales, conforme a los lineamientos entregados por el CSIRT de la Defensa Nacional. Las funciones de los CSIRT Institucionales de la Defensa Nacional serán determinadas por la reglamentación que el Ministerio de	**Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. En el sector de la defensa nacional se constituirán Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales de la Defensa Nacional, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional.** **Se podrán constituir CSIRT Institucionales, conforme a los lineamientos entregados por el CSIRT de la Defensa Nacional.** **Las funciones de los CSIRT Institucionales de la Defensa Nacional serán determinadas por la reglamentación que el**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Defensa Nacional dicte al efecto, de conformidad a la política de ciberdefensa y a los lineamientos generales que entregue la Agencia. Artículo 28. Deber de reporte al CSIRT de la Defensa Nacional. Todas las instituciones de la defensa nacional deberán reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos al CSIRT de la Defensa Nacional. El CSIRT de la Defensa Nacional reportará a la Agencia todos los incidentes identificados cuando no se ponga en riesgo la seguridad y la defensa nacional.”. **(Artículo 27, nuevo, unanimidad 8x0. Indicación número 151, y artículo 121, inciso final, del Reglamento del Senado).** **(Artículo 28, nuevo, unanimidad 8x0. Indicación número 152).** **ooooo**	**Ministerio de Defensa Nacional dicte al efecto, de conformidad a la política de ciberdefensa y a los lineamientos generales que entregue la Agencia.** **Artículo 28. Deber de reporte al CSIRT de la Defensa Nacional. Todas las instituciones de la defensa nacional deberán reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos al CSIRT de la Defensa Nacional. El CSIRT de la Defensa Nacional reportará a la Agencia todos los incidentes identificados cuando no se ponga en riesgo la seguridad y la defensa nacional.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	TÍTULO VI De la reserva de información en el sector público en materia de ciberseguridad	**ARTÍCULO 29** Consultar en su lugar el que se señala a continuación:	TÍTULO VI De la reserva de información en el sector público en materia de ciberseguridad
	Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de los CSIRT, sean el CSIRT Nacional, de Gobierno, Defensa o los CSIRT Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales órganos de la Administración del Estado tome conocimiento en el	"Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con estos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de estas.	**Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con estos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	desempeño de sus funciones o con ocasión de éstas.		**con ocasión de estas.**
	Los estudios e informes que elabore la Agencia podrán eximirse de dicho carácter con la autorización su Director Nacional, en las condiciones que éste indique.	Los estudios e informes que elabore la Agencia podrán eximirse de dicho carácter con la autorización de su Director o Directora Nacional, en las condiciones que este indique.	**Los estudios e informes que elabore la Agencia podrán eximirse de dicho carácter con la autorización de su Director o Directora Nacional, en las condiciones que este indique.**
	Los funcionarios de CSIRT, sean del CSIRT Nacional, de Gobierno, Defensa o de los CSIRT Sectoriales, que hubieren tomado conocimiento de los antecedentes a que se refiere el inciso primero, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.	Los funcionarios y funcionarias de la Agencia y del CSIRT Nacional, de Defensa o de los Sectoriales que hubieren tomado conocimiento de los antecedentes a que se refiere el inciso primero, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.	**Los funcionarios y funcionarias de la Agencia y del CSIRT Nacional, de Defensa o de los Sectoriales que hubieren tomado conocimiento de los antecedentes a que se refiere el inciso primero, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.**
	De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de riesgos y los registros previstos en el artículo 6º, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la	De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 6, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.	**De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 6, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Nación o el interés nacional. **Adicionalmente, serán considerada como información secreta o reservada, la siguiente:** **i. Las matrices de riesgos de ciberseguridad;** **ii. Los planes de continuidad operacional y planes ante desastres;** **iii. Los planes de acción y mitigación de riesgos de ciberseguridad y,** **iv. Los reportes de incidentes de ciberseguridad.**	Adicionalmente, serán considerada como información secreta o reservada, la siguiente: i. Las matrices de riesgos de ciberseguridad; ii. Los planes de continuidad operacional y planes ante desastres, y iii. Los planes de acción y mitigación de riesgos de ciberseguridad.”. **(Inciso primero, unanimidad 8x0. Indicaciones números 153, 154, y 155).** **(Inciso segundo, unanimidad 8x0. Indicación números 156, y artículo 121, inciso final, del Reglamento del Senado).** **(Inciso tercero, unanimidad 8x0. Indicaciones números 157 y 158, y**	**seguridad de la Nación o el interés nacional.** **Adicionalmente, serán considerada como información secreta o reservada, la siguiente:** **i. Las matrices de riesgos de ciberseguridad;** **ii. Los planes de continuidad operacional y planes ante desastres, y** **iii. Los planes de acción y mitigación de riesgos de ciberseguridad.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		artículo 121, inciso final, del Reglamento del Senado). **(Incisos cuarto y quinto, unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	
	Artículo 30. Extensión de la obligación de reserva. La obligación de guardar secreto regirá, además, para aquellos que, sin ser funcionarios **(_)** de la Agencia, tomaren conocimiento de las solicitudes para la ejecución de procedimientos especiales de obtención de información, de los antecedentes que las justifiquen y de las resoluciones judiciales que se dicten al efecto.	**ARTÍCULO 30** Agregar, a continuación de la voz "funcionarios" la expresión "o funcionarias". **(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	Artículo 30. Extensión de la obligación de reserva. La obligación de guardar secreto regirá, además, para aquellos que, sin ser funcionarios **o funcionarias** de la Agencia, tomaren conocimiento de las solicitudes para la ejecución de procedimientos especiales de obtención de información, de los antecedentes que las justifiquen y de las resoluciones judiciales que se dicten al efecto.
	Artículo 31. Deber de reserva de la Agencia. La Agencia cautelará especialmente la reserva de los secretos o información comercial sensible que llegare a conocer en el		Artículo 31. Deber de reserva de la Agencia. La Agencia cautelará especialmente la reserva de los secretos o información comercial sensible que llegare a conocer en el

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	desempeño de su labor, como también el respeto a los derechos fundamentales de las personas, particularmente el respeto y resguardo del derecho a la vida privada y el derecho a la protección de datos personales.		desempeño de su labor, como también el respeto a los derechos fundamentales de las personas, particularmente el respeto y resguardo del derecho a la vida privada y el derecho a la protección de datos personales.
	Artículo 32. Sanciones. La infracción a las obligaciones dispuestas en el presente título, serán sancionadas en la forma prevista en los artículos 246, 247 o 247 bis, todos del Código Penal, según corresponda. Lo anterior es sin perjuicio de la responsabilidad administrativa que procediere.		Artículo 32. Sanciones. La infracción a las obligaciones dispuestas en el presente título, serán sancionadas en la forma prevista en los artículos 246, 247 o 247 bis, todos del Código Penal, según corresponda. Lo anterior es sin perjuicio de la responsabilidad administrativa que procediere.
	TÍTULO VII De las infracciones y sanciones **Artículo 33. De las infracciones. Serán consideradas infracciones**	**ARTÍCULO 33** Reemplazarlo por el siguiente: “Artículo 33. De las infracciones. Las sanciones a las infracciones de la	TÍTULO VII De las infracciones y sanciones **Artículo 33. De las infracciones. Las sanciones a las infracciones**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	para efectos de esta ley:	presente ley cometidas por instituciones privadas serán las siguientes:	**de la presente ley cometidas por instituciones privadas serán las siguientes:**
	a) Retardar o entregar fuera del plazo señalado la información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;	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.	**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) Negar injustificadamente información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;	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.	**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) Entregar maliciosamente información falsa o manifiestamente errónea, e;	c) Las infracciones gravísimas serán sancionadas con multa de 10.001 a 20.000 unidades tributarias mensuales.	**c) Las infracciones gravísimas serán sancionadas con multa de 10.001 a 20.000 unidades tributarias mensuales.**
	d) Incumplir los deberes previstos en el párrafo 2° del Título II.	Se consideran infracciones leves el	**Se consideran infracciones leves**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Podrán imponerse, a beneficio fiscal, multas entre 10 y 20.000 Unidades Tributarias Mensuales, de conformidad a la gravedad de la infracción. Para determinar la cuantía de la multa, se entenderá por: **a) Faltas gravísimas: aquellas señaladas en los literales b) y c) del inciso precedente. En este caso, la multa será de hasta a 20.000 Unidades Tributarias Mensuales.** **b) Faltas graves: aquellas señaladas en el literal a) del inciso precedente. En este caso, la multa será de hasta 10.000 Unidades Tributarias Mensuales.** **c) Faltas leves: aquellas obligaciones señaladas en esta ley cuyo incumplimiento negligente o injustificado no tenga señalada una sanción especial, caso en el que la multa será de 10 a 5.000 Unidades**	incumplimiento de las obligaciones señaladas en esta ley que no tenga señalada una sanción especial. Se consideran infracciones graves, las siguientes: a) Entregar fuera de plazo la información a la autoridad u organismo de la Administración del Estado habilitado por ley para requerirla. b) Incumplir la obligación de reportar establecida en el artículo 7. c) Incumplir los deberes previstos en los artículos 5 y 6 de la presente ley, cuando el infractor sea un operador de servicios esenciales.	**el incumplimiento de las obligaciones señaladas en esta ley que no tenga señalada una sanción especial.** **Se consideran infracciones graves, las siguientes:** **a) Entregar fuera de plazo la información a la autoridad u organismo de la Administración del Estado habilitado por ley para requerirla.** **b) Incumplir la obligación de reportar establecida en el artículo 7.** **c) Incumplir los deberes previstos en los artículos 5 y 6 de la presente ley, cuando el infractor sea un operador de servicios**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Tributarias Mensuales.	Las siguientes infracciones se consideran gravísimas, cuando el infractor sea un operador de servicios esenciales: a) Negar injustificadamente información a la autoridad u organismo de la Administración del Estado habilitado para requerirla. b) Entregar información falsa o manifiestamente errónea a la autoridad u organismo de la Administración del Estado habilitado para requerirla. c) Incumplir la obligación de reportar establecida en el artículo 7. d) Incumplir los deberes previstos en los artículos 5 y 6 de la presente ley, cuando el infractor tenga, además, la calidad de operador de importancia vital. La multa será fijada teniendo en consideración si el infractor adoptó las medidas necesarias para	**esenciales.** **Las siguientes infracciones se consideran gravísimas, cuando el infractor sea un operador de servicios esenciales:** **a) Negar injustificadamente información a la autoridad u organismo de la Administración del Estado habilitado para requerirla.** **b) Entregar información falsa o manifiestamente errónea a la autoridad u organismo de la Administración del Estado habilitado para requerirla.** **c) Incumplir la obligación de reportar establecida en el artículo 7.** **d) Incumplir los deberes previstos en los artículos 5 y 6 de la presente ley, cuando el infractor tenga, además, la calidad de operador de importancia vital.** **La multa será fijada teniendo en consideración si el infractor**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	La multa será fijada teniendo en consideración si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del riesgo, la gravedad de los efectos de los ataques, la reiteración en la infracción dentro del plazo de tres años y la capacidad económica del infractor. **Cuando cualquiera de las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.** **Las infracciones cometidas por funcionarios de la Administración del Estado o de los órganos del Estado se regirán por su**	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 por unos mismos hechos y fundamentos jurídicos, el infractor pudiese ser sancionado con arreglo a esta ley y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad. En ningún caso se podrá aplicar al infractor, por los mismos hechos y fundamentos jurídicos, dos o más sanciones administrativas. Las infracciones previstas en esta ley prescribirán a los tres años de cometidas, plazo que se interrumpirá con la notificación de la formulación de cargos por los hechos constitutivos de las mismas.”.	**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 por unos mismos hechos y fundamentos jurídicos, el infractor pudiese ser sancionado con arreglo a esta ley y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad.** **En ningún caso se podrá aplicar al infractor, por los mismos hechos y fundamentos jurídicos, dos o más sanciones administrativas.** **Las infracciones previstas en esta ley prescribirán a los tres años de cometidas, plazo que se interrumpirá con la notificación de la formulación de cargos por los**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	respectivo estatuto sancionatorio.	**(Unanimidad 8x0. Indicaciones número 159 y 161).**	**hechos constitutivos de las mismas.**
		ARTÍCULO 34 Sustituirlo por el que se señala a continuación:	
	Artículo 34. Procedimiento. Las sanciones que se cursen con motivo de las infracciones contempladas en el artículo precedente, serán impuestas por resolución del Director de la Agencia, de conformidad a lo dispuesto en esta ley.	"Artículo 34. Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan las instituciones privadas por vulneración de las leyes, reglamentos, estatutos y demás normas que las rijan, o por incumplimiento de las instrucciones y órdenes que les imparta la Agencia, así como la aplicación de las sanciones correspondientes se sujetará a las siguientes reglas especiales:	**Artículo 34. Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan las instituciones privadas por vulneración de las leyes, reglamentos, estatutos y demás normas que las rijan, o por incumplimiento de las instrucciones y órdenes que les imparta la Agencia, así como la aplicación de las sanciones correspondientes se sujetará a las siguientes reglas especiales:**
	El procedimiento sancionatorio deberá fundarse en un procedimiento racional y justo, que será establecido en un reglamento dictado por el Ministerio del Interior y Seguridad	a) El procedimiento sancionatorio será instruido por la Agencia.	**a) El procedimiento sancionatorio será instruido por la Agencia.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Pública y deberá, al menos, establecer: **a) El procedimiento para designar al funcionario de la Agencia que llevará adelante el procedimiento;** **b) El contenido de la formulación de cargos, la cual deberá señalar circunstanciadamente los hechos constitutivos de infracción, las normas legales que fueron infringidas y la gravedad de la infracción;**	b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Junto con la apertura del expediente, la Agencia deberá designar un funcionario o una funcionaria responsable de la instrucción del procedimiento, que recibirá el nombre de instructor o instructora. En el evento de que producto de una denuncia se iniciare un procedimiento administrativo sancionador, el denunciante tendrá la calidad de interesado, para todos los efectos legales. c) La Agencia podrá formular cargos en contra de la institución privada, señalando tanto una descripción clara y precisa de los hechos que se estimen constitutivos de infracción y la fecha de su verificación, así como las normas que se estimen infringidas, la sanción y cualquier otro antecedente que sirva para sustentar la formulación.	**b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Junto con la apertura del expediente, la Agencia deberá designar un funcionario o una funcionaria responsable de la instrucción del procedimiento, que recibirá el nombre de instructor o instructora. En el evento de que producto de una denuncia se iniciare un procedimiento administrativo sancionador, el denunciante tendrá la calidad de interesado, para todos los efectos legales.** **c) La Agencia podrá formular cargos en contra de la institución privada, señalando tanto una descripción clara y precisa de los hechos que se estimen constitutivos de infracción y la fecha de su verificación, así como las normas que se estimen infringidas, la sanción y cualquier**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		d) La formulación de cargos deberá notificarse a la institución privada mediante carta certificada dirigida a su domicilio postal o mediante comunicación al correo electrónico que haya registrado en la Agencia.	**otro antecedente que sirva para sustentar la formulación.** **d) La formulación de cargos deberá notificarse a la institución privada mediante carta certificada dirigida a su domicilio postal o mediante comunicación al correo electrónico que haya registrado en la Agencia.**
	c) El plazo para formular descargos, el cual no podrá ser inferior a 15 días hábiles;	e) La institución privada tendrá un plazo de quince días hábiles para presentar sus descargos. En esa oportunidad, la institución privada podrá acompañar todos los antecedentes que estime pertinentes para desacreditar los hechos imputados. Junto con los descargos, la institución privada deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones, si no lo hubiere hecho previamente.	**e) La institución privada tendrá un plazo de quince días hábiles para presentar sus descargos. En esa oportunidad, la institución privada podrá acompañar todos los antecedentes que estime pertinentes para desacreditar los hechos imputados. Junto con los descargos, la institución privada deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones, si no lo hubiere hecho previamente.**
	d) Un periodo para rendir y observar la prueba, el cual no podrá ser inferior a 10 días hábiles, pudiendo aportar las partes los medios de prueba que	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.	**f) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia examinará el mérito de los antecedentes y**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	estimen pertinentes;	En el caso de que existan hechos sustanciales, pertinentes y controvertidos, la Agencia podrá ordenar la recepción de los demás medios probatorios que procedan, para lo cual deberá abrir un término probatorio de diez días hábiles. g) La Agencia dará lugar a las medidas o diligencias probatorias que solicite la institución privada en sus descargos, siempre que sean pertinentes y necesarias. En caso contrario, la rechazará mediante resolución fundada. h) Los hechos investigados y las responsabilidades de los presuntos infractores podrán acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica. i) La Agencia tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.	**podrá ordenar la realización de las pericias e inspecciones que sean pertinentes. En el caso de que existan hechos sustanciales, pertinentes y controvertidos, la Agencia podrá ordenar la recepción de los demás medios probatorios que procedan, para lo cual deberá abrir un término probatorio de diez días hábiles.** **g) La Agencia dará lugar a las medidas o diligencias probatorias que solicite la institución privada en sus descargos, siempre que sean pertinentes y necesarias. En caso contrario, la rechazará mediante resolución fundada.** **h) Los hechos investigados y las responsabilidades de los presuntos infractores podrán acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.** **i) La Agencia tendrá amplias facultades para solicitar antecedentes o informes que**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		j) Cumplidos los trámites señalados en los literales anteriores, el instructor o instructora emitirá, dentro de diez días hábiles, un dictamen en el cual propondrá la absolución o la sanción que a su juicio corresponda aplicar. Dicho dictamen deberá contener la individualización del o de los infractores; la relación de los hechos investigados y la forma como se ha llegado a comprobarlos, y la proposición al Director o Directora de las sanciones que estimare procedente aplicar o de la absolución de uno o más de los infractores.	**contribuyan a su resolución.** **j) Cumplidos los trámites señalados en los literales anteriores, el instructor o instructora emitirá, dentro de diez días hábiles, un dictamen en el cual propondrá la absolución o la sanción que a su juicio corresponda aplicar. Dicho dictamen deberá contener la individualización del o de los infractores; la relación de los hechos investigados y la forma como se ha llegado a comprobarlos, y la proposición al Director o Directora de las sanciones que estimare procedente aplicar o de la absolución de uno o más de los infractores.**
	e) La forma y contenido de la resolución que absuelve o condena, la cual deberá contener la exposición de los hechos, el razonamiento que permite arribar a la resolución y la decisión que acoge o desecha los cargos formulados.	k) Emitido el dictamen, el instructor o instructora elevará los antecedentes al Director o Directora, quien resolverá en el plazo de quince días hábiles, dictando al efecto una resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. No obstante, el Director o Directora podrá ordenar la	**k) Emitido el dictamen, el instructor o instructora elevará los antecedentes al Director o Directora, quien resolverá en el plazo de quince días hábiles, dictando al efecto una resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. No obstante, el Director**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		realización de nuevas diligencias o la corrección de vicios de procedimiento, fijando un plazo para tales efectos, dando audiencia al investigado. Ninguna persona podrá ser sancionada por hechos que no hubiesen sido materia de cargos.	**o Directora podrá ordenar la realización de nuevas diligencias o la corrección de vicios de procedimiento, fijando un plazo para tales efectos, dando audiencia al investigado. Ninguna persona podrá ser sancionada por hechos que no hubiesen sido materia de cargos.**
		l) La resolución que ponga fin al procedimiento sancionatorio deberá ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por la institución privada, y contendrá la declaración de haberse configurado por la institución privada la infracción a la normativa aplicable, o su absolución, según corresponda. En caso de que la Agencia considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida.	**l) La resolución que ponga fin al procedimiento sancionatorio deberá ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por la institución privada, y contendrá la declaración de haberse configurado por la institución privada la infracción a la normativa aplicable, o su absolución, según corresponda. En caso de que la Agencia considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Tratándose de sectores regulados, las sanciones serán impuestas por los reguladores o fiscalizadores sectoriales y el procedimiento corresponderá al determinado por la normativa sectorial respectiva.	m) La resolución que establezca la infracción a la normativa sobre ciberseguridad y aplique la sanción correspondiente deberá ser fundada. Esta resolución deberá indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia que resuelve el procedimiento por infracción de ley será reclamable mediante recurso de reposición que se podrá interponer en el plazo de cinco días hábiles contados desde la notificación, el que deberá ser resuelto por el Director o Directora dentro del plazo de treinta días hábiles. n) El procedimiento administrativo de infracción de ley no podrá superar los seis meses contados desde la notificación a que se refiere el literal d) anterior.”. **(Unanimidad 9x0. Indicación**	**a la gravedad de la infracción cometida.** **m) La resolución que establezca la infracción a la normativa sobre ciberseguridad y aplique la sanción correspondiente deberá ser fundada. Esta resolución deberá indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia que resuelve el procedimiento por infracción de ley será reclamable mediante recurso de reposición que se podrá interponer en el plazo de cinco días hábiles contados desde la notificación, el que deberá ser resuelto por el Director o Directora dentro del plazo de treinta días hábiles.** **n) El procedimiento administrativo de infracción de ley no podrá superar los seis meses contados desde la notificación a que se refiere el**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		número 163, y artículo 121, inciso final, del Reglamento del Senado).	**literal d) anterior.**
		°°°°°	
		Luego, incorporar los siguientes artículos 35, 36 y 37, nuevos:	
		"Artículo 35. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:	**Artículo 35. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:**
		a) El reclamante señalará en su	**a) El reclamante señalará en su**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, cuando procediere, las razones por las cuales el acto le causa agravio. b) La Corte podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior. Asimismo, podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente. c) Recibida la reclamación, la Corte requerirá el informe de la Agencia, concediéndole un plazo de diez días hábiles al efecto. d) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de	**escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, cuando procediere, las razones por las cuales el acto le causa agravio.** **b) La Corte podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior. Asimismo, podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente.** **c) Recibida la reclamación, la Corte requerirá el informe de la Agencia, concediéndole un plazo de diez días hábiles al efecto.** **d) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Procedimiento Civil. e) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla. f) Si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, cuando sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda. g) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá rechazar o acoger la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda, y mantener, dejar sin efecto o modificar la sanción impuesta al responsable o su absolución, según sea el caso. h) Contra la resolución de la Corte de Apelaciones no procederá recurso alguno.	**Procedimiento Civil.** **e) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.** **f) Si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, cuando sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.** **g) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá rechazar o acoger la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda, y mantener, dejar sin efecto o modificar la sanción impuesta al responsable o su absolución, según sea el caso.** **h) Contra la resolución de la Corte de Apelaciones no procederá**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda. Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente. Asimismo, los organismos de la Administración del Estado deberán someterse a las medidas tendientes a subsanar o prevenir las infracciones que indique la Agencia. Las infracciones a los principios y	**recurso alguno.** **i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda.** **Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente.** **Asimismo, los organismos de la Administración del Estado deberán someterse a las medidas tendientes a subsanar o prevenir las infracciones que indique la Agencia.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		obligaciones contenidos en los artículos 21 y 29 serán sancionadas con multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del organismo público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza del incidente y el número de personas afectadas, si las hubiere. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor. Si el organismo público persiste en la infracción, se le aplicará al jefe superior del organismo público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días hábiles. Las infracciones en que incurra un organismo público serán determinadas por la Agencia, de acuerdo al procedimiento establecido en el artículo 34.	**Las infracciones a los principios y obligaciones contenidos en los artículos 21 y 29 serán sancionadas con multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del organismo público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza del incidente y el número de personas afectadas, si las hubiere. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor.** **Si el organismo público persiste en la infracción, se le aplicará al jefe superior del organismo público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días hábiles.** **Las infracciones en que incurra un organismo público serán determinadas por la Agencia, de acuerdo al procedimiento**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Habiéndose configurado la infracción, las sanciones administrativas señaladas en este artículo serán aplicadas por la Agencia. Con todo, la Contraloría General de la República, a petición de la Agencia podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y proponer las sanciones que correspondan. En contra de las resoluciones de la Agencia se podrá deducir el reclamo de ilegalidad establecido en el artículo 35. Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia y del organismo o servicio de que se trate dentro del plazo de cinco días hábiles contados desde que la respectiva resolución quede firme. Artículo 37. Responsabilidad del funcionario o funcionaria infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el	**establecido en el artículo 34.** **Habiéndose configurado la infracción, las sanciones administrativas señaladas en este artículo serán aplicadas por la Agencia. Con todo, la Contraloría General de la República, a petición de la Agencia podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y proponer las sanciones que correspondan.** **En contra de las resoluciones de la Agencia se podrá deducir el reclamo de ilegalidad establecido en el artículo 35.** **Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia y del organismo o servicio de que se trate dentro del plazo de cinco días hábiles contados desde que la respectiva resolución quede firme.** **Artículo 37. Responsabilidad del**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios o funcionarias del organismo público, la responsabilidad administrativa se hará efectiva con sujeción a las normas estatutarias que rijan al organismo en que se produjo la infracción. En caso de que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios o funcionarias involucrados es responsable de alguna de las infracciones gravísimas señaladas en el artículo 33 de esta ley, esta conducta se considerará una contravención grave a la probidad administrativa.”. **(Artículo 35, nuevo, unanimidad 9x0. Indicación número 164).** **(Artículos 36 y 37, nuevos, unanimidad 10x0. Indicación número 164, y artículo 121, inciso final, del Reglamento del Senado).**	**funcionario o funcionaria infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios o funcionarias del organismo público, la responsabilidad administrativa se hará efectiva con sujeción a las normas estatutarias que rijan al organismo en que se produjo la infracción.** **En caso de que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios o funcionarias involucrados es responsable de alguna de las infracciones gravísimas señaladas en el artículo 33 de esta ley, esta conducta se considerará una contravención grave a la probidad administrativa.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		°°°°°	
		ARTÍCULO 35 Pasa a ser artículo 38, sustituido por el que se indica a continuación:	
	Artículo 35. Agravante especial. Si como consecuencia de la perpetración de un delito resultare la destrucción, inutilización o alteración grave del funcionamiento de infraestructura crítica de la información, se impondrá la pena que corresponda, aumentada en un grado. **Lo mismo se observará cuando el delito consistiere en la alteración o supresión de los datos soportados por infraestructura de la información calificada como crítica o en la obstaculización del acceso o la alteración perjudicial del funcionamiento de un sistema informático que formare parte de la Infraestructura Crítica de la**	"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.".	**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.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Información.	**(Unanimidad 10x0. Indicación número 165).**	
	TÍTULO VIII Del Comité Interministerial de Ciberseguridad	**ARTÍCULO 36** Pasa a ser artículo 39, reemplazado por el que sigue:	TÍTULO VIII Del Comité Interministerial de Ciberseguridad
	Artículo 36. Comité Interministerial de Ciberseguridad. Créase el Comité Interministerial de Ciberseguridad, en adelante el Comité, cuya función será asesorar al Ministro del Interior y Seguridad Pública en materias de ciberseguridad relevantes para el funcionamiento de los órganos de la Administración del Estado y de servicios esenciales.	"Artículo 39. Comité Interministerial sobre Ciberseguridad. Créase el Comité Interministerial sobre Ciberseguridad, en adelante el Comité, que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país. En el ejercicio de sus funciones, el Comité deberá: a) Asesorar al Presidente de la	**Artículo 39. Comité Interministerial sobre Ciberseguridad. Créase el Comité Interministerial sobre Ciberseguridad, en adelante el Comité, que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país.** **En el ejercicio de sus funciones, el Comité deberá:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		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 esta incida en materias de ciberseguridad. c) Coordinar la implementación de la Política Nacional de Ciberseguridad. d) Aprobar la lista de servicios esenciales propuesto por la Agencia, y sus modificaciones. e) Aprobar la lista de operadores de importancia vital propuesto por la Agencia, y sus modificaciones. f) Apoyar las funciones de la Agencia Nacional de Ciberseguridad en lo que resulte necesario.	**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 esta incida en materias de ciberseguridad.** **c) Coordinar la implementación de la Política Nacional de Ciberseguridad.** **d) Aprobar la lista de servicios esenciales propuesto por la Agencia, y sus modificaciones.** **e) Aprobar la lista de operadores de importancia vital propuesto por la Agencia, y sus modificaciones.** **f) Apoyar las funciones de la Agencia Nacional de**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		g) Revisar y tener en consideración las recomendaciones del Consejo Multisectorial sobre Ciberseguridad.”. **(Unanimidad 10x0. Indicación número 167).**	**Ciberseguridad en lo que resulte necesario.** **g) Revisar y tener en consideración las recomendaciones del Consejo Multisectorial sobre Ciberseguridad.**
		<u>ARTÍCULO 37</u> Pasa ser artículo 40, consultando en su lugar el siguiente texto:	
	Artículo 37. De los integrantes del Comité. El Comité será presidido por el Subsecretario del Interior y estará integrado por los siguientes miembros permanentes:	“Artículo 40. De los integrantes del Comité. El Comité estará integrado por los siguientes miembros permanentes:	**Artículo 40. De los integrantes del Comité. El Comité estará integrado por los siguientes miembros permanentes:**
		a) Por el Subsecretario del Interior o quien este designe.	**a) Por el Subsecretario del Interior o quien este designe.**
	a) Por el Subsecretario de Defensa o quien éste designe;	b) Por el Subsecretario de Defensa o quien este designe.	**b) Por el Subsecretario de Defensa o quien este designe.**
	b) Por el Subsecretario de Relaciones Exteriores o quien	c) Por el Subsecretario de Relaciones Exteriores o quien este	**c) Por el Subsecretario de Relaciones Exteriores o quien**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	éste designe; **c) Por el Subsecretario de Justicia o quien éste designe;** **d) Por el Subsecretario General de la Presidencia o quien éste designe;** **e) Por el Subsecretario de Telecomunicaciones o quien éste designe;** **f) Por el Subsecretario de Economía y Empresas de Menor Tamaño o quien éste designe;** **g) Por el Subsecretario de Hacienda o quien éste designe;** **h) Por el Subsecretario de Minería o quien éste designe;** **i) Por el Subsecretario de Energía o quien éste designe;** **j) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien éste designe;** **k) Por el Director Nacional de la**	designe. d) Por el Subsecretario General de la Presidencia o quien este designe. e) Por el Subsecretario de Telecomunicaciones o quien este designe. f) Por el Subsecretario de Hacienda o quien este designe. g) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien este designe. h) Por el Director o Directora	**este designe.** **d) Por el Subsecretario General de la Presidencia o quien este designe.** **e) Por el Subsecretario de Telecomunicaciones o quien este designe.** **f) Por el Subsecretario de Hacienda o quien este designe.** **g) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien este designe.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Agencia Nacional de Inteligencia; **l) Por el Director Nacional de la Agencia Nacional de Ciberseguridad;** **m) Por un representante de la Subsecretaría del Interior, experto en materias de ciberseguridad.** **Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios de la Administración del Estado u otras autoridades públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.**	Nacional de la Agencia Nacional de Inteligencia. i) Por el Director o Directora Nacional de la Agencia Nacional de Ciberseguridad, quien lo presidirá. Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios o funcionarias de la Administración del Estado u otras autoridades públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.”. **(Unanimidad 10x0. Indicación número 169, y artículo 121, inciso final, del Reglamento del Senado).**	**h) Por el Director o Directora Nacional de la Agencia Nacional de Inteligencia.** **i) Por el Director o Directora Nacional de la Agencia Nacional de Ciberseguridad, quien lo presidirá.** **Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios o funcionarias de la Administración del Estado u otras autoridades públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.**
	Artículo 38. De la secretaría ejecutiva. El Comité contará con una Secretaría Ejecutiva radicada en la	**<u>ARTÍCULO 38</u>** Pasa a ser artículo 41.	**Artículo 41.** De la secretaría ejecutiva. El Comité contará con una Secretaría Ejecutiva radicada en la

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Agencia, la que prestará el apoyo técnico, administrativo y de contenidos para el desarrollo de las reuniones del Comité. **El Director Nacional de la Agencia dirigirá la Secretaría Ejecutiva y le corresponderá, entre otras funciones, despachar las convocatorias, según le instruya el Subsecretario del Interior; coordinar y registrar las sesiones del Comité e implementar los acuerdos que se adopten.**	**Inciso segundo** Sustituirlo por el que sigue: "Al Director o Directora Nacional de la Agencia le corresponderá, entre otras funciones, convocar, dirigir y registrar las sesiones e implementar los acuerdos que se adopten.". **(Unanimidad 10x0. Indicación número 171, y artículo 121, inciso final, del Reglamento del Senado).**	Agencia, la que prestará el apoyo técnico, administrativo y de contenidos para el desarrollo de las reuniones del Comité. **Al Director o Directora Nacional de la Agencia le corresponderá, entre otras funciones, convocar, dirigir y registrar las sesiones e implementar los acuerdos que se adopten.**
	Artículo 39. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios **(_)** que estén en conocimiento de	**ARTÍCULO 39** Pasa a ser artículo 42. Agregar, a continuación de la voz "funcionarios" la expresión "o	**Artículo 42.** De la información reservada. Constituido el Comité en sesión secreta, los funcionarios **o funcionarias** que estén en

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	información reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición. La revelación de la información será sancionada de conformidad al delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.	funcionarias". **(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	conocimiento de información reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición. La revelación de la información será sancionada de conformidad al delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.
	Artículo 40. Del reglamento. Un reglamento expedido por el **Ministerio del Interior y Seguridad Pública** fijará las normas de funcionamiento del Comité.	**ARTÍCULO 40** Pasa a ser artículo 43, sustituyendo la expresión "Ministerio del Interior y Seguridad Pública" por "Ministerio encargado de la seguridad pública". **(Unanimidad 10x0. Indicación número 172).**	**Artículo 43.** Del reglamento. Un reglamento expedido por el **Ministerio encargado de la seguridad pública** fijará las normas de funcionamiento del Comité.
		°°°°°	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Luego, intercalar el siguiente Título IX, nuevo: "Título IX Órganos autónomos constitucionales". **(Unanimidad 10x0. Indicación número 173).** °°°°°	**Título IX** **Órganos autónomos constitucionales**
		°°°°° A continuación, introducir un artículo 44, nuevo, del tenor que sigue: "Artículo 44. Regímenes especiales. Corresponderá a las autoridades superiores de los órganos internos del Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la	**Artículo 44. Regímenes especiales. Corresponderá a las autoridades superiores de los órganos internos del Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Justicia Electoral y el Consejo Nacional de Televisión adoptar las medidas especiales de ciberseguridad señaladas en el artículo 6 de la presente ley, debiendo dictar para ello las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, pudiendo requerir para ello la asistencia técnica de la Agencia Nacional de Ciberseguridad. En este caso, las referencias al reglamento contenidas en el artículo 6, se entenderán efectuadas a las normas que adopten los respectivos órganos internos. Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios y funcionarias, en relación a las infracciones a esta ley que se produzcan y, del mismo modo, les corresponderá ejercer las demás funciones y adoptar las decisiones que esta ley encomienda	**Banco Central, el Servicio Electoral y la Justicia Electoral y el Consejo Nacional de Televisión adoptar las medidas especiales de ciberseguridad señaladas en el artículo 6 de la presente ley, debiendo dictar para ello las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, pudiendo requerir para ello la asistencia técnica de la Agencia Nacional de Ciberseguridad. En este caso, las referencias al reglamento contenidas en el artículo 6, se entenderán efectuadas a las normas que adopten los respectivos órganos internos.** **Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios y funcionarias, en relación a las infracciones a esta ley que se produzcan y, del mismo modo, les corresponderá ejercer las demás funciones y adoptar las decisiones que esta ley encomienda a la Agencia, para**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		a la Agencia, para fines de dar cumplimiento a lo previsto en este artículo. Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia. Sin perjuicio de ello, deberán acordar mecanismos de coordinación, cooperación, reporte de incidentes e intercambio de información sobre ciberseguridad, respecto de la Agencia y las demás autoridades o instancias previstas en esta ley, incluyéndose la conformación o participación en equipos de respuesta a incidentes de ciberseguridad. En este contexto, si además fuere requerido el acceso por parte de la Agencia a redes y sistemas informáticos de los referidos órganos, deberá contarse con su autorización previa, debiendo cautelarse para ello la continuidad de sus operaciones. En caso de que los antecedentes que se soliciten o la información a la que se acceda sean confidenciales o reservados, la Agencia deberá conservarlos en ese carácter.	**fines de dar cumplimiento a lo previsto en este artículo.** **Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia. Sin perjuicio de ello, deberán acordar mecanismos de coordinación, cooperación, reporte de incidentes e intercambio de información sobre ciberseguridad, respecto de la Agencia y las demás autoridades o instancias previstas en esta ley, incluyéndose la conformación o participación en equipos de respuesta a incidentes de ciberseguridad. En este contexto, si además fuere requerido el acceso por parte de la Agencia a redes y sistemas informáticos de los referidos órganos, deberá contarse con su autorización previa, debiendo cautelarse para ello la continuidad de sus operaciones. En caso de que los antecedentes que se soliciten o la información a la que se acceda sean confidenciales o reservados, la Agencia deberá conservarlos**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		Corresponderá a los señalados órganos determinar e informar a la Agencia sobre su carácter de operador de importancia vital, en los términos del artículo 4, e informarle, con la periodicidad que se acuerde, las infraestructuras, servicios o funciones específicos que se identifiquen en esta condición. Asimismo, si el órgano autónomo constitucional revistiere además el carácter de autoridad sectorial, deberá considerarse su opinión previa en relación con las personas o entidades reguladas o supervisadas por ella, que pudieren calificarse como operadores de importancia vital.”. **(Unanimidad 8x0, indicación número 174, y 10x0, indicación número 174 bis).** **°°°°°**	**en ese carácter.** **Corresponderá a los señalados órganos determinar e informar a la Agencia sobre su carácter de operador de importancia vital, en los términos del artículo 4, e informarle, con la periodicidad que se acuerde, las infraestructuras, servicios o funciones específicos que se identifiquen en esta condición.** **Asimismo, si el órgano autónomo constitucional revistiere además el carácter de autoridad sectorial, deberá considerarse su opinión previa en relación con las personas o entidades reguladas o supervisadas por ella, que pudieren calificarse como operadores de importancia vital.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
LEY N° 20.424, ESTATUTO ORGÁNICO DEL MINISTERIO DE DEFENSA NACIONAL TÍTULO III DEL ESTADO MAYOR CONJUNTO DE SU FUNCIONAMIENTO Y ORGANIZACIÓN (artículos 25 a 28)	TÍTULO IX De las modificaciones a otros cuerpos legales	**TÍTULO IX** Pasa a ser Título X, sin cambios en su denominación. **ARTÍCULO 41** Pasa a ser artículo 45, reemplazado por el que sigue:	**TÍTULO X** De las modificaciones a otros cuerpos legales
Artículo 25.- El Estado Mayor Conjunto es el organismo de trabajo y asesoría permanente del Ministro de Defensa Nacional en materias que tengan relación con la preparación y empleo conjunto de las Fuerzas Armadas. Al Estado Mayor Conjunto le corresponderán las siguientes funciones: a) Servir de órgano de asesoría y trabajo en la conducción estratégica para enfrentar las situaciones que puedan demandar los estados de excepción constitucional y, en particular, los casos de guerra	**Artículo 41. Incorpórase al siguiente literal k), nuevo, en el artículo 25 de la ley Nº 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional:**	“Artículo 45. Incorpórase, en el artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, la siguiente letra k), nueva:	**Artículo 45. Incorpórase, en el artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, la siguiente letra k), nueva:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
externa o crisis internacional que afecte a la seguridad exterior de la República. b) Elaborar y mantener actualizada la planificación secundaria. c) Proponer al Ministro el texto de los informes al Congreso Nacional sobre las políticas y planes de la defensa nacional, en aquellas materias que sean de su competencia. Le corresponderá especialmente, y en coordinación con la Subsecretaría para las Fuerzas Armadas, proponer el texto de los informes al Congreso Nacional relativos a la planificación de desarrollo de la fuerza y sobre el estado de avance de su ejecución. d) Asegurar la correspondencia, en materia de desarrollo y empleo de la fuerza, entre la planificación secundaria y la planificación institucional y operativa. e) Proponer al Ministro la doctrina y reglamentación conjunta y asegurar que la documentación institucional respectiva corresponda con			

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
aquéllas. f) Planificar, preparar, disponer y apoyar el entrenamiento conjunto de las Fuerzas Armadas. g) Servir de órgano de asesoría y trabajo para la planificación y coordinación de las actividades de los medios chilenos que participen en misiones de paz. h) Participar en la evaluación de los proyectos de adquisición e inversión de las Fuerzas Armadas. i) Elaborar y proponer al Ministro los proyectos de adquisición e inversión conjuntos. j) Proveer de inteligencia a la Subsecretaría de Defensa para efectos de la planificación primaria. Para todos los efectos de la ley Nº 19.974, se entenderá que la Dirección de Inteligencia de la Defensa, dependiente del Estado Mayor de la Defensa Nacional, mantendrá dicha condición y denominación en la estructura para el Estado Mayor Conjunto fijada en			

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
esta ley.	**“k) Conducir el Centro Coordinador CSIRT del Sector Defensa en coordinación con la Subsecretaría de Defensa.”.**	“k) Conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa.”.”. **(Unanimidad 7x0. Indicación número 177).**	**“k) Conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa.”.**
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		°°°°° Luego, incorporar los siguientes artículos 46, 47 y 48, nuevos: “Artículo 46. Introdúcense las siguientes enmiendas a 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:	**Artículo 46. Introdúcense las siguientes enmiendas a 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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
"TÍTULO I DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES (artículos 1° al 10) Artículo 2°.- Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado		1. Incorpórase, en el artículo 2°, los siguientes incisos finales, nuevos:	**Budapest:** **1. Incorpórase, en el artículo 2°, los siguientes incisos finales, nuevos:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
la información, se aplicará la pena de presidio menor en sus grados medio a máximo.		“No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que se cumplan las siguientes condiciones: 1) Haber reportado el acceso y las vulnerabilidades de seguridad detectadas en su investigación al responsable de las redes y sistemas informáticos afectados, en forma inmediata y a más tardar en el momento en que alerte a la Agencia Nacional de Ciberseguridad; 2) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia Nacional de Ciberseguridad; 3) Que el acceso no haya sido realizado con el ánimo de	**“No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que se cumplan las siguientes condiciones:** **1) Haber reportado el acceso y las vulnerabilidades de seguridad detectadas en su investigación al responsable de las redes y sistemas informáticos afectados, en forma inmediata y a más tardar en el momento en que alerte a la Agencia Nacional de Ciberseguridad;** **2) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia Nacional de Ciberseguridad;** **3) Que el acceso no haya sido realizado con el ánimo de**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
TÍTULO III		apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, ex filtración o destrucción de datos, y 4) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad. Tampoco será objeto de sanción penal la persona que comunique a la Agencia información una vulnerabilidad potencial de la que haya tomado conocimiento en su contexto laboral o con ocasión de la prestación de sus servicios, ni se considerará que ha incumplido con ello su obligación de secreto profesional.”.	**apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, ex filtración o destrucción de datos, y** **4) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad.** **Tampoco será objeto de sanción penal la persona que comunique a la Agencia información una vulnerabilidad potencial de la que haya tomado conocimiento en su contexto laboral o con ocasión de la prestación de sus servicios, ni se considerará que ha incumplido con ello su obligación de secreto profesional.”.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
DISPOSICIONES FINALES (artículos 15 al 21) **Artículo 16.- Autorización e Investigación Académica. Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.** **LEY N° 19.974, SOBRE EL SISTEMA DE INTELIGENCIA DEL ESTADO Y CREA LA AGENCIA NACIONAL DE INTELIGENCIA** **TITULO III** **CAPITULO 1°** **DE LA AGENCIA NACIONAL DE INTELIGENCIA** (artículos 7° y 8°)		2. Derógase el artículo 16.	**2. Derógase el artículo 16.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
Artículo 8º.- Corresponderán a la Agencia Nacional de Inteligencia, en adelante la Agencia, las siguientes funciones: a) Recolectar y procesar información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia y de efectuar apreciaciones globales y sectoriales, de acuerdo con los requerimientos efectuados por el Presidente de la República. b) Elaborar informes periódicos de inteligencia, de carácter secreto, que se remitirán al Presidente de la República y a los ministerios u organismos que él determine. c) Proponer normas y procedimientos de protección de los sistemas de información crítica del Estado. d) Requerir de los organismos de inteligencia de las Fuerzas Armadas y de las Fuerzas de Orden y Seguridad Pública, así como de la Dirección Nacional de Gendarmería,		Artículo 47. Incorpórase, en el artículo 8° de la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia, el siguiente literal h), nuevo:	**Artículo 47. Incorpórase, en el artículo 8° de la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia, el siguiente literal h), nuevo:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
la información que sea del ámbito de responsabilidad de estas instituciones y que sea de competencia de la Agencia, a través del canal técnico correspondiente. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados. e) Requerir de los servicios de la Administración del Estado comprendidos en el artículo 1° de la ley Nº 18.575 los antecedentes e informes que estime necesarios para el cumplimiento de sus objetivos, como asimismo, de las empresas o instituciones en que el Estado tenga aportes, participación o representación mayoritarios. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados, a través de la respectiva jefatura superior u órgano de dirección, según corresponda. f) Disponer la aplicación de medidas de inteligencia, con objeto de			

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
detectar, neutralizar y contrarrestar las acciones de grupos terroristas, nacionales o internacionales, y de organizaciones criminales transnacionales. g) Disponer la aplicación de medidas de contrainteligencia, con el propósito de detectar, neutralizar y contrarrestar las actividades de inteligencia desarrolladas por grupos nacionales o extranjeros, o sus agentes, excluyendo las del inciso segundo del artículo 20.		“h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general,	**“h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		de los servicios que este debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.”.	**funciones del Estado y, en general, de los servicios que este debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.”.**
LEY N° 7.401, QUE REPRIME LAS ACTIVIDADES QUE VAYAN CONTRA LA SEGURIDAD EXTERIOR DEL ESTADO Artículo 8°.- Por reclamarlo la necesidad imperiosa de la defensa del Estado, autorízase al Presidente de la República para dictar una o más de las siguientes medidas: **a) Prohibir total o parcialmente en**			

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
las comunicaciones cablegráficas, telefónicas, telegráficas, radiotelegráficas y radiotelefónicas con el exterior, el uso de claves o cualquier otro sistema cifrado o disimulado, y la transmisión de mensajes en determinados idiomas extranjeros; b) Prohibir el uso de transmisores de radio a personas determinadas de nacionalidad extranjera; c) Cancelar o darles carácter provisional a los permisos de residencia de extranjeros en el país, y d) Señalar lugares de permanencia forzosa para determinados extranjeros o localidades o zonas en que les esté prohibido residir. Las medidas anteriormente señaladas sólo podrán adoptarse respecto de las personas que, por cualquier medio tiendan a favorecer a una potencia en guerra con algún país de América o sus aliados, o perjudicar a éstos.		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.”. **(Unanimidad 9x0. Indicación número 178).** °°°°°	**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.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
Las facultades indicadas en las letras c) y d) se otorgan conforme al N° 13 del artículo 44 de la Constitución Política del Estado, sólo por el plazo de seis meses. En los casos de las letras c) y d), el afectado podrá reclamar ante la Corte Suprema dentro del plazo y con sujeción al procedimiento señalado en la ley 3,446, de 12 de Diciembre de 1918, sin perjuicio de las medidas de seguridad que se adopten. Este Tribunal conocerá del reclamo en pleno o por medio de alguna de sus salas de fondo. Las trasgresiones a las medidas decretadas por el Presidente de la República en conformidad a este artículo, serán sancionadas con presidio menor en su grado mínimo.			
	TÍTULO X Disposiciones transitorias	**<u>TÍTULO X</u>** Pasa a ser Título XI, sin cambios en su denominación.	**TÍTULO XI** Disposiciones transitorias

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ARTÍCULO PRIMERO TRANSITORIO Reemplazarlo por el siguiente:	
	Artículo Primero Transitorio.- Facúltase al Presidente de la República para que en el plazo de un año de publicada en el Diario Oficial la presente ley, establezca mediante uno o más decretos con fuerza de ley, expedidos por intermedio del Ministerio del Interior y Seguridad Pública, los que también deberán ser suscritos por el Ministro de Hacienda, las normas necesarias para regular las siguientes materias: **1.Fijar la planta de personal de la Agencia Nacional de Ciberseguridad.** **En el ejercicio de esta facultad, el Presidente de la República deberá dictar todas las normas necesarias para la adecuada estructuración y operación de la planta de personal que fije, así como el número de cargos para**	"Artículo primero. Entrada en vigencia y personal. Facúltase al Presidente de la República para que en el plazo de un año de publicada en el Diario Oficial la presente ley, establezca mediante uno o más decretos con fuerza de ley expedidos a través del Ministerio del Interior y Seguridad Pública, los que también deberán ser suscritos por el Ministro de Hacienda, las normas necesarias para regular las siguientes materias:	**Artículo primero. Entrada en vigencia y personal. Facúltase al Presidente de la República para que en el plazo de un año de publicada en el Diario Oficial la presente ley, establezca mediante uno o más decretos con fuerza de ley expedidos a través del Ministerio del Interior y Seguridad Pública, los que también deberán ser suscritos por el Ministro de Hacienda, las normas necesarias para regular las siguientes materias:**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	cada planta, los requisitos específicos para el ingreso y promoción de dichos cargos, sus denominaciones y niveles jerárquicos para efectos de la aplicación de lo dispuesto en el Título VI de la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica, y en el artículo 8º del decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda. Igualmente, fijará su sistema de remuneraciones y las normas necesarias para la fijación de las remuneraciones variables, en su aplicación transitoria. **Además, podrá establecer las normas para el encasillamiento del personal en la planta que fije, las que podrá incluir a los funcionarios que se traspasen desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.** **2. Determinar la fecha para la entrada en vigencia de las plantas que fije, del traspaso y del**	1. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación	**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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	encasillamiento que se practique. Además, fijará la fecha en que la Agencia entrará en funcionamiento, pudiendo contemplar un período para su implementación.	y uno a contar del cual entrará en operaciones.	**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.	**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. Determinar la dotación máxima de personal de la Agencia Nacional de Ciberseguridad, a cuyo respecto no regirá la limitación establecida en el inciso segundo del artículo 10 de la ley Nº 18.834.	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.	**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. Disponer, sin solución de continuidad, el traspaso de los funcionarios titulares de planta y a contrata, desde la Subsecretaría del Interior.	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	**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**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		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	**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**
	En el respectivo decreto con fuerza de ley que fije la planta de personal, se determinará la forma en que se realizará el traspaso y el número de funcionarios que serán traspasados por estamento y calidad jurídica, pudiéndose establecer, además, el plazo en que se llevará a cabo este proceso, quienes mantendrán, al menos, el mismo grado que tenía		

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	a la fecha del traspaso. A contar de la fecha del traspaso, el cargo del que era titular el funcionario traspasado se entenderá suprimido de pleno derecho en la planta de la institución de origen. Del mismo modo, la dotación máxima de personal se disminuirá en el número de funcionarios traspasados. **La individualización del personal traspasado se realizará a través de decretos expedidos bajo la fórmula "Por orden del Presidente de la República", por intermedio del Ministerio del Interior y Seguridad Pública. Conjuntamente con el traspaso del personal, se traspasarán los recursos presupuestarios que se liberen por este hecho.**	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	**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 dotación máxima**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	5. Los requisitos para el desempeño de los cargos que se establezcan en el ejercicio de la facultad prevista en este artículo no serán exigibles para efectos del encasillamiento respecto de los funcionarios titulares y a contrata en servicio a la fecha de entrada en vigencia del o de los respectivos decretos con fuerza de ley. Asimismo, a los funcionarios o funcionarias a contrata en servicio a la fecha de entrada en vigencia del o de los respectivos decretos con fuerza de ley, y a aquellos cuyos contratos se prorroguen en las mismas condiciones, no les serán exigibles los requisitos que se establezcan en los decretos con fuerza de ley correspondientes. **El uso de las facultades señaladas en este artículo quedará sujeto a las siguientes restricciones, respecto del personal al que afecte:** **a) No podrá tener como consecuencia ni podrán ser**	mensual. 5. Determinar la dotación máxima de personal de la Agencia.	**de personal de la Agencia.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	considerados como causal de término de servicios, supresión de cargos, cese de funciones o término de la relación laboral del personal traspasado. **b) No podrá significar pérdida del empleo, disminución de remuneraciones respecto del personal titular de un cargo de planta, modificación de los derechos estatutarios y previsionales del personal traspasado. Tampoco importará cambio de la residencia habitual de los funcionarios fuera de la Región en que estén prestando servicios, a menos que se lleve a cabo con su consentimiento.** **c) Respecto del personal que en el momento del encasillamiento sea titular de un cargo de planta, cualquier diferencia de remuneraciones se pagará mediante una planilla suplementaria, la que se absorberá por los futuros mejoramientos de remuneraciones que correspondan a los funcionarios,**		

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	excepto los derivados de reajustes generales que se otorguen a los trabajadores del sector público. Dicha planilla mantendrá la misma imponibilidad que aquella de las remuneraciones que compensa. Además, a la planilla suplementaria se le aplicará el reajuste general antes indicado. **d) Los funcionarios traspasados conservarán la asignación de antigüedad que tengan reconocida, así como también el tiempo computable para dicho reconocimiento.** **6.Podrá disponer el traspaso, en lo que corresponda, de los bienes que determine, desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.**	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.”. **(Unanimidad 9x0. Indicación número 179).**	**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.**
		<u>ARTÍCULO SEGUNDO TRANSITORIO</u>	

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Artículo Segundo Transitorio.- El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº 19.882, podrá nombrar, a partir de la publicación de la presente ley, al primer Director **(_)** de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública. En el acto de nombramiento, el Presidente de la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director **(_)**, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director **(_)** se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese solo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la	Sustituir su denominación por "Artículo segundo". Agregar, a continuación de la voz "Director" la expresión "o Directora", las tres veces que aparece. **(Unanimidad. Artículo 121, inciso final, del Reglamento del Senado).**	**Artículo segundo.** El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº 19.882, podrá nombrar, a partir de la publicación de la presente ley, al primer Director **o Directora** de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública. En el acto de nombramiento, el Presidente de la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director **o Directora**, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director **o Directora** se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese solo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	respectiva planta de personal.		respectiva planta de personal.
	Artículo Tercero Transitorio.- El Presidente de la República, por decreto supremo expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia Nacional de Ciberseguridad y podrá modificar el presupuesto del Ministerio del Interior y Seguridad Pública. Para los efectos anteriores podrá crear, suprimir o modificar las partidas, capítulos, programas, ítems, asignaciones y glosas presupuestarias que sean pertinentes.	**ARTÍCULO TERCERO TRANSITORIO Y ARTÍCULO CUARTO TRANSITORIO** Considerarlos como artículos tercero y cuarto, respectivamente, sin enmiendas. **(Adecuación formal).**	**Artículo tercero.** El Presidente de la República, por decreto supremo expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia Nacional de Ciberseguridad y podrá modificar el presupuesto del Ministerio del Interior y Seguridad Pública. Para los efectos anteriores podrá crear, suprimir o modificar las partidas, capítulos, programas, ítems, asignaciones y glosas presupuestarias que sean pertinentes.
	Artículo Cuarto Transitorio.- Dentro del plazo de ciento ochenta días posteriores a la publicación de la ley, el Ministerio del Interior y Seguridad Pública deberá expedir los reglamentos señalados en esta ley.		**Artículo cuarto.** Dentro del plazo de ciento ochenta días posteriores a la publicación de la ley, el Ministerio del Interior y Seguridad Pública deberá expedir los reglamentos señalados en esta ley.

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Artículo Quinto Transitorio.- En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás órganos de la Administración del Estado reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de éstos, de conformidad a lo dispuesto en el artículo 22, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.	**ARTÍCULO QUINTO TRANSITORIO** Reemplazarlo por el que sigue: “Artículo quinto. En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás organismos del Estado reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de estos, de conformidad a lo dispuesto en el artículo 21, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.”. **(Unanimidad 9x0. Indicación número 182, y artículo 121, inciso final, del Reglamento del Senado).**	**Artículo quinto. En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás organismos del Estado reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de estos, de conformidad a lo dispuesto en el artículo 21, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ARTÍCULO SEXTO TRANSITORIO Sustituirlo por el que se transcribe a continuación:	
	Artículo Sexto Transitorio.- Para los efectos de la renovación parcial de los miembros del Consejo Técnico de la Agencia a que se refiere el inciso segundo del artículo 17, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período: **a) Dos consejeros durarán en sus cargos por un plazo de dos tres años;** **b) Dos consejeros durarán en sus cargos por un plazo de seis años.**	"Artículo sexto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 16, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período: a) Tres consejeros durarán en sus cargos un plazo de tres años. b) Tres consejeros durarán en sus cargos un plazo de seis años.". **(Unanimidad 9x0. Indicación número 184).**	**Artículo sexto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 16, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período:** **a) Tres consejeros durarán en sus cargos un plazo de tres años.** **b) Tres consejeros durarán en sus cargos un plazo de seis años.**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
	Artículo Séptimo Transitorio.- El mayor gasto fiscal que represente la aplicación de la presente ley durante su primer año presupuestario de vigencia se financiará con cargo al presupuesto el Ministerio del Interior y Seguridad Pública. No obstante lo anterior, el Ministerio de Hacienda con cargo a la partida presupuestaria Tesoro Público podrá suplementar dicho presupuesto en la parte del gasto que no pudiere financiar con esos recursos. Para los años siguientes, se financiará de acuerdo con lo determinen las respectivas leyes de Presupuestos del Sector Público.”.	**ARTÍCULO SÉPTIMO TRANSITORIO** Considerarlo como artículo séptimo. **(Adecuación formal).**	**Artículo séptimo.** El mayor gasto fiscal que represente la aplicación de la presente ley durante su primer año presupuestario de vigencia se financiará con cargo al presupuesto el Ministerio del Interior y Seguridad Pública. No obstante lo anterior, el Ministerio de Hacienda con cargo a la partida presupuestaria Tesoro Público podrá suplementar dicho presupuesto en la parte del gasto que no pudiere financiar con esos recursos. Para los años siguientes, se financiará de acuerdo con lo determinen las respectivas leyes de Presupuestos del Sector Público.
		°°°°° Introducir la siguiente disposición transitoria, nueva: “Artículo octavo. Sobre los servicios	**Artículo octavo. Sobre los**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		esenciales. Hasta que no se dicten los respectivos decretos señalados en el artículo 4 de la ley, serán calificados como servicios esenciales para los efectos de esta ley, los servicios públicos de telecomunicaciones, incluyendo los servicios de transmisión de datos; los servicios de generación, transmisión y distribución eléctrica; los servicios sanitarios y de suministro de agua potable, excluyendo los servicios sanitarios rurales; los servicios bancarios y financieros; las prestaciones de salud, incluyendo cualquier institución pública o privada que realice tratamiento de datos personales de salud, salvo aquellos prestados por municipios o corporaciones municipales; los órganos de la administración del Estado, excluyendo a las municipalidades y gobernaciones provinciales y regionales; el Poder Judicial, y el Poder Legislativo. La Agencia identificará, mediante resolución exenta, los operadores de importancia vital que quedarán sujetos a las obligaciones establecidas en el artículo 6 de esta	**servicios esenciales. Hasta que no se dicten los respectivos decretos señalados en el artículo 4 de la ley, serán calificados como servicios esenciales para los efectos de esta ley, los servicios públicos de telecomunicaciones, incluyendo los servicios de transmisión de datos; los servicios de generación, transmisión y distribución eléctrica; los servicios sanitarios y de suministro de agua potable, excluyendo los servicios sanitarios rurales; los servicios bancarios y financieros; las prestaciones de salud, incluyendo cualquier institución pública o privada que realice tratamiento de datos personales de salud, salvo aquellos prestados por municipios o corporaciones municipales; los órganos de la administración del Estado, excluyendo a las municipalidades y gobernaciones provinciales y regionales; el Poder Judicial, y el Poder Legislativo. La Agencia identificará, mediante resolución exenta, los operadores de importancia vital que quedarán**

NORMATIVA VIGENTE	PROYECTO DE LEY APROBADO EN GENERAL POR EL SENADO	MODIFICACIONES INTRODUCIDAS POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICAS, UNIDAS	TEXTO PROPUESTO POR LAS COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS
		ley.”. **(Unanimidad 9x0. Indicación número 185).** **ooooo**	**sujetos a las obligaciones establecidas en el artículo 6 de esta ley.”.**