SENADO
REPÚBLICA DOMINICANA
Departamento Técnico de Revisión Legislativa

Santo Domingo de Guzmán D.N.
02 de noviembre de 2021

DETEREL 1181 /2021

A La : Comisión Permanente de **Transporte y Telecomunicaciones**

Vía : **Licda. Rosemary Cedeño Nieves**
Coordinadora de Comisiones Permanentes.

CC : **Lic. José Domingo Carrasco Estévez.**
Secretaria General Legislativa Interina.

De : **Welnel D. Féliz F.**
Director Departamento Técnico de Revisión Legislativa

Asunto : Informe adicional sobre el Proyecto de Ley sobre Gestión de la Ciberseguridad en la Republica Dominicana.

Referencia : Oficio No. 0000006962, del 29 de abril de 2021
(**Expediente No. 000636- 2021-PLO-SE)**

Luego de tomada en consideración la iniciativa de ley descrita en el asunto y enviada a la Comisión Permanente de Transporte y Telecomunicaciones en fecha, 24 de abril del año 2021, esta Dirección Técnica de Revisión Legislativa procedió a su análisis en los aspectos constitucional, legal y de la técnica legislativa, remitiendo a esta comisión de estudio sus ponderaciones al respecto y contenidas en el informe de referencia: DETEREL 388/2021.

No obstante, lo planteado en el indicado informe de DETEREL, los miembros de la Comisión decidieron acoger parcialmente las consideraciones de esta dirección técnica, aportando una redacción legislativa alterna, y acordaron realizar una redacción

alterna de la iniciativa legislativa 000636-2021-PLO-SE, tomando como base la redacción aportada por la comisión.

En tal virtud, esta dirección procedió a la realización de la referida redacción alterna, producto de sugerencias de este departamento técnico y de la propuesta legislativa alterna presentada por la comisión de estudio, en tal sentido, expondremos algunos puntos debatidos durante la celebración de las reuniones de estudio:

1. Los vistos o antecedentes legales fueron revisados y adecuados según paramentos dispuestos por la técnica legislativa, ordenándolos de manera jerárquica y por fecha, y colocando primero, su número seguido de la fecha y luego el titulo o nombre de la ley;

2. El nombre del órgano se modificó y pasó a nombrarse "Instituto Nacional de Ciberseguridad";

3. Las redacciones de las definiciones fueron revisadas, cuidando de que cada definición este contenida en el cuerpo de la norma y fueron colocadas en orden alfabético;

4. Este departamento técnico sugirió la adecuación de los principios que sustentan la ley o que sirven como guía de actuación en el ejercicio de la ley y que fueron propuestos por la comisión de estudio, ya que el contenido de los mismos no estaba redactado de acuerdo a los parámetros establecido por las reglas de técnica legislativa para este tipo de contenido en las leyes, no obstante, permanecieron con el mismo contenido sugeridos por la Comisión de estudio;

5. La estructura temática de la propuesta se dispuso en capítulos y secciones, colocando su nombre a cada una de ellas y agrupando y particularizando sus mandatos de forma homogéneos a partir del modelo adoptado por la Constitución de la República, y se colocaron los epígrafes con precisión y fidelidad a los contenidos de los artículos;

6. Las atribuciones del Instituto Nacional de Ciberseguridad, fueron adecuadas, pues el contenido presentado contenía atribuciones que pertenecen al Consejo Nacional de Ciberseguridad, y al director ejecutivo por la naturaleza de sus funciones;

7. El nombre del Consejo Nacional de Ciberseguridad fue homogenizado en toda la estructura de la parte normativa de la propuesta, pues en varias partes se leía "Consejo Directivo…";

8. Se le adicionaron normas de creación del Consejo Nacional de Ciberseguridad y de la Dirección Ejecutiva del Instituto Nacional de Ciberseguridad;

9. Varios de los articulos que integran esta propuesta de ley, fueron adecuados en su contenido, pues tenían faltas en su redacción que dificultaban su comprensión y en su contenido se visualizaban varias disposiciones encerradas en un mismo artículo, por lo que fueron divididas en párrafos con la finalidad de aportar más claridad a la norma;

10. En cuanto a régimen sancionatorio establecido en la propuesta:

10.1. La potestad sancionadora fue desarrollada conforme las sugerencias emitidas por este departamento técnico en su informe DETREL 388/2021;

10.2. Se estableció la degradación de las faltas administrativas en: leves, graves y muy graves y se indicaron sus respectivas sanciones;

10.3. Los articulos sobre recursos administrativos fueron creados y establecidos en articulos independientes, realizando diferencias entre los recursos a sanciones a los órganos y entres de naturaleza privada y a los a órganos y entes de naturaleza publica;

11. Se adecuó toda la parte relativa a las disposiciones finales de la ley según los elementos establecidos por la técnica legislativa.

Finalmente, del conjunto de los señalamientos precedentes y de las solicitudes de la Comisión Permanente de Transporte y Telecomunicaciones, esta Dirección Técnica de Revisión Legislativa realizó la siguiente redacción alterna:

Ley sobre Gestión de la Ciberseguridad en República Dominicana

Considerando primero: Que en noviembre de 2019 la República Dominicana se adhirió a los principios del Llamado de París para la Confianza y la Seguridad en el Ciberespacio;
Considerando segundo: Que la Resolución de la Asamblea General de las Naciones Unidas núm. A/70/174, del 22 de julio de 2015, sobre el Grupo de Expertos Gubernamentales y sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, estableció un grupo de normas voluntarias de comportamiento responsable de los Estados en el ciberespacio, cuyo fin es reducir los riesgos a la paz, seguridad y estabilidad internacional;

Considerando tercero: Que la Constitución dominicana en su artículo 7, establece: "La República Dominicana es un Estado Social y Democrático de Derecho, organizado en forma de República unitaria, fundada en el respeto de la dignidad humana, los derechos fundamentales, el trabajo, la soberanía popular y la separación e independencia de los poderes públicos.";

Considerando cuarto: Que en su artículo 8, la Constitución de la República consagra lo siguiente: "Es función esencial del Estado, la protección efectiva de los derechos de la persona, el respeto de su dignidad y la obtención de los medios que le permitan perfeccionarse de forma igualitaria, equitativa y progresiva, dentro de un marco de libertad individual y de justicia social, compatible con el orden público y el bienestar general y los derechos de todos y todas.";

Considerando quinto: Que el artículo 260 de la Constitución indica que: "Constituyen objetivos de alta prioridad nacional: 1) Combatir actividades criminales transnacionales que pongan en peligro los intereses de la República y de sus habitantes; 2) Organizar y sostener sistemas eficaces que prevengan o mitiguen daños ocasionados por desastres naturales y tecnológicos;

Considerando sexto: Que el artículo 63 de la Constitución se refiere al Derecho a la educación, y especifica que toda persona tiene derecho a una educación integral, de calidad, permanente, en igualdad de condiciones y oportunidades, así como de los centros educativos para incorporar el conocimiento y aplicación de las nuevas tecnologías y de sus innovaciones, por lo que constituye una necesidad inminente la gestión de ciberseguridad en el país;

Considerando séptimo: Que el artículo 6 de la Estrategia Nacional de Ciberseguridad al referirse al pilar sobre Marco Legal y Fortalecimiento Institucional establece como parte de su objetivo general el fortalecimiento del marco legal que incide en los temas relacionados con la ciberseguridad;

Considerando octavo: Que mediante el Decreto núm. 230-18, del 19 de junio de 2018, se estableció la Estrategia Nacional de Ciberseguridad 2018-2021 y se creó el Centro

Nacional de Ciberseguridad (CNCS), el cual figura como un órgano del Ministerio de la Presidencia de la República Dominicana y es necesario que sean fortalecidos su rol y facultades para que cuente con autonomía, personalidad jurídica propia, autonomía funcional, presupuestaria, administrativa, técnica y patrimonio propio, para que pueda regular su estructura y funcionamiento;

Considerando noveno: Que determinados entes reguladores han establecido normativas de ciberseguridad para sus correspondientes sectores, y que otros podrían hacerlo en el futuro y que, por tanto, las disposiciones establecidas en dichas normas deben aplicarse a los sectores regulados siempre y cuando las mismas contengan requisitos cuyos efectos sean, como mínimo, equivalentes a los de las obligaciones que establece esta ley;

Considerando décimo: Que para dar respuesta efectiva a las amenazas e incidentes de ciberseguridad es necesario establecer un marco nacional de ciberseguridad que norme la adopción de medidas para prevenirlos, gestionarlos y darles respuesta efectiva, así como regular los aspectos relativos a la ciberseguridad de las infraestructuras críticas a nivel nacional;

Considerando décimoprimero: Que, debido a la importancia de las infraestructuras críticas, para el bienestar nacional, es necesario que se establezcan obligaciones con la finalidad de salvaguardar la ciberseguridad y aumentar la ciberresiliencia a nivel nacional. Estas obligaciones comprenden deberes como entrega de información, notificación de incidentes, realización de auditorías de ciberseguridad y evaluaciones de riesgo, así como la ejecución de ejercicios de ciberseguridad periódicos;

Considerando decimosegundo: Que deben conferirse al Centro Nacional de Ciberseguridad las competencias necesarias para dar cumplimiento a esta ley, y en especial lo dispuesto en la Ley núm. 107-13, del 6 de agosto de 2013, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo; la Ley Núm. 41-08, del 16 de enero de 2008, de Función Pública y Crea la Secretaria de Estado de Administración Pública y la Ley núm. 13-07, del 5 de febrero de 2007, que Crea el Tribunal Contencioso Tributario y Administrativo;

Considerando decimotercero: Que la República Dominicana cuenta con el Equipo de Respuesta a Incidentes Cibernéticos (CSIRT-RD) que funge como el punto de contacto, a nivel nacional, para la prevención, detección y gestión de incidentes generados en los sistemas de información del Gobierno y en las infraestructuras críticas nacionales;

Considerando decimocuarto: Que el Centro Nacional de Ciberseguridad, y, en consecuencia, el Equipo de Respuesta a Incidentes Cibernéticos (CSIRT-RD), deben disponer de recursos técnicos, financieros y humanos adecuados para garantizar que puedan realizar de manera efectiva y eficiente las funciones que se les atribuyen esta ley;

Considerando decimoquinto: Que la cooperación entre los sectores público y privado es esencial para la ciberseguridad dado que la mayor parte de los sistemas de información son propiedad u operados por el sector privado. A tal fin, es esencial fomentar el intercambio de información, buenas prácticas y asesoramiento sobre aspectos relacionados con la ciberseguridad de los sistemas de información;

Considerando decimosexto: Que la información sobre incidentes de ciberseguridad tiene cada vez mayor utilidad para las empresas y para la población en general, es necesario que se ponga a disposición del público información general sobre los principales incidentes de ciberseguridad que afecten a los sistemas de información a nivel nacional, sin dejar de lado el respeto a las disposiciones sobre intercambio de información confidencial, y el carácter privado a la hora de divulgar información sobre los incidentes;

Considerando decimoséptimo: Que la investigación en materia de ciberseguridad es esencial debido a que muchos de los avances en el área provienen de los grandes esfuerzos de la comunidad de investigación y que dichos esfuerzos pueden ser menoscabados y, con ello, la propia seguridad, por conductas que inhiben la publicación y la divulgación de vulnerabilidades de ciberseguridad, resultando pertinente un régimen de divulgación responsable de vulnerabilidades basada en la buena fe y tomando en consideración las medidas necesarias para minimizar el daño que pueda causarse por tal divulgación;

Considerando decimoctavo: Que debido a la gravedad y peligro que algunos incidentes y amenazas cibernéticas representan para las infraestructuras críticas, y por tanto a los intereses de la República Dominicana, resulta necesario que los riesgos de seguridad cibernética sean considerados entre aquellos capaces de justificar la declaratoria de los estados de excepción previstos en la Constitución;

Considerando decimonoveno: Que esta ley observa los derechos y garantías fundamentales reconocidos por la Constitución de la República Dominicana, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído;

Considerando vigésimo: Que esta ley debe entenderse, sin perjuicio de que el Estado puede adoptar las medidas necesarias para fortalecer las infraestructuras tecnológicas para garantizar la protección de los intereses esenciales para su seguridad, preservar el orden público y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales;

Considerando vigesimoprimero: Que se hace imprescindible para el país, contar con un mecanismo que coadyuve a determinar qué sistemas de información cumplen los criterios para ser considerados infraestructuras críticas sobre los cuales se prestan servicios esenciales y contribuyan con la creación de una cultura de colaboración y confianza cibernética que integren y fortalezcan el ecosistema digital de la sociedad dominicana;

Vista: La Constitución de la República;

Vista: La Resolución núm. 20/8, del 5 de julio de 2012, sobre la Promoción, la Protección y el Disfrute de los Derechos Humanos en el Internet, del Consejo de Derechos Humanos de las Naciones Unidas;

Vista: La Resolución núm. 20/13, del 26 de junio de 2012, sobre la Promoción, la Protección y el Disfrute de los Derechos Humanos en el Internet, del Consejo de Derechos Humanos de las Naciones Unidas;

Vista: La Resolución núm. 68/167, del 18 de diciembre de 2013, sobre el Derecho a la Privacidad en la Era Digital, de la Asamblea General de las Naciones Unidas;

Vista: La Resolución núm. 69/166, del 18 de diciembre de 2014, sobre el Derecho a la Privacidad en la Era Digital, de la Asamblea General de las Naciones Unidas;

Vista: La Resolución de la Asamblea General de las Naciones Unidas A/68/98, del 24 de junio de 2013, Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional;

Vista: La Resolución de la Asamblea General de las Naciones Unidas A/70/174, del 22 de julio de 2015, 13º Congreso de las Naciones Unidas sobre Grupo de Expertos Gubernamentales y sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional;

Visto: El Llamamiento de París, del 12 de noviembre de 2018, para la Confianza y la Seguridad en el Ciberespacio;

Visto: El reporte final de la Comisión Global sobre la Estabilidad en el Ciberespacio (GCCS), de noviembre de 2019;

Vista: La Ley núm. 200-04, del 28 de julio de 2004, Ley General de Libre Acceso a la Información Pública;

Vista: La Ley núm. 13-07, del 5 de febrero de 2007, que crea el Tribunal Contencioso Tributario y Administrativo;

Vista: La Ley núm. 53-07, del 23 de abril de 2007, sobre Crímenes y Delitos de Alta Tecnología;

Vista: La Ley núm. 41-08, del 16 de enero de 2008, de Función Pública y Crea la Secretaría de Estado de Administración Pública;

Vista: La Ley núm. 1-12, del 25 de enero de 2012, que establece la Estrategia Nacional de Desarrollo 2030;

Vista: La Ley núm. 247-12, del 9 de agosto de 2012, Ley Orgánica de la Administración Pública;

Vista: La Ley núm. 107-13, del 6 de agosto de 2013, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo;

Vista: El Decreto núm. 134 -14, del 9 de abril de 2014, que dicta el Reglamento de Aplicación de la Ley Orgánica No. 1-12, que establece la Estrategia Nacional de Desarrollo de la República Dominicana 2030;

Visto: El Decreto núm. 230-18, del 19 de junio de 2018, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021.

HA DADO LA PRESENTE LEY:

CAPÍTULO I
DEL OBJETO, ÁMBITO DE APLICACIÓN, DEFINICIONES Y PRINCIPIOS DE LA LEY

Artículo 1.- Objeto. Esta ley tiene por objeto fortalecer el marco normativo para la gestión de la seguridad cibernética de las infraestructuras de tecnologías de la información y comunicación de la Administración Pública y de las infraestructuras críticas en la República Dominicana.

Artículo 2.- Ámbito de aplicación. Esta ley es aplicable en todo el territorio nacional y regula a toda persona física o jurídica, pública o privada, nacional o extranjera, ubicada total o parcialmente en la República Dominicana, que gestione sistemas de información cuyo funcionamiento es indispensable para la operación de una infraestructura crítica nacional o para la operación de las infraestructuras de tecnologías de la información y comunicación de la Administración Pública.

Párrafo. Los principios y reglas de esta ley son aplicables para los órganos que ejercen función o actividad de naturaleza administrativa en los poderes legislativo y judicial, y a los órganos y entes de rango constitucional, siempre que resulten compatibles con su normativa específica, no desvirtúen la naturaleza, la independencia y las funciones que la Constitución les otorga, garantizando la separación de los poderes.

Artículo 3.- Definiciones. Para los fines de esta ley se entiende por:

1) **Amenaza:** Es la actividad, conocida o sospechada, que, de producirse, tendría o podría tener un efecto adverso sobre la ciberseguridad de una o más infraestructuras críticas o alguno de sus componentes, incluyendo sistemas informáticos complementarios o accesorios;

2) **Ciberseguridad:** Se refiere al estado y al conjunto de prácticas orientadas a mantenerlo, en el que un activo, sistema de información o servicio tecnológico de información y comunicación reúne las siguientes condiciones:

   1) Si está protegido contra acceso no autorizado;
   2) Si se mantiene disponible y operativo;
   3) Si se mantiene la integridad del activo, sistema o servicio; y
   4) Si se mantiene la integridad y confidencialidad de la información almacenada, procesada o transmitida a través del sistema de información.

3) **Evento**: Es cualquier ocurrencia observable en un sistema, red o activo tecnológico;

4) **Incidente**: Es todo evento que tenga o inminentemente pueda tener un efecto adverso sobre la ciberseguridad de una o más infraestructuras críticas, de alguno de sus componentes, de la información procesada, almacenada o transmitida por esta, o que constituye una violación o amenaza inminente de violación de las políticas o procedimientos de ciberseguridad vigentes o de las políticas de uso aceptable;

5) **Indicadores de Compromiso**: Son todas aquellas informaciones relevantes que describen cualquier incidente de ciberseguridad, evento, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento;

6) **Ingeniería Social**: Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas;

7) **Operador:** Es la entidad u organismo responsable del funcionamiento de una infraestructura crítica. En los casos donde la infraestructura crítica es propiedad conjunta de más de una persona u operada por más de una entidad, incluye a cada operador de manera individual o en su conjunto. Cuando una infraestructura crítica es propiedad del Gobierno y es operada por alguna instancia pública, privada o cualquier otro tipo de organismo, éste será tratado como el operador de la infraestructura crítica para los fines de esta ley;

8) **Servicio esencial:** Es todo servicio que resulte ser necesario para la seguridad nacional, defensa, relaciones exteriores, economía, salud, seguridad u orden público de República Dominicana;

9) **Sistema de Información:** Es todo dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitando, los sistemas electrónicos, informáticos, telemáticos y de telecomunicaciones que, separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros. Hace referencia a cualquier sistema de tecnología de la información o cualquier sistema de tecnología operacional como un sistema de control industrial, un controlador lógico programable, un sistema de control de supervisión y adquisición de datos, o un sistema de control distribuido;

10) **Vinculación con un operador de infraestructura critica:** Se refiere a que una persona es funcionaria, empleada o suplidora de un operador de una infraestructura crítica. En el caso de sistemas de información, esta vinculación alude a que estos son propiedad de o son manejados por funcionarios y empleados del operador de una infraestructura crítica o que son utilizados para suplir un servicio a éste;

11) **Vulnerabilidad:** Es cualquier debilidad en un sistema de información, sus procedimientos de seguridad, su implementación o en sus controles internos, que podrían permitir la materialización de una amenaza;

Artículo 4.- Principios. Para los fines de aplicación de esta ley, se reconocen los principios incluidos en el Llamado de París, del 12 de noviembre de 2018, para la Confianza y la Seguridad en el Ciberespacio; los principios del reporte final de la Comisión Global sobre la Estabilidad en el Ciberespacio (GCCS), de noviembre de 2019; y, en adición, se establecen los siguientes principios:

1) **Colaboración.** La República Dominicana colaborará en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el uso de las tecnologías de información y comunicación y evitar las prácticas en la esfera de estas tecnologías que se consideran que son perjudiciales o que pueden poner en peligro la paz y la seguridad tanto nacional como internacional.

2) **Prevención de actividades Ilícitas.** La República Dominicana hará sus mayores esfuerzos para evitar que su territorio sea utilizado para la comisión de hechos ilícitos que tengan repercusiones nacionales o internacionales mediante la utilización de las tecnologías de información y comunicación.

3) **Intercambio de Información.** La República Dominicana cooperará con otros Estados para intercambiar información, prestar asistencia mutua, entablar acciones penales por el uso de las tecnologías de información y comunicación con fines delictivos o terroristas y aplicar otras medidas de cooperación para hacer frente a las amenazas e incidentes de ciberseguridad.

4) **Protección de los Derechos Humanos.** La República Dominicana, contribuirá en garantizar la utilización segura de las tecnologías de información y comunicación, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión, y en consecuencia, respeta lo dispuesto por las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos de las Naciones Unidas sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General de las Naciones Unidas sobre el derecho a la privacidad en la era digital.

5) **Protección de las Infraestructuras Críticas.** La República Dominicana no realizará ni apoyará de forma deliberada actividades en la esfera de las tecnologías de información y comunicación contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañen intencionalmente infraestructuras críticas que prestan servicios al público o dificulten de otro modo su utilización y funcionamiento.

6) **Solicitudes de Asistencia.** La República Dominicana atenderá las solicitudes de asistencia de otros Estados cuyas infraestructuras críticas fueren objeto de actos malintencionados relacionados con las tecnologías de información y comunicación.

También atenderá las solicitudes para mitigar toda actividad malintencionada relacionada con las tecnologías de información y comunicación originada en su territorio contra infraestructuras críticas de otro Estado, teniendo siempre en cuenta la soberanía de todos los Estados involucrados.

7) **Cadena de Suministro.** La República Dominicana deberá adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro con miras a que los usuarios finales confíen en la seguridad de los productos relacionados con las tecnologías de información y comunicación. Asimismo, el país deberá hacer sus mayores esfuerzos para evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las tecnologías de información y comunicación, así como el uso de funciones ocultas y dañinas.

8) **Divulgación Responsable de las Vulnerabilidades.** La República Dominicana deberá alentar la divulgación responsable de las vulnerabilidades relacionadas con las tecnologías de información y comunicación y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para estas tecnologías o a infraestructuras dependientes de ellas.

CAPÍTULO II
DEL INSTITUO NACIONAL DE CIBERSEGURIDAD

SECCIÓN I
DE LA CREACIÓN

Artículo 5.- Creación del Instituto Nacional de Ciberseguridad. Se crea el Instituto Nacional de Ciberseguridad, adscrito al Ministerio de la Presidencia, como un ente derecho público con personalidad jurídica, autonomía funcional, presupuestaria, administrativa, técnica y patrimonial.

Párrafo. El Ministerio de la Presidencia ejercerá el respectivo control de tutela sobre el Instituto Nacional de Ciberseguridad, con el propósito de ejercer la supervisión necesaria y garantizar su adecuado funcionamiento y organización bajo el principio de unidad de la Administración Pública.

Artículo 6.- Sede. El Instituto Nacional de Ciberseguridad tendrá su sede en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, con jurisdicción nacional, pudiendo establecerse a todas las dependencias que resulten necesarias para el buen desarrollo y funcionamiento del servicio, de acuerdo con la disponibilidad presupuestaria de la entidad.

Artículo 7.- Misión. El Instituto Nacional de Ciberseguridad tiene por misión velar por la seguridad cibernética de las infraestructuras de tecnologías de la información y comunicación de la Administración Pública, y de las infraestructuras críticas de la República Dominicana, en cumplimiento de los mandatos previstos en esta ley y su reglamentación, y en coordinación con los entes reguladores sectoriales competentes.

Artículo 8.- Atribuciones. El Instituto Nacional de Ciberseguridad tiene las siguientes atribuciones:

1) La identificación y designación de las infraestructuras críticas nacionales, de conformidad con esta ley y su reglamentación;

2) Emitir directrices y normas técnicas para el fortalecimiento y gestión de la ciberseguridad sobre los asuntos previstos en esta ley y su reglamentación, y supervisar su cumplimiento;

3) Establecer sistemas y mecanismos de alertas ante vulnerabilidades, amenazas e incidentes de ciberseguridad en las infraestructuras de tecnologías de la información y comunicación de la Administración Pública;

4) Establecer la Estrategia Nacional de Ciberseguridad, así como coordinar y evaluar su implementación y revisión periódica;

5) Promover la creación de laboratorios de investigación en temas de ciberseguridad;

6) Promover la creación de redes de cooperación entre los sectores público, privado, academia y sociedad para la difusión y promoción de la ciberseguridad;

7) Fomentar el desarrollo de capacidades y buenas prácticas en materia de ciberseguridad, así como la creación de equipos sectoriales de respuesta a incidentes (CSIRT sectoriales), con los cuales mantendrá una estrecha colaboración y coordinación;

8) Crear inteligencia de amenazas en base a información de alertas e incidentes de ciberseguridad de las entidades de su comunidad atendida, y distribuirla a los CSIRT sectoriales y demás partes interesadas;

9) Establecer y mantener un vínculo fluido y una relación colaborativa con otros organismos nacionales e internacionales de similar naturaleza; y

10) Apoyar, propiciar y liberar la creación de redes de cooperación entre las instituciones públicas, organizaciones académicas, de la sociedad civil, y entidades privadas para el impulso de la Estrategia Nacional de Ciberseguridad.

Párrafo. El Instituto Nacional de Ciberseguridad ejercerá sus atribuciones en coordinación con los entes reguladores sectoriales de ciberseguridad.

Artículo 9.- Emisión de políticas y normas técnicas. El Instituto Nacional de Ciberseguridad podrá establecer políticas y normas técnicas para el fortalecimiento y gestión de la ciberseguridad, en lo siguiente:

1) El diseño, la configuración, la seguridad y las operaciones de una infraestructura crítica;

2) Las responsabilidades y deberes del operador de una infraestructura crítica;

3) La delimitación de los cambios y tipos de cambios que se considerarán cambios sustanciales de una infraestructura crítica, y el procedimiento para su notificación al Instituto Nacional de Ciberseguridad;

4) La delimitación de los incidentes y tipos de incidentes de ciberseguridad de una infraestructura crítica, y el procedimiento para su notificación al Instituto Nacional de Ciberseguridad;

5) Los requisitos y la forma de llevar a cabo las auditorías de ciberseguridad y las evaluaciones de riesgo cibernético que debe llevar a cabo el operador de una infraestructura crítica;

6) La forma y naturaleza de los ejercicios de ciberseguridad que se pueden realizar;

7) Las facultades y el procedimiento para prevenir e investigar los incidentes de ciberseguridad;

8) Las medidas correctivas que se deben tomar para dar respuesta a las amenazas e incidentes de ciberseguridad; y

9) Todos los demás asuntos que sean expresamente establecidos en la reglamentación de esta ley.

Párrafo I. En el caso de infraestructuras críticas que pertenezcan a sectores regulados, las directrices y normas técnicas emitidas por el Instituto Nacional de Ciberseguridad deberán ser refrendadas por los entes y órganos reguladores sectoriales competentes.

Párrafo II. Las políticas y normas técnicas referidas en este artículo, serán de cumplimiento obligatorio para todos los entes y órganos de la administración pública central, en el ámbito del Poder Ejecutivo.

Párrafo III. Los entes y órganos son responsables de la prevención, detección, respuesta y recuperación de los incidentes de ciberseguridad que pudieren afectarlos.

SECCIÓN II
DEL CONSEJO NACIONAL DE CIBERSEGURIDAD

Artículo 10.- Creación del Consejo Nacional de Ciberseguridad. Se crea el Consejo Nacional de Ciberseguridad, como órgano colegiado y máxima autoridad del Instituto Nacional de Ciberseguridad encargado de establecer y orientar las políticas para la gestión de la cibernética de las infraestructuras de tecnologías de la información y comunicación de la Administración Pública y de las infraestructuras críticas en la República Dominicana.

Artículo 11.- Integración. El Consejo Nacional de Ciberseguridad está integrado por:

1) El ministro de la Presidencia, quien lo preside;

2) El ministro de Relaciones Exteriores;

3) El ministro de Defensa;

4) El ministro de Interior y Policía;

5) El ministro de Turismo;

6) El Procurador General de la República;

7) El Gobernador del Banco Central de la República Dominicana;

8) El director general de la Policía Nacional;

9) El director del Departamento Nacional de Investigaciones;

10) El presidente del Consejo Directivo del Instituto Dominicano de las Telecomunicaciones; y

11) El director de la Oficina Gubernamental de Tecnologías de la Información y Comunicación.

Párrafo I. El director ejecutivo del Instituto Nacional de Ciberseguridad ejercerá la secretaría del Consejo Nacional de Ciberseguridad, con voz, pero sin voto
Párrafo II. Los miembros del Consejo Nacional de Ciberseguridad podrán hacerse representar por un funcionario de jerarquía inmediatamente inferior, quienes deberán ser designados mediante comunicación dirigida al ministro de la Presidencia, en su calidad de presidente del Consejo.

Párrafo III. El Consejo Nacional de Ciberseguridad podrá invitar a participar en sus reuniones a representantes de los poderes del Estado, de otros entes u órganos, así como a otras personas y representantes de organizaciones, públicas o privadas, pero en ningún caso, los invitados podrán participar en las deliberaciones del Consejo.

Párrafo IV. El Consejo Nacional de Ciberseguridad tendrá un sub-consejo técnico, integrado por un representante de cada una de las entidades que forman parte de este Consejo Nacional de Ciberseguridad, y quienes serán designados mediante comunicación dirigida al ministro de la Presidencia, en su calidad de presidente del Consejo, cuyas atribuciones serán establecidas por reglamento.

Articulo 12.- Convocatoria. El Consejo Nacional de Ciberseguridad será convocado por escrito, por su presidente, y sesionará de forma ordinaria la primera semana de cada trimestre, y extraordinaria, todas las veces que se requiera.

Párrafo. - En caso de fuerza mayor o circunstancias imprevistas, el Consejo Nacional de Ciberseguridad puede ser convocado por la mitad más uno de sus miembros.

Artículo 13.- Cuórum. El Consejo Nacional de Ciberseguriodad podrá deliberar válidamente, con la mitad más uno de sus miembros.

Artículo 14.- Decisiones. Las decisiones se toman por mayoría de votos, entendiéndose esto por más de la mitad de los votos de los miembros presentes en la reunión.

Párrafo. En caso de empate, el presidente tendrá el voto decisivo.

Artículo 15.- Atribuciones. El Consejo Nacional de Ciberseguridad tendrá las siguientes atribuciones:

1) Aprobar la Estrategia Nacional de Ciberseguridad, su evaluación y actualización periódica, elaborada y presentada por el director ejecutivo;

2) Aprobar las designaciones, mediante resolución motivada, de las infraestructuras críticas nacionales, sometidas por el director ejecutivo;

3) Dictar las directrices y normas técnicas que correspondan;

4) Aprobar los reglamentos internos de la institución, elaborados por el director ejecutivo;

5) Aprobar la estructura orgánica, funcional y de cargos de la institución, elaborados por el director ejecutivo;

6) Aprobar el Plan Estratégico Institucional y el Plan Operativo Anual, elaborados por el director ejecutivo;

7) Aprobar el presupuesto de la institución y los informes de ejecución presupuestaria elaborados por el director ejecutivo;

8) Aprobar las memorias y balances anuales elaborados por el director ejecutivo;

9) Definir políticas, establecer directrices y elaborar propuestas de estrategias y planes de acción para el desarrollo de la Estrategia Nacional de Ciberseguridad, a fin de que las entidades y academias a las que correspondan su ejecución puedan gestionar los proyectos conforme a tales directrices.

SECCIÓN III
DE LA DIRECCION EJECUTIVA

Artículo 16.- Dirección Ejecutiva. Se crea la Dirección Ejecutiva del Instituto Nacional de Ciberseguridad, como instancia técnica y de representación legal del Instituto.

Artículo 17.- Director ejecutivo. El Instituto Nacional de Ciberseguridad tendrá como máximo funcionario administrativo al director ejecutivo, el cual deberá cumplir con los siguientes requisitos:

1) Ser ciudadano dominicano y en pleno ejercicio de sus derechos civiles y políticos;

2) Ser profesional de ingeniería en tecnologías de la información y sistemas, derecho, economía o áreas afines, con estudios especializados en alguna de las siguientes disciplinas: seguridad de la información, ciberseguridad, políticas públicas, gestión de riesgo;

3) Tener experiencia por más de diez años en el ejercicio profesional de alguna de las áreas señaladas en el numeral 2 de este artículo;

4) Tener experiencia gerencial comprobada.

Artículo 18.- Impedimentos. No podrán ser designados como director ejecutivo del Instituto Nacional de Ciberseguridad, las siguientes personas:

1) Las personas que estuvieren sub júdice, o cumpliendo condena o que hayan sido condenadas a penas aflictivas o infamantes; y

2) Las personas que hayan sido jurídicamente incapacitadas o declaradas interdictos.

Artículo 19.- Designación. El director ejecutivo será nombrado por el Poder Ejecutivo por un período de dos (2) años, el cual podrá ser ratificado hasta dos (2) períodos adicionales consecutivos.

Artículo 20.-Causales. El director ejecutivo podrá ser removido en sus funciones, por cualquiera de las causas siguientes:

1) Cuando por incapacidad física no hubiere podido desempeñar su cargo durante seis (6) meses;

2) Por condena a pena privativa de libertad;

3) Cuando se demostrare negligencia manifiesta en el cumplimiento de sus funciones, en caso de incumplimiento evidente de los objetivos del INCS o en el caso de que, sin debida justificación, deje de cumplir las obligaciones que le corresponden, de acuerdo con la ley y su reglamentación;

4) Cuando viole la obligación de confidencialidad establecida en la ley;

5) Cuando no se inhiba en los casos en los que debiere hacerlo; y

6) Cuando fuere responsable de actos u operaciones fraudulentas, ilegales o evidentemente opuestas a los fines e intereses de la institución, siempre que dicha

responsabilidad haya sido retenida en virtud de una decisión definitiva e irrevocable.

Párrafo. Las causales que dan lugar a la remoción del director ejecutivo serán presentadas por oficio dirigido al presidente del Consejo Nacional de Ciberseguridad, por recomendación, de al menos, dos terceras partes de sus integrantes.

Artículo 21.- Atribuciones. El director ejecutivo del Instituto Nacional de Ciberseguridad tendrá las siguientes atribuciones:

1) Ejercer la secretaría del Consejo Nacional de Ciberseguridad;

2) Cumplir y hacer cumplir las disposiciones de esta ley y su reglamentación, asegurando la correcta aplicación de sus principios y disposiciones;

3) Orientar, dirigir, coordinar, supervisar y controlar el ejercicio de las atribuciones del Instituto Nacional de Ciberseguridad cuya facultad no esté expresamente asignada al Consejo Nacional en esta ley y su reglamentación;

4) Representar legalmente al Instituto Nacional de Ciberseguridad, ante terceros y en justicia, pudiendo en tal calidad firmar válidamente toda clase de contratos y documentos;

5) Elaborar y proponer al Consejo Nacional de Ciberseguridad del Instituto Nacional de Ciberseguridad el proyecto de Estrategia Nacional de Ciberseguridad y coordinar su implementación y evaluación;

6) Dirigir el proceso administrativo para la identificación y designación de las infraestructuras críticas nacionales;

7) Llevar un registro centralizado de las vulnerabilidades, amenazas e incidentes de ciberseguridad;

8) Recomendar al Poder Ejecutivo sobre iniciativas, proyectos y programas, de carácter general, para el fortalecimiento y gestión de la ciberseguridad en el país;

9) Velar por la coordinación entre el CSIRT-RD y los entes u órganos reguladores sectoriales competentes, con los CSIRT sectoriales, si los hubiese, y con los operadores de infraestructuras críticas nacionales, según

corresponda, en la prevención, detección, investigación y respuesta a vulnerabilidades, amenazas e incidentes de ciberseguridad;

10) Elaborar y proponer al Consejo Nacional de Ciberseguridad iniciativas, directrices y normas técnicas que corresponda dictar al Instituto Nacional de Ciberseguridad;

11) Elaborar y proponer al Consejo Nacional de Ciberseguridad los proyectos de reglamentos internos de la institución;

12) Elaborar y proponer al Consejo Nacional de Ciberseguridad los proyectos de estructura orgánica, funcional y de cargos de la institución;

13) Nombrar y remover a los servidores públicos del Instituto Nacional de Ciberseguridad, de acuerdo con las leyes y los procedimientos que rigen la materia;

14) Elaborar y proponer al Consejo Nacional de Ciberseguridad el Plan Estratégico Institucional y el Plan Operativo Anual;

15) Elaborar y proponer al Consejo Nacional los proyectos de presupuesto de la institución y dirigir y supervisar la ejecución presupuestaria;

16) Elaborar y proponer al Consejo Nacional de Ciberseguridad las memorias y balances anuales;

17) Contratar para la institución los servicios profesionales y técnicos, de acuerdo a las leyes y los procedimientos que rigen la materia;

18) Gestionar las asignaciones presupuestarias y otros recursos financieros necesarios para el funcionamiento de la institución;

19) Realizar todas las gestiones que considere necesarias ante los organismos internacionales, para procurar la cooperación y el desarrollo e implementación de proyectos acorde con objetivos e intereses de la institución;

20) Ejercer las demás funciones que le encomiende esta ley, su reglamentación y el Consejo Nacional del Instituto Nacional de Ciberseguridad; y

21) Coordinar la realización de análisis forenses de incidentes de ciberseguridad en infraestructuras críticas nacionales que no constituyan crimen o delito.

Artículo 22.- Equipo Nacional de Respuesta a Incidentes Cibernéticos. El Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) es una unidad operativa que funcionará bajo la supervisión del director ejecutivo del Instituto Nacional de Ciberseguridad.

Párrafo I. El CSIRT-RD tendrá por objeto la identificación, detección, protección, respuesta y recuperación de incidentes de ciberseguridad generados en las infraestructuras críticas nacionales y en los activos, sistemas y servicios de tecnología de la información y comunicación de los entes y órganos de la Administración Pública.

Párrafo II. En el ejercicio de sus funciones, el CSIRT-RD coordinará con los entes u órganos reguladores sectoriales competentes, con los CSIRT sectoriales, con los operadores de infraestructuras críticas y con los demás entes y órganos de la Administración Pública, así como con organismos nacionales e internacionales de naturaleza similar.

CAPÍTULO III
DE LAS INFRAESTRUCTURAS CRÍTICAS Y DE LOS INCIDENTES DE CIBERSEGURIDAD DE IMPACTO SIGNIFICATIVO

SECCIÓN I
DE LAS INFRAESTRUCTURAS CRÍTICAS

Artículo 23.- Designación como infraestructura crítica. La designación de las infraestructuras críticas nacionales se hará mediante acto administrativo emitido por el Consejo Nacional de Ciberseguridad, previa realización de un análisis de riesgo de aquellos activos y sistemas de información, cuyo funcionamiento y ciberseguridad, a juicio del Consejo Nacional de Ciberseguridad , del ente u órgano regulador sectorial competente y del operador del activo del sistema o servicio de que se trate, se considere indispensable para la disponibilidad y prestación continua de un servicio esencial en el país.

Párrafo I. La reglamentación de esta ley establecerá el procedimiento administrativo para la designación como infraestructura crítica, en el marco del cual se realizará el análisis de riesgo correspondiente.

Párrafo II. El acuerdo de inicio de dicho procedimiento administrativo deberá ser debidamente motivado y será emitido por el Ministro de la Presidencia, en su condición de presidente del Consejo Nacional de Ciberseguridad.

Párrafo III. El acuerdo de inicio del procedimiento administrativo para la designación como infraestructura crítica, será notificado por el ente u órgano regulador sectorial correspondiente o por el Instituto Nacional de Ciberseguridad, en aquellos sectores donde no exista dicho ente u órgano regulador sectorial, a toda persona que reúna los criterios para ser designada como operador de infraestructura crítica, quien proporcionará a su ente regulador sectorial o en su defecto al Instituto Nacional de Ciberseguridad, la información relacionada con el activo, sistema o servicio tecnológico de información y comunicación, conforme a lo establecido en la reglamentación de esta ley.

Párrafo IV. La entrega de informaciones al Instituto Nacional de Ciberseguridad y a los entes y órganos reguladores sectoriales competentes en cumplimiento de esta disposición, no será considerada como una vulneración de la confidencialidad previamente establecida por leyes, reglamentos, contratos o códigos de conducta profesionales.

Párrafo V. La reglamentación de esta ley establecerá el contenido mínimo de la resolución de designación como infraestructura crítica nacional, la cual, en todos los casos, deberá ser debidamente motivada e incluir la descripción precisa del activo, sistema o servicio tecnológico de información y comunicación designado como infraestructura crítica, la identificación precisa de la persona designada como operador y la indicación de las vías y plazos para recurrir dicha decisión.

Artículo 24.- Duración de la designación de una infraestructura crítica. La designación como infraestructura crítica, así como la designación de su operador, tendrá una duración de cinco (5) años, contados a partir del día siguiente al que fuera notificada.

Párrafo I. El Instituto Nacional de Ciberseguridad, de oficio o a instancia de parte interesada, podrá iniciar el procedimiento administrativo para retirar la designación como infraestructura crítica, cuando existan elementos suficientes para determinar que el activo, sistema o servicio tecnológico de información y comunicación ya no cumple con los criterios para ser considerado como infraestructura crítica.

Párrafo II. A más tardar ocho (8) meses antes del término de la designación como infraestructura crítica, el Instituto Nacional de Ciberseguridad iniciará de oficio, junto a los entes y órganos reguladores sectoriales competentes, la elaboración de un estudio de análisis de riesgo para determinar si el activo, sistema o servicio tecnológico de información y comunicación, sigue cumpliendo con los criterios para ser considerado como infraestructura crítica.

Párrafo III El costo del estudio de análisis de riesgo y la preparación de la documentación correspondiente establecido en el párrafo II de este artículo, será asumido por el operador de la infraestructura crítica en cuestión.

Artículo 25.- Notificación de cambios. En un plazo de siete (7) días, el operador de una infraestructura crítica notificará al Instituto Nacional de Ciberseguridad, al ente u órgano regulador sectorial competente y, si lo hubiese, al CSIRT sectorial, todos los cambios sustanciales realizados en el diseño, la configuración, la seguridad o el funcionamiento de dicha infraestructura.

Párrafo I. Un cambio se considerará sustancial si afecta o puede afectar la ciberseguridad de la infraestructura crítica o la capacidad del operador de la infraestructura crítica para responder a una amenaza o incidente de ciberseguridad que afecte a dicha infraestructura crítica.

Párrafo II. Los cambios en la propiedad legal o en beneficio de una infraestructura crítica, incluida cualquier parte de dicha propiedad, los cambios en el control efectivo sobre dicha infraestructura y los cambios en la capacidad y los derechos para hacer cambios a estas, se reputarán cambios sustanciales.

Artículo 26.- Punto de contacto único. El operador de una infraestructura crítica notificará al Instituto Nacional de Ciberseguridad, al ente u órgano regulador sectorial competente o, si lo hubiese, al CSIRT sectorial, la designación de su oficial de seguridad o quien haga las funciones de éste, qué servirá como punto de contacto único entre la infraestructura crítica y el CSIRT-RD y el CSIRT sectorial, según corresponda.

Artículo 27.- Auditorías de ciberseguridad y evaluaciones de riesgo de infraestructuras críticas. El operador de una infraestructura crítica deberá:

1) Realizar de forma continua evaluaciones de riesgo cibernético de la infraestructura crítica y presentar reportes de resultados de dichas evaluaciones al menos una vez al año o con la frecuencia que en su caso particular le indique el Instituto Nacional de Ciberseguridad; y

2) Llevar a cabo auditorías sobre su cumplimiento con esta ley, su reglamentación y los estándares de ciberseguridad aplicables definidos por el Instituto Nacional de Ciberseguridad, al menos una vez cada dos (2) años, o con la frecuencia que le indique el Instituto Nacional de Ciberseguridad o el ente u órgano regulador sectorial competente, según corresponda. Esta auditoría deberá ser realizada por un auditor elegible, de conformidad a lo establecido en el párrafo IV del artículo 28.

Articulo 28.- Informe resultante. El operador de la infraestructura crítica, a más tardar treinta (30) días después de la finalización de la auditoría o la evaluación del riesgo cibernético, proporcionará una copia del informe resultante de la auditoría o evaluación al ente u órgano regulador sectorial competente, y en caso de que no hubiese, al Instituto Nacional de Ciberseguridad.

Párrafo I. El ente u órgano regulador sectorial competente deberá enviar copia del informe de auditoría o evaluación establecida en este artículo, al Instituto Nacional de Ciberseguridad.

Párrafo II. Cuando el informe resultante de una auditoría evidencie que cualquier aspecto de la auditoría no se llevó a cabo de manera satisfactoria, de conformidad con los criterios mínimos establecidos en la reglamentación correspondiente, el ente u órgano regulador sectorial competente, o en caso de que no lo hubiese, el Instituto Nacional de Ciberseguridad, podrá ordenar de nuevo al operador de la infraestructura crítica que haga que el auditor lleve a cabo ese aspecto de la auditoría. El ente u órgano regulador sectorial competente deberá enviar copia de dicho informe al Instituto Nacional de Ciberseguridad.

Párrafo III. Cuando el informe resultante de una auditoría evidencie hallazgos de no conformidad, el ente u órgano regulador sectorial competente, o en caso de que no lo hubiese, el Instituto Nacional de Ciberseguridad, podrá ordenar al operador de la infraestructura crítica que lleve a cabo los planes de acción o remediación requeridos para solventar dichos hallazgos, de conformidad con la reglamentación correspondiente.

Párrafo IV. El Instituto Nacional de Ciberseguridad definirá un banco de entidades de auditoría elegibles, a partir de un marco de calificaciones o criterios claramente definidos en función de niveles de experiencias, credenciales, reputación, certificaciones, y otros indicadores afines, a los fines de asegurar las capacidades requeridas y necesarias para dar cumplimiento a esta ley.

Artículo 29.- Otros casos en los que se podrá ordenar auditorías. El Instituto Nacional de Ciberseguridad o el ente u órgano regulador sectorial competente, según corresponda, podrá ordenar una auditoría de una infraestructura crítica en los siguientes casos:

1) Si el operador de una infraestructura crítica no ha cumplido con una disposición de esta ley, sus reglamentos o los estándares de ciberseguridad aplicables; y

2) Si la información proporcionada por el operador de una infraestructura crítica de conformidad con esta ley es falsa, engañosa, inexacta o incompleta.

Artículo 30.- Costo de la auditoria. La auditoría será realizada por un auditor designado por el Instituto Nacional de Ciberseguridad o el ente u órgano regulador sectorial competente, según corresponda, y su costo será asumido por el operador de la infraestructura crítica.

Párrafo. Si el operador de una infraestructura crítica realiza un cambio sustancial en el diseño, la configuración, la seguridad o el funcionamiento de dicha infraestructura, el Instituto Nacional de Ciberseguridad o el ente u órgano regulador sectorial competente, según corresponda, podrá ordenar al operador que realice otra auditoría o evaluación de riesgo.

Artículo 31.- Ejercicios de ciberseguridad. El Instituto Nacional de Ciberseguridad, el ente u órgano regulador sectorial competente o, si los hubiere, el CSIRT sectorial, según corresponda, realizará ejercicios de ciberseguridad de manera rutinaria, con el fin de probar el estado de listeza de los operadores de diferentes infraestructuras críticas para responder a incidentes de ciberseguridad importantes.

Párrafo I. Es obligación del operador de una infraestructura crítica, participar en los ejercicios de ciberseguridad, a solicitud de Instituto Nacional de Ciberseguridad, del órgano regulador sectorial competente o, si los hubiere, del CSIRT sectorial, según corresponda.

Párrafo II. El Instituto Nacional de Ciberseguridad deberá crear y mantener actualizado un manual con políticas o procedimientos donde describa el alcance, los tipos de ejercicios, los requerimientos, los indicadores a medir, la frecuencia con la que se realizaran estos ejercicios y esquemas de planificación relacionados.

SECCIÓN II
DE LOS INCIDENTES DE CIBERSEGURIDAD DE IMPACTO SIGNIFICATIVO

Artículo 32.- Incidentes de ciberseguridad de impacto significativo. Se considerará que un incidente de ciberseguridad tiene un impacto significativo si cumple al menos una de las siguientes condiciones:

1) El impacto del incidente de ciberseguridad es, al menos, grave de acuerdo con el grado de consecuencias determinado en la evaluación del riesgo realizada en el marco de lo establecido en los artículos 23, 24 y 33;

2) Debido al incidente de ciberseguridad, la prestación del servicio esencial no puede continuar después de haber pasado el tiempo máximo permitido de interrupción del

servicio, de conformidad con el acuerdo de nivel de servicio pertinente o los requerimientos para la continuidad del servicio;

3) La continuidad del servicio de algún otro proveedor de servicio esencial se interrumpe debido al incidente de ciberseguridad;

4) Para la solución del incidente de ciberseguridad se requiere aplicar alguna de las medidas extraordinarias establecidas en la evaluación del riesgo realizada en el marco de lo establecido en los artículos 23, 24 y 33, o en otro documento, si los hubiere, que describa el restablecimiento de la continuidad del servicio o la seguridad del sistema de información; y

5) Los servicios que ofrece la infraestructura crítica, o el proveedor de otro servicio o usuarios del servicio sufren o puede sufrir daños significativos debido al incidente de ciberseguridad.

Artículo 33.- Deber de informar sobre incidentes de ciberseguridad. El operador de una infraestructura crítica notificará a su CSIRT sectorial correspondiente y si no lo hubiere, al Instituto Nacional de Ciberseguridad, al ente u órgano regulador sectorial competente, dentro de las veinticuatro (24) horas de tener conocimiento sobre la ocurrencia de:

1) Todo incidente de ciberseguridad que tenga o pueda tener un impacto significativo en la ciberseguridad o en la continuidad del servicio de la infraestructura crítica;

2) Todo incidente de ciberseguridad que tenga o pueda tener un impacto significativo en la ciberseguridad de cualquier sistema de información bajo el control del operador que esté interconectado o que se comunique con la infraestructura crítica;

3) Cualquier otro tipo de incidente de ciberseguridad con respecto a la infraestructura crítica que el Instituto Nacional de Ciberseguridad, el ente u órgano regulador sectorial competente o, si lo hubiese, el CSIRT sectorial haya especificado al operador.

Párrafo I. El operador de la infraestructura crítica está obligado a notificar a las personas posiblemente afectadas por los incidentes establecidos en este artículo o al público en general, si las personas afectadas no pueden ser notificadas individualmente, en un plazo no mayor a las setenta y dos (72) horas, contadas a partir de tener conocimiento sobre los mismos.

Párrafo II. En caso de incumplimiento, la notificación de los incidentes establecidos en este artículo podrá ser realizada por el Instituto Nacional de Ciberseguridad, el ente u órgano regulador sectorial competente o, si lo hubiese, el CSIRT sectorial, sin perjuicio de las sanciones que puedan corresponder al operador por dicho incumplimiento.

Párrafo III. El operador de la infraestructura crítica está obligado a enviar a su CSIRT sectorial, y si no lo hubiere, al Instituto Nacional de Ciberseguridad, un informe sobre la respuesta y resolución del incidente.

Párrafo IV. El informe sobre la respuesta y resolución del incidente incluirá información sobre las causas del incidente de ciberseguridad, el tiempo dedicado a su resolución, las medidas aplicadas, el impacto del mismo y toda otra información requerida por la reglamentación de esta ley.

Párrafo V. El operador de una infraestructura crítica establecerá mecanismos técnicos y procedimentales con el fin de detectar amenazas e incidentes de ciberseguridad los cuales podrán incluir el uso de equipos de respuesta a incidentes, la implementación de estándares de ciberseguridad, entre otros.

Párrafo VI. Sin perjuicio de las disposiciones establecidas en este artículo, el operador de una infraestructura crítica puede notificar al CSIRT sectorial, y si no lo hubiere, al Instituto Nacional de Ciberseguridad, sobre cualquier incidente cibernético, aunque el mismo no tenga un impacto significativo.

Párrafo VII. Los CSIRT sectoriales deberán notificar al CSIRT-RD sobre la ocurrencia de los incidentes de ciberseguridad que impacten las infraestructuras críticas dentro de su sector.

CAPÍTULO IV
DE LAS RESPUESTAS A LAS AMENAZAS E INCIDENTES DE LA CIBERSEGURIDAD

Artículo 34.- Acciones para prevenir y gestionar incidentes de ciberseguridad. Cuando el Instituto Nacional de Ciberseguridad haya recibido información sobre una amenaza o incidente de ciberseguridad de impacto significativo, deberá informar al ente u órgano regulador sectorial competente o al CSIRT sectorial correspondiente, o en su defecto el Instituto Nacional de Ciberseguridad, para que, ejerciendo las facultades establecidas en esta ley, realice todas las acciones que sean necesarias para prevenir y gestionar la amenaza o incidente de ciberseguridad en una infraestructura crítica, procurando:

1) Evaluar el impacto o el impacto potencial de la amenaza o incidente de ciberseguridad;

2) Eliminar la amenaza de ciberseguridad o prevenir cualquier daño o daño adicional derivado del incidente de ciberseguridad; o

3) Prevenir que un nuevo incidente de ciberseguridad se derive de esa amenaza o incidente de ciberseguridad.

Artículo 35.- Responsabilidad de notificar un incidente de ciberseguridad. En el caso de que la información sobre un incidente de ciberseguridad de impacto significativo sea recibida inicialmente por un CSIRT sectorial, el mismo tendrá la responsabilidad de notificar a la unidad operativa (CSIRT-RD) del Instituto Nacional de Ciberseguridad, con el fin de que el mismo pueda ser correlacionado con otros incidentes significativos reportados de otros sectores de Infraestructura Crítica.

Artículo 36.- Medios para la prevención y gestión de incidentes. Las acciones mencionadas en el artículo 34, permitirán al Instituto Nacional de Ciberseguridad o CSIRT sectorial, si tuviese, tomar las siguientes medidas para proteger la ciberseguridad de las infraestructuras críticas:

1) Requerir a un operador de infraestructura crítica cualquier información relacionada a un incidente de ciberseguridad de impacto significativo por el que se vea afectado;

2) Requerir a un operador de infraestructura crítica o al operador de un sistema de información vinculado a dicho operador, que lleve a cabo las medidas correctivas y/o preventivas, para dar respuesta al incidente de ciberseguridad, de conformidad con el reglamento correspondiente;

3) Solicitar al operador de un sistema de información vinculado a un operador de una infraestructura crítica que tome cualquier acción dentro del marco de ayudar con la gestión del incidente de ciberseguridad:

    a) Preservar el estado del sistema de información;

    b) Monitorear el sistema de información por un período de tiempo específico; y

    c) Realizar un análisis del sistema de información para detectar vulnerabilidades de ciberseguridad y evaluar la manera y el alcance del sistema de información afectado por el incidente de ciberseguridad.

Artículo 37.- Entrega de información. La entrega de la información requerida por el CSIRT sectorial, y en caso de que no lo hubiese, por el Instituto Nacional de Ciberseguridad en virtud de sus facultades para gestionar y prevenir incidentes de ciberseguridad, no será considerada como una vulneración de la confidencialidad previamente establecida por leyes, reglamentos, contratos o códigos de conducta profesionales.

Párrafo I. La información que sea entregada al CSIRT sectorial, y en caso de que no lo hubiese, al Instituto Nacional de Ciberseguridad, se considerará reservada y confidencial según el artículo 56 de esta ley.

Párrafo II. En caso de que el sistema de información se vea en peligro inminente por una amenaza o incidente de ciberseguridad, que puede dañarlo o destruirlo significativamente, el CSIRT sectorial, y en caso de que no lo hubiese, el Instituto Nacional de Ciberseguridad puede disponer con carácter inmediato que se suspenda la utilización de este sistema o cualquiera de sus componentes hasta que se elimine la causa que lo amenaza.

Artículo 38.- Divulgación responsable de vulnerabilidades. No se considerará que una persona infringió disposiciones legales sobre la confidencialidad, integridad y disponibilidad de datos y sistemas de información o que incurrió en un incumplimiento de leyes, reglamentos, contratos y códigos de conducta profesionales por el hecho de comunicar, publicar o divulgar vulnerabilidades, siempre que dicha divulgación se haga basándose en la buena fe.

Párrafo I. Con la finalidad de asegurar la buena fe de la persona que divulgue una vulnerabilidad, se tomará en cuenta que no se haya solicitado recompensas bajo coerción o amenaza de publicación de la información; que no se otorgue un tiempo razonable de al menos noventa (90) días calendario, para solucionar la vulnerabilidad antes de publicarla o divulgarla; que en el proceso de identificación, la persona tomó las previsiones necesarias para prevenir incidentes a la privacidad, degradación o fallas en el servicio y destrucción o manipulación de la data y que la persona que divulga una vulnerabilidad considerará el impacto de dicha divulgación y tener un cuidado razonable para minimizar el daño que pueda causarse por tal divulgación.

Párrafo II. Del proceso de identificación de vulnerabilidades basadas en la buena fe, quedan excluidos métodos que pudieran conducir a denegación de servicio; a pruebas

físicas, utilización de código malicioso; ingeniería social y alteración, eliminación, exfiltración o destrucción de data.

CAPÍTULO V
DEL RÉGIMEN SANCIONADOR

Artículo 39.- Potestad sancionadora. La potestad sancionadora respecto de las infracciones administrativas tipificadas en esta ley será ejercida:

1) Por el ente u órgano regulador del sector al que pertenece la infraestructura crítica;

2) En los casos de infraestructuras críticas de sectores que no cuenten con un ente u órgano regulador, por el Instituto Nacional de Ciberseguridad; y

3) Por los entes y órganos pertenecientes a la administración pública, cuando la infraestructura crítica les pertenezca o funcione bajo su responsabilidad.

Párrafo. El director ejecutivo del Instituto Nacional de Ciberseguridad impondrá las sanciones correspondientes a las infracciones administrativas, en los demás casos no previstos en este artículo.

Artículo 40. – Responsabilidad. Son responsables por las infracciones administrativas contenidas en esta ley:

1) Los operadores responsables del funcionamiento de una infraestructura crítica de naturaleza privada; y

2) Los operadores responsables del funcionamiento de una infraestructura crítica pertenecientes al Estado.

Artículo 41. - Clasificación. Las infracciones administrativas establecidas en esta ley, se clasifican en: leves, graves y muy graves.

Artículo 42.- Infracciones administrativas leves. Se considerarán infracciones administrativas leves y serán castigadas con multa de veinte (20) a cincuenta (50) salarios mínimos del sector público las siguientes:

1) No cumplir con notificar de cambios sustanciales en una infraestructura crítica de acuerdo al procedimiento y plazos establecidos por la normativa técnica;

2) No cumplir con designar y notificar al Instituto Nacional de Ciberseguridad de un Punto de Contacto Único para una infraestructura crítica, de acuerdo al procedimiento y plazos establecidos por la normativa técnica;

3) No cumplir con notificar de cambio de operador de una infraestructura crítica de acuerdo al procedimiento y plazos establecidos por la normativa técnica;

4) No cumplir con notificar los incidentes de ciberseguridad al Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes y los CSIRT sectoriales de acuerdo al procedimiento y plazos establecidos por la normativa técnica;

5) No cumplir con notificar los incidentes de ciberseguridad a las personas posiblemente afectadas;

6) No cumplir con establecer mecanismos técnicos y procedimentales con el fin de detectar amenazas e incidentes de ciberseguridad;

7) No cumplir con enviar al Instituto Nacional de Ciberseguridad, a los entes u órganos reguladores sectoriales competentes y a los CSIRT sectoriales un informe que incluya información sobre las causas de un incidente de ciberseguridad, el tiempo dedicado a su resolución, las medidas aplicadas y el impacto de este de acuerdo al procedimiento y plazos establecidos por la normativa técnica; y

8) No remitir la auditoría o la evaluación del riesgo cibernético al Instituto Nacional de Ciberseguridad, a los entes u órganos reguladores sectoriales competentes y a los CSIRT sectoriales en los plazos establecidos.

Artículo 43.- Infracciones administrativas graves. Se considerarán infracciones administrativas graves y serán castigadas con multa de cincuenta (50) a cien (100) salarios mínimos del sector público, las siguientes:

1) Reincidir en cualquiera de las infracciones administrativas establecidas como leves;

2) No cumplir con llevar a cabo auditorías o la evaluación de riesgo sobre su cumplimiento con esta ley;

3) No cumplir la entrega de información requerida por el Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes y los CSIRT sectoriales dentro del plazo requerido; grave

4) No llevar a cabo las auditorías, sus planes de acción correctivos o la evaluación de riesgo de manera satisfactoria;

5) No participar en un ejercicio de ciberseguridad requerido por el Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes o los CSIRT sectoriales;

6) No proporcionar información, registros o documentos requeridos por el Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes o los CSIRT sectoriales para responder a un incidente de ciberseguridad;

7) Realizar un cambio sustancial a una infraestructura crítica y no llevar a cabo la auditoría o evaluación de riesgo posterior al cambio sustancial; y

8) No cumplir con las disposiciones de los reglamentos dictados en materia de ciberseguridad por el ente regulador correspondiente o en su defecto por el Instituto Nacional de Ciberseguridad.

Artículo 44.- Infracciones administrativas muy graves. Se considerarán infracciones administrativas muy graves y serán castigadas con multa de cien (100) a doscientos (200) salarios mínimos del sector público, las siguientes:

1) Reincidir en cualquiera de las infracciones administrativas establecidas como graves;

2) Obstruir o impedir que se lleve a cabo una auditoría o evaluación de riesgo;

3) No cumplir con una orden de prohibición de utilizar un sistema de información o cualquiera de sus partes en caso de que el Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes o los CSIRT sectoriales los hayan notificado;

4) No cumplir con una orden emitida por el Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes o los CSIRT sectoriales con la finalidad de prevenir, detectar o contrarrestar cualquier amenaza o incidente de ciberseguridad; y

5) Obstruir al Instituto Nacional de Ciberseguridad, los entes u órganos reguladores sectoriales competentes y los CSIRT sectoriales o a quien este designe para hacer

cumplir cualquier medida emitida a fin de identificar, detectar o contrarrestar cualquier amenaza de ciberseguridad.

Párrafo. La reincidencia en las violaciones a las infracciones administrativas señaladas en este artículo, serán sancionadas con el duplo de la pena.

Artículo 45.- Pago de las multas. Las multas impuestas como sanciones administrativas deberán ser pagadas dentro de un plazo de un (1) mes a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución sancionadora.

Párrafo. En caso de incumplimiento, se generará un recargo por mora de tres por ciento (3%) mensual sobre el saldo insoluto de la multa.

Artículo 46.- Sanción operadores del Estado. Los funcionarios públicos directamente responsables de la operación de una infraestructura critica del Estado, que incurran en algunas de las infracciones administrativas establecidas en los artículos 42, 43 y 44 serán pasibles de ser sancionados con la suspensión de sus funciones por hasta noventa (90) días, sin disfrute de salarios, según lo establecido en el artículo 83 de la Ley núm. 41-08, del 16 de enero de 2008, Ley de Función Pública y Crea la Secretaria de Estado de Administración Pública o lo señalado en su ley respectiva como una falta similar.

Artículo 47.- Cese de los actos que dieron lugar a la sanción. La imposición y cumplimiento de las sanciones administrativas no implica la convalidación de la situación irregular, debiendo el infractor cesar de inmediato los actos que dieron lugar a la sanción.

Artículo 48. - Prescripción de infracciones. Las infracciones administrativas previstas en esta ley, prescriben a los tres (3) años contados desde el día en que la infracción se hubiere cometido, de conformidad con lo establecido en la Ley Núm. 107-13, del 6 de agosto de 2013, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo.

Artículo 49. - Prescripción de sanciones. Las sanciones administrativas previstas en esta ley, prescriben a los tres (3) años contados desde el día siguiente a aquel en que adquiera firmeza la resolución sancionadora, de conformidad con lo establecido en la Ley Núm. 107-13, del 6 de agosto de 2013, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo.

Artículo 50. - Recursos administrativos. Los recursos administrativos respecto de las resoluciones sancionadoras se harán conforme a la Ley Núm. 107-13, del 6 de agosto de 2013, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo.

Articulo 51.- Recursos de órganos pertenecientes a la administración pública. Los recursos respecto de las sanciones impuestas por los entes y órganos pertenecientes a la administración pública, cuando la infraestructura crítica les pertenezca o funcione bajo su responsabilidad, se harán conforme a lo establecido por la Ley núm. 41-08, del 16 de enero de 2008, Ley de Función Pública y Crea la Secretaria de Estado de Administración Pública o las leyes respectivas de cada órgano extrapoder o poderes del Estado.

Artículo 52.- Recurso contencioso-administrativo. El recurso contencioso-administrativo respecto de las resoluciones sancionadoras, se hará conforme a la Ley Núm. 13-07, del 5 de febrero de 2007, que crea el Tribunal Contencioso Tributario y Administrativo.

CAPÍTULO VI
DE LAS DISPOSICIONES GENERALES

Artículo 53.- Colaboración de las entidades de persecución penal con la ciberseguridad. Toda autoridad competente que en el curso de una investigación de un ciberdelito que considere que el mismo puede constituir una amenaza de ciberseguridad a una o más infraestructuras críticas nacionales, deberá informar de manera inmediata al Instituto Nacional de Ciberseguridad y brindar la colaboración pertinente.

Párrafo. El Instituto Nacional de Ciberseguridad deberá informar todo incidente cibernético que pueda constituir un ciberdelito a las autoridades competentes en investigación y persecución del ciberdelito.

Artículo 54.- Coordinaciones sectoriales ante incidentes de ciberseguridad. Podrán existir, de forma individual o conjunta, unidades administrativas o comisiones de respuesta a incidentes cibernéticos, que se denominarán CSIRT sectoriales, las cuales coordinarán con la unidad operativa (CSIRT-RD) del Instituto Nacional de Ciberseguridad y con el ente u órgano regulador sectorial competente, según corresponda, la respuesta conjunta ante incidentes de ciberseguridad.

Párrafo I. Los CSIRT sectoriales podrán comunicarse con organismos de seguridad del Estado y los medios de comunicación para poner en conocimiento los incidentes de ciberseguridad dentro de sus respectivos sectores.

Párrafo II. La comunicación con otros CSIRT sectoriales nacionales o internacionales, con organismos internacionales, se realizará a través del CSIRT-RD, en cumplimiento al rol de organismo de intercambio de información sobre indicadores de compromiso, correspondiente del Instituto Nacional de Ciberseguridad.

Artículo 55.- Responsabilidades. Los órganos y entes de la administración pública, así como las personas físicas y personas jurídicas de derecho privado, son responsables de la prevención, detección, respuesta y recuperación de los incidentes de ciberseguridad que pudieren afectarlos.

Párrafo I. En caso de comprobarse o advertirse incumplimiento de sus obligaciones, negligencia o mala práctica comprobada, el regulador sectorial o el Instituto Nacional de Ciberseguridad, según corresponda, podrá someter al responsable a los procesos sancionadores administrativos correspondientes, sin perjuicio de las acciones civiles y penales que pudiera generar su actuación u omisión.

Párrafo II. La investigación penal del origen de las amenazas e incidentes de ciberseguridad y sus responsables estará a cargo de las fuerzas del orden y cuerpos de seguridad y de investigación y persecución según lo disponga la legislación sobre ciberdelincuencia.

Artículo 56.- Información reservada por seguridad del Estado. Se declaran clasificadas como informaciones reservadas y, por ende, sujetas a las limitaciones y excepciones dispuestas por la Ley núm. 200-04, del 28 de julio de 2004, Ley General de Libre Acceso a la Información Pública, las siguientes informaciones del Instituto Nacional de Ciberseguridad:

1) Las especificaciones técnicas de los sistemas de información, así como los detalles que permitan individualizar su ubicación, y forma de suministro eléctrico;

2) Los datos personales de todo aquel que preste servicio en el Instituto Nacional de Ciberseguridad;

3) La topología y la arquitectura de la red y de la infraestructura tecnológica y de telecomunicaciones;

4) Los esquemas de direcciones de Protocolo de Internet (IP), públicas y privadas;

5) Los códigos de acceso, los protocolos de encriptación de los sistemas y redes;

6) Las rutas de enlace desde las prestadoras de servicios de telecomunicaciones;

7) Tráfico de internet entrante y saliente;

8) Plan de continuidad, protección y recuperación ante desastres, de las operaciones; y

9) Los datos producidos por el CSIRT-RD y los CSIRT sectoriales existentes, excepto Inteligencia de Amenazas de ciberseguridad, anonimizada.

Párrafo I. Las informaciones antes señaladas se podrán obtener a solicitud del Ministerio Público, a raíz de una investigación penal, sin perjuicio de lo que disponen los artículos 26, 27, 28 y 29 de la Ley núm. 200-04, 28 de julio de 2004, Ley General de Libre Acceso a la Información Pública.

Párrafo II. Los funcionarios o empleados del Instituto Nacional de Ciberseguridad tienen la obligación de guardar el secreto y confidencialidad que requieren los asuntos relacionados con su trabajo, debido a su naturaleza o en virtud de instrucciones especiales, hasta un plazo de cinco (5) años luego de haber cesado en el cargo.

Artículo 57.- Sostenibilidad financiera. Las actividades y operaciones del Instituto Nacional de Ciberseguridad serán financiadas por:

1) Los recursos provenientes del Presupuesto General del Estado;

2) Los recursos provenientes de las donaciones y la cooperación internacional no reembolsable;

3) Cualquier otro ingreso que provenga de leyes especiales o aportes específicos;

4) De las multas impuestas por el Instituto Nacional de Ciberseguridad conforme a las disposiciones de esta ley;

5) De un cincuenta por ciento (50%) del importe total de las multas impuestas por otras autoridades sancionadoras conforme a las disposiciones de esta ley.

Párrafo. El Instituto Nacional de Ciberseguridad está sujeto al sistema de control de los fondos públicos previstos en la Constitución de la República.

CAPÍTULO VII
DE LAS DISPOSICIONES FINALES

Artículo 58.- Reglamento. El Poder Ejecutivo dictará el reglamento de aplicación de esta ley en un plazo de doce (12) meses contados a partir de la promulgación de esta ley.

Artículo 59.- Entrada en vigencia. Esta ley entrará en vigencia a partir de la fecha de su promulgación y publicación según lo establecido en la Constitución de la República y transcurridos los plazos fijados en el Código Civil de la República Dominicana.

Atentamente,

Wernel D. Féliz F.
Director