Ley No. _____ 2021 sobre de Gestión de la Ciberseguridad en República Dominicana

SENADO DE LA REPUBLICA
SECRETARIA GENERAL LEGISLATIVA
FECHA 22/4/2021 HORA 1:22 P.M.
RECIBIDO POR Roxana Sánchez

EL CONGRESO NACIONAL

En nombre de la República

Ley No. _____ - 2021

CONSIDERANDO PRIMERO: Que la Constitución de la República, en su artículo 7 establece que 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 SEGUNDO: Que la Constitución de la República, en su artículo 8 establece que 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 TERCERO: Que el artículo 260 de nuestra Constitución establece como objetivos de alta prioridad nacional el *combatir actividades criminales transnacionales que pongan en peligro los intereses de la República y de sus habitantes,* y *organizar y sostener sistemas eficaces que prevengan o mitiguen daños ocasionados por desastres naturales y tecnológicos*;

CONSIDERANDO CUARTO: Que las tecnologías de información y comunicación desempeñan un papel imprescindible para las actividades económicas y sociales, y, por tanto, para el desarrollo de la República Dominicana. Que cualquier vulnerabilidad en las redes y sistemas de

información que soportan los servicios que se ofrecen a través de las mismas representa un grave riesgo para que se materialicen amenazas o incidentes de ciberseguridad atentatorios contra la seguridad de dichas redes y sistemas de información que podrían interrumpir, parcial o totalmente, las actividades económicas del país, generando considerables pérdidas financieras y menoscabando la confianza de los usuarios;

CONSIDERANDO QUINTO: Que mediante el Decreto Núm. 230-18 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 SEXTO: 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 SÉPTIMO: 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 OCTAVO: 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 NOVENO: 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 de Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, Ley Núm. 41-08, del 16 de enero de 2008, de Función Pública, y la Ley Núm. 13-07, que crea el Tribunal Contencioso Tributario y Administrativo;

CONSIDERANDO DÉCIMO: 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 UNDÉCIMO: 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 la presente Ley;

CONSIDERANDO DÉCIMO SEGUNDO: Que la presente 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 DÉCIMO TERCERO: Que la Resolución de la Asamblea General de las Naciones Unidas 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 DÉCIMO CUARTO: 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 DÉCIMO QUINTO: 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 DÉCIMO SEXTO: 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 DÉCIMO SÉPTIMO: 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;

CONSIDERANDO DÉCIMO OCTAVO: 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 DÉCIMO NOVENO: 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 VIGÉSIMO: 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 VIGÉSIMO PRIMERO: Que la presente 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.

VISTA: La Constitución de la República Dominicana del 13 junio de 2015;

VISTA: La Ley Núm. 107-13, del 6 de agosto del año 2013, de Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo;

VISTA: La Ley Núm. 247-12, del 9 de agosto del año 2012, Orgánica de Administración Pública;

VISTA: La Ley No. 1-12, del 25 de enero del año 2012, sobre la Estrategia Nacional de Desarrollo 2030.

VISTA: La Ley Núm. 41-08, del 16 de enero de 2008, de Función Pública;

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

VISTA: La Ley Núm. 13-07, del 5 de febrero del año 2017, que crea el Tribunal Contencioso Tributario y Administrativo;

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

VISTO: El Decreto Núm. 230-18, del 19 de junio del año 2018, que establece la Estrategia Nacional de Ciberseguridad 2018-2021 y que crea el Centro Nacional de Ciberseguridad;

VISTO: El Decreto No.134-14, del 9 de abril del año 2014, que establece el Reglamento de la Estrategia Nacional de Desarrollo 2030;

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

VISTO: El Llamado de París 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.

Ha dado la siguiente ley:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1.-Objeto. La presente ley regula la prevención, gestión y respuestas a las amenazas e incidentes de ciberseguridad y otros aspectos relativos a la seguridad cibernética de las infraestructuras críticas en República Dominicana

Artículo 2.-Ámbito de aplicación. La presente ley aplica a toda persona física o jurídica, pública o privada, nacional o extranjera ubicada total o parcialmente en la República Dominicana.

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

1. **Amenaza.** Es el acto o actividad (conocida o sospechada) llevada a cabo en o a través de un sistema de información, que puede poner en peligro inminentemente o perjudicar la ciberseguridad de esa u otra computadora o sistema de información.

2. **Ciberseguridad.** Refiere al estado, y al conjunto de prácticas orientadas a mantenerlo, en el que un sistema de información está protegido contra el acceso no autorizado; estado mediante el cual:
    a) El sistema de información sigue estando disponible y operativo;
    b) Se mantiene la integridad del sistema de información; y
    c) 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 pone en peligro o que tiene un efecto adverso a la confidencialidad, integridad o disponibilidad de un sistema de información o la información que es procesada, almacenada o transmitida por el mismo.
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. **Infraestructuras críticas.** Son aquellas redes, servicio tecnológico de información o comunicación y sistemas de información, cuyo funcionamiento es indispensable para el correcto y eficaz funcionamiento del Estado Dominicano, por lo que su interrupción o destrucción tendría un impacto importante en el desempeño de sus funciones.
7. **Operador.** Es la entidad u organismo responsable del funcionamiento diario 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.
8. **Riesgo cibernético.** Es todo evento, circunstancia o hecho identificable que tenga un posible efecto adverso en la seguridad de las redes y en los sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza o incidente que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen corporativa.
9. **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.

10. **Sistema de Información.** Refiere a todo dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como a cualquier sistema de alta tecnología, incluyendo, pero no limitando, a 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. De igual forma, hace referencia a cualquier sistema de tecnología de la información y/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.
11. **Vinculación con un operador de infraestructura critica.** 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 este.
12. **Vulnerabilidad.** Es cualquier debilidad en un sistema de información que pueda ser explotada por una o más amenazas de ciberseguridad.

Artículo 4.-Principios. Con la finalidad de promover un ciberespacio abierto, seguro, estable, accesible y pacífico, y propiciar la ciberseguridad tanto a nivel nacional como internacional, la República Dominicana reconoce y actúa en virtud de los principios incluidos en el Llamado de París para la Confianza y la Seguridad en el Ciberespacio y los principios y normas establecidos por la Comisión Global sobre la Estabilidad del Ciberespacio, así como también los siguientes:

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 Humano.** 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 a estas tecnologías o a infraestructuras dependientes de ellas.

CAPÍTULO II
ADMINISTRACIÓN

Artículo 5.-Creación del Centro Nacional de Ciberseguridad. Se crea el Centro Nacional de Ciberseguridad, como continuación de la actual dependencia homónima del Ministerio de la Presidencia, pasando a ser un ente derecho público con personalidad jurídica propia, autonomía funcional, presupuestaria, administrativa, técnica y patrimonio propio, adscrito al Ministerio de la Presidencia.

Artículo 6.-Sede. El Centro Nacional de Ciberseguridad tendrá su sede en la ciudad de Santo Domingo, Distrito Nacional, con jurisdicción nacional, pudiendo establecerse a nivel nacional 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.-Función del Centro Nacional de Ciberseguridad. El Centro Nacional de Ciberseguridad tiene la función esencial de velar por el cumplimiento de los mandatos previstos en la presente ley, su reglamento de aplicación y las normativas dictadas por su Consejo Directivo, a fin de prevenir, gestionar y responder a los incidentes y amenazas de ciberseguridad en República Dominicana.

Artículo 8.-Carácter vinculante de las decisiones del Centro Nacional de Ciberseguridad (CNSC). Las decisiones que en materia de ciberseguridad sean tomadas por el Centro Nacional de Ciberseguridad, tendrán carácter obligatorio para todos los entes y órganos de la Administración Pública, así como las entidades privadas, especialmente aquellas infraestructuras críticas que proveen servicios esenciales.

Artículo 9.-Conformación del Centro Nacional de Ciberseguridad. El Centro Nacional de Ciberseguridad estará integrado por un órgano colegiado que se denominará Consejo Nacional de Ciberseguridad, su máxima autoridad, y por una Dirección Ejecutiva, quien tendrá a su cargo la dirección, control y representación del Centro Nacional de Ciberseguridad.

Artículo 10.-De la estructura organizativa del Centro Nacional de Ciberseguridad. El Centro Nacional de Ciberseguridad contará con las

siguientes dependencias básicas, las cuales estarán supervisadas por la Dirección Ejecutiva:

1. Una dirección denominada Equipo de Coordinación de Estrategias de Ciberseguridad, que tendrá por objeto la elaboración, desarrollo, actualización y evaluación de la Estrategia Nacional de Ciberseguridad, la formulación de políticas derivadas de dicha estrategia y la definición de las iniciativas, programas y proyectos que lleven a la realización exitosa de ésta;
2. Una dirección denominada Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT RD), que tiene a su cargo la prevención, detección y gestión de incidentes generados en los sistemas de información relevantes del Estado e infraestructuras críticas nacionales;
3. Una dirección administrativa y financiera; y,
4. Una dirección jurídica.

Párrafo.- El Centro Nacional de Ciberseguridad podrá crear otros equipos y dependencias según entienda necesario para el cumplimiento de esta ley.

Artículo 11.- Composición del Consejo Directivo del Centro Nacional de Ciberseguridad. El Consejo Directivo estará compuesto por las siguientes entidades:

1) Ministerio de la Presidencia, el cual lo preside.
2) Dirección Ejecutiva, representada por su Director Ejecutivo, quien ostentará la calidad de secretario, máximo órgano administrativo y miembro de pleno derecho del Consejo, con voz, pero sin voto.
3) Ministerio de Defensa.
4) Ministerio de Interior y Policía.
5) Procuraduría General de la República.
6) Policía Nacional.
7) Departamento Nacional de Investigaciones.
8) Instituto Dominicano de las Telecomunicaciones.
9) Oficina Presidencial de Tecnologías de la Información y Comunicación.
10) El Ministerio de Relaciones Exteriores.
11) La Administración Monetaria y Financiera.

Párrafo I.- Los miembros del Consejo solo podrán hacerse representar en las reuniones por un funcionario de jerarquía inmediatamente inferior.

Párrafo II.- El Consejo Directivo tendrá la facultad, cuando el caso lo amerite, de solicitar la participación de otros representantes del Estado, tales como: el Poder Legislativo, el Poder Judicial, así como a representantes de la academia, operadores de infraestructuras críticas, del sector privado y la ciudadanía en general.

Artículo 12.-Decisiones del Consejo Directivo del Centro Nacional de Ciberseguridad. Las decisiones del Consejo serán tomadas con apego a las disposiciones de la Ley Núm. 107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, en lo referente al funcionamiento de los órganos colegiados, guardando, de ser necesario, la debida confidencialidad de la información en virtud de que se vean envueltas informaciones privadas preponderantes o informaciones públicas preponderantes, en el marco de la Ley Núm. 200-04, General de Libre Acceso a la Información Pública. Esto no obsta a que toda decisión que sea tomada por el Consejo será debidamente motivada.

Artículo 13.-Atribuciones del Consejo Nacional de Ciberseguridad. El Consejo Nacional de Ciberseguridad tendrá las siguientes atribuciones:

1. Coordinar el funcionamiento interinstitucional del Centro Nacional de Ciberseguridad;
2. Aprobar el Plan Operativo Nacional y el Plan Estratégico Institucional del Centro Nacional de Ciberseguridad y sus actualizaciones, su presupuesto y los estados financieros;
3. Aprobar el Plan de Acción y Revisión de la Estrategia Nacional de Ciberseguridad;
4. Definir políticas, establecer directrices y elaborar propuestas de estrategias y planes para someterlas a la aprobación del Poder Ejecutivo;
5. Garantizar mecanismos eficaces de financiamiento, sostenibilidad y el buen funcionamiento para el Centro Nacional de Ciberseguridad.

Artículo 14.-Dirección Ejecutiva. El Centro Nacional de Ciberseguridad tendrá como máximo funcionario administrativo a un Director Ejecutivo, el cual cumplirá con los siguientes requisitos:

1. Ser ciudadano dominicano y en pleno ejercicio de sus derechos civiles;
2. Tener más de 30 años de edad;
3. Ser profesional de ingeniería, derecho, economía o áreas afines, con estudios especializados en alguna de las siguientes disciplinas: seguridad de la información, ciberseguridad, políticas públicas, gestión de riesgo;
4. Tener experiencia por más de diez años en alguna de las áreas anteriormente señaladas;
5. Tener experiencia gerencial comprobada.

Artículo 15.-Impedimentos para la Dirección Ejecutiva. No podrán ejercer la función de la Dirección Ejecutiva, las siguientes personas:

1. Los miembros del Congreso Nacional;
2. Los miembros activos del Poder Judicial;
3. Los que desempeñen cargos o empleos remunerados en cualesquiera de los organismos de Estado o de las municipalidades, ya sea por elección popular o mediante nombramiento, salvo los cargos de carácter docente;
4. Las personas que estuvieren *sub judice*, o cumpliendo condena o que hayan sido condenadas a penas aflictivas o infamantes;
5. Aquellas que por cualquier razón sean legalmente incapaces.

Artículo 16.-Designación. La Dirección Ejecutiva será elegida por medio de un decreto del Poder Ejecutivo en base a una propuesta de tres candidatos presentada por los demás miembros del Consejo Directivo del Centro Nacional de Ciberseguridad.

Párrafo. - El mandato del Director Ejecutivo durará un período de cuatro años y no podrá ser elegido para nuevos períodos sucesivos.

Artículo 17.-Remoción del Director Ejecutivo. El Director Ejecutivo podrá ser removido o sustituido en sus funciones, en cualquiera de los casos siguientes:

1. Cuando por incapacidad física no hubiere podido desempeñar su cargo durante seis (6) meses;
2. Por condena definitiva a pena criminal;
3. Cuando se demostrare negligencia manifestada en el cumplimiento de sus funciones o en el caso de que, sin debida justificación, deje de cumplir las obligaciones que le corresponde, de acuerdo con la ley y sus reglamentos;
4. Cuando fuere responsable de actos u operaciones fraudulentas, ilegales o evidentemente opuestas a los fines e intereses de la institución; y
5. Por recomendación del Consejo Directivo, debidamente tramitada al Poder Ejecutivo.

Artículo 18.-Atribuciones de la Dirección Ejecutiva del Centro Nacional de Ciberseguridad. La Dirección Ejecutiva del Centro Nacional de Ciberseguridad tendrá las siguientes atribuciones:

1. Diseñar las políticas y los estatutos, reglamentos y manuales organizativos y de funciones de la institución;
2. Administrar los recursos de la institución acorde a la planificación anual;
3. Representar legalmente a la institución;

4. Proponer las remuneraciones del personal de la institución, de conformidad con las leyes que regulan la materia;
5. Elaborar el Plan de Acción y Revisión de la Estrategia Nacional de Ciberseguridad, que será aprobado por el Consejo Directivo;
6. Disponer las medidas de seguridad necesarias y suficientes para proteger toda aquella información o datos que, por sus características, deban permanecer en condición de confidencialidad, con el objeto de prevenir el uso indebido de éstos;
7. Convocar las sesiones del Consejo Nacional de Ciberseguridad y determinar los asuntos a ser incorporados en la agenda;
8. Presentar informes periódicos de las actividades realizadas y estadísticas recopiladas, así como aprobar y divulgar la memoria anual de la institución
9. Asegurar que el Centro Nacional de Ciberseguridad cumpla el rol de intercambio de información sobre indicadores de compromiso
10. Ejecutar cualquier otra función señalada por el Consejo Nacional de Ciberseguridad o los reglamentos de la presente ley.

Artículo 19.-Atribuciones del Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC). El Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) tendrá las siguientes atribuciones:

1. 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 a las que correspondan su ejecución puedan gestionar los proyectos conforme a tales directrices;
2. Elaborar y mantener un catálogo de las actividades que sobre ciberseguridad desarrollen las instituciones involucradas;
3. Coordinar con los entes y órganos del Estado, en los ámbitos de sus respectivas competencias, la implementación y el cumplimiento de los objetivos y prioridades establecidos en la Estrategia Nacional de Ciberseguridad;
4. Sensibilizar a los distintos segmentos de la sociedad sobre la importancia de la ciberseguridad como la herramienta fundamental para asegurar los servicios que ofrecen a través de sus sistemas de información;
5. Evaluar las ejecutorias en el marco de la Estrategia Nacional de Ciberseguridad y reportar anualmente al Director Ejecutivo;
6. Apoyar, propiciar y liderar la creación de redes de cooperación entre los instituciones públicas, organizaciones académicas y entidades privadas para el impulso de la Estrategia Nacional de Ciberseguridad;

7. Contribuir a la difusión y promoción para la creación de una cultura nacional de ciberseguridad;
8. Contribuir a la adopción de una posición país unificada a través de la coordinación e integración de las iniciativas de los diferentes sectores de la sociedad vinculadas con la ciberseguridad;
9. Cualquier otra atribución que le sea encomendada por la Dirección Ejecutiva.

Artículo 20.-Atribuciones del Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD). El Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD) tendrá los siguientes cometidos:

1. Asistir en la respuesta a incidentes de ciberseguridad de los operadores de infraestructuras críticas
2. Coordinar con los responsables de la seguridad de la información de los operadores de infraestructuras críticas para la prevención, detección, manejo y recopilación de información sobre incidentes de ciberseguridad;
3. Asesorar y difundir información para incrementar los niveles de ciberseguridad,
4. Desarrollar herramientas, técnicas de protección y defensa de los operadores de infraestructuras críticas;
5. Alertar ante amenazas y vulnerabilidades de ciberseguridad en las infraestructuras críticas; críticas;
6. Realizar las tareas preventivas que correspondan, para garantizar la ciberseguridad de las infraestructuras críticas;
7. Realizar análisis forenses de los incidentes de ciberseguridad reportados que no constituyan un crimen o delito;
8. Centralizar los reportes y llevar un registro de toda la información sobre incidentes de ciberseguridad ocurridos en las infraestructuras críticas;
9. Fomentar el desarrollo de capacidades y buenas prácticas, así como la creación de Equipos Sectoriales de Respuestas a Incidentes;
10. Coordinar y asesorar los Equipos Sectoriales de Respuestas a Incidentes y entidades, tanto del nivel público como privado, y de la sociedad civil para responder ante incidentes de ciberseguridad;
11. Establecer y mantener un vínculo fluido y una relación colaborativa con otros organismos nacionales e internacionales de similar naturaleza;
12. Fomentar y coordinar la creación de laboratorios orientados a la investigación en temas de ciberseguridad; y

13. Cualquier otra función que le sea encomendada por la Dirección Ejecutiva.

Párrafo.-El personal del Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) está autorizado para recibir y acceder a toda la información y los documentos necesarios para realizar sus funciones.

Artículo 21.-Colaboración de las entidades de persecución penal con la Ciberseguridad. Toda autoridad competente que en el curso de una investigación de un ciberdelito considere que el mismo puede constituir una amenaza de ciberseguridad debe informar de manera inmediata al Centro Nacional de Ciberseguridad y brindar la colaboración pertinente.

Artículo 22.-De las coordinaciones sectoriales. Los entes y órganos del Estado podrán crear de forma individual o conjunta unidades coordinadoras de respuesta a incidentes cibernéticos (CSIRT sectoriales), las cuales coordinarán con el Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) los objetivos de, en el marco de sus respectivos sectores, velar por la ciberseguridad, el cumplimiento de la presente ley y su reglamento de aplicación, así como de las normativas dictadas por el Centro Nacional de Ciberseguridad.

Párrafo.- 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. En cambio, la comunicación con otros CSIRT sectoriales, con organismos internacionales, con proveedores de plataforma de inteligencia de amenazas, entre otros, se realizarán a través del CSIRT-RD, acorde con el rol de organismo de intercambio de información sobre indicadores de compromiso correspondiente al Centro Nacional de Ciberseguridad (CNCS).

Artículo 23.-De las responsabilidades. Cada uno de los órganos y entes del sector público es responsable de la prevención, detección, respuesta y recuperación de los incidentes de ciberseguridad del que sea víctima, así como de la implementación de las posibles soluciones frente a futuras amenazas e incidentes. En caso de incumplimiento, el responsable podrá ser sometido a los procesos sancionadores administrativos correspondientes, independientemente de las acciones civiles y penales que pudiera generar su actuar.

Párrafo I.- El proceso sancionador administrativo se realizará por el organismo correspondiente, respetando el debido proceso y los principios recogidos en la Ley Núm. 107-13, de Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo.

Párrafo II.- La investigación 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 según lo disponga la legislación sobre ciberdelincuencia.

Artículo 24.-De la información reservada por seguridad del Estado. Debido al interés público preponderante, se declaran clasificadas como informaciones reservadas y, por ende, sujetas a las limitaciones y excepciones dispuestas por la Ley Núm. 200-04, General de Libre Acceso a la Información Pública, los datos producidos por el Equipo Nacional de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD), que no representen indicadores de compromiso. 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, General de Libre Acceso a la Información Pública.

Artículo 25.-De la sostenibilidad financiera. Las actividades y operaciones del Centro 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 a las entidades del Estado y entidades privadas que hayan incumplido las obligaciones puestas a su cargo conforme las disposiciones de esta Ley.

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

Artículo 26.-Exención impositiva. El Centro Nacional de Ciberseguridad estará exento del pago de todos los impuestos nacionales, municipales, gravámenes, tasas, arbitrios y contribuciones en general que pudieran recaer sobre los actos o negocios jurídicos que realice.

Artículo 27.-Contratación de personal. El personal del Centro Nacional de Ciberseguridad podrá acogerse al régimen de carrera administrativa especial, la cual será diseñada para tales fines en coordinación con el Ministerio de Administración Pública.

Artículo 28.-Remuneración. Todos los funcionarios y empleados del Centro Nacional de Ciberseguridad devengarán salarios competitivos con los del mercado, para funcionarios de calificación similar en el mercado privado.

Artículo 29.-De la confidencialidad y el deber de secreto. Los funcionarios o empleados del Centro 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, aún después de haber cesado en el cargo.

Artículo 30.-Sanción a la inobservancia de la confidencialidad y el deber de secreto. Los funcionarios o empleados que violen la confidencialidad y el deber de secreto establecido en esta ley serán sancionados de conformidad con lo dispuesto por la Ley Núm. 41-08, de Función Pública, sin perjuicio de las acciones penales y civiles que puedan ser perseguidas.

Artículo 31.-Normativa. El Centro Nacional de Ciberseguridad, en su facultad normativa, puede establecer normativas para llevar a cabo los propósitos y disposiciones de esta Ley. Sin limitación a lo previamente indicado, podrá dictar normas con respecto a todos o cualquiera de los siguientes asuntos:

1. El procedimiento para la designación de una infraestructura como crítica;
2. Las normas técnicas o de otro tipo relacionadas con la ciberseguridad que deben mantenerse respecto de las infraestructuras críticas;
3. Las responsabilidades y deberes del operador de una infraestructura crítica;
4. El tipo de cambios que se consideran cambios sustanciales en el diseño, la configuración, la seguridad o las operaciones de una infraestructura crítica que debe ser notificada por el operador de la infraestructura crítica;
5. El tipo de incidentes de ciberseguridad que deben ser notificados al Centro Nacional de Ciberseguridad;
6. Los requisitos y la forma de llevar a cabo las auditorías de ciberseguridad y las evaluaciones de riesgo de ciberseguridad que debe llevar a cabo el operador de una infraestructura crítica;
7. La forma y naturaleza de los ejercicios de ciberseguridad que se pueden realizar;
8. Las facultades para investigar y prevenir incidentes de ciberseguridad;
9. Las medidas correctivas que se deben tomar para dar respuesta a las amenazas e incidentes de ciberseguridad;
10. El establecimiento de estándares en relación con los productos o servicios de ciberseguridad que se provean a nivel nacional;
11. Todos los asuntos y cosas que según la presente ley se requieren o que sean necesarios o convenientes para ser prescritos para dar efecto a esta Ley.

CAPÍTULO III
DE LAS INFRAESTRUCTURAS CRÍTICAS

Artículo 32.-Designación como infraestructura crítica. El Centro Nacional de Ciberseguridad efectuará un análisis de riesgo sobre las infraestructuras críticas nacionales y, sujeto a los resultados arrojados, podrá, mediante notificación al operador de un sistema de información, designar el mismo como una infraestructura crítica para los fines de esta Ley, siempre que se entienda que:

1. El sistema de información es necesario para la prestación continua de un servicio esencial, y la pérdida o el compromiso del sistema tendrá un efecto debilitante en la disponibilidad del servicio esencial en el país; y
2. El sistema de información se encuentra total o parcialmente en el país.

Artículo 33.-Contenido de la notificación de designación de infraestructura crítica. La notificación a un operador de un sistema informático por el que dicho sistema se designa como crítico deberá:

1. Identificar el sistema de información que se está designando como una infraestructura crítica;
2. Identificar al operador del sistema de información designado como infraestructura crítica;
3. Informar al operador del sistema de información sobre sus deberes y responsabilidades en virtud de esta ley y sus reglamentos;
4. Solicitar la designación de la persona que será escogido como punto de contacto único de la infraestructura crítica;
5. Informar al operador del sistema de información que podrá recurrir la designación como infraestructura crítica en un plazo no mayor a catorce (14) días después de la fecha de la notificación;
6. Informar al operador del sistema de información que puede recurrir la designación, y proporcionar información sobre el procedimiento aplicable.

Artículo 34.-Duración de la designación de una infraestructura crítica. La designación como operador de una infraestructura crítica tendrá una duración de cinco (5) años, a menos que sea retirado por el Centro Nacional de Ciberseguridad antes de la expiración de dicho período.

Artículo 35.-Contestación a la designación de infraestructura crítica. En virtud de lo dispuesto en los numerales 5 y 6 del Artículo 33, la persona que recibe una notificación de designación como infraestructura crítica puede, en caso de que así sea, demostrar al Centro Nacional de Ciberseguridad que:

1. No puede cumplir con los requisitos de la designación porque no tiene control efectivo sobre las operaciones del sistema de información, ni la capacidad o el derecho de realizar cambios en dicho sistema; y
2. Otra persona tiene un control efectivo sobre las operaciones del sistema de información y la capacidad y el derecho de realizar cambios en dicho sistema.

Párrafo I.- Si el Centro Nacional de Ciberseguridad está de acuerdo con que las circunstancias mencionadas en los numerales 1 y 2 del presente artículo, podrá enmendar la notificación emitida, y dirigirá esa notificación modificada a la persona mencionada en el numeral 1 del presente artículo.

Párrafo II.- Si en algún momento el operador de la infraestructura crítica deja de tener el control, la capacidad y el derecho de realizar cambios en el sistema de información, debe notificarlo al Centro Nacional de Ciberseguridad sin demora alguna.

Párrafo III.- Cuando una infraestructura crítica es propiedad del Gobierno y es operada por una alguna instancia pública, privada o cualquier otro tipo de organismo, éste será tratado como el operador de la infraestructura crítica para los fines de la presente ley.

Artículo 36.-Entrega de información. Si el Centro Nacional de Ciberseguridad tiene motivos para creer que un sistema de información puede cumplir los criterios de una infraestructura crítica podrá requerir que cualquier persona que parezca estar ejerciendo control sobre un sistema de información, le proporcione dentro de un período razonable la información relevante relacionada con ese sistema de información, con el fin de determinar si dicho sistema cumple con los criterios de una infraestructura crítica.

Párrafo I.- La respuesta dada al Centro Nacional de Ciberseguridad en el marco de este artículo comprenderá al menos la siguiente información:

1. La función que el sistema cumple;
2. Las personas u otros sistemas de información que son atendidos por dicho sistema;
3. Información relacionada con el diseño del sistema de información;
4. Información sobre la configuración y seguridad del sistema;
5. Información sobre el diseño, la operación, la configuración y la seguridad de cualquier otro sistema de información bajo su control que esté interconectado o que se comunique con el sistema;
6. Cualquier otra información que el Centro Nacional de Ciberseguridad pueda requerir para determinar si el sistema de información cumple con los criterios de una infraestructura crítica o el nivel de ciberseguridad de la misma.

Párrafo II.- La entrega de la información requerida por el Centro Nacional de Ciberseguridad para determinar si un sistema de información cumple los criterios de una infraestructura crítica no será considerada como una vulneración de la confidencialidad previamente establecida por leyes, reglamentos, contratos o códigos de conducta profesionales. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en esta Ley.

Artículo 37.-Retiro de la designación como infraestructura crítica. El Centro Nacional de Ciberseguridad, a solicitud de un operador o por sí mismo, podrá retirar la designación de cualquier infraestructura crítica en cualquier momento si entiende que el sistema de información ya no cumple con los criterios para ser considerado como tal.

Artículo 38.-Notificación de cambios. Si el operador de una infraestructura crítica realiza un cambio sustancial en el diseño, la configuración, la seguridad o el funcionamiento de dicha infraestructura después de que se haya proporcionado información al Centro Nacional de Ciberseguridad de conformidad con lo dispuesto en esta ley, notificará el cambio a este último a más tardar treinta (30) días después de realizado el cambio.

Párrafo.- A los efectos de este artículo 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.

Artículo 39.-Punto de contacto único. El operador de una infraestructura crítica notificará al Centro Nacional de Ciberseguridad la designación de su oficial de seguridad o quien haga las funciones de éste que servirá como punto de contacto único entre la infraestructura crítica y el centro.

Artículo 40.-Cambio en la propiedad de la infraestructura crítica. Cuando haya algún cambio en la propiedad legal o en beneficio (incluida cualquier parte de dicha propiedad) de una infraestructura crítica, el nuevo operador de la infraestructura crítica informará al Centro Nacional de Ciberseguridad del cambio en la propiedad a más tardar siete (7) días después de la fecha de ese cambio de titularidad.

Artículo 41.-Deber de informar sobre incidentes de ciberseguridad con respecto a la infraestructura crítica. El operador de una infraestructura crítica notificará al Centro Nacional de Ciberseguridad a más tardar veinticuatro (24) horas después de tener conocimiento sobre la ocurrencia de:

1. Un incidente de ciberseguridad que tenga un impacto significativo en la ciberseguridad o en la continuidad del servicio de la infraestructura crítica;

2. Un incidente de ciberseguridad prescrito con respecto a 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 Centro Nacional de Ciberseguridad haya especificado al operador.

Párrafo I.- La obligación prevista en los numerales 1), 2) y 3) precedentes, no limita el derecho del operador de una infraestructura crítica de notificar al Centro Nacional de Ciberseguridad cualquier incidente cibernético, aunque el mismo no tenga un impacto significativo. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en esta Ley.

Párrafo II.- Dentro de un plazo razonable, el operador de una infraestructura crítica está obligado a notificar a las personas posiblemente afectadas por el incidente de ciberseguridad con un impacto significativo o al público en general si las personas afectadas no pueden ser notificadas individualmente.

Párrafo III.- Si el operador de una infraestructura crítica no cumple con la obligación de notificación prevista en párrafo anterior en un plazo razonable, el Centro Nacional de Ciberseguridad podrá notificar a las personas afectadas o al público en general, informando también al operador de una infraestructura crítica de dicha notificación. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en esta Ley.

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

Párrafo V.- Al resolver un incidente de ciberseguridad con un impacto significativo, el operador de una infraestructura está obligado a enviar al Centro Nacional de Ciberseguridad un informe sobre la resolución del mismo. Este informe incluirá información sobre las causas del incidente de ciberseguridad, el tiempo dedicado a su resolución, las medidas aplicadas y el impacto del mismo. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en esta ley.

Párrafo VI.- El procedimiento de notificación de un incidente de ciberseguridad y el formato del informe podrán establecerse mediante un reglamento del Centro Nacional de Ciberseguridad.

Artículo 42.-Incidentes de ciberseguridad de impacto significativo. Para los fines del Numeral 1 del Artículo 41Artículo 41.- de la presente ley, se considerará que un incidente de ciberseguridad tiene un impacto significativo si se 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 preparada sobre la base del Artículo 43.- Artículo 43 de la presente ley;
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 un 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 se interrumpe debido al incidente de ciberseguridad;
4. Las medidas extraordinarias establecidas en la evaluación del riesgo preparadas en virtud del Artículo 43Artículo 43.- de la presente ley o en otro documento si lo hubiere, que describa el restablecimiento de la continuidad del servicio o la seguridad del sistema de información necesitan aplicarse para resolver el incidente de ciberseguridad;
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 43.-Auditorías de ciberseguridad y evaluaciones de riesgo de infraestructuras críticas. El operador de una infraestructura crítica deberá:

1. Al menos una vez cada dos (2) años (o con la frecuencia que le indique el Centro Nacional de Ciberseguridad en cualquier caso particular), a partir de la fecha de su designación como infraestructura critica, llevar a cabo auditorías sobre su cumplimiento con esta ley, sus reglamentos y/o estándares de ciberseguridad aplicables, a ser llevados a cabo por un auditor aprobado o designado por el Centro Nacional de Ciberseguridad; y,
2. Al menos una vez al año, a partir de la fecha de su designación como infraestructura crítica, realice una evaluación de riesgo de ciberseguridad de la infraestructura crítica.

Párrafo I.- El operador de la infraestructura crítica, a más tardar treinta (30) días después de la finalización de la auditoría o la evaluación del riesgo de ciberseguridad, proporcionará una copia del informe resultado de la auditoría o evaluación al Centro Nacional de Ciberseguridad. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en esta Ley.

Párrafo II.- Cuando al Centro Nacional de Ciberseguridad comprenda que el informe resultante de una auditoría indique que cualquier aspecto de la auditoría no se llevó a cabo de manera satisfactoria, podrá ordenar al operador de la infraestructura crítica que haga que el auditor lleve a cabo ese aspecto de la auditoría de nuevo. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en la presente ley.

Artículo 44.-Otros casos en los que se podrá ordenar auditorías. El Centro Nacional de Ciberseguridad podrá también 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 la presente ley, sus reglamentos y/o estándares de ciberseguridad aplicables; o
2. Si la información proporcionada por el operador de una infraestructura crítica de conformidad con el Artículo 36.-Artículo 36 de la presente ley es falsa, engañosa, inexacta o incompleta.

Párrafo I.- En estos casos la auditoría será realizada por un auditor designado por el Centro Nacional de Ciberseguridad y el costo de dicha auditoría será asumido por el operador de la infraestructura crítica.

Párrafo II.- Si el operador de una infraestructura crítica realiza un cambio sustancial en el diseño, la configuración, la seguridad o el funcionamiento de dicha infraestructura, según se indica en el Artículo 38, el Centro Nacional de Ciberseguridad podrá ordenar al operador que realice otra auditoría o evaluación de riesgo. En caso de incumplimiento a esta obligación, será sancionado conforme lo descrito en esta Ley.

Artículo 45.-Ejercicios de ciberseguridad.

El Centro Nacional de Ciberseguridad podrá realizar ejercicios de ciberseguridad con el fin de probar el estado de listeza de los operadores de diferentes infraestructuras críticas para responder a incidentes de ciberseguridad importantes. El operador de una infraestructura crítica participará en los ejercicios de ciberseguridad cuando el Centro Nacional de Ciberseguridad lo solicite.

CAPÍTULO IV
RESPUESTAS A LAS AMENAZAS E INCIDENTES DE LA CIBERSEGURIDAD

Artículo 46.-Facultades para prevenir y gestionar incidentes de ciberseguridad. Cuando el Centro Nacional de Ciberseguridad ha recibido información sobre una amenaza o incidente de ciberseguridad de podrá ejercer o autorizar a un CSIRT sectorial para que ejerza las facultades aquí mencionadas y que sean necesarias para prevenir y gestionar la amenaza o incidente de ciberseguridad en una infraestructura crítica, con el fin de:

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 47.-Medios para la prevención y gestión de incidentes del Centro Nacional de Ciberseguridad. Las facultades mencionadas en el Artículo 46Artículo 46.-, permitirán al Centro Nacional de Ciberseguridad o la entidad que este designe tomar las siguientes medidas para proteger la ciberseguridad de las infraestructuras críticas:

1. Exigir a cualquier persona vinculada a un operador de infraestructura crítica que responda a cualquier interrogante o proporcione una declaración sobre la amenaza o el incidente de ciberseguridad;
2. Exigir a cualquier persona vinculada a un operador de infraestructura crítica que presente cualquier registro físico o electrónico, documento, que se encuentre en su posesión, o que proporcione cualquier información que considere relacionada con cualquier asunto relevante para la gestión de la amenaza o incidente de ciberseguridad;
3. Inspeccionar, copiar o tomar extractos de dicho registro o documento o copia del registro o documento mencionado en el numeral 2 del presente artículo;
4. Requerir información a cualquier persona que parezca estar familiarizada con los hechos y circunstancias relacionados con la amenaza o el incidente de ciberseguridad;
5. Ordenar a cualquier persona vinculada a un operador de infraestructura crítica que lleve a cabo las medidas correctivas, o que deje de llevar a cabo alguna actividad, según se le especifique, en relación con un sistema de información del que se tenga causa razonable para sospechar que fue afectado por el incidente de ciberseguridad, para minimizar las vulnerabilidades de ciberseguridad en el sistema de información;
6. Exigir al operador de un sistema de información vinculado a un operador de una infraestructura crítica que tome cualquier acción para ayudar con la investigación, incluyendo, pero no limitado a:
    a) Preservar el estado del sistema de información;
    b) Monitorear el sistema de información por un período de tiempo específico;
    c) Realizar un escaneo 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; y

d) Permitir que el personal del Centro Nacional de Ciberseguridad o la entidad que este designe conecte cualquier equipo al sistema de información, o instale cualquier programa, según sea necesario para el propósito de la investigación.

7. Ingresar al lugar donde se encuentra el sistema de información que está o estuvo afectado por en un incidente de ciberseguridad de una infraestructura crítica o se crea tuvo alguna participación en dicho incidente;
8. Acceder, inspeccionar y verificar el funcionamiento de un sistema de información del que se tenga causa razonable para sospechar que se haya visto afectado por el incidente de ciberseguridad, se crea tuvo alguna participación en dicho incidente o usar o hacer que se use cualquier sistema de información para buscar los datos contenidos en o disponibles para tal sistema de información;
9. Realizar un escaneo de un sistema de información vinculado al operador de una infraestructura crítica para detectar vulnerabilidades de ciberseguridad en el mismo;
10. Tomar posesión de cualquier sistema de información u otro equipo vinculado a un operador de una infraestructura crítica con el fin de realizar un examen o análisis adicional, con el consentimiento del operador:
    a) Para la toma de posesión de un sistema de información según se describe en este numeral 10, se tendrá en cuenta elementos como: la necesidad para los fines de la investigación, que no exista un método menos disruptivo para lograr el propósito de la investigación y que el beneficio de la investigación supera el perjuicio causado al operador del sistema.
    b) El Centro Nacional de Ciberseguridad o la entidad que este designe, inmediatamente después de completar el examen o análisis adicional del sistema de información que se tomó en posesión, lo devolverá al operador.
11. Hacer una copia de, o extractos de, cualquier registro electrónico o programa contenido en el sistema de información del cual se tenga causa razonable para sospechar que está o fue afectado por el incidente de ciberseguridad;

Párrafo I.- La entrega de la información requerida por el Centro Nacional de Ciberseguridad en virtud de sus facultades para investigar 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 II.- Toda la información que sea entregada o accedida por el Centro Nacional de Ciberseguridad o la entidad que este designe se considerará reservada y confidencial según el Artículo 24Artículo 24.-.

Artículo 48.-Medidas de ciberseguridad. El Centro Nacional de Ciberseguridad podrá tomar medidas de carácter especial cuando tenga fuertes indicios de que ello resulta necesario para prevenir, detectar o contrarrestar cualquier amenaza grave e inminente a la prestación de cualquier servicio esencial en la República Dominicana. Las medidas podrán incluir, sin limitación alguna:

1) Exigir a cualquier persona vinculada a un operador de infraestructura crítica que se le proporcione cualquier información, incluyendo información en tiempo real, que sea necesaria para identificar, detectar o contrarrestar cualquier amenaza de este tipo;
2) Exigir a cualquier persona vinculada a un operador de infraestructura crítica que se le proporcione información relacionada con el diseño, configuración, operación o la ciberseguridad de cualquier sistema de información;
3) Requerir a cualquier persona vinculada a un operador de infraestructura crítica que se apliquen medidas como la eliminación de software malicioso de un sistema de información, la instalación de actualizaciones de software para hacer frente a las vulnerabilidades de ciberseguridad, desconectar temporalmente los sistemas de información infectados de una red y el redireccionamiento del tráfico de datos malintencionados hacia un sistema de información designado.

Párrafo.- 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 Centro 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 49.-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. - Con la finalidad de asegurar la buena fe de la persona que divulgue una vulnerabilidad se tomará en cuenta que:

1) No se haya solicitado recompensas bajo coerción o amenaza de publicación de la información;

2) No se otorgue un tiempo razonable para solucionar la vulnerabilidad antes de publicarla o divulgarla; y,

3) 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.

Artículo 50.-Estado de alarma cibernética. Un estado de alarma cibernética es un estado durante el cual la ciberseguridad en los sistemas de información de las infraestructuras críticas está gravemente en peligro y, por lo tanto, los intereses de la República Dominicana pueden ser violentados o amenazados. Para considerar que las infraestructuras críticas están gravemente en peligro se tomará cuenta los siguientes aspectos:

1. Se crea que existe un riesgo de que se cause un daño significativo a una infraestructura crítica;
2. Se crea que existe un riesgo de interrupción en la prestación de un servicio esencial a través de un sistema informático.
3. Se crea que existe una amenaza para la seguridad nacional, la defensa, las relaciones exteriores, la economía y las finanzas, la salud, la seguridad o el orden público de República Dominicana; o
4. La amenaza o incidente de ciberseguridad es de naturaleza grave, en términos de la gravedad del daño que puede causar a las personas o el número de sistemas de información o el valor de la información puesta en riesgo.

Artículo 51.-Declaración del estado de alarma cibernética. El estado de alarma cibernética será declarado por el presidente de la República por recomendación motivada del Director Ejecutivo del Centro Nacional de Ciberseguridad.

Artículo 52.-Declaración de estado de excepción y gestión de riesgos de desastres. El Centro Nacional de Ciberseguridad (CNCS) recomendará al presidente de la República cuando considere que el estado de alarma cibernética deba dar lugar a la declaración de uno de los estados de excepción previstos en la Constitución. De igual forma, comunicará a las instituciones que, conforme a la legislación vigente, encabecen el sistema de prevención, mitigación y respuestas a riesgos desastres, cuando interprete que una amenaza, vulnerabilidad o incidente de ciberseguridad resulte importante para el cumplimiento de las tareas asociadas a ese sistema.

Párrafo I.- El Reglamento de aplicación de la presente ley aportará la forma y los criterios que deberá observar el CNCS para proceder a las comunicaciones referidas en el presente artículo y la información mínima que cada una deberá contener.

Párrafo II.- Las decisiones y medidas de carácter general emitidas por el Centro Nacional de Ciberseguridad, de conformidad con los artículos 47 y 48

de la presente ley, antes de la declaración de estado de excepción, seguirán siendo efectivas, siempre y cuando dichas medidas no contradigan las medidas declaradas por el gobierno.

Artículo 53.-Entrada en vigor y período del estado de alarma cibernética. La decisión sobre la declaración del estado de alarma cibernética entrará en vigor en el momento en que se estipule en dicha decisión y la misma se declarará por un período máximo de tiempo necesario de siete (7) días. El período dado puede prolongarse; pero el período total de un estado de alarma cibernética declarado no excederá de treinta (30) días.

Párrafo I.- Durante el estado de alarma cibernética, el Director Ejecutivo del Centro Nacional de Ciberseguridad informará al gobierno sobre los elementos justificativos del estado de alarma cibernética, las acciones implementadas y sobre el estado de los incidentes, vulnerabilidades y amenazas.

Párrafo II.- En virtud de la declaración de estado de alarma cibernética, las medidas establecidas en los artículos 47 y 48 dirigidas a los operadores de infraestructuras críticas y a las personas y sistemas informáticos vinculados a éstos, tendrán cumplimiento general, extendiéndose a todas las personas físicas y morales, públicas y privadas.

Párrafo III.- El estado de alarma cibernética no se declarará en caso de que la amenaza a la ciberseguridad de las infraestructuras críticas pueda ser evitada por las actividades del Centro Nacional de Ciberseguridad de conformidad con esta ley.

Párrafo V.- El estado de alarma cibernética terminará después del período dado, a menos que el director del CNCS decida terminarlo antes o por declaración de uno de los estados de excepción previstos en la Constitución que así lo disponga.

CAPÍTULO V
RÉGIMEN SANCIONADOR

SECCIÓN I
SANCIONES ADMINISTRATIVAS

Artículo 54.-Facultad sancionadora. El Centro Nacional de Ciberseguridad, como órgano encargado de velar por el cumplimiento de la presente ley es el responsable por ejercer el régimen sancionador conforme se describe en el presente capítulo.

Artículo 55.-Faltas administrativas. Se considerarán faltas administrativas las siguientes:

1. No cumplir con una comunicación de entrega de información requerida por el Centro Nacional de Ciberseguridad;
2. No cumplir con una notificación de cambios sustanciales en una infraestructura crítica;
3. No cumplir con designar un Punto de Contacto Único para una infraestructura crítica;
4. No cumplir con notificar un cambio de operador de una infraestructura crítica;
5. No cumplir con notificar los incidentes de ciberseguridad al Centro Nacional de Ciberseguridad;
6. No cumplir con notificar los incidentes de ciberseguridad a las personas posiblemente afectadas;
7. No cumplir con establecer mecanismos técnicos y procedimentales con el fin de detectar amenazas e incidentes de ciberseguridad;
8. No cumplir con enviar al Centro Nacional de Ciberseguridad 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 del mismo;
9. No cumplir con llevar a cabo auditorías o la evaluación de riesgo sobre su cumplimiento con esta ley;
10. No remitir la auditoría o la evaluación del riesgo de ciberseguridad al Centro Nacional de Ciberseguridad en los plazos establecidos;
11. No llevar a cabo las auditorías o la evaluación de riesgo de manera satisfactoria;
12. Realizar un cambio sustancial a una infraestructura crítica y no llevar a cabo la auditoría o evaluación de riesgo;
13. Obstruir o impedir que se lleve a cabo una auditoría o evaluación de riesgo;
14. No participar en un ejercicio de ciberseguridad requerido por el Centro Nacional de Ciberseguridad;
15. No proporcionar información, registros o documentos requeridos por el Centro Nacional de Ciberseguridad para responder a un incidente de ciberseguridad;
16. No cumplir con una orden emitida por el Centro Nacional de Ciberseguridad con la finalidad de prevenir, detectar o contrarrestar cualquier amenaza o incidente de ciberseguridad;

17. Obstruir al Centro Nacional de Ciberseguridad o a quien este designe para hacer cumplir cualquier medida emitida a fin de identificar, detectar o contrarrestar cualquier amenaza de ciberseguridad;
18. No cumplir con una orden de prohibición de utilizar un sistema de información o cualquiera de sus partes en caso de que el Centro Nacional de Ciberseguridad los haya notificado;
19. No cumplir con las disposiciones de los reglamentos dictados por el Centro Nacional de Ciberseguridad.

Artículo 56.-Excepción a la imposición de sanción. El operador de una infraestructura critica no será responsable de una falta administrativa en caso de que pueda demostrar haber hecho todo lo posible y lo que es posible exigir, para evitar el incumplimiento de las obligaciones establecidas por esta ley.

Artículo 57.-De las sanciones. A quienes incurran en las faltas administrativas en esta ley, el Centro Nacional de Ciberseguridad, sin perjuicio de las sanciones civiles y penales, serán sancionadas con una multa equivalente a un monto entre los veinte (20) y doscientos (200) salarios mínimos del sector público, observando el principio de proporcionalidad de las sanciones

Párrafo I.- El pago de la sanción no implica la convalidación de la situación irregular, debiendo el infractor cesar de inmediato los actos que dieron lugar a la sanción.

Párrafo II.- Los montos de las sanciones serán cobrados por el Centro Nacional de Ciberseguridad. Los ingresos de estas sanciones pasarán a formar parte de su presupuesto operativo.

Párrafo III.- El monto de las sanciones debe abonarse a más tardar treinta (30) días después de la entrada en vigor de la decisión de su imposición y será aumentado mensualmente, en un tres (3%) por ciento del monto original, cada vez, si en el plazo previsto para su pago no hubieren sido canceladas por el imputado.

Artículo 58.-Prescripción de las sanciones. Las faltas impuestas por esta ley prescriben en a los tres (3) años de la ocurrencia del evento.

Párrafo I.- El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla

Párrafo II.- La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 59.-Recurso de reconsideración. Quienes sean sancionados por la comisión de las faltas administrativas contenidas en esta ley podrán ejercer un

recurso de reconsideración con las formalidades y plazos establecidos en la Ley Núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, por ante el mismo órgano que dictó la decisión. El recurso de reconsideración será ante el Consejo Directivo del Centro Nacional de Ciberseguridad.

Artículo 60.-Recurso contencioso administrativo. El recurso contencioso Administrativo a las sanciones impuestas se hará según lo establecido en la Ley Núm. 13-07, que crea el Tribunal Contencioso Tributario y Administrativo.

SECCIÓN II
SANCIONES PENALES

Artículo 61.-Sanciones al desacato durante un estado de alarma cibernética. Toda persona que violente o vulnere las directrices o instrucciones emanadas por el Centro Nacional de Ciberseguridad (CNCS) durante un estado de alarma cibernética, atentando así contra los intereses fundamentales y seguridad de la nación será sancionada de la siguiente forma:

1. El desacato de una persona debido a su negligencia que no haya tenido como consecuencia perjuicios, con multa equivalente entre cien (50) a quinientos (500) y/o prisión de entre tres (3) meses y un (1) año, considerando las razones de negligencia o imprudencia que determinaron la inobservancia
2. El desacato de una persona en que se verifique la materialización de algún perjuicio será castigado con las penas que van desde las destinadas al acceso ilicitico a aquellas reservadas para los crímenes y delitos contra la nación cometidos mediante un sistema informático, electrónico, telemático o de telecomunicaciones contemplados en la legislación penal especializada en materia ciberdelincuencia, considerando la intención y la gravedad del perjuicio causado.

CAPÍTULO VI
DISPOSICIÓNES FINALES

Artículo 62.-Disposición derogatoria. Se derogan por sustitución los artículos 11 al 24 del Decreto Núm. 230-18 que establece la Estrategia Nacional de Ciberseguridad 2018-2021 y que crea el Centro Nacional de Ciberseguridad. La parte restante del Decreto estará vigente hasta que el Poder Ejecutivo establezca mediante decreto el reglamento de aplicación de la presente ley.

Artículo 63.-Reglamento de aplicación. En un plazo no mayor a 6 meses de la entrada en vigencia de la presente ley, el Poder Ejecutivo promulgará el decreto que establecerá el reglamento de aplicación de la presente ley.

Artículo 64.-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.

DADA...

FARIDE RAFUL
SENADORA DEL DISTRITO NACIONAL

SENADO
DISTRITO NACIONAL
REPÚBLICA DOMINICANA

SENADO REPÚBLICA DOMINICANA
DISTRITO NACIONAL
Faride Raful

OSDN – 0145/2021

Santo Domingo, D.N.
22 de abril de 2021

SENADO DE LA REPUBLICA
SECRETARIA GENERAL LEGISLATIVA
FECHA 22/4/2021 HORA 1:22 P.M.
RECIBIDO POR Rosana Sánchez

Señor
Arq. Eduardo Estrella
Presidente
Senado de la República
Su Despacho.

Vía:
Dr. Domingo Carrasco
Secretario General Legislativo

Distinguido Presidente:

Muy cortésmente, le solicitamos poner en agenda el Anteproyecto de Ley de Ciberseguridad, el cual persigue fortalecer el marco administrativo de la seguridad informática en la República Dominicana. Este lleva a nivel de ley la Estrategia Nacional de Ciberseguridad y da mayor relevancia al Centro que lo coordina, creado por el Decreto Núm. 230-18, el cual pasa de ser una dependencia a convertirse en ente público con personalidad jurídica propia y autonomía funcional y financiera.

Adicionalmente, con la aprobación de esta propuesta, República Dominicana enriquece su ordenamiento jurídico interno atendiendo las normas de cumplimiento voluntario de grupos como la Comisión Global sobre la Estabilidad del Ciberespacio, el Llamado de París para la Confianza y la Seguridad en el Ciberespacio, pero sobre todo tomando en cuenta el contenido de las Normas del Grupo de Expertos Gubernamentales de la Naciones Unidas del 2015 (UNGGE). A la vez, se pone especial énfasis en las obligaciones que deben cumplir los operadores de infraestructuras críticas, en la prevención y gestión de incidentes de ciberseguridad.

Esperando contar con su buena disposición,

Muy atentamente,

SENADO DISTRITO NACIONAL REPÚBLICA DOMINICANA

Faride Raful
Senadora Distrito Nacional

FR/op

Anexo: Citado.

distrito@senado.gob.do
Congreso Nacional, Av. Jiménez Moya, Sto. Dgo. Rep. Dominicana.
Oficina: 1 (809) 532-5561 Ext. 5274 • distritonacional@senado.com.do • wwwfaride2020.com