Danilo Medina
Presidente de la República Dominicana

NÚMERO: 230-18

CONSIDERANDO: Que el artículo 7 de la Constitución establece que la República Dominicana es un Estado Social y Democrático de Derecho, organizado en forma de República unitaria, fundado 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: Que el artículo 8 de la Constitución de la República 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, compatibles con el orden público, el bienestar general y los derechos de todos y todas.

CONSIDERANDO: Que el derecho a la intimidad está consagrado como un derecho fundamental en nuestra Constitución, garantizándose el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, sus documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo, así como la inviolabilidad del secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo cuando sea mediante autorizaciones otorgadas por un juez o autoridad competente, de conformidad con la ley.

CONSIDERANDO: Que los derechos fundamentales vinculan a todos los poderes públicos, los cuales deben garantizar su efectividad, de conformidad con la Constitución y las leyes.

CONSIDERANDO: Que la integración de las telecomunicaciones y las tecnologías de la información y la comunicación (TIC) en nuestras actividades económicas y sociales ha creado una creciente dependencia de estas en el ámbito mundial, pues se han convertido en esenciales para el desarrollo económico, cohesión social y seguridad nacional.

CONSIDERANDO: Que la alta incidencia de las telecomunicaciones y las tecnologías de la información y la comunicación (TIC) en el desarrollo de las actividades económicas, sociales y gubernamentales, hace imprescindible la adopción de medidas que garanticen la protección de los activos críticos de información del Estado y la seguridad de la información por parte de las instituciones públicas y privadas y demás sectores que han incorporado el uso de estas tecnologías.

CONSIDERANDO: Que conscientes de la necesidad de implementar instrumentos indispensables para responder a las nuevas amenazas que afectan a las naciones y sus ciudadanos, los Estados integrados en los principales organismos internacionales han acordado la realización de esfuerzos mancomunados para la adopción de estrategias

integrales sobre ciberseguridad que tengan impacto nacional, regional y mundial para prevenir eficazmente el riesgo ante cualquier ataque cibernético y poder responder a estos en caso de que se presenten.

CONSIDERANDO: Que el Estado dominicano en el proceso de desarrollo y crecimiento de las políticas y estrategias integrales que propician el uso extensivo e incluyente de las tecnologías de la información y la comunicación (TIC) ha entendido la necesidad de establecer mecanismos eficientes que respondan a las nuevas y graves amenazas que surgen a través de estas.

CONSIDERANDO: Que el artículo 260 de la Constitución de la República establece como objetivos de alta prioridad nacional: 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: Que en el artículo 16 de la Ley núm. 1-12, del 25 d enero de 2015, que establece la Estrategia Nacional de Desarrollo 2030 , relativo al uso de las tecnologías de la información y la comunicación (TIC) se establece que en el diseño y ejecución de los programas, proyectos y actividades en que se concretan las políticas públicas, se deberá promover el uso de las tecnologías de la información y comunicación como instrumento para mejorar la gestión pública y fomentar una cultura de transparencia y acceso a la información, mediante la eficientización de los procesos de provisión de servicios públicos y la facilitación del acceso a los mismos.

CONSIDERANDO: Que el Programa República Digital, creado mediante Decreto núm. 258-16, del 16 de septiembre de 2016, y concebido como el conjunto de políticas y acciones que promueven la inclusión de las tecnologías de información y comunicación en los procesos productivos, educativos, gubernamentales y a los servicios ciudadanos, tiene como eje transversal la ciberseguridad para el desarrollo de un Estado digital.

CONSIDERANDO: Que la responsabilidad de crear un entorno seguro y fiable en el ciberespacio corresponde al Estado, eje transversal del esquema de seguridad y defensa nacional preestablecido.

CONSIDERANDO: Que la ciberseguridad constituye la garantía para que los Estados salvaguarden sus infraestructuras críticas y el derecho de sus habitantes de utilizar las tecnologías de la información y la comunicación (TIC) de manera segura y confiable, basándose en la colección de herramientas, dispositivos, regulaciones y mejores prácticas para proteger el ciberespacio y los activos de los usuarios y organizaciones.

CONSIDERANDO: Que el Instituto Dominicano de las Telecomunicaciones (INDOTEL), en su calidad de órgano regulador de las telecomunicaciones y como integrante de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología

(CICDAT), ha asumido un rol activo en el desarrollo de un marco común de políticas y lineamientos en materia de ciberseguridad para el país, a fin de garantizar la protección adecuada de la información, en el marco de su deber de asegurar el principio de servicio universal, objetivo de interés público y social establecido en la Ley núm. 153-98, del 27 de mayo de 1998, General de Telecomunicaciones.

CONSIDERANDO: Que en el marco de la modernización de la gestión del Estado, el Instituto Dominicano de las Telecomunicaciones (INDOTEL) ha propuesto la adopción de una Estrategia Nacional de Ciberseguridad y la creación de un Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD), en consonancia con la tendencia internacional, lo que permitirá establecer las directrices a ser adoptadas para que nuestro país se encuentre en condiciones de detectar, mitigar y, en general, gestionar incidentes generados en los sistemas de información del Estado y en todas las infraestructuras críticas nacionales.

CONSIDERANDO: Que la Estrategia Nacional de Ciberseguridad 2018-2021 debe contemplar la creación de un órgano responsable de coordinar las acciones relacionadas con la ciberseguridad en el ámbito nacional.

CONSIDERANDO: Que la Comisión Interamericana de Telecomunicaciones (CITEL), el Comité Interamericano contra el Terrorismo (CICTE) y la Reunión de Ministros de Justicia o Procuradores Generales de las Américas (REMJA) elaboraron una estrategia hemisférica para la seguridad cibernética en la región, conforme a lo dispuesto por la Resolución AG/RES. 2004 (XXXIV-0/04) de la Asamblea General de la Organización de Estados Americanos (OEA), del 8 de junio de 2004.

CONSIDERANDO: Que, mediante la Resolución núm. 158-12, del 11 de junio de 2012, del Congreso Nacional, el Estado dominicano ratificó el Convenio sobre la Cibercriminalidad, suscrito en Budapest el 23 de noviembre de 2001, cuyo objetivo es la prevención de los actos que pongan en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de estos, y el establecimiento de esfuerzos comunes para la luchar contra tales delitos y proveer a las autoridades competentes de las herramientas para investigarlos y perseguirlos penalmente.

CONSIDERANDO: Que la Estrategia Nacional de Ciberseguridad 2018-2021debe establecer las líneas de acción a ser implementadas para mitigar el riesgo y minimizar el impacto de las amenazas cibernéticas en los sistemas de información y proteger las infraestructuras críticas para que la población utilice de manera confiada los servicios que se ofrecen a través de las tecnologías de la información y la comunicación (TIC).

CONSIDERANDO: Que en el marco de la Estrategia Nacional de Ciberseguridad 2018-2021 resulta de alto interés el establecimiento de un Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) para prevenir, mitigar y responder a los incidentes cibernéticos.

Danilo Medina
Presidente de la República Dominicana

VISTA: La Constitución de la República, proclamada el 13 junio de 2015.

VISTO: El Convenio sobre la Cibercriminalidad, suscrito en Budapest el 23 de noviembre de 2001, ratificado por el Congreso Nacional, mediante Resolución núm. 158-12, del 11 de junio de 2012.

VISTA: La Ley núm. 153-98, del 27 de mayo de 1998, General de las Telecomunicaciones.

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

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.

VISTA: La Ley núm. 1-12, del 25 d enero de 2015, que establece la Estrategia Nacional de Desarrollo 2030.

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

VISTO: El Decreto núm. 134-14, del 9 de abril de 2014, que establece el Reglamento de Aplicación de la Ley Orgánica núm. 1-12.

VISTO: El Decreto núm. 258-16, del 16 de septiembre de 2016, que crea el Programa República Digital, para promover la inclusión de las tecnologías de información y comunicación en los procesos productivos, educativos, gubernamentales y de servicios a los ciudadanos y crea e integra la Comisión Presidencial de República Digital.

VISTA: La Resolución AG/RES.2004 (XXXIV-0/04), del 8 de junio de 2004, de la Asamblea General de la Organización de Estados Americanos (OEA) para la Adopción de una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética.

VISTA: La Declaración de Santo Domingo AG/DEC. 46 (XXXVI-O/06), del 6 de junio de 2006, sobre Gobernabilidad y Desarrollo en la Sociedad del Conocimiento, de la Organización de los Estados Americanos (OEA).

Danilo Medina
Presidente de la República Dominicana

VISTO: El Acuerdo de Cooperación en materia de Seguridad Cibernética entre el Instituto Dominicano de las Telecomunicaciones (INDOTEL) y la Secretaría General de la Organización de Estados Americanos (SG/OEA), firmado el 20 de noviembre de 2015.

En ejercicio de las atribuciones que me confiere el artículo 128 de la Constitución de la República dicto el siguiente:

D E C R E T O:

Artículo 1. Objeto del decreto. El objeto de este decreto es establecer y regular la Estrategia Nacional de Ciberseguridad 2018-2021.

Artículo 2. Misión de la Estrategia Nacional de Ciberseguridad 2018-2021. La Estrategia Nacional de Ciberseguridad 2018-2021 tiene como misión establecer los mecanismos de ciberseguridad adecuados para la protección del Estado, sus habitantes y, en general, del desarrollo y la seguridad nacional.

Artículo 3. Visión de la Estrategia Nacional de Ciberseguridad 2018-2021. Para el año 2021 la República Dominicana cuenta con un ciberespacio más seguro, en el que están implementadas las medidas necesarias para el desarrollo confiable de las actividades productivas y lúdicas de toda la población, de conformidad con la Constitución y demás leyes del ordenamiento jurídico dominicano.

Artículo 4. Pilares de la Estrategia Nacional de Ciberseguridad 2018-2021. El marco de acción de la Estrategia Nacional de Ciberseguridad 2018-2021 se desarrollará contemplando cuatro (4) pilares estratégicos:

1. Marco Legal y Fortalecimiento Institucional.

2. Protección de Infraestructuras Críticas Nacionales e Infraestructuras TI del Estado.

3. Educación y Cultura Nacional de Ciberseguridad.

4. Alianzas Nacionales e Internacionales.

Artículo 5. Pilar 1: Marco Legal y Fortalecimiento Institucional. El objetivo general de este pilar es fortalecer el marco legal que incide en los temas relacionados con la ciberseguridad y las capacidades de las unidades especializadas y competentes para prevenir, investigar y decidir sobre crímenes y delitos de alta tecnología. De este se derivan los siguientes objetivos específicos y líneas de acción:

Objetivo específico 1: Fortalecer el marco jurídico que facilite un ciberespacio seguro en la República Dominicana.

Línea de acción 1.1: Establecer y ejecutar un plan de actualización y reforma detallada del marco jurídico vigente e identificar las oportunidades de mejora, para recomendar y aplicar las modificaciones correspondientes.

Línea de acción 1.2: Establecer y ejecutar un plan de actualización y reformas periódicas del marco regulatorio, tomando en consideración la naturaleza cambiante de la materia.

Objetivo específico 2: Fortalecer la capacidad de los órganos de investigación de crímenes y delitos de alta tecnología del Estado para recolectar y procesar adecuadamente la evidencia electrónica.

Línea de acción 2.1: Realizar una evaluación de las capacidades de los órganos de investigación para determinar el nivel de capacidad que existe en el Distrito Nacional y cada una de las provincias del país.

Línea de acción 2.2: Incluir en el plan de estudios de las escuelas de los órganos de investigación, la recopilación de la evidencia electrónica y cursos de desarrollo profesional continuo para la investigación, procesamiento y conservación de evidencias electrónicas.

Línea de acción 2.3: Fortalecer la relación del servicio de la Policía Nacional con el público para fomentar la colaboración ciudadana y la confianza para la notificación sobre delitos cibernéticos e incidentes de impacto nacional.

Línea de acción 2.4: Desarrollar las normas y directrices para el procesamiento de las escenas de hechos o sucesos que puedan contener potencial evidencia electrónica, su manipulación, cadena de custodia, procesamiento y conservación para su posterior presentación en los tribunales, de conformidad con los principios del debido proceso establecidos en el artículo 69 de la Constitución de la República.

Objetivo específico 3: Aumentar y fortalecer la capacidad del Ministerio Público y sus organismos auxiliares para perseguir, y del Poder Judicial para decidir, sobre delitos cibernéticos de manera adecuada y justa.

Línea de acción 3.1: Desarrollar una formación específica tanto para el Ministerio Público y sus organismos auxiliares como para el Poder Judicial sobre delitos cibernéticos y evidencia digital con el objetivo de mejorar sus conocimientos y promover la aplicación coherente de la ley.

Artículo 6. Pilar 2: Protección de Infraestructuras Críticas Nacionales e Infraestructuras TI del Estado. El objetivo general de este pilar es asegurar el continuo funcionamiento y la protección de la información almacenada en las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado. De este se derivan los siguientes objetivos específicos y líneas de acción:

Objetivo específico 1: Identificar las infraestructuras críticas nacionales y las infraestructuras TI relevantes del Estado y efectuar un análisis de riesgo.

Línea de acción 1.1: Establecer los criterios que determinan el grado de criticidad de una infraestructura, basado en los estándares internacionales en la materia.

Línea de acción 1.2: Catalogar las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado de acuerdo a los criterios que determinan su grado de criticidad, incluyendo los servicios colaterales que las soportan.

Línea de acción 1.3: Efectuar análisis de riesgo sobre las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado y determinar su nivel de vulnerabilidad.

Objetivo específico 2: Elaborar e implementar un plan de robustecimiento de la seguridad de las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado, así como de los servicios colaterales que las soportan, frente a las amenazas cibernéticas.

Línea de acción 2.1: Considerar las mejores prácticas en la gestión de la ciberseguridad.

Línea de acción 2.2: Analizar, mejorar e implementar las normas emitidas por los entes reguladores correspondientes.

Línea de acción 2.3: Establecer e implementar esquemas de gobernabilidad que permitan la supervisión y evaluación periódicas de las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado.

Objetivo específico 3: Mejorar la coordinación intersectorial e interinstitucional para la protección de los sistemas de información y las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado y el sector privado.

Línea de acción 3.1: Establecer un Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD).

Línea de acción 3.2: Promover la creación de Equipos Sectoriales de Respuestas a Incidentes Cibernéticos en los sectores que así lo requieran para gestionar los riesgos de ciberseguridad y reportar oportunamente sus operaciones y hallazgos al Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD)..

Línea de acción 3.3: Definir el protocolo para el intercambio de información y comunicación entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos y el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD).

Línea de acción 3.4: Establecer y hacer cumplir requisitos mínimos de seguridad, listeza forense y planes de recuperación de las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado.

Objetivo específico 4: Elaborar un plan de respuesta ante incidentes cibernéticos en las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado y el sector privado.

Línea de acción 4.1: Identificar los organismos principales en el área de respuesta a incidentes que puedan proporcionar apoyo crítico a las infraestructuras críticas nacionales e infraestructuras TI del Estado y el sector privado, en base al Plan Nacional de Respuesta a Incidentes de Ciberseguridad.

Línea de acción 4.2: Definir el protocolo de activación y acción de los organismos de respuesta frente a incidentes de ciberseguridad.

Línea de acción 4.3: Coordinar y monitorear las actividades de recuperación de incidentes hasta asegurar el estado normal de operación.

Líneas de acción 4.4: Crear un plan de ejercicios periódicos de simulación de incidentes y prácticas ante incidentes cibernéticos en las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado y el sector privado.

Artículo 7. Pilar 3: Educación y Cultura Nacional de Ciberseguridad. El objetivo general de este pilar es fomentar la inclusión de la formación en ciberseguridad en todos los niveles del sistema educativo e impulsar una cultura nacional de ciberseguridad. De este se derivan los siguientes objetivos específicos y líneas de acción:

Objetivo específico 1: Incorporar el manejo de los conceptos fundamentales de la seguridad de la información en las escuelas públicas y privadas.

Línea de acción 1.1: Incluir planes de capacitación en materia de ciberseguridad al personal docente de nivel básico y secundario, con énfasis en la equidad de género.

Línea de acción 1.2: Adecuar los planes de estudio de educación básica y secundaria para incluir la ciberseguridad y el cibercivismo, con énfasis en la equidad de género.

Objetivo específico 2: Aumentar la disponibilidad de programas educativos de grado y postgrado en seguridad de la información.

Línea de acción 2.1: Extender los planes de capacitación en materia de ciberseguridad al personal docente universitario de grado y postgrado, con énfasis en la equidad de género.

Línea de acción 2.2: Fortalecer en materia de ciberseguridad los pénsum de las carreras tecnológicas y de derecho, entre otras, de las universidades públicas y privadas.

Línea de acción 2.3: Crear un marco de coordinación para implementar programas avanzados de investigación en ciberseguridad, en cooperación con instituciones académicas.

Línea de acción 2.4: Desarrollar programas de formación, desarrollo y captación de talentos en materia de ciberseguridad.

Objetivo específico 3: Mejorar las capacidades técnicas y procesales de ciberseguridad en las entidades del Gobierno y del sector privado que operan infraestructuras críticas nacionales e infraestructuras TI.

Línea de acción 3.1: Establecer programas de formación continua de los recursos humanos en la prevención, protección y respuesta de las amenazas cibernéticas.

Línea de acción 3.2: Establecer un sistema de certificación emitida por parte de una institución acreditada para el personal de ciberseguridad.

Objetivo específico 4: Sensibilizar a la sociedad civil y política en los temas de ciberseguridad y el uso responsable de las tecnologías de la información.

Línea de acción 4.1: Realizar campañas de educación sobre los aspectos de ciberseguridad.

Línea de acción 4.2: Crear un plan nacional para la protección en línea de los niños, niñas y adolescentes.

Línea de acción 4.3: Desarrollar programas de incentivos para las organizaciones del sector privado que colaboren con el Gobierno en las campañas de sensibilización

Línea de acción 4.4: Llevar a cabo una encuesta nacional para determinar el nivel de conocimiento sobre la materia del sector público, en sentido general, y sectores específicos.

Artículo 8. Pilar 4: Alianzas Nacionales e Internacionales. El objetivo general de este pilar es establecer alianzas nacionales e internacionales entre los sectores público y privado, así como con la sociedad civil y organismos e instituciones internacionales. De este se derivan los siguientes objetivos específicos y líneas de acción:

Objetivo específico 1: Fomentar mecanismos de cooperación nacional entre los sectores público y privado, así como con la sociedad civil.

Línea de acción 1.1: Establecer alianzas para la creación de una plataforma que permita compartir información de incidentes, amenazas, mejores prácticas, directrices, eventos e iniciativas de creación de capacidad y resiliencia cibernética.

Objetivo específico 2: Fomentar la relación con organismos e instituciones internacionales para facilitar la cooperación transfronteriza y crear más confianza en el área de respuesta a incidentes regionales y en la colaboración y el intercambio de información internacional.

Línea de acción 2.1: Fomentar los acuerdos bilaterales y multilaterales para cooperación, intercambio de experiencias e información relacionada con la ciberseguridad y la lucha contra la ciberdelincuencia.

Línea de acción 2.2: Asegurar la participación de República Dominicana en los foros internacionales sobre los avances de la ciberseguridad y la lucha contra la ciberdelincuencia.

Línea de acción 2.3: Identificar los países con objetivos de investigación y desarrollo similares a los del país y fomentar el intercambio de información y conocimiento con estos.

Artículo 9. Plan de Acción y Revisión. Dentro de los noventa (90) días siguientes a la emisión de este decreto se establecerá el Plan de Acción y Revisión, en el que se definirán las actividades prioritarias, los plazos, el presupuesto y las instituciones responsables de la implementación de cada una de las acciones. En este se identificarán y acordarán los indicadores claves para asegurar que la Estrategia Nacional de Ciberseguridad 2018-2021 esté cumpliendo con sus metas y objetivos. También se definirá el marco de evaluación para fines de seguimiento y mejora continua.

Párrafo. De esta forma, la Estrategia Nacional de Ciberseguridad 2018-2021 será revisada a los dieciocho (18) meses de su implementación para identificar lecciones aprendidas, suministrar recomendaciones en cuanto a si existe o no la necesidad de modificar los objetivos e identificar el grado de cumplimiento de los indicadores claves definidos en el marco de evaluación. Las revisiones subsiguientes serán definidas en el Plan Estratégico Institucional y Operativo Anual del Centro Nacional de Ciberseguridad.

Artículo 10. Creación del Centro Nacional de Ciberseguridad. Se crea el Centro Nacional de Ciberseguridad como dependencia del Ministerio de la Presidencia de la República Dominicana.

Artículo 11. Objeto del Centro Nacional de Ciberseguridad. El Centro Nacional de Ciberseguridad tiene por objeto la elaboración, desarrollo, actualización y evaluación de la Estrategia Nacional de Ciberseguridad 2018-2021, la formulación de políticas derivadas de dicha estrategia y la definición de las iniciativas, programas y proyectos que lleven a la realización exitosa de esta, así como la prevención, detección y gestión de incidentes

generados en los sistemas de información relevantes del Estado e infraestructuras críticas nacionales.

Artículo 12. Conformación del Centro Nacional de Ciberseguridad. El Centro Nacional de Ciberseguridad estará integrado por un Consejo Directivo, su máxima autoridad, y por una Dirección Ejecutiva.

Párrafo I. El Consejo Directivo estará compuesto por las siguientes entidades:

a) Ministerio de la Presidencia, el cual lo preside.
b) Dirección Ejecutiva del Centro Nacional de Ciberseguridad, representada por su Director Ejecutivo, quien ostentará la calidad de Secretario y miembro de pleno derecho del Consejo.
c) Ministerio de Defensa.
d) Ministerio de Interior y Policía.
e) Procuraduría General de la República.
f) Policía Nacional.
g) Departamento Nacional de Investigaciones (DNI).
h) Instituto Dominicano de las Telecomunicaciones (INDOTEL).
i) Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC).

Párrafo II. El Consejo Directivo tendrá la facultad, cuando el caso lo amerite, de requerir la participación de otros representantes del Estado, tales como: el Ministerio de Relaciones Exteriores, la Dirección Nacional de Control de Drogas, la Administración Monetaria y Financiera, la Academia, operadores de infraestructuras críticas, el sector privado, el Poder Legislativo, el Poder Judicial y la ciudadanía en general.

Párrafo III. Además, el Centro Nacional de Ciberseguridad contará con dos equipos principales: un Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) y un Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD), el cual se auxiliará de los Equipos Sectoriales de Respuestas a Incidentes.

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

a) Articular, alinear e insertar en los entes y órganos del Estado las distintas iniciativas en materia de ciberseguridad.

b) Prestar asesoría en la ejecución de las iniciativas en materia de ciberseguridad.

c) Celebrar contratos, acuerdos y convenios en materia de ciberseguridad.

d) Recomendar la adhesión de la República Dominicana a los acuerdos, convenios y tratados internacionales en materia de ciberseguridad.

e) Incentivar una cultura de resguardo, control y manejo adecuado de la información de los entes del Estado.

f) Impulsar y promover, a nivel nacional, los aspectos jurídicos, tecnológicos, de formación y de gestión de la ciberseguridad.

g) Coadyuvar en el establecimiento de líneas de investigación asociadas al área de ciberseguridad del Estado dominicano.

h) Colaborar y proponer legislación, normas y estrategias destinadas a incrementar los esfuerzos con la finalidad de aumentar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías de la información y la comunicación.

i) Liderar actividades de capacitación, entrenamiento y sensibilización en la prevención de incidentes cibernéticos y en el buen uso de las tecnologías de la información y comunicación a las instituciones del Estado.

j) Ser el punto de contacto entre el Estado Dominicano y otros organismos nacionales e internacionales de similar naturaleza.

k) Apoyar a las fuerzas de orden y cuerpos de seguridad e investigación para la prevención e investigación de crímenes y delitos que involucren tecnologías de la información y comunicación en sistemas informáticos de los órganos y entes del Estado.

l) Elaborar y difundir recomendaciones, buenas prácticas y estándares en materia de protección de activos de información críticos.

m) Emitir su opinión cuando le sea solicitada o cuando por la naturaleza del incidente de ciberseguridad estime pertinente.

n) Cualquier otra función que les sea encomendada para garantizar la seguridad en los sistemas informáticos de las entidades del Estado.

Artículo 14. Funciones del Consejo Directivo del Centro Nacional de Ciberseguridad. El Consejo Directivo del Centro Nacional de Ciberseguridad tendrá las siguientes funciones:

a) Coordinar el funcionamiento interinstitucional del Centro Nacional de Ciberseguridad.

b) Aprobar el Plan Operativo Nacional del Centro Nacional de Ciberseguridad y sus actualizaciones, su presupuesto y los estados financieros.

c) Aprobar el Plan de Acción y Revisión de la Estrategia Nacional de Ciberseguridad 2018-2021;

d) Aprobar el Plan Estratégico Institucional de Ciberseguridad.

e) Definir políticas, establecer directrices y elaborar propuestas de estrategias y planes para someterlas a la aprobación del Poder Ejecutivo.

f) Garantizar mecanismos eficaces de financiamiento para el Centro Nacional de Ciberseguridad.

g) Garantizar la sostenibilidad y el buen funcionamiento del Centro Nacional de Ciberseguridad.

Artículo 15. Funciones de la Dirección Ejecutiva del Centro Nacional de Ciberseguridad. La Dirección Ejecutiva del Centro Nacional de Ciberseguridad tendrá las siguientes funciones:

a) Diseñar las políticas y aprobar los estatutos, reglamentos y manuales organizativos y de funciones de la institución.

b) Administrar los recursos de la institución acorde a la planificación anual.

c) Representar legalmente a la institución.

d) Fijar las remuneraciones del personal de la institución, de conformidad con las leyes que regulan la materia.

e) Elaborar el Plan de Acción y Revisión de la Estrategia Nacional de Ciberseguridad 2018-2021;

f) Disponer las medidas de seguridad necesarias y suficientes para proteger todas aquellas informaciones o datos que por sus características deban permanecer en condición de confidencialidad, con el objeto de prevenir el uso indebido de estos.

g) Presentar informes periódicos de las actividades realizadas y estadísticas recopiladas, así como aprobar y divulgar la memoria anual de la institución.

h) Convocar las sesiones del Consejo Directivo y determinar los asuntos a ser incorporados en la agenda.

i) Ejecutar cualesquier otra función señalada por otras normativas.

Artículo 16. Funciones del Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC). El Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) tendrá las siguientes funciones:

a) Definir políticas, establecer directrices y elaborar propuestas de estrategias y planes de acción para el desarrollo de la Estrategia Nacional de Ciberseguridad 2018-2021, a fin de que las entidades a las que correspondan su ejecución puedan gestionar los proyectos conforme a tales directrices.

b) Elaborar y mantener un catálogo de las actividades que sobre ciberseguridad desarrollen los sectores involucrados.

c) Coordinar con los sectores, en los ámbitos de sus respectivas competencias, la implementación y el cumplimiento de los objetivos y prioridades establecidos en la Estrategia Nacional de Ciberseguridad 2018-2021.

d) Sensibilizar a los distintos sectores de la vida nacional sobre la importancia de la ciberseguridad como la herramienta fundamental para asegurar los servicios que ofrecen a través de sus sistemas de información.

e) Evaluar las ejecutorias en el marco de la Estrategia Nacional de Ciberseguridad 2018-2021 y reportar anualmente al Director Ejecutivo.

f) Proponer al Gobierno, sin perjuicio de las competencias que correspondan a los diversos estamentos del Estado, las líneas generales de la posición dominicana en los foros y organismos internacionales relacionados con la ciberseguridad.

g) Apoyar, propiciar y liderar la creación de redes de cooperación entre los sectores público, privado y académico para el impulso de la Estrategia Nacional de Ciberseguridad 2018-2021.

h) Contribuir a la difusión y promoción para la creación de una cultura nacional de ciberseguridad.

i) 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.

j) Cualquier otra función que les sea encomendada para garantizar la seguridad en los sistemas informáticos de las entidades del Estado.

Artículo 17. Funciones del Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD). El Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD) tendrá los siguientes cometidos:

a) Asistir en la respuesta a incidentes de seguridad cibernética a los organismos de su comunidad objetivo afectados.

b) Coordinar con los responsables de la seguridad de la información de los organismos de su comunidad objetivo para la prevención, detección, manejo y recopilación de información sobre incidentes cibernéticos.

c) Asesorar y difundir información para incrementar los niveles de seguridad de las tecnologías de la información y la comunicación (TIC), desarrollar herramientas, técnicas de protección y defensa de los organismos de su comunidad objetivo.

d) Alertar ante amenazas y vulnerabilidades de seguridad en sistemas informáticos de los organismos de su comunidad objetivo.

e) Realizar las tareas preventivas que correspondan para garantizar la seguridad en sistemas informáticos de los organismos de su comunidad objetivo.

f) Coordinar planes de recuperación de desastres.

g) Realizar análisis forenses de los incidentes de seguridad cibernética reportados que no constituyan crimen o delito.

h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad cibernética ocurridos en sistemas informáticos de los organismos de su comunidad objetivo.

i) Fomentar el desarrollo de capacidades y buenas prácticas así como la creación de Equipos Sectoriales de Respuestas a Incidentes.

j) 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 seguridad cibernética.

k) Establecer y mantener un vínculo fluido y una relación colaborativa con otros organismos nacionales e internacionales de respuesta internacionales de similar naturaleza.

l) Fomentar y coordinar la creación de laboratorios orientados a la investigación en temas de ciberseguridad.

m) Cualquier otra función que les sea encomendada para garantizar la seguridad en los sistemas informáticos de las entidades del Estado.

Artículo 18. De las coordinaciones sectoriales. Cada entidad del Gobierno, a través de su unidad de seguridad de la información o la que haga sus veces, creará una unidad coordinadora de respuesta a incidentes cibernéticos, la cual coordinará con el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) para cumplir sus objetivos, a través del responsable que será designado a tales fines por cada entidad del Estado dominicano.

Artículo 19. De la responsabilidad. El resguardo de la integridad de la información es responsabilidad del organismo que la genera o administra. La investigación del origen de los ataques y sus responsables, así como la implementación de las posibles soluciones frente a futuros ataques de seguridad a las redes informáticas, corresponde a las autoridades de cada organismo que haya sufrido el incidente cibernético.

Artículo 20. De la información secreta por seguridad del Estado. Debido al interés público preponderante, se declaran clasificadas como informaciones secretas y, por ende, sujetas a las limitaciones y excepciones dispuestas por la Ley núm. 200-04, del 28 de julio de 2004, General de Libre Acceso a la Información Pública las siguientes:

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

b) Los datos personales de todo aquel que preste servicio en el Centro Nacional de Ciberseguridad.

c) La topología y arquitectura de la red y la infraestructura tecnológica y de telecomunicaciones.

d) Los esquemas de direcciones de Protocolo de Internet (IP), públicas y privadas.

e) La configuración y credenciales de acceso de los equipos.

f) Los códigos de acceso y protocolos de encriptación de los sistemas y redes.

g) Las rutas de enlace desde las prestadoras de servicios de telecomunicaciones.

h) Tráfico de internet entrante y saliente.

i) Plan de continuidad, protección y recuperación ante desastres de las operaciones.

Artículo 21. De la información reservada. Los datos producidos por el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD), se consideran información reservada. Se pueden 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, del 28 de julio de 2004, General de Libre Acceso a la Información Pública.

Artículo 22. De la confidencialidad y el deber de secreto. Los funcionarios o empleados del Centro Nacional de Ciberseguridad tienen la obligación de guardar la reserva y confidencialidad que requieren los asuntos relacionados con su trabajo, especialmente los concernientes al Estado en razón de su naturaleza o en virtud de instrucciones especiales, aún después de haber cesado en el cargo. En ese sentido, en caso de difundir, hacer circular, retirar o reproducir de los archivos de las oficinas documentos o asuntos confidenciales o de cualquier naturaleza que los servidores públicos tengan conocimiento por su investidura oficial, serán sancionados de conformidad con lo dispuesto por la Ley núm. 41-08, del 16 de enero de 2008, de Función Pública.

Artículo 23. De la sostenibilidad financiera. Las actividades y operaciones del Centro Nacional de Ciberseguridad serán financiadas con los montos que se les asignen en la Ley de Presupuesto General del Estado y las donaciones y recursos provenientes de la cooperación técnica internacional y cualquier otro ingreso que provenga de leyes especiales o aportes específicos.

Artículo 24. De las estrategias complementarias. Se instruye a los organismos competentes a que dentro de los sesenta (60) días siguientes a la entrada en vigor de este decreto presenten las políticas y planes de acción necesarios en materia de ciberdelincuencia, ciberterrorismo, ciberdefensa, ciberguerra y criptografía.

DADO en Santo Domingo de Guzmán, Distrito Nacional, capital de la República, a los diecinueve (19 días del mes de junio del año dos mil dieciocho (2018), año 175 de la Independencia y 155 de la Restauración.

DANILO MEDINA