NÚMERO: 313-22

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 éstas en el ámbito mundial, pues se han convertido en esenciales para el desarrollo económico, cohesión social y seguridad nacional, lo cual hace imprescindible la adopción de medidas que garanticen la protección de los activos críticos de información del Estado, así como en general la seguridad de la información por parte de las instituciones públicas y privadas.

CONSIDERANDO: Que, en tal sentido, 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.

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, que establece la Estrategia Nacional de Desarrollo 2030, del 25 de enero de 2012, 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 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, normativas, regulaciones y mejores prácticas para proteger el ciberespacio, y los activos de los usuarios y organizaciones.

CONSIDERANDO: Que, en el marco de los actuales esfuerzos de modernización del Estado, y tomando en cuenta el período de vigencia de la actual Estrategia Nacional de Ciberseguridad, es oportuno actualizar esta, en consonancia con la tendencia internacional, para fortalecer las directrices y políticas públicas orientadas a detectar, mitigar y gestionar incidentes generados en los sistemas de información del Estado y en todas las infraestructuras críticas nacionales establece las líneas de acción a ser implementadas para mitigar el riesgo, 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).

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

VISTA: La resolución del Congreso Nacional núm. 158-12, del 11 de junio de 2012, que aprueba el Convenio sobre la Cibercriminalidad, suscrito el 23 de noviembre de 2001, en Budapest.

VISTA: La ley núm. 53-07, del 23 de abril de 2007, sobre Crímenes y Delitos de Alta Tecnología.

VISTA: La ley núm. 267-08, del 4 de julio de 2008, sobre Terrorismo, y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista.

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

VISTO: El decreto núm. 230-18, del 15 de junio de 2018, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021.

VISTO: El decreto núm. 189-07, del 3 de abril de 2007, sobre Directiva de Seguridad y Defensa Nacional.

VISTO: El decreto núm. 71-21, del 8 de febrero de 2021, que crea el Gabinete de Transformación Digital.

VISTO: El decreto núm. 527-21, del 26 de agosto de 2021, que aprueba los objetivos y líneas de acción de la Agenda Digital 2030 como estrategia nacional de transformación digital y define los objetivos a corto, mediano y largo plazo.

VISTA: La resolución de la Junta Monetaria núm. 181101-02, del 1 de noviembre de 2018, que establece el Reglamento de Seguridad Cibernética y de la Información.

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

DECRETO:

ARTÍCULO 1. Objeto y vigencia de la Estrategia Nacional de Ciberseguridad 2030. Se aprueba la Estrategia Nacional de Ciberseguridad 2030, con vigencia hasta el 31 de diciembre de 2030, con el objeto de fortalecer el marco nacional de ciberseguridad, fomentando la concientización y creación de entornos digitales seguros, confiables y resilientes, que promuevan una sociedad digital dentro de un esquema de inclusión y de respeto a los derechos fundamentales.

ARTÍCULO 2. Misión de la Estrategia Nacional de Ciberseguridad 2030. La Estrategia Nacional de Ciberseguridad 2030 tiene como misión establecer los mecanismos adecuados de

ciberseguridad que protejan al Estado, los sectores productivos y los ciudadanos, para garantizar un ecosistema de ciberseguridad favorable para el desarrollo nacional, y sobre un ciberespacio seguro, resiliente y confiable.

ARTÍCULO 3. Visión de la Estrategia Nacional de Ciberseguridad 2030. Para el año 2030, 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, dentro del marco del respeto de los derechos fundamentales.

ARTÍCULO 4. Principios rectores de la Estrategia Nacional de Ciberseguridad 2030. La Estrategia Nacional de Ciberseguridad 2030 se rige por los siguientes principios:

1. Colaboración. El Estado 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. El Estado hará sus mayores esfuerzos para evitar que su territorio sea utilizado para la comisión de hechos ilícitos mediante la utilización de las tecnologías de información y comunicación.

3. Intercambio de información. El Estado 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 fundamentales. El Estado contribuirá en garantizar la utilización segura de las tecnologías de información y comunicación, a fin de garantizar el pleno respeto de los derechos fundamentales.

5. Protección de las infraestructuras críticas. El Estado 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. El Estado 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. El Estado adoptará 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 Estado realizará 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. El Estado alentará la divulgación responsable de las vulnerabilidades relacionadas con las tecnologías de información y comunicación y compartirá la información conexa sobre los recursos disponibles ante tales vulnerabilidades, a fin de limitar o eliminar las amenazas potenciales para estas tecnologías o infraestructuras dependientes de ellas.

ARTÍCULO 5. Objetivos estratégicos de la Estrategia Nacional de Ciberseguridad 2030. La Estrategia Nacional de Ciberseguridad 2030 está conformada por los siguientes objetivos estratégicos, así como sus respectivos objetivos específicos y líneas de acción:

OBJETIVO ESTRATÉGICO 1: Fortalecimiento de la capacidad institucional. Fortalecer las capacidades de las entidades y organismos especializados de apoyo, para mejorar la prevención, detección, respuesta y recuperación en materia de ciberseguridad. Asimismo, contribuir al fortalecimiento de las instituciones del Estado, en todo el contexto de la ciberseguridad.

Objetivo específico 1.1: Fortalecimiento integral de las entidades y organismos especializados de apoyo en el ámbito de la gestión y seguimiento de ciberseguridad.

Línea de acción 1.1.1: Fortalecer las entidades y organismos especializados de apoyo en la gestión, seguimiento, monitoreo y evaluación de ciberseguridad, a nivel de recursos tecnológicos, financieros, humanos, entre otros.

Línea de acción 1.1.2: Fortalecer la gobernanza de las entidades y organismos especializados de apoyo y de las instituciones de investigación y persecusión del ciberdelito.

Línea de acción 1.1.3: Desarrollar planes de formación, capacitación y sensibilización para funcionarios y servidores en materia de ciberseguridad.

Línea de acción 1.1.4: Crear mecanismos seguros y ágiles para reportes y denuncias de forma presencial y digital, así como también simplificar dichos trámites.

Objetivo específico 1.2: Fortalecimiento de las instituciones del Estado en materia de ciberseguridad a nivel de estructuras, formación, estándares y lineamientos para el fortalecimiento de la seguridad de la información.

Línea de acción 1.2.1: Articular la revisión de las estructuras actuales de tecnologías de la información (TI) de las instituciones del Estado para establecer una estructura independiente, enfocada en la ciberseguridad, conforme a las buenas prácticas internacionales, con fines de priorizar los pilares fundamentales de la seguridad de la información en las instituciones del Estado.

Línea de acción 1.2.2: Diseñar un plan de formación, capacitación y sensibilización en ciberseguridad para personal responsable de la seguridad de la información en las instituciones del Estado.

Línea de acción 1.2.3: Elaborar, definir y garantizar cumplimiento de los estándares para la seguridad de las Tecnologías de la Información y Comunicación (TIC) en el Estado.

OBJETIVO ESTRATÉGICO 2: Protección y resiliencia de infraestructuras. Asegurar el continuo funcionamiento de las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) del Estado.

Objetivo específico 2.1: Fortalecer la protección de las infraestructuras críticas nacionales y las de tecnologías de la información (TI) del Estado.

Línea de acción 2.1.1: Elaborar y establecer un plan nacional de respuesta a incidentes de ciberseguridad, y contingencias a riesgos, que procure la adecuada actuación en la gestión de incidentes cibernéticos, riesgos de emergencia y crisis nacional.

Línea de acción 2.1.2: Identificar y apoyar los organismos principales en el área de respuesta a incidentes que puedan proporcionar soporte a las infraestructuras críticas nacionales y a las infraestructuras tecnologías de la información (TI) del Estado y del sector privado en función al Plan Nacional de Respuesta a Incidentes de Ciberseguridad.

Línea de acción 2.1.3: Desarrollar y establecer los protocolos de activación y acción para los organismos de respuesta, y todo el ciclo de gestión de los incidentes.

Línea de acción 2.1.4: Elaborar y establecer un plan nacional de comunicación e intercambio de información ante crisis de incidentes de seguridad cibernética.

Línea de acción 2.1.5: Fortalecer los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT) y promover el establecimiento de los mismos en los sectores críticos nacionales.

Línea de acción 2.1.6: Diseñar, establecer y poner en marcha un plan de ejercicios de simulación de incidentes cibernéticos para las infraestructuras críticas nacionales y las instituciones del Estado.

Objetivo específico 2.2: Fortalecer la gestión de riesgos, identificar las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) relevantes del Estado y efectuar un análisis de riesgo.

Línea de acción 2.2.1: Establecer una metodología común para la gestión de los riesgos cibernéticos, y sus lineamientos, así como los mecanismos de gobernabilidad, para la supervisión, evaluación y medición periódica de implementación y cumplimiento de las políticas de tecnologías de información, los planes de riesgos y de continuidad operativa, en conformidad con las mejores prácticas, y alineada a los estándares y metodologías internacionales para las infraestructuras criticas nacionales y de las instituciones del Estado, y promover su adopción en el sector privado.

Línea de acción 2.2.2: Establecer los criterios que determinan el grado de criticidad de una infraestructura, basado en los estándares internacionales en la materia.

Línea de acción 2.2.3: Catalogar las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado de acuerdo con los criterios que determinan su grado de criticidad, incluyendo los servicios colaterales que las soportan.

Línea de acción 2.2.4: Efectuar análisis de riesgo sobre las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado y determinar su nivel de vulnerabilidad, contemplando la inclusión de los perfiles de riesgos sectoriales más críticos para la sociedad y la economía nacional.

Objetivo específico 2.3 Elaborar los reglamentos, normas, estándares y lineamientos para el fortalecimiento de la coordinación y respuesta a incidentes de ciberseguridad en las infraestructuras críticas nacionales y de tecnologías de la información (TI) del Estado.

Línea de acción 2.3.1: Evaluar las normas y reglamentaciones emitidas por reguladores sectoriales para someter propuestas de actualizaciones a estos órganos, atendiendo a estándares internacionales.

Línea de acción 2.3.2: Apoyar la elaboración y el establecimiento de reglamentos sectoriales y en el diseño del modelo de gobernanza del sector.

Línea de acción 2.3.3: Elaborar y establecer los protocolos de intercambio de información entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT), las instituciones del Estado, las infraestructuras críticas y el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), para la gestión de los incidentes de ciberseguridad.

OBJETIVO ESTRATÉGICO 3: Educación y cultura. Promover y fortalecer la educación, sensibilización y cultura nacional de ciberseguridad.

Objetivo específico 3.1: Fomentar la inclusión de la formación y sensibilización en ciberseguridad en todos los niveles del sistema educativo.

Línea de acción 3.1.1: Establecer una política de desarrollo de competencias digitales en la población con énfasis en la ciberseguridad, contemplando programas de educación, formación técnica, sensibilización y concientización para lograr un ciberespacio más seguro.

Línea de acción 3.1.2: Fortalecer los programas de educación en ciberseguridad de las instituciones de educación superior y técnicos, en los diferentes niveles de grado, técnico, licenciatura, maestrías y doctorado, para aumentar la disponibilidad y calidad de las ofertas académicas y profesionales especializados.

Línea de acción 3.1.3: Incorporar contenidos básicos de ciberseguridad, en las asignaturas de tecnología de información de los programas de formación de las diferentes carreras, en las instituciones de educación superior y técnicos superior para fortalecer la concienciación y cultura de la ciberseguridad a nivel profesional.

Línea de acción 3.1.4: Incorporar en el programa de educación básica e intermedia, contenidos de ciberseguridad para fortalecer la sensibilización, concienciación y cultura de la ciberseguridad en los estudiantes y profesores de esos niveles.

Línea de acción 3.1.5: Diseñar un programa de cooperación para la implementación de formaciones especializadas en coordinación con las instituciones académicas.

Línea de acción 3.1.6: Implementar sistema de certificación emitida por institución acreditada para formación especializada en ciberseguridad.

Línea de acción 3.1.7: Diseñar e implementar programas de pasantías para fomentar nuevos talentos en materia de ciberseguridad con el apoyo y cooperación de las instituciones de educación intermedia, superior y técnicos profesional.

Línea de acción 3.1.8: Diseñar un programa de desarrollo de cibertalentos para apoyar la demanda de recursos especializados en el sector de la seguridad de la información.

Objetivo específico 3.2: Impulsar una cultura nacional de ciberseguridad en todo el país enfocada a las diferentes poblaciones vulnerables.

Línea de acción 3.2.1: Desarrollar un programa general de concientización para sensibilizar y fortalecer el entendimiento de ciberseguridad, conocer los riesgos, amenazas

y forma de abordarlos estos temas, para niños, adolescentes, adultos mayores, mipymes, el sector público y privado, entre otros.

Línea de acción 3.2.2: Desarrollar campañas de sensibilización, en medios tradicionales y digitales, con el apoyo del sector público, privado, la academia, organizaciones de medios y las organizaciones de la sociedad civil para fortalecer la cultura de ciberseguridad, promover la protección en línea de la información personal, y buenas prácticas en el uso de plataformas en línea y redes sociales.

Línea de acción 3.2.3: Implementar programas de reconocimiento para diversos sectores en apoyo a la cooperación en los esfuerzos de concientización y cultura de ciberseguridad a la población.

OBJETIVO ESTRATÉGICO 4: Alianzas públicas y privadas, nacionales e internacionales. Establecer alianzas nacionales e internacionales entre los sectores público y privado, sociedad civil y organismos e instituciones internacionales, para facilitar la cooperación técnica, operativa y de capacitación, así como generar los mecanismos que permitan una mejor articulación de las políticas exteriores relacionadas con la ciberseguridad.

Objetivo específico 4.1: Realizar alianzas nacionales e internacionales para fortalecer la cooperación.

Línea de acción 4.1.1: Establecer acuerdos marcos de cooperación técnica, operativa y de capacitación para el fortalecimiento de la ciberseguridad

Línea de acción 4.1.2: Fortalecer las alianzas con el sector privado, organizaciones de la sociedad civil y la academia para reafirmar la confianza ciudadana en la seguridad cibernética.

Línea de acción 4.1.3: Fomentar la relación con organismos e instituciones internacionales para facilitar la cooperación transfronteriza.

Línea de acción 4.1.4: Asegurar la participación de la República Dominicana en los foros internacionales.

Línea de acción 4.1.5: Monitorear y evaluar el nivel de cumplimiento país con los acuerdos y gobernanza del ciberespacio a nivel internacional.

OBJETIVO ESTRATÉGICO 5: Investigación y desarrollo de la ciberseguridad y su entorno. Promover el análisis, la investigación y el desarrollo de la ciberseguridad y su entorno a nivel nacional e internacional.

Objetivo específico 5.1 Fomentar la investigación, el desarrollo y la innovación de la ciberseguridad y su entorno.

Línea de acción 5.1.1: Promover programas de emprendimientos e innovaciones en la industria de ciberseguridad.

Línea de acción 5.1.2: Incentivar el análisis y las investigaciones para el fortalecimiento y desarrollo de capacidades a nivel país.

Línea de acción 5.1.3: Desarrollar estudios, y promover la generación de estadísticas y creación de indicadores para apoyar en el desarrollo de políticas públicas, basadas en evidencias, vinculado al ecosistema de ciberseguridad.

Línea de acción 5.1.4: Realizar encuestas regionales o nacionales, análisis de datos, y evaluaciones para medir el impacto de la Estrategia Nacional de Ciberseguridad 2030 en diferentes sectores.

Línea de acción 5.1.5: Promover estudios de investigación en el desarrollo y adopción de nuevas tecnologías disruptivas y su impacto en la ciberseguridad.

OBJETIVO ESTRATÉGICO 6: Fortalecimiento del marco normativo. Fortalecer el marco normativo y regulatorio que incide en los temas relacionados con la ciberseguridad.

Objetivo específico 6.1: Fortalecer y garantizar el cumplimiento de las normativas legales, técnicas y regulatorias de ciberseguridad al margen del contexto actual del país y el entorno.

Línea de acción 6.1.1: Monitorear, revisar y analizar el marco legal y normativo vinculado a la ciberseguridad, ciberdefensa, ciberterrorismo y ciberdelito, y proponer un plan de actualización que garanticen un ecosistema nacional seguro, frente al contexto de nuevas amenazas y riesgos cibernéticos producto de las tecnologías emergentes, velando por la protección de los derechos humanos en línea, la niñez y el consumidor en línea, la protección de datos personales, las prioridades nacionales y los estándares internacionales relevantes.

Línea de acción 6.1.2: Elaborar las normativas y los estándares técnicos aplicables a la ciberseguridad y promover su adopción.

Línea de acción 6.1.3: Impulsar el cumplimiento de las normativas en materia de ciberseguridad por parte de los organismos de la administración pública.

ARTÍCULO 6. Estrategias complementarias de la Estrategia Nacional de Ciberseguridad 2030. Las estrategias complementarias persiguen unificar de manera integral a la Estrategia Nacional de Ciberseguridad 2030 todos los esfuerzos en materia de ciberdelincuencia y ciberdefensa y ciberterrorismo.

PÁRRAFO I. Estrategia complementaria de Ciberdelincuencia. La implementación y el presupuesto de las iniciativas derivadas del plan de acción complementario de ciberdelincuencia

quedan bajo la responsabilidad de la Procuraduría General de la República y la Policía Nacional, con el propósito de fortalecer las capacidades operativas de las unidades de prevención, investigación y persecución del ciberdelito del Ministerio Público y la Policía Nacional, de conformidad con los siguientes objetivos específicos y líneas de acción:

Objetivo específico 1. Alineado al objetivo estratégico 1 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer las capacidades operativas de los organismos encargados del cumplimiento de la ley en la recolección y procesamiento de la evidencia electrónica.

Línea de acción 1.1: Realizar una evaluación en los órganos de investigación a nivel nacional para determinar brechas de capacidades.

Línea de acción 1.2: Fortalecer el plan de estudios de las escuelas de los órganos de investigación, con contenidos de recopilación de evidencia electrónica, y desarrollar formación continua para fomentar la investigación, el procesamiento y la conservación de evidencias electrónicas.

Línea de acción 1.3: Fortalecer la relación del servicio de la Policía Nacional con el ciudadano y público en general, para aumentar la confianza.

Línea de acción 1.4: Fomentar la colaboración ciudadana en la notificación de delitos cibernéticos e incidentes de impacto nacional.

Línea de acción 1.5: Desarrollar las normas y directrices para el procesamiento de las escenas de hechos o sucesos que contengan potencial de evidencia electrónica, su manipulación, cadena de custodia, procesamiento y conservación para su posterior presentación en los tribunales.

Línea de acción 1.6: Desplegar a nivel nacional las unidades de investigación de ciberdelito.

Objetivo específico 2: Alineado al objetivo estratégico 1 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer la prevención ciudadana ante los ciberdelitos.

Línea de acción 2.1: Crear la unidad de ciberpatrullaje preventivo para fortalecer la protección del ciudadano ante los ciberdelitos.

Línea de acción 2.2: Desarrollar un ciberobservatorio de análisis y estudio de nuevas conductas.

Línea de acción 2.3: Promover la creación de canales de divulgación y campañas de información en todos los medios de comunicación de nuevas tendencias, conductas y metodologías del ciberdelito.

Objetivo específico 3: Alineado al objetivo estratégico 1 de la Estrategia Nacional de Ciberseguridad 2030, busca aumentar y fortalecer la capacidad del Ministerio Público y sus organismos auxiliares para perseguir, así como del Poder Judicial para decidir, sobre delitos cibernéticos de manera adecuada y justa.

> **Línea de acción 3.1:** Desarrollar un programa de formación específica para el Ministerio Público y sus organismos auxiliares, así como para el Poder Judicial sobre delitos cibernéticos y evidencias electrónicas, con el objetivo de mejorar sus conocimientos y fortalecer la aplicación coherente de la ley.

Objetivo específico 4: Alineado al objetivo estratégico 3 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer la formación de los miembros de la Policía Nacional.

> **Línea de acción 4.1:** Fortalecer la capacitación del recurso humano en materia de investigación en ciberdelito a miembros de la institución de la Policía Nacional.

Objetivo específico 5: Alineado al objetivo estratégico 4 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer la cooperación internacional en materia de ciberdelincuencia.

> **Línea de acción 5.1:** Fortalecer los lazos de cooperación internacional en materia de preservación e intercambio de evidencia electrónica.

> **Línea de acción 5.2:** Fomentar los acuerdos bilaterales y multilaterales para cooperación, intercambio de experiencias y combate de la ciberdelincuencia.

PÁRRAFO II. Estrategias complementarias de Ciberdefensa y Ciberterrorismo. La implementación y el presupuesto de las iniciativas derivadas del plan de acción complementario de ciberdefensa y ciberterrorismo quedan bajo la responsabilidad del Ministerio de Defensa, el Departamento Nacional de Investigaciones (DNI) y la Dirección Nacional Antiterrorista, con el propósito de dotar de políticas y mecanismos de ciberdefensa, que permitan la prevención, mitigación y respuesta a ataques de ciberterrorismo mediante la integración y coordinación del Centro Nacional Antiterrorista, de conformidad con los siguientes objetivos específicos y líneas de acción:

Objetivo específico 1. Alineado al objetivo estratégico 1 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer normas de cumplimiento y seguimiento de acuerdo con estándares aplicables a las infraestructuras de seguridad y defensa nacional.

> **Línea de acción 1.1:** Revisar y elaborar normas y estándares para el fortalecimiento y la protección de las infraestructuras de seguridad y defensa nacional, así como también garantizar su cumplimiento.

Objetivo específico 2. Alineado al objetivo estratégico 1 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer las capacidades en materia de formación en ciberseguridad a miembros del Ministerio de Defensa.

> **Línea de acción 2.1:** Fortalecer las capacidades cibernéticas de los responsables de las infraestructuras de seguridad y defensa nacional.
>
> **Línea de acción 2.2:** Fomentar y actualizar las capacidades en materia de ciberseguridad y ciberdefensa de los responsables de las infraestructuras de tecnologías de la información (TI) de las dependencias castrenses.

Objetivo específico 3. Alineado al objetivo estratégico 1 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer las estructuras institucionales de gestión y respuesta a incidentes cibernéticos.

> **Línea de acción 3.1:** Revisar y actualizar las estructuras organizacionales en las dependencias responsables de gestionar operaciones de ciberseguridad y ciberdefensa.

Objetivo específico 4. Alineado al objetivo estratégico 2 de la Estrategia Nacional de Ciberseguridad 2030, busca fomentar la capacidad de defensa en el ciberespacio.

> **Línea de acción 4.1:** Desarrollar un plan de ejercicios de ciberdefensa para fortalecer la defensa en el ciberespacio.

Objetivo específico 5. Alineado al objetivo estratégico 3 de la Estrategia Nacional de Ciberseguridad 2030, busca fomentar la cultura sobre ciberseguridad y ciberdefensa en los miembros del Ministerio de Defensa.

> **Línea de acción 5.1:** Revisar e incluir ciberseguridad y ciberdefensa en la oferta académica de los programas de formación para cadetes.
>
> **Línea de acción 5.2:** Desarrollar programas de concientización sobre las nuevas amenazas cibernéticas dirigidas a seguridad y defensa.
>
> **Línea de acción 5.3:** Proponer la creación de una escuela de comando y operaciones cibernéticas para el Ministerio de Defensa.

Objetivo específico 6. Alineado al objetivo estratégico 4 de la Estrategia Nacional de Ciberseguridad 2030, busca impulsar alianzas nacionales e internacionales para el fortalecimiento de la cooperación entre Estados o agencias en materia de ciberdefensa.

> **Línea de acción 6.1:** Coordinar con los países amigos para promover la cooperación en materia de ciberdefensa.

Línea de acción 6.2: Promover la actualización de los acuerdos existentes para contemplar el componente de ciberdefensa en el margen de cooperación establecido.

Objetivo específico 7: Alineado al objetivo estratégico 4 de la Estrategia Nacional de Ciberseguridad 2030, busca fortalecer la cooperación interinstitucional entre las dependencias castrenses para mejorar la respuesta oportuna a incidentes cibernéticos de seguridad y defensa.

Línea de acción 7.1: Fortalecer la interacción y comunicación efectiva de los puntos de contacto de las instituciones y dependencias del Ministerio de Defensa y el Equipo de Respuesta a Incidentes Cibernéticos de Defensa (CSIRT-Defensa) del Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5i).

Objetivo específico 8: Alineado al objetivo estratégico 6 de la Estrategia Nacional de Ciberseguridad 2030, busca actualizar el marco jurídico del ciberterrorismo.

Línea de acción 8.1: Proponer la actualización de la ley núm. 267-08 sobre terrorismo y contemplar el cumplimiento de estándares internacionales en la prevención y mitigación del ciberterrorismo.

Objetivo específico 9: Alineado al objetivo estratégico 6 de la Estrategia Nacional de Ciberseguridad 2030, busca desarrollar el marco doctrinario para las operaciones de ciberseguridad y ciberdefensa.

Línea de acción 9.1: Identificar tácticas, técnicas, procedimientos y lecciones aprendidas, más utilizadas en el marco de las operaciones cibernéticas aplicables a seguridad y defensa.

ARTÍCULO 7. Monitoreo y seguimiento de la Estrategia Nacional de Ciberseguridad 2030. El Centro Nacional de Ciberseguridad, a través de su Dirección Ejecutiva, será responsable de monitorear y dar seguimiento al desarrollo e implementación de la Estrategia Nacional de Ciberseguridad 2030, al logro de sus respectivos objetivos y a la ejecución del plan de acción, con base en los indicadores y metas aprobados por su Consejo Directivo.

PÁRRAFO. El monitoreo y seguimiento de los indicadores y metas de la Estrategia Nacional de Ciberseguridad 2030 se realizarán trimestralmente. Los avances serán presentados trimestralmente al Consejo Directivo del Centro Nacional de Ciberseguridad y semestralmente al Gabinete de Transformación Digital.

ARTÍCULO 8. Monitoreo y seguimiento de las estrategias complementarias. Los respectivos órganos encargados de las estrategias complementarias de ciberdelincuencia y ciberdefensa y ciberterrorismo serán responsables de monitorear y dar seguimiento al desarrollo e implementación de estas, al logro de sus respectivos objetivos y a la ejecución de sus planes de acción.

PÁRRAFO. El monitoreo y seguimiento de los indicadores y metas de las estrategias complementarias de ciberdelincuencia y ciberdefensa y ciberterrorismo se realizarán trimestralmente. Los avances serán presentados trimestralmente al Consejo Directivo del Centro Nacional de Ciberseguridad y semestralmente al Gabinete de Transformación Digital.

ARTÍCULO 9. Actualización de la Estrategia Nacional de Ciberseguridad 2030. El Consejo Directivo del Centro Nacional de Ciberseguridad podrá monitorear, revisar y actualizar, conforme al período establecido de cada 2 años, la implementación de la Estrategia Nacional de Ciberseguridad 2030 y las estrategias complementarias, pudiendo ajustar los indicadores y metas previamente aprobados.

ARTÍCULO 10. Colaboración de los entes y órganos de la Administración Pública. Los entes y órganos de la Administración Pública deberán prestar, dentro del ámbito de sus respectivas competencias, las colaboraciones requeridas por el Centro Nacional de Ciberseguridad y demás órganos responsables para la implementación de la Estrategia Nacional de Ciberseguridad 2030 y las estrategias complementarias.

ARTÍCULO 11. Alineación con instrumentos de planificación. Los planes, programas y proyectos que se deriven de la Estrategia Nacional de Ciberseguridad 2030 y las estrategias complementarias deberán establecer prioridades, objetivos y metas consistentes y alineados con la Estrategia Nacional de Desarrollo y demás instrumentos del Sistema Nacional de Planificación e Inversión Pública. El Ministerio de Economía, Planificación y Desarrollo proporcionará la asistencia técnica necesaria para garantizar dicha alineación. Las metas y planes de acción aprobados serán incorporados a las iniciativas presidenciales correspondientes de los órganos responsables de su ejecución.

ARTÍCULO 12. Modificación del decreto núm. 230-18. Se modifica el párrafo I del artículo 12 del decreto núm. 230-18, del 19 de junio de 2018, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021, para que disponga lo siguiente:

> "**Párrafo I**. El Consejo Directivo estará compuesto por los titulares de los siguientes órganos:
>
> a) Ministerio de la Presidencia, el cual lo preside.
> b) Ministerio de Defensa.
> c) Ministerio de Interior y Policía.
> d) Ministerio de Relaciones Exteriores.
> e) Banco Central de la República Dominicana.
> f) Procuraduría General de la República (PGR).
> g) Departamento Nacional de Investigaciones (DNI).
> h) Instituto Dominicano de las Telecomunicaciones (INDOTEL).
> i) Oficina Gubernamental de Tecnología de la Información y Comunicación (OGTIC).
> j) Policía Nacional (PN).

k) Dirección Ejecutiva del Centro Nacional de Ciberseguridad (CNCS), la cual ostenta la secretaría.

ARTÍCULO 12. Remisión del presente decreto. Envíese a las instituciones correspondientes, para su conocimiento y ejecución.

DADO en Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los catorce (14) días del mes de junio del año dos mil veintidós (2022), año 179 de la Independencia y 159 de la Restauración.

LUIS ABINADER