



LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

NÚMERO: 612-24

CONSIDERANDO: Que, durante el presente siglo, uno de los grandes desafíos que a nivel global han enfrentado los Estados en materia de seguridad pública es el uso delictivo de las redes informáticas y la información electrónica.

CONSIDERANDO: Que los delitos en el ciberespacio, junto con otros fenómenos globales como el terrorismo, el narcotráfico, la delincuencia organizada transnacional y la corrupción, han requerido respuestas uniformes de la comunidad internacional mediante normativas enfocadas en la prevención, represión y mecanismos efectivos de cooperación y asistencia judicial internacional.

CONSIDERANDO: Que, en el ámbito de la ciberseguridad, el principal marco normativo internacional al cual la República Dominicana está adherida es el Convenio sobre Cibercriminalidad, suscrito en Budapest el 23 de noviembre de 2001, junto con sus protocolos adicionales.

CONSIDERANDO: Que, en el ámbito interamericano, la Organización de Estados Americanos (OEA), a través de la Resolución AG/RES. 2004 (XXXIV-0/04), respaldó que las recomendaciones formuladas por el Grupo de Expertos Gubernamentales en su reunión inicial sirvan como la contribución de las REMJA para el desarrollo de la Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética a que se refiere la resolución de la Asamblea General de la OEA AG/RES. 1939 /XXXIII-O/03), así como solicitar al Grupo que, a través de su Presidencia, continúe apoyando el proceso de elaboración de dicha Estrategia.

CONSIDERANDO: Que la República Dominicana, en cumplimiento de sus compromisos internacionales, ha incorporado en su legislación interna disposiciones sobre la prevención, detección y sanción de delitos cibernéticos, como lo establece la Ley núm. 53-07, Sobre Crímenes y Delitos de Alta Tecnología.

CONSIDERANDO: Que, al tenor de lo anterior se han emitido reglamentos del Consejo Directivo del Instituto Dominicano de las Telecomunicaciones para la obtención y preservación de datos por parte de proveedores de servicios, y sobre ciberseguridad en la prestación de acceso a internet. Asimismo, se ha creado, mediante decreto, una estructura institucional en el marco de la Estrategia Nacional de Ciberseguridad, conformada por el Centro Nacional de Ciberseguridad, el Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) y el Equipo de Respuestas a Incidentes Cibernéticos (CSIRT-RD).

CONSIDERANDO: Que el actual marco institucional en materia de ciberseguridad se enfoca principalmente en abordar la ciberseguridad desde una perspectiva de seguridad pública.

CONSIDERANDO: Que el crecimiento de la ciberdelincuencia a nivel global ha superado los desafíos de la seguridad pública, convirtiéndose en uno de los principales retos para la seguridad nacional de los Estados.





LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

CONSIDERANDO: Que, en consonancia con lo anterior, la Ley núm. 1-24, que crea el Sistema Nacional de Inteligencia, asigna a su órgano rector, la Dirección Nacional de Inteligencia (DNI), la responsabilidad de garantizar la seguridad cibernética en las telecomunicaciones. Esta ley establece la obligación de contribuir a la implementación de sistemas eficaces para prevenir o mitigar los daños causados por desastres tecnológicos o amenazas cibernéticas a las infraestructuras críticas nacionales, así como asegurar la protección de los sistemas de tecnologías de la información de la Administración Pública.

CONSIDERANDO: Que, dada la importancia de la capacidad del Estado para anticiparse a los riesgos derivados del mal uso de las redes informáticas y la información electrónica, es necesario reorientar la estructura institucional en ciberseguridad, creando una organización administrativa más eficaz dentro del marco de la seguridad y defensa nacional.

CONSIDERANDO: Que el artículo 260 de la Constitución de la República establece como objetivo de alta prioridad nacional combatir las actividades criminales transnacionales que amenacen los intereses del país y sus habitantes, así como organizar sistemas eficaces que no solo prevengan o mitiguen daños por desastres naturales, sino también aquellos de origen tecnológico.

CONSIDERANDO: Que la Constitución de la República crea el Consejo de Seguridad y Defensa Nacional como órgano consultivo encargado de asesorar al presidente en la formulación de políticas y estrategias en materia de seguridad, por lo que, para enfrentar adecuadamente los desafíos de la ciberseguridad, dicho consejo debe contar con una estructura permanente que le permita cumplir con su misión de manera efectiva.

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

VISTA: La Ley núm. 1-24, que crea el Sistema Nacional de Inteligencia y la Dirección Nacional de Inteligencia (DNI), del 15 de enero de 2024.

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

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

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

VISTO: El Decreto núm. 86-21, que establece el Reglamento de Composición y Funcionamiento del Consejo de Seguridad y Defensa Nacional, del 12 de febrero de 2021.

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





LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

VISTO: El Decreto núm. 189-07, que define la Directiva de Defensa y Seguridad Nacional, del 3 de abril de 2007.

VISTO: El Decreto núm. 313-22, que establece la Estrategia Nacional de Ciberseguridad 2030, del 14 de junio de 2022.

VISTO: El Decreto núm. 685-22, que establece los principios y lineamientos generales que servirán de base a los entes y órganos de la Administración Pública, para la adopción de los controles, políticas y estándares para incrementar los niveles de madurez cibernética en el sector público, la notificación obligatoria de eventos e incidentes de ciberseguridad, así como el intercambio de información sobre amenazas cibernéticas, del 18 de noviembre de 2022.

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

DECRETO

ARTÍCULO 1. Objeto. Este decreto reorganiza las competencias del Estado en materia de ciberseguridad, con los siguientes objetivos:

1. Ubicar el Centro Nacional de Ciberseguridad como órgano de apoyo al Consejo de Seguridad y Defensa Nacional.
2. Transferir las funciones técnicas de prevención y respuesta a incidentes cibernéticos a la Dirección Nacional de Inteligencia (DNI).
3. Crear el Instituto Criptográfico Nacional, bajo la dependencia de la Dirección Nacional de Inteligencia, con el propósito de cumplir sus atribuciones legales en el ámbito preventivo de la seguridad cibernética, en especial en lo relacionado con los sistemas y redes de información de la Administración del Estado.

ARTÍCULO 2. Modificaciones al Decreto núm. 313-22. Se modifican los artículos 7, 8, y 9 del Decreto núm. 213-22, del 14 de junio de 2022, para que en lo adelante se lean de la manera siguiente:

ARTÍCULO 7. Monitoreo y seguimiento de la Estrategia Nacional de Ciberseguridad 2030. *La Comisión Técnica Especializada en Ciberseguridad del Centro Nacional de Ciberseguridad será responsable de monitorear y supervisar el desarrollo e implementación de la Estrategia Nacional de Ciberseguridad 2030, asegurando el cumplimiento de sus objetivos y la ejecución del plan de acción, basándose en los indicadores y metas aprobados por la Comisión.*

PÁRRAFO. *El monitoreo y seguimiento de los indicadores y metas de la Estrategia Nacional de Ciberseguridad 2030 se realizarán trimestralmente. Los avances se presentarán trimestralmente*





LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

a la Comisión Técnica Especializada en Ciberseguridad del Centro Nacional de Ciberseguridad, y semestralmente al Gabinete de Transformación Digital.

ARTÍCULO 8. Monitoreo y seguimiento de las estrategias complementarias. Los órganos responsables de las estrategias complementarias de ciberdelincuencia, ciberdefensa y ciberterrorismo serán los encargados de monitorear y supervisar su desarrollo e implementación, asegurando el logro de sus objetivos y la ejecución de sus respectivos planes de acción.

PÁRRAFO. El monitoreo y seguimiento de los indicadores y metas de las estrategias complementarias de ciberdelincuencia, ciberdefensa y ciberterrorismo se realizarán trimestralmente. Los avances se presentarán trimestralmente a la Comisión Técnica Especializada en Ciberseguridad del Centro Nacional de Ciberseguridad, y semestralmente al Gabinete de Transformación Digital.

ARTÍCULO 9. Actualización de la Estrategia Nacional de Ciberseguridad 2030. La Comisión Técnica Especializada en Ciberseguridad del Centro Nacional de Ciberseguridad podrá monitorear, revisar y actualizar la implementación de la Estrategia Nacional de Ciberseguridad 2030 y las estrategias complementarias cada dos años, realizando los ajustes necesarios en los indicadores y metas previamente aprobados.

ARTÍCULO 3. Modificaciones al Decreto núm. 230-18. Se modifican los artículos 10, 12, y 14 del Decreto núm. 230-18, del 19 de junio de 2018, para que en lo adelante se lean de la manera siguiente:

ARTÍCULO 10. Creación del Centro Nacional de Ciberseguridad. Se crea el Centro Nacional de Ciberseguridad como órgano de apoyo especializado del Consejo de Seguridad y Defensa Nacional.

ARTÍCULO 12. Conformación del Centro Nacional de Ciberseguridad. El Centro Nacional de Ciberseguridad estará integrado por una Comisión Técnica Especializada en Ciberseguridad (CTEC), y por una Dirección Ejecutiva.

PÁRRAFO I. La Comisión Técnica Especializada en Ciberseguridad estará conformada por delegados técnicos especialistas en ciberseguridad provenientes de las siguientes instituciones públicas:

- a) La Dirección Nacional de Inteligencia, quien la coordina y funge a su vez como enlace con el Consejo de Seguridad y Defensa Nacional.
- b) El Ministerio de la Presidencia (MINPRE).
- c) El Ministerio de Defensa.





LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

- d) *El Ministerio de Interior y Policía*
- e) *La Procuraduría General de la República;*
- f) *El Banco Central de la República Dominicana;*
- g) *La Oficina Gubernamental de las Tecnologías de Información y Comunicaciones (OGTIC).*
- h) *La Policía Nacional.*
- i) *El Instituto Dominicano de las Telecomunicaciones (INDOTEL).*
- j) *El Instituto Tecnológico de las Américas (ITLA).*

PÁRRAFO II. *La Comisión Técnica Especializada en Ciberseguridad tendrá la facultad, cuando el caso lo amerite, de invitar a participar a otros representantes del Estado y del sector privado, tales como: el Ministerio de Relaciones Exteriores, la Dirección Nacional de Control de Drogas, la Administración Monetaria y Financiera, el Poder Legislativo, el Poder Judicial, la Academia y operadores de infraestructura crítica.*

ARTÍCULO 14. Funciones de la Comisión Técnica Especializada del Centro Nacional de Ciberseguridad. *La Comisión Técnica Especializada 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.*





LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

ARTÍCULO 4. Integración del ECEC y CSIRT-RD a la Dirección Nacional de Inteligencia (DNI). Se dispone que el Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) y el Equipo de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) queden bajo de la Dirección Nacional de Inteligencia (DNI), en consecuencia, se deroga el párrafo III del artículo 12 del Decreto núm. 230-18, del 19 de junio de 2018.

ARTÍCULO 5. Creación del Instituto Criptográfico Nacional (ICN). Se crea el Instituto Criptográfico Nacional (ICN), como dependencia de la Dirección Nacional de Inteligencia (DNI), responsable de coordinar la acción de los diferentes entes y órganos de la Administración del Estado que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, así como los sistemas de tecnologías de la información que procesan, almacenan o transmiten información clasificada.

PÁRRAFO. El Instituto Criptográfico Nacional tendrá las siguientes funciones:

- a) Elaborar y difundir guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la administración del Estado.
- b) Establecer y mantener un sistema de gestión orientado al uso apropiado y eficaz de recursos criptográficos orientados a la protección reservada.
- c) Fungir como un organismo de certificación y acreditación para el otorgamiento de accesos y autorizaciones de seguridad a aquellos individuos u organizaciones que requieran tener acceso a información considerada como reservada y de interés para garantizar la seguridad nacional.
- d) Evaluar y definir un catálogo de tecnologías seguras que tengan como propósito almacenar, procesar o transmitir información considerada como reservada, según los criterios definidos en la normativa orientada a tales fines.
- e) Velar por la formación del personal de la Administración en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.
- f) Realizar acuerdos de cooperación con la comunidad académica y científica, tendentes al análisis y estudio de la soberanía digital.

ARTÍCULO 6. Traspaso de las estructuras jerárquicas y organizativas que componen el actual Centro Nacional de Ciberseguridad. El Ministerio de la Presidencia coordinará, con el Consejo de Seguridad y Defensa Nacional y la Dirección Nacional de Inteligencia (DNI), el traspaso del personal y los medios materiales del Centro Nacional de Ciberseguridad al Consejo de Seguridad y Defensa Nacional, así como el traspaso del Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) y el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) a la Dirección Nacional de Inteligencia (DNI).





LUIS ABINADER

PRESIDENTE DE LA REPÚBLICA DOMINICANA

ARTÍCULO 7. Responsabilidad de compartir información sensible para la seguridad cibernética nacional. Aquellos entes y órganos que conforman la Administración Pública dominicana, bajo la dependencia del Poder Ejecutivo, incluyendo los organismos desconcentrados, autónomos y descentralizados están en la obligación de comunicar a la DNI cualquier incidencia, riesgo o amenaza a la seguridad cibernética y de la información que sufran.

PÁRRAFO I. Aquellos organismos especializados del sector público que por su naturaleza constituyan equipos y capacidades de respuesta a incidentes cibernéticos (CSIRT) deben coordinar su actuación con la DNI.

PÁRRAFO II. Las entidades y organismos del sector privado que posean equipos y capacidades de respuesta a incidentes cibernéticos (CSIRT) podrán convenir acuerdos de asistencia mutua y colaboración con la DNI.

PÁRRAFO III. El tratamiento de estas informaciones, así como los niveles de autorización a estas, será definido por la DNI a partir de las facultades y rigurosidades de ley.

ARTÍCULO 8. Envíese a las instituciones correspondientes para su conocimiento y ejecución.

DADO en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República, a los 22 días del mes de octubre del año dos mil veinticuatro (2024), año 181 de la Independencia y 162 de la Restauración.

LUIS ABINADER

