



Estrategia Nacional de Ciberseguridad 2030

República Dominicana

CONTENIDO

RESUMEN EJECUTIVO	2
INTRODUCCIÓN	2
MISIÓN.....	4
VISIÓN	4
PRINCIPIOS RECTORES	4
REFERENCIA NORMATIVA Y DOCUMENTAL	5
ESTRATEGIA NACIONAL DE CIBERSEGURIDAD	7
Pilar No. 1: MARCO LEGAL Y FORTALECIMIENTO INSTITUCIONAL	8
Pilar No. 2: PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS NACIONALES E INFRAESTRUCTURAS TI DEL GOBIERNO.....	8
Pilar No. 3: EDUCACIÓN Y CULTURA NACIONAL DE CIBERSEGURIDAD	9
Pilar No. 4: ALIANZAS NACIONALES E INTERNACIONALES.....	9
INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2021-2024	10
ESTRATEGIA COMPLEMENTARIA DE CRIPTOGRAFIA.....	10
INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA DE CRIPTOGRAFIA	11
ESTRATEGIA COMPLEMENTARIA DE CIBERDELINCUENCIA.....	11
INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA DE CIBERDELINCUENCIA	12
ESTRATEGIA DE CIBERDEFENSA, CIBERGUERRA y CIBERTERRORISMO	13
INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA DE CIBERDEFENSA, CIBERGUERRA Y CIBERTERRORISMO	14
MODELO DE GOBERNANZA, IMPLEMENTACIÓN Y SEGUIMIENTO.....	14

RESUMEN EJECUTIVO

La Estrategia Nacional de Ciberseguridad 2022-2030 delinea los objetivos y líneas de acción que el Estado Dominicano, tiene como primordial responsabilidad durante este periodo, alcanzar y desarrollar, para fomentar y fortalecer el ecosistema de ciberseguridad, atendiendo a los objetivos ODS y a los indicadores internacionales de desarrollo y buenas prácticas en materia de ciberseguridad.

En el marco de la Agenda Digital 2030, nuestro proyecto país de transformación digital hacia el 2030, en su Eje transversal de Ciberseguridad, se contempla la actualización de la Estrategia Nacional de Ciberseguridad al 2030, con el objetivo de definir las iniciativas a corto, mediano y largo plazo para garantizar un ecosistema de ciberseguridad favorable para todo el desarrollo de las iniciativas que forman parte del portafolio de proyectos del Plan de Acción de la Agenda Digital 2030. Para esta actualización, se han contemplado y consensado las recomendaciones de todos los sectores involucrados en la economía nacional, al margen del tema de la ciberseguridad a nivel país, a fin de garantizar una inclusión de todos los aspectos y retos al margen de los nuevos tiempos.

La Estrategia Nacional de Ciberseguridad – ENCS, es revisada cada tres (3) años, y su actualización es el resultado del consenso y participación de todos los actores del sector público, privado, organizaciones de la sociedad civil, academia y ciudadanos en general, con el firme propósito de consolidar y aunar esfuerzos alineados a los nuevos retos en materia de ciberseguridad, para garantizar la estabilidad de todos los sectores productivos y económicos del país.

La ENCS dispone de los indicadores para medir su nivel de cumplimiento e impacto, incorporando en esta actualización las estrategias complementarias y sus respectivos indicadores, incorporadas en esta reciente actualización, para los fines de fortalecer los esfuerzos país a nivel interinstitucional. Estos indicadores resumen el esfuerzo y objetivos que el Centro Nacional de Ciberseguridad tiene como firme propósito alcanzar, para garantizar un ciberespacio más seguro y fiable

INTRODUCCIÓN

La integración de las tecnologías de la información y la comunicación (TIC) en todas las esferas de nuestra actividad económica y social cotidiana han creado, a nivel mundial, una gran y creciente dependencia de la información y de las TIC mismas, por parte de los individuos, organizaciones y los gobiernos interconectados, pues son esenciales para el desarrollo económico, la cohesión social y la seguridad nacional en todas las naciones.

El uso masivo de las TIC ha traído consigo la aparición de amenazas cibernéticas que ponen en riesgo los sistemas de información y en especial aquellos que soportan los servicios esenciales de un país: las infraestructuras críticas del Estado, cuya destrucción, pérdida de funcionalidad o interrupción temporal podría afectar de forma grave la economía, la sociedad y la seguridad nacional. En tal sentido, la protección de las redes y sistemas de información públicos y privados debe ser prioridad de los gobiernos para garantizar la prestación continua de servicios a la nación.

En República Dominicana, de acuerdo a las informaciones proporcionadas por los organismos nacionales de investigación de crímenes y delitos de alta tecnología, los delitos que con mayor frecuencia son cometidos, a través de las infraestructuras informáticas y de telecomunicaciones, son: robos de identidad y clonaciones de

tarjetas de crédito, estafas y fraudes a través de internet, abuso sexual de niños, niñas y adolescentes, pornografía infantil, violencia contra las mujeres, la difamación e injuria en redes sociales, la interrupción de servicios TIC, tanto deliberados como no deseados, y la manipulación fraudulenta de las conexiones telefónicas, incluyendo el sabotaje y secuestro de centrales telefónicas privadas. Cada día surgen nuevas amenazas en todo el mundo, y el panorama delictivo va variando y respondiendo a esquemas de criminalidad organizada. Adicionalmente, existen otras amenazas de igual o mayor peligro de las cuales el país debe estar protegido.

Por lo anterior, resulta imperioso proteger las infraestructuras interconectadas y actuar ante estas amenazas, mediante acciones coordinadas, tanto a nivel nacional como global, dirigidas a prevenir, responder y recuperarse de estos crímenes y delitos, velando por la protección de la seguridad y el desarrollo nacional.

Desde el 2003, el gobierno dominicano ha desarrollado un marco legislativo armonizado con las mejores prácticas internacionales para la penalización de la delincuencia cibernética y el manejo de evidencia electrónica, la regulación del envío de correo electrónico comercial no solicitado (SPAM, siglas en inglés) y el establecimiento de un marco de cooperación internacional. También, algunas entidades trabajan conjuntamente para abordar las cuestiones de ciberseguridad, integradas en la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT), creada por la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología.

No obstante, las medidas anteriormente señaladas, la capacidad nacional de respuesta del país para hacer frente a las amenazas e incidentes cibernéticos presenta grandes oportunidades de coordinación interinstitucional y fortalecimiento para responder con eficacia a las mismas.

El Estado Dominicano, en el año 2018, promulgó el decreto No. 230-18, creando el Centro Nacional de Ciberseguridad y estableciendo la Estrategia Nacional de Ciberseguridad.

El Gobierno Dominicano, encabezado por su Presidente, Luis Abinader, en el marco de las políticas públicas, ha creado mediante la promulgación del decreto No. 71-21, el Gabinete de Transformación digital, el cual tiene como principal responsabilidad, elaborar la “Agenda Digital”, que define la estrategia nacional de transformación digital país, cuyo objetivo es promover el desarrollo digital de la República Dominicana a través del aprovechamiento de las tecnologías digitales en un marco de sostenibilidad e inclusión social, con la participación de los sectores público, privado, academia y sociedad civil.

Citando el artículo No. 1, párrafo II, de este decreto, “la Agenda Digital promoverá la competitividad del país a través del desarrollo y fortalecimiento de la infraestructura digital, el desarrollo de competencias digitales en la población y el tejido productivo, la inversión en tecnología, el emprendimiento e innovación tecnológica, la generación de empleos, el desarrollo de la economía digital, la mejora de la eficiencia de la administración pública, el fortalecimiento de la transparencia y la rendición de cuentas, y la participación de la ciudadanía, en consonancia con lo establecido por la Estrategia Nacional de Desarrollo 2030 (END), y los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas”.

La confianza en el uso del ciberespacio, como una opción viable para el desarrollo económico, social y la seguridad nacional es de vital importancia en la era digital. En tal sentido, y como eje transversal a todos los componente de la Agenda Digital 2030, el eje de Ciberseguridad, con su **Estrategia Nacional de**

Ciberseguridad de la República Dominicana 2030, establece los objetivos y líneas de acción que garantizan un entorno favorable para el desarrollo de todos los sectores productivos del país, garantizando un ecosistema de ciberseguridad seguro, reduciendo el impacto de las amenazas cibernéticas y protegiendo los sistemas de información y con atención especial las infraestructuras críticas nacionales y las infraestructuras de TI relevantes del Gobierno. Todo esto facilitando como Estado, que la ciudadanía pueda utilizar los servicios que se ofrecen a través de las TIC, confiados en la seguridad de los mismos.

La Estrategia cuenta con cuatro pilares: 1) Marco Legal y Fortalecimiento Institucional, 2) Protección de Infraestructuras Críticas Nacionales e Infraestructuras TI del Gobierno, 3) Educación y Cultura Nacional de Ciberseguridad, y 4) Alianzas Nacionales e Internacionales, que tiene por finalidad establecer un mecanismo de diálogo y cooperación entre todos los sectores de la sociedad para promover las mejores prácticas, identificar problemas comunes y desarrollar soluciones adecuadas para hacer frente a las amenazas cibernéticas.

MISIÓN

Establecer los mecanismos adecuados de ciberseguridad que protejan al Estado, los sectores productivos y a los ciudadanos, para garantizar un ecosistema de ciberseguridad favorable para el desarrollo económico nacional, en el marco de la transformación digital al 2030 y sobre un ciberespacio seguro, resiliente y confiable.

VISIÓN

Al 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 a los Derechos Humanos.

PRINCIPIOS RECTORES

República Dominicana avanza en nuestra misión y logrará nuestros objetivos de ciberseguridad alineando los departamentos actividades de acuerdo con los siguientes principios rectores:

1. Priorización de riesgos. La principal responsabilidad del CNCS es proteger el ecosistema de ciberseguridad de República Dominicana y debemos priorizar nuestros esfuerzos para enfocarnos en los riesgos sistémicos y los mayores Amenazas y vulnerabilidades de seguridad cibernética que enfrenta el pueblo estadounidense y nuestra patria.

2. Rentabilidad. El ciberespacio es muy complejo y los esfuerzos del CNCS para aumentar La ciberseguridad debe evaluarse continuamente y volver a priorizarse para garantizar los mejores resultados. por inversiones realizadas.

3. **Innovación y agilidad.** El ciberespacio es un dominio en evolución con riesgos emergentes. Aunque la proliferación de tecnología conlleva nuevos riesgos, también proporciona una oportunidad de innovación. CNCS debe predicar con el ejemplo en la investigación, desarrollo, adaptarse y emplear capacidades de ciberseguridad de vanguardia y permanecer ágil en sus esfuerzos para mantenerse al día con las amenazas y tecnologías en evolución.

4. **Colaboración.** El crecimiento y desarrollo de Internet ha sido impulsado principalmente por el sector privado y la seguridad del ciberespacio es un desafío intrínsecamente transversal. Para lograr nuestros objetivos de ciberseguridad, debemos trabajar de manera colaborativa en nuestros Componentes y con otros socios federales y no federales.

5. **Enfoque global.** Se requiere un compromiso y una colaboración internacionales sólidos para lograr nuestros objetivos nacionales de ciberseguridad. El CNCS debe comprometerse internacionalmente para gestionar los riesgos cibernéticos globales, responder a incidentes mundiales e interrumpir el crecimiento amenazas cibernéticas transnacionales, así como alentar a otras naciones y entidades extranjeras a adoptar las políticas necesarias para crear una Internet abierta, interoperable, segura y confiable.

6. **Renta variable equilibrada.** El ciberespacio empodera a las personas y permite la prosperidad en todo el mundo. La ciberseguridad no es un fin en sí misma, y los esfuerzos para mitigar los riesgos de ciberseguridad deben también apoyan el comercio internacional, fortalecen la seguridad internacional y fomentan la libertad expresión e innovación.

7. **Valores nacionales.** El CNCS debe defender la privacidad, los derechos civiles y las libertades civiles de acuerdo con las leyes y políticas aplicables. El Departamento potencia nuestros programas de ciberseguridad para tener éxito integrando protecciones de privacidad desde el principio y empleando una capa enfoque de la supervisión de la privacidad y las libertades civiles.

REFERENCIA NORMATIVA Y DOCUMENTAL

La presente Estrategia se enmarca en las siguientes disposiciones:

1- **Constitución de la República:** Título XII, De las Fuerzas Armadas, de la Policía Nacional y de la Seguridad y Defensa, Capítulo III, de la Seguridad y Defensa, Artículo 260 sobre Objetivos de Alta Prioridad. Constituyen objetivos de alta prioridad nacional:

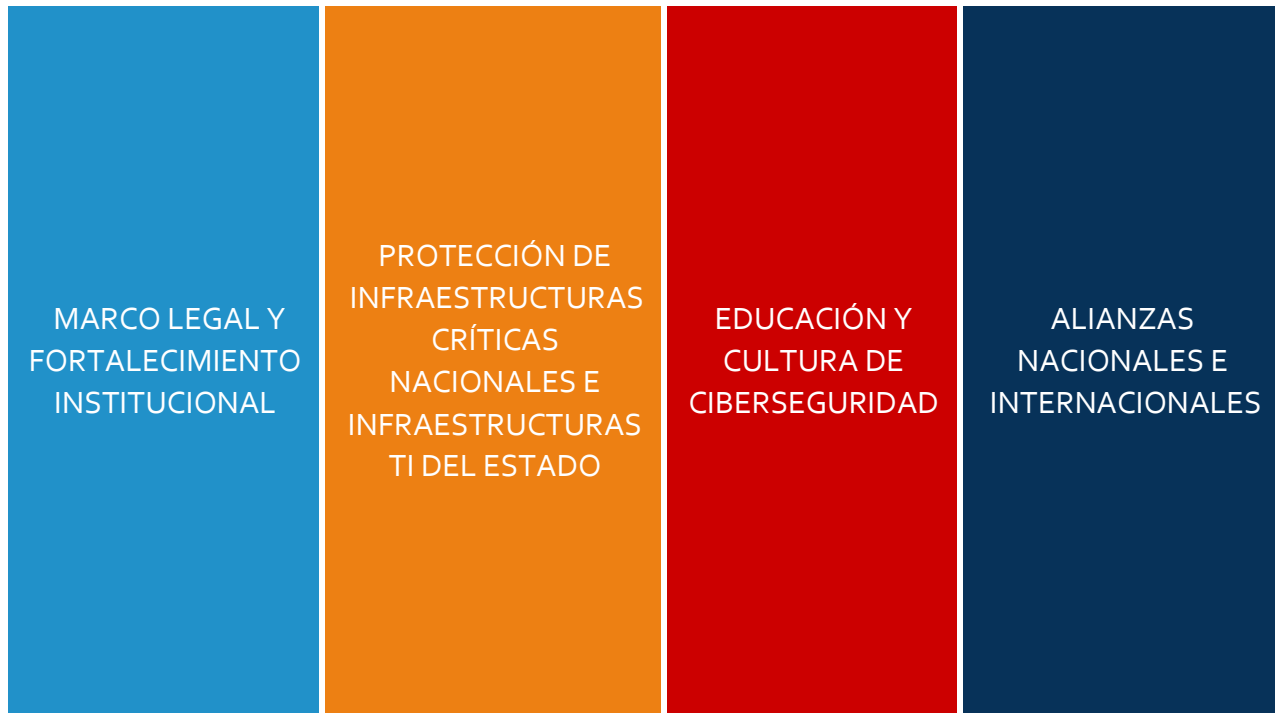
- Combatir actividades criminales transnacionales que pongan en peligro los intereses de la República y de sus habitantes.
- Organizar y sostener sistemas eficaces que prevengan o mitiguen daños ocasionados por desastres naturales y tecnológicos.

2- **Estrategia Nacional de Desarrollo (END 2030):** Que establece en su Artículo 16 sobre el Uso de las Tecnologías de la Información y la Comunicación, que *“en el diseño y ejecución de los programas, proyectos y actividades en que se concretan las políticas públicas, deberá promoverse 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”.

- 3- **Convenio del Consejo de Europa sobre Ciberdelincuencia o Convenio de Budapest (ETS-185):** ratificado por la República Dominicana el 11 de junio del 2012 mediante la Resolución 15812 publicada en la Gaceta Oficial número 10675.
- 4- **Resolución AG/RES.2004 (XXXIV-o/04) del 8 de junio del 2004, de la Asamblea General de la Organización de los Estados Americanos (OEA):** para la Adopción de una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, así como todas las declaraciones del Comité Interamericano contra el Terrorismo (CICTE) que hacen referencia a la Seguridad Cibernética.
- 5- **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).
- 6- **Plan de Acción de Ginebra de la Cumbre Mundial para la Sociedad de la Información (CMSI),** así como las áreas prioritarias de la CMSI post 2015, surgidas del proceso de consulta de la CMSI+10.
- 7- **Plan Regional para la Sociedad de la Información para América Latina y el Caribe (eLAC 2018).**
- 8- **Agenda para el Desarrollo Sostenible (ODS):** que establece en su Objetivo 17 que las TIC deben cumplir un papel fundamental en el fortalecimiento de los medios de ejecución mediante el aumento de la cooperación y coordinación internacionales, el fomento de la transferencia tecnológica, la creación de capacidades, el impulso de alianzas multipartitas y el favorecimiento y la mejora del control de datos y la rendición de cuentas.
- 9- **Ley No. 53-07, contra Crímenes y Delitos de Alta Tecnología** de fecha 23 de abril del 2007.
- 10- **Decreto No. 258-18, sobre el Programa República Digital 2016-2020:** que establece la ciberseguridad como transversal a sus cuatro ejes estratégicos. **Decr**
- 11- **Ley No. 267-08 sobre Terrorismo,** y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista. **Ley**
- 12- **Decreto 189-07,** que establece la Directiva de Seguridad y Defensa Nacional de la República Dominicana. **Decr**
- 13- **Decreto 71-21,** que crea el Gabinete de Transformación Digital, órgano responsable de la formulación, coordinación, seguimiento y control de la implementación de la Agenda Digital. **Decr**
- 14- **Decreto 52721,** que aprueba los objetivos y líneas de acción de la Agenda Digital 2030 como estrategia nacional de transformación digital. **Decr**

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD



La Estrategia Nacional de Ciberseguridad, se enmarca en cuatro (4) pilares, con sus respectivos objetivos citados a continuación:

1. **Pilar No. 1 – Marco Legal y Fortalecimiento Institucional:** 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.
2. **Pilar No. 2 – Protección de infraestructuras:** Asegurar el continuo funcionamiento de las infraestructuras críticas nacionales e infraestructuras TI relevantes del Gobierno y la protección de la información contenida en las mismas.
3. **Pilar No. 3 – Educación y Cultura:** Fomentar la inclusión de la formación en ciberseguridad en todos los niveles del sistema educativo e impulsar una cultura nacional de ciberseguridad.
4. **Pilar No. 4: - Alianzas Nacionales e Internacionales:** Establecer alianzas nacionales e internacionales entre los sectores público-privado-sociedad civil y organismos e instituciones internacionales.

Pilar No. 1: MARCO LEGAL Y FORTALECIMIENTO INSTITUCIONAL

Un esfuerzo efectivo de ciberseguridad requiere el establecimiento y la revisión periódica del marco legal relevante que respalda las TIC. Esto requiere la actualización de leyes, procedimientos y políticas penales para abordar los incidentes de ciberseguridad y responder al delito cibernético. Como prioridad, el derecho penal y los procedimientos deben revisarse para garantizar la prevención, investigación y enjuiciamiento de todas las formas de delito cibernético. Además, se debe introducir legislación que garantice la seguridad de las infraestructuras críticas de información.

Objetivo General: 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	
Objetivo Específico	Líneas de acción
1.1 Fortalecimiento del desarrollo institucional en el ámbito de la ciberseguridad	1.1.1 Fortalecer las capacidades de los actores vinculados a la gestión de la política de ciberseguridad a través de la captación de recursos y cooperación nacional e internacional

Pilar No. 2: PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS NACIONALES E INFRAESTRUCTURAS TI DEL GOBIERNO

El enfoque principal, en lo que respecta a la ciberseguridad de las infraestructuras críticas y de las infraestructuras TI relevantes del Gobierno, es establecer mecanismos de prevención, detección, respuesta y mitigación a las amenazas cibernéticas.

Objetivo General: Asegurar el continuo funcionamiento y la protección de la información almacenada en las infraestructuras críticas nacionales e infraestructuras TI relevantes del Gobierno.	
Objetivos Específicos	Líneas de Acción
2.1 Fortalecer la protección de las infraestructuras críticas nacionales e infraestructuras TI del Estado.	2.1.1 Fortalecer la gestión del riesgo cibernético para procurar el cumplimiento de los modelos de madurez en la protección de infraestructuras críticas e infraestructura TI del Estado.



	2.1.2 Establecer un plan nacional de respuesta a incidentes de ciberseguridad que procure la adecuada actuación en la gestión de incidentes cibernéticos
	2.1.3 Establecer un plan nacional de comunicación ante crisis de incidentes de seguridad cibernética
	2.1.4 Promover el establecimiento de los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos – CSIRT.

Pilar No. 3: EDUCACIÓN Y CULTURA NACIONAL DE CIBERSEGURIDAD

Para que un país pueda enfrentar de manera efectiva las amenazas cibernéticas, se requiere formar técnicos y profesionales en el área de seguridad de la información y desarrollar una cultura nacional de ciberseguridad que haga consciente a la sociedad de las consecuencias de las mismas y de cómo combatirlas.

Objetivo General: Fomentar la inclusión de la formación en ciberseguridad en todos los niveles del sistema educativo e impulsar una cultura nacional de ciberseguridad	
Objetivo Específico	Línea de Acción
3.1 Promover la educación y cultura nacional de ciberseguridad.	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 y concientización para lograr un ciberespacio más seguro

Pilar No. 4: ALIANZAS NACIONALES E INTERNACIONALES

Para la construcción de un ciberespacio seguro es fundamental establecer alianzas nacionales e internacionales entre los sectores público-privado-sociedad civil y organismos e instituciones internacionales.



Objetivo General: Establecer alianzas nacionales e internacionales entre los sectores público-privado, sociedad civil y organismos e instituciones internacionales.	
Objetivos Específicos	Líneas de Acción
4.1 Realizar alianzas nacionales e internacionales.	4.1.1 Establecer marcos de cooperación técnica, operativa y de capacitación para el fortalecimiento de la Ciberseguridad, la Ciberinteligencia, la Ciberdefensa y la lucha contra la ciberdelincuencia.

INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2021-2024

Indicador	Periodo	Fuente	Línea base	Año base	Meta 2024

ESTRATEGIA COMPLEMENTARIA DE CRIPTOGRAFIA

Objetivo General: Disponer de la mayor capacidad tecnológica de encriptación y desciframiento del estado dominicano. Esto debido a que esta tecnología se ha clasificado como un armamento para las naciones en el mundo	
Objetivos Específicos	Líneas de Acción
1. Garantizar que el Estado Dominicano utilizara herramientas criptográficas para asegurar la	1.1 Establecer y ejecutar las políticas y regulaciones para el uso de los elementos y técnicas de criptografía a nivel nacional.



confidencialidad, integridad de datos, Autenticación de la información, autorización e irrefutabilidad y servicios accesorios, como también la certificación y acreditación de las entidades certificadoras.	1.2 Establecer una estructura orgánica y operativa que ejecute las acciones del centro.
	1.3 Concertar con organismos internacionales un plan de cooperación y educación
2. El desarrollo de normativas generales que deben indicar la aplicación de criptografía en cada caso y escenario concreto, del Estado Dominicano	2.1 Establecer un registro nacional de códigos a ser utilizados por el estado de manera uniforme.
3. Monitorear la distribución de claves de cifrado en el estado dominicano	3.1 Establecer un centro de monitoreo activo a nivel nacional.

INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA DE CRIPTOGRAFIA

Indicador	Periodo	Fuente	Línea base	Ano base	Meta 2024

ESTRATEGIA COMPLEMENTARIA DE CIBERDELINCUENCIA



Objetivo General: Fortalecer las capacidades operativas de las unidades de prevención, investigación y persecución del Cibercriminológico	
Objetivos Específicos	Líneas de Acción
Fortalecer las capacidades operativas de las unidades de investigación de Cibercriminológico	Desplegar a nivel nacional las unidades de investigación
Fortalecer la capacitación del recurso humano de las unidades de investigación, jueces y fiscales	Fortalecer las capacidades de las unidades de investigación
	Fortalecer las capacidades de los actores del ministerio público en materia de cibercriminología
Fortalecer la cooperación internacional	Fortalecer los lazos de cooperación internacional e ingresar a la Policía Nacional como signatario de nuevos acuerdos y convenios
Fortalecimiento de la prevención	Crear la unidad de Ciberpatrullaje preventivo
	Desarrollar un Ciberobservatorio de análisis y estudio de nuevas conductas
	Crear canales de divulgación de nuevas conductas y metodologías del Cibercriminológico

INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA DE CIBERDELINCUENCIA

Indicador	Periodo	Fuente	Línea base	Ano base	Meta 2024



ESTRATEGIA DE CIBERDEFENSA, CIBERGUERRA y CIBERTERRORISMO

Objetivo General: Dotar a las Fuerzas Armadas de la República Dominicana, de políticas y mecanismos de Ciberdefensa, que permitan la prevención, mitigación y respuesta a ataques cibernéticos de Ciberterrorismo y ciberguerra mediante la integración y coordinación del Centro Nacional Antiterrorismo	
Objetivos Específicos	Líneas de Acción
Identificar, analizar y clasificar las infraestructuras críticas relativas a la defensa nacional	Identificar las infraestructuras de TI relevantes a la defensa
Robustecimiento de infraestructuras críticas relativas a la defensa, y creación de normas de cumplimiento y seguimiento de acuerdo a estándares definidos en el Plan de Acción del Pilar No. 2	Crear el Plan de robustecimiento de infraestructuras de TI
Creación y coordinación de grupos o entes de apoyo nacional para el fortalecimiento y eficientización de las herramientas de seguridad, mediante seguimiento y monitoreo constante de los ataques locales e internacionales.	Desarrollar el Plan de Respuesta a incidentes y ataques
Complementar el pilar No. 4 de la ENCS, relativo al fortalecimiento de la cooperación internacional	Fortalecer la coordinación interinstitucional
Crear y actualizar las capacidades, de los responsables de las infraestructuras críticas relativas a la defensa nacional	Fortalecer las capacidades institucionales de atención y respuesta

INDICADORES LOCALES E INTERNACIONALES – ESTRATEGIA DE CIBERDEFENSA, CIBERGUERRA Y CIBERTERRORISMO

Indicador	Periodo	Fuente	Línea base	Ano base	Meta 2024

MODELO DE GOBERNANZA, IMPLEMENTACIÓN Y SEGUIMIENTO

El Centro Nacional de Ciberseguridad, dentro del marco de gobernanza de la Ciberseguridad a nivel del Estado Dominicano, tiene la responsabilidad de implementar, dar seguimiento a la ejecución y monitorear todas las iniciativas y proyectos, que se derivan de la Estrategia Nacional de Ciberseguridad. El Centro cuenta con un Consejo Directivo, como su máxima autoridad, conformado por las siguientes instituciones miembros:

1. Ministerio de la Presidencia, que lo preside
2. Ministerio de Defensa
3. Ministerio de Interior y Policía
4. Procuraduría General de la República
5. Policía Nacional
6. Departamento Nacional de Investigaciones
7. Instituto Dominicano de las Telecomunicaciones
8. Oficina Gubernamental de Tecnologías de la Información y Comunicación
9. El Director Ejecutivo del Centro Nacional de Ciberseguridad (CNCS), en calidad de Secretario y miembro del Consejo

El Consejo tiene la facultad, en el caso que 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 Infraestructura Crítica, Sector Privado, Poder Legislativo, Poder Judicial y ciudadanía en general.

El Centro Nacional de Ciberseguridad, en el marco de la Agenda Digital 2030, da seguimiento a los indicadores claves locales e internacionales, establecidos en el portafolio de proyectos del documento de Agenda Digital 2030, para asegurar que la Estrategia Nacional de Ciberseguridad, esté cumpliendo con sus metas y objetivos.

La Estrategia Nacional de Ciberseguridad es actualizada cada tres años, esto da oportunidad de aprovechar e 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 clave definidos en el marco de evaluación.

Para esta actualización de la Estrategia Nacional de Ciberseguridad, las instituciones responsables de ejecutar los planes complementarios vinculados a Ciberdelincuencia, Ciberterrorismo, Ciberdefensa, Ciberguerra y Criptografía, han presentado las Estrategias correspondientes, para los fines de garantizar que los objetivos e iniciativas vinculadas a cada asunto de ciberseguridad, queden alineados a los objetivos de transformación digital, la Agenda Digital 2030 y la Estrategia Nacional de Ciberseguridad, así como el logro de los indicadores vinculados a las mismas.

-----FIN DEL DOCUMENTO-----