Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE INFORMACIÓN

NACC/DCA/11 — NI/26
09/06/23

Undécima Reunión de Directores de Aviación Civil de Norteamérica, Centroamérica y Caribe (NACC/DCA/11)

Varadero, Cuba, 28 al 30 de junio de 2023

Cuestión 5 del Orden del Día: **Implementación regional NAM/CAR de seguridad de la aviación/facilitación**

AVANCES EN CIBERSEGURIDAD DE LA AVIACIÓN CIVIL

(Nota presentada por República Dominicana)

RESUMEN EJECUTIVO	
En esta nota se resumen las iniciativas en curso y los avances producidos en materia de ciberseguridad por el Estado dominicano quien tiene como meta salvaguardar las infraestructuras críticas de manera segura y confiable. En esta nota informativa se presenta la situación sobre la ley de ciberseguridad, la actualización de las políticas, el entrenamiento continuo de los recursos humanos de la Organización, así como futuras medidas para seguir mejorando.	
Objetivo Estratégico:	• Objetivo estratégico 3 – Seguridad de la aviación y facilitación

1. Introducción

1.1 El Estado tiene como misión establecer los mecanismos adecuados de ciberseguridad que lo protejan, así como, los sectores productivos y a los ciudadanos, todo esto con la finalidad de garantizar un ecosistema de ciberseguridad favorable para el desarrollo económico nacional, en el marco de la transformación digital y sobre un ciberespacio seguro, resiliente y confiable.

2. Desarrollo

2.1 El Decreto 230-18 Crea la Estrategia Nacional de Ciberseguridad 2018-2021 que establece los mecanismos de ciberseguridad adecuados para la protección del Estado, sus habitantes y, en general, del desarrollo y la seguridad nacional para crear en República Dominicana un ciberespacio más seguro y confiable. Se hace especial énfasis en el Art. 6 del Decreto referente al pilar 2 de la Estrategia sobre Protección de Infraestructuras Críticas Nacionales e Infraestructuras de Tecnología de la Información y Comunicación (**TIC**), del Estado. En este mismo decreto se crea el Centro Nacional de Ciberseguridad como una dependencia del Ministerio de la Presidencia de la República Dominicana.

2.2. Cabe destacar que el Centro Nacional de Ciberseguridad es el organismo facultado por el Estado dedicado al desarrollo de la ciberseguridad, al fortalecimiento de la confianza digital del usuario dominicano y a la protección de la infraestructura crítica y tecnológica del Estado dominicano.

2.3 El decreto antes mencionado es actualizado el 14 de junio del año 2022 promulgando así el decreto 313-22 el cual establece 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 de desarrollo sostenible y a los indicadores internacionales de desarrollo y buenas prácticas en materia de ciberseguridad.

2.4 La estrategia 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 la TIC, confiados en la seguridad de estos.

2.5 La Estrategia cuenta con cuatro pilares:1) Marco Legal y Fortalecimiento Institucional, 2) Protección de Infraestructuras Críticas Nacionales e Infraestructuras TIC 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.

2.6 Es importante destacar que la República Dominicana avanzó 30 posiciones en el Índice Nacional de Ciberseguridad (NCSI, por sus siglas en ingles), el cual mide la preparación de los países para prevenir amenazas y gestionar incidentes cibernéticos, de acuerdo al reporte, el país alcanzó un nivel de desarrollo de un 71% entre 2022 y 2023, por lo que pasó de la posición 58 a la 28, en el ranking que mide el e-Governance Academy Fundation de la República de Estonia.

3. Marco regulatorio

3.1. El Estado dominicano tiene en vigencia la Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología: Tiene como objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en prejuicio de personas físicas o morales en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

3.2. La Ley núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

3.3. Actualmente se encuentra en el Senado Dominicano para aprobación un proyecto de ley de Ciberseguridad, el cual tiene el objeto fortalecer el marco normativo para la gestión de la seguridad cibernética de las infraestructuras de tecnologías de la información y comunicación de la Administración pública y de las infraestructuras críticas del estado.

4. Capacitación

4.1 El CESAC, como entidad perteneciente al Ministerio de Defensa, mediante el CSIRT-Defensa del Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (**C5i**), lleva a cabo capacitación continua en aspectos de ciberseguridad mediante su plataforma de captación de talentos.

4.2 El Centro Nacional de Ciberseguridad, quien es la entidad competente en materia de ciberseguridad de la República Dominicana, recientemente fue convocado al sector de la aviación civil para participar en una sesión de Análisis de Riesgo de las Infraestructuras Criticas de Información, esto en cooperación con el proyecto CyberNet de la Unión Europea, con el fin de identificar las infraestructuras criticas del sector de la aviación civil y saber cómo defenderlas ante cualquier ciberataque.

5. Conclusión

5.1 La adopción de la Estrategia de Ciberseguridad de la República Dominicana marca un hito para el desarrollo del ciberespacio dominicano. Los desafíos asociados a la ciberseguridad son de naturaleza variada y compleja, siendo uno de los principales la definición del marco legal aplicable, es por esta razón que el Estado dominicano tiene el compromiso del establecimiento y la revisión periódica del marco legal. Como prioridad, el derecho penal y los procedimientos deben revisarse para garantizar la prevención, investigación y enjuiciamiento de todas las formas de delito cibernético.

5.2 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, actualmente el Estado se encuentra identificando cuáles son las infraestructuras críticas en el sector de la aviación civil, lo que demuestra el compromiso que se tiene para alcanzar un ciberespacio más seguro.

— FIN —