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

NOTA DE ESTUDIO

NACC/DCA/12 — NE/17
21/06/24

Doceava Reunión de Directores de Aviación Civil de Norteamérica, Centroamérica y Caribe (NACC/DCA/12)

Placenta, Belize 09-11 Julio 2024

Cuestión 3 del Orden del Día: **Seguridad de la Aviación (AVSEC) y Facilitación (FAL)**

Iniciativa para la protección de sistemas críticos de tecnología de la información, las comunicaciones y los datos críticos conexos utilizados para proteger la aviación civil de interferencias ilícitas aeronáuticas en los Estados Miembros de COCESNA

(Presentada por Belice, Costa Rica, El Salvador, Guatemala, Honduras y Nicaragua)

RESUMEN EJECUTIVO

Esta Nota de Estudio presenta la iniciativa de COCESNA en materia de ciberseguridad para apoyar y orientar a las Autoridades de Aviación Civil de los Estados Miembros en el establecimiento de políticas e implementación de medidas para la protección de los sistemas críticos de tecnología de la información y las comunicaciones aeronáuticas. Además de, brindar una guía hacia los explotadores de la industria de la aviación para su propia identificación y protección; incluyendo aeropuertos, explotadores de aeronaves, proveedores ATS, proveedores de servicios de comunicación, agentes de servicios de escala, entre otros.

Con la finalidad de fomentar una interpretación común entre los Estados sobre las ciber amenazas, riesgos y la formulación de criterios; para reforzar la seguridad de la aviación y la facilitación.

Acción:	Las acciones sugeridas se presentan en la Sección 5.
Objetivos Estratégicos:	a. Identificar y definir los sistemas de tecnologías de la información, comunicación y datos críticos utilizados para la aviación civil, en cada uno de los Estados Miembros de COCESNA. b. Identificar amenazas internas y externas comunes que pueden repercutir en los datos y sistemas de aviación a través de un análisis de riesgos. c. Homologar un criterio de evaluación de riesgo, para llevar a cabo evaluaciones continuas y establecer medidas en caso interferencia ilícita. d. Establecer medidas mínimas de protección de sistemas de tecnologías de la información y la comunicación críticos.

	e. Detectar ciberataques mediante el establecimiento de un sistema de observación continua de la seguridad de la información. f. Brindar orientación a la industria de la aviación para la protección de sus sistemas y minimizar ciberataques que puedan afectar la aviación civil en la región.
Referencias:	• Anexo 17 OACI • Doc.8973 OACI • Capítulo 18 del Manual de seguridad de la aviación (Doc 8973 – Restringido) • Manual de seguridad de la gestión del tráfico aéreo (Doc 9985 – Restringido) • Orientación sobre la política de ciberseguridad y Cultura de ciberseguridad en la aviación civil.

1. Introducción

1.1 En el contexto actual de la aviación civil, se prevé que el tráfico aéreo aumente a largo plazo, la tecnología siga una evolución acelerada, las operaciones sean cada vez más complejas y, consecuentemente, las condiciones operacionales se vuelvan más difíciles. Los rápidos cambios tecnológicos están alterando la forma en que funciona la aviación civil y haciendo que el sistema sea más vulnerable frente a las amenazas de ciberseguridad. Las ciberactividades malintencionadas pueden afectar a la aviación civil de diversas maneras, desde una breve disrupción de las operaciones hasta consecuencias catastróficas. Los riesgos se están incrementando velozmente, por lo que se necesita de forma apremiante un marco de ciberseguridad sostenible a nivel internacional, regional y nacional.

1.2 La creación de una infraestructura de ciberseguridad sólida, sustentada en una estrecha cooperación entre los Estados, la industria, permite la creación de una conciencia común sobre la ciberseguridad que desemboque, a la postre, en un sistema de aviación civil más seguro y resiliente.

1.3 Como parte del compromiso con la protección de la seguridad de la aviación civil de sus Estados Miembros, COCESNA, a través de sus diferentes gerencias: Agencia Centroamericana para la Seguridad Aeronáutica, Agencia Centroamericana de Navegación Aérea, Tecnología Informática y en coordinación con el Grupo Regional AVSEC de Centroamérica, integrado por los especialistas AVSEC de la región centroamericana, considerando la importancia de las disposiciones del Anexo 17 al Convenio sobre Aviación Civil Internacional, en particular la Norma 4.9.1 en donde dispone se identifiquen los sistemas de tecnología de la información y las comunicaciones y datos críticos que se empleen para los fines de la aviación civil, y que en función de una evaluación de riesgos elaboren y lleven a la práctica las medidas que correspondan para protegerlos de interferencia ilícita, se dio a la tarea de poner en marcha la iniciativa para para la identificación, evaluación de riesgos y protección de sistemas críticos de tecnología de la información, las comunicaciones y los datos críticos conexos utilizados operacionalmente en la aviación civil y que puedan ser objeto de interferencias ilícitas aeronáuticas en los Estados Miembros de COCESNA.

2. Discusión

2.1 La ciberseguridad no es un concepto nuevo en el ámbito de la aviación civil. No obstante, como las amenazas de ciberseguridad se han vuelto cada vez más frecuentes, se ha convertido en uno de los elementos centrales de los debates y análisis de riesgos y vulnerabilidades del sistema de aviación civil. El sector de la aviación civil está particularmente en situación de riesgo porque los ciberataques tienen más posibilidades de prosperar en un sector cuyos componentes aumentan de forma interdependiente desde el punto de vista funcional y digital, y también porque los mecanismos de ciberdefensa que usa actualmente el sector de la aviación civil aún no son adecuados para hacer frente a esta amenaza persistente y adaptable.

2.2 Dada la naturaleza polifacética y multidisciplinaria de la ciberseguridad, y en vista de que los ciberataques pueden afectar de forma simultánea una amplia gama de áreas y propagarse con rapidez, es imperioso concebir una visión común y definir una estrategia de ciberseguridad.
Esto puede lograrse mediante:

- el reconocimiento de parte de los Estados de sus obligaciones en virtud del Convenio sobre Aviación Civil Internacional (Convenio de Chicago) de velar por la seguridad operacional y la seguridad y continuidad de la aviación civil, incluida la ciberseguridad;

- la coordinación de la ciberseguridad de la aviación entre las autoridades estatales a fin de garantizar una gestión eficaz y eficiente de los riesgos de ciberseguridad a escala mundial; y

- el compromiso de todas las partes interesadas de la aviación de profundizar la resiliencia en este ámbito y protegerse contra los ciberataques que pudieran afectar la seguridad operacional, la seguridad de la aviación y la continuidad del sistema de transporte aéreo.

2.3 Considerando que en materia de ciberseguridad COCESNA inició con el establecimiento de un Objetivo Especifico dentro del Plan Estratégico orientado a “Implementar Ciberseguridad acorde a las buenas prácticas del sector aeronáutico y tecnológico”, y a través de lo cual ha logrado establecer iniciativas que van desde un marco normativo, socialización, implementación de medidas de protección y grupos de ciberseguridad y en apoyo a la detección de necesidades específicas en materia de ciberseguridad identificadas a través de las asistencias técnicas en seguridad de la aviación, llevadas a cabo en sus Estados Miembros, y uniendo esfuerzos para comenzar con esta iniciativa tomando como referencia las iniciativas implementadas a nivel interno.

2.4 Las acciones que se realizan y que son parte de la implementación de medidas mínimas de esta iniciativa regional centroamericana para la seguridad y protección de las operaciones de aviación civil, dentro de los Estados Miembros Belice, Costa Rica, El Salvador, Guatemala, Honduras y Nicaragua son:

a) Protección de los sistemas y los datos contra el acceso, la modificación y el uso no autorizados;
b) Control sobre la falta de disponibilidad e integridad debida a fallas en la compilación de programas informáticos y/o mala utilización de configuraciones
c) Reducción de la manipulación indebida de los sistemas y sus datos.

3. Avances

3.1 Dada la creciente importancia de la ciberseguridad y la necesidad de proteger el sistema de aviación contra nuevas amenazas en los Estados de la región centroamericana y en el marco del proyecto Asociación de Aviación UE – América Latina y el Caribe (EU-LAC APP) se coordinó una reunión con la Agencia de Seguridad Aérea de la Unión Europea (EASA) en donde ofreció una visión general del enfoque europeo hacia la ciberseguridad, la capacidad de poder brindar entrenamiento en materia de ciberseguridad y el intercambio de experiencias con COCESNA.

3.2 Además, se identificaron áreas de interés mutuo y cooperación futura en la gestión del riesgo de la ciberseguridad de la aviación.

4. Hoja de Ruta

4.1 Identificación de sistemas de información, comunicación y datos identificados como críticos desde una perspectiva de seguridad operacional de la aviación:

4.2 Como parte del inicio en el proceso de mitigación de interferencias ilícitas en la industria de la aviación, se les recomienda a los Estados Miembros que los riesgos de Ciberseguridad se identifiquen y se evalúen, teniendo en cuenta todas las consecuencias posibles de un ataque al sistema de aviación civil por ejemplo: protección, seguridad, eficiencia, continuidad del servicio, etc; así como las posibles fuentes de las amenazas y las vulnerabilidades que puedan existir.

4.3 Además, se recomienda que la identificación y evaluación de los riesgos de ciberseguridad las coordine y sean realizadas por un grupo de expertos en cibernética y en aviación civil, de ser posible con experiencia en ciberseguridad y deberían estar en la capacidad de poder identificar sus sistemas de información, comunicación y datos que pueden identificarse como críticos, esto para poder delimitar el alcance y la capacidad del Estado en el momento que sus sistemas sean amenazados, y así poder gestionar de mejor manera una amenaza en el tema de ciberseguridad.

4.4 Para ello hemos planteado un formato, que permita llevar a cabo dicha identificación de sistemas de información, comunicación y datos críticos según el Estado

ESTADOS MIEMBROS COCESNA Belice, Costa Rica, El Salvador, Guatemala, Honduras y Nicaragua			
Entidades Gubernamentales	Operadores de Aeropuerto	Explotadores Aéreos	Industria en General

4.5 Desarrollo de una evaluación de riesgos específicos para los sistemas críticos identificados. Análisis de las posibles amenazas y vulnerabilidades, considerando tanto factores tecnológicos como humanos (tomando en cuenta que la Gerencia de TI ya cuenta con un análisis de riesgo interno, esto se podría replicar en la región CA, con apoyo del personal de TI de las autoridades de Aviación Civil y otras entidades pertinentes, en caso de que existan). Se podría iniciar con Guatemala y Honduras.

4.6 Evaluación del riesgo

a. Como parte de un proceso de evaluación de riesgos, los Estados Miembros deberían, por medio de sus respectivas autoridades designadas y como política de ciberseguridad nacional, trabajar con personal calificado para realizar evaluaciones continuas de la vulnerabilidad e interdependencia de sus sistemas, y así establecer medidas para mitigar posibles ciberataques y verificar la aplicación de tales medidas como parte de sus actividades ordinarias de observación del cumplimiento (p. ej., inspecciones y auditorías).

b. Dentro de estas evaluaciones los Estados Miembros con el apoyo de las autoridades nacionales de aviación civil deben realizar dichas evaluaciones bajo una metodología en donde se tomen en cuenta los componentes principales del riesgo:

   i. Escenario de la amenaza: la identificación y posible descripción de un acto de interferencia ilícito y los métodos para llevar a cabo dicho acto, las autoridades nacionales de los Estados deberán crear un escenario lo más real posible.
   ii. Probabilidad de ataque: Los Estados deberán revisar la probabilidad de que se produzca un ataque a los sistemas cibernéticos en materia de aviación, sin excluir ninguno de ellos por más complejo que parezcan.
   iii. Consecuencias: en caso de llevarse a cabo un ciberataque a los sistemas en materia de aviación cual es la magnitud y los efectos que puedan repercutir (humanos, económicos y políticos).
   iv. Vulnerabilidad: Los Estados deben ser capaces de autoidentificar sus vulnerabilidades existentes en cuanto a la magnitud de un ciberataque.
   v. Riesgo residual: Una vez analizada la probabilidad, consecuencias y vulnerabilidad, el riesgo que pueda persistir aun tomando medidas de acuerdo a estas variables.

c. Una vez los Estados y sus autoridades nacionales de aviación civil, lleven a cabo dicha evaluación de riesgo, es importante el establecimiento de criterios mínimos para la protección de los sistemas de tecnologías de la información y la comunicación y los datos críticos conexos utilizados para proteger la aviación civil de interferencias ilícitas que deben ser implementadas por cada uno de los Estados y sus autoridades de aviación civil.

(**En esta parte se podría enlistar cuales son las medidas determinadas para la protección**)

d. <u>Infraestructura de ciberseguridad:</u> Está relacionado con la administración técnica de los dispositivos y de las herramientas de ciberseguridad, como ser (Sin ser limitativas):

- Antivirus;
- Antispam;
- Firewall;
- Web Application Firewall (WAF);
- Escaneo de vulnerabilidades;
- Vídeo vigilancia;
- Soporte remoto;
- Encriptación de datos;

- Borrado seguro.

e. Gestión de activos TI: Relacionado con la administración de los equipos y dispositivos tecnológicos que incluye:

- Ciclo de vida de los activos TI (Planificación, provisión, administración, descargo);
- Clasificación de activos TI;
- Identificación de activos críticos;
- Inventario de Hardware;
- Inventario y asignación de licencias de Software;
- Gestión de parches

5. Conclusión

5.1 La protección de sistemas críticos de tecnología de la información, comunicaciones y datos en la aviación civil es fundamental para garantizar la seguridad y eficiencia operativa. La implementación de medidas robustas de ciberseguridad, protocolos de encriptación y sistemas de monitoreo continuo son esenciales para prevenir amenazas y asegurar la integridad de la información en este sector altamente sensible. La colaboración entre entidades gubernamentales, entidades aeronáuticas y expertos en ciberseguridad es clave para mantener un entorno aéreo seguro y confiable.

5.2 La seguridad de la aviación, como una base fundamental para el crecimiento y la sostenibilidad de la industria de la aviación, necesita de la integración de medidas armonizadas y aplicadas por los Estados Miembros, en donde se dé el intercambio del conocimiento y experiencias que permitan la ejecución de buenas prácticas y oportunidades de mejora estandarizadas para lograr elevar los niveles de cumplimiento y dar reconocimiento a la región centroamericana como un promotor de acciones en materia de seguridad de la aviación, que orienten a garantizar la protección de la aviación civil contra actos de interferencia ilícita a través de medios tecnológicos que puedan afectar sus sistemas críticos de información, comunicaciones y datos

6. Acción sugerida:

6.1 Se invita a la reunión a:

a) Tomar en consideración las iniciativas emprendidas por los Estados Miembros de COCESNA para la implementación de ciberseguridad a nivel regional.
b) Impulsar a los Estados y organizaciones sobre el desarrollo de iniciativas, establecimiento de medidas, desarrollo de planes que fomenten la protección de sistemas críticos de tecnología de la información, las comunicaciones y los datos críticos conexos utilizados, para proteger la aviación civil de interferencias ilícitas aeronáuticas.
c) Promover el compartir las lecciones aprendidas, y los beneficios obtenidos con sus implementaciones para beneficio de otros Estados y organizaciones.

— FIN —