Organización de Aviación Civil Internacional
Oficina Regional Sudamericana
Decimoctava Reunión de Autoridades de Aviación Civil de la Región Sudamericana (RAAC/18)
(Sao Paulo, Brasil, 24 al 26 de febrero de 2025)

RAAC/18-NE/40
06/02/25

Cuestión 5A del Orden del Día: **Efectividad en los planes**

FORTALECIENDO LA CIBERSEGURIDAD EN LA AVIACIÓN CIVIL: PLAN DE TRABAJO COLABORATIVO PARA LA PROTECCION DE LA AVIACIÓN CIVIL

Nota presentada por Colombia, "*El País de la Belleza*"

RESUMEN

La digitalización creciente de la aviación civil ha generado una mayor vulnerabilidad a los ciberataques, que afectan tanto la seguridad operacional como las infraestructuras críticas del sector. Estos ciberataques, cada vez más frecuentes y sofisticados, amenazan la seguridad de los pasajeros, las operaciones aéreas y la reputación de la industria. En este contexto, la ciberseguridad se ha convertido en una prioridad estratégica, con el fin de proteger los sistemas de navegación, comunicación y gestión de vuelos, entre otros. La Organización de Aviación Civil Internacional (OACI) ha desarrollado una Estrategia y un Plan de Acción de Ciberseguridad para guiar a los Estados y actores clave en la implementación de medidas efectivas de seguridad cibernética.

Para abordar estos desafíos, es fundamental adoptar un enfoque integral y colaborativo. Esto incluye la creación de marcos de ciberseguridad específicos para la aviación civil, la formación de equipos especializados y la implementación de centros de respuesta a incidentes cibernéticos. Además, la cooperación internacional y regional entre los Estados de la región SAM es esencial para mejorar la coordinación en la lucha contra las amenazas cibernéticas transfronterizas. La capacitación del personal, desde el operativo hasta los directivos, en aspectos técnicos y de gobernanza en ciberseguridad, es crucial para prevenir y mitigar los efectos de los ciberataques en la aviación civil.

Referencias
- Anexo 17 de OACI: Seguridad de la aviación AVSEC.
- Documento OACI: Estrategia de Ciberseguridad de la Aviación.
- Documento OACI: Orientación sobre la política de Ciberseguridad.
- Documento OACI: Resolución A41-19 Abordar la Ciberseguridad en la Aviación civil.
- Documento OACI: Plan de acción de Ciberseguridad

Objetivos estratégicos:	***1.*** *Cada vuelo es seguro (Safety and Security)* ***2.*** *Ningún País se queda atrás.* ***3.*** *El Convenio de Aviación Civil Internacional y otros Tratados, Leyes y Reglamentos abordan todos los Desafíos* ***4.*** *El desarrollo económico del transporte aéreo asegura la prosperidad económica y el bienestar social para todos*

1. Introducción

1.1 La creciente digitalización de la aviación civil ha transformado radicalmente el sector, exponiéndolo a una vulnerabilidad cibernética sin precedentes. Los ciberataques, cada vez más sofisticados y frecuentes, ponen en riesgo tanto la seguridad operacional, amenazando vidas a bordo, como la seguridad de la aviación civil en su conjunto, afectando infraestructuras críticas, operaciones y reputación. Ante esta realidad, fortalecer la ciberseguridad se ha convertido en una imperativa estratégica para garantizar la continuidad y la resiliencia del sector.

1.2 La OACI, en su Estrategia de Ciberseguridad de la Aviación y el Plan de acción de Ciberseguridad, ha proporcionado un sólido marco de referencia para abordar estos desafíos. Sin embargo, la implementación efectiva de estas recomendaciones requiere de una acción coordinada y sostenida a nivel regional, así como de un compromiso firme por parte de todos los actores involucrados, desde los Estados miembros hasta la industria y la academia

2. Discusión

2.1 La creciente interconexión de los sistemas en la aviación civil, impulsada por la digitalización y la automatización, ha transformado radicalmente el sector, exponiéndolo a una vulnerabilidad cibernética sin precedentes. Esta nueva realidad plantea desafíos significativos que requieren una respuesta coordinada y global.

Los ciberataques contra la aviación civil no son una amenaza hipotética, sino una realidad tangible. Los actores maliciosos pueden comprometer sistemas críticos como el control de tráfico aéreo, los sistemas de navegación y los sistemas de gestión de vuelos, poniendo en riesgo la seguridad de millones de pasajeros y tripulantes. Además, los ciberataques pueden causar interrupciones significativas en las operaciones aéreas, generando pérdidas económicas millonarias y dañando la reputación del sector.

Los principales riesgos a los que se enfrenta la aviación civil incluyen:

- Pérdida de confidencialidad: Robo de datos sensibles de pasajeros y empresas.

- Pérdida de integridad: Manipulación de datos críticos para el funcionamiento de los sistemas.

- Pérdida de disponibilidad: Interrupción de los servicios de navegación aérea, sistemas de comunicación, sistemas que sirven de apoyo a la seguridad de la aviación civil y otros sistemas críticos.

- Daño a la reputación: Pérdida de confianza de los pasajeros y las partes interesadas.

3. Conclusión

3.1 Ante esta problemática, se hace imperativo adoptar un enfoque integral y colaborativo para fortalecer la ciberseguridad en la aviación civil. En este sentido dentro de la definición de acciones para la implementación de la estrategia para la estrategia de la aviación civil de la región SAM se deberían contemplar las siguientes propuestas que buscan:

3.1.1 Establecer un marco de referencia sólido o creación de un framework de ciberseguridad específico para la aviación civil que proporcionará a los Estados y las partes interesadas, una guía clara y concisa sobre cómo implementar medidas de seguridad efectivas. Este Framework debería destacar, entre otros, la importancia de:

- Compromiso de la alta dirección: Los altos directivos de las organizaciones deben liderar y respaldar activamente las iniciativas de ciberseguridad, asignando los recursos necesarios y estableciendo una cultura de seguridad a todos los niveles.
- Gobernanza eficaz: Implementar un marco de gobernanza sólido que defina roles, responsabilidades y procesos claros para la gestión de la ciberseguridad, incluyendo la creación de un comité de ciberseguridad a nivel directivo.
- Política de Ciberseguridad: lineamientos mínimos en materia de ciberseguridad que se deben implementar a nivel técnico y regulatorio para la protección de los sistemas críticos a nivel de TI/TO con todas las partes interesadas que hacen parte del sector.
- Desarrollo de talento especializado: Es fundamental invertir en la formación y capacitación continua del personal en ciberseguridad para garantizar un equipo altamente cualificado para el sector de la aviación. Atraer y retener a estos profesionales es crucial debido al manejo de información sensible y los altos costos asociados a la rotación

3.1.2 Fortalecer y crear los lineamientos para que se establezcan los procedimientos para la conformación de la estructura organizacional, y los procedimientos de un CSIRT dedicado a la aviación civil (Centro de Respuesta a Incidentes de Ciberseguridad), que permitan una respuesta más rápida y coordinada ante incidentes cibernéticos, minimizando el impacto en las operaciones aéreas, que contenga los siguientes aspectos:

- Centralización: Consolidar los esfuerzos de respuesta a incidentes en un único centro, con capacidad para atender todos los eventos cibernéticos a nivel de infraestructuras críticas y coordinar acciones de respuesta.
- Articulación: Establecer una estrecha colaboración con todas las partes interesadas que conforman el sector de la aviación civil en cada uno de los estados contratantes, y con otros CSIRT nacionales e internacionales, para compartir información y mejores prácticas.
- Capacitación: Equipar al personal del CSIRT con las herramientas y conocimientos necesarios para responder de manera efectiva a los incidentes cibernéticos a los que se enfrenta este sector.

3.1.3 Fomentar la cooperación internacional en la Ciberseguridad y la colaboración entre los Estados de la región SAM es fundamental para compartir información, mejores prácticas y recursos, y para desarrollar una respuesta coordinada a las amenazas cibernéticas transfronterizas, que tenga en cuenta los siguiente:

- Intercambio de información: desarrollar una plataforma tecnológica de intercambio de información en materia de ciberseguridad única para el sector de la aviación civil para compartir experiencias, conocimientos y lecciones aprendidas en materia de ciberseguridad entre todos los estados miembros.
- Cooperación con estados de la Región SAM: Fortalecer la cooperación con estados de la región SAM para abordar de manera conjunta las amenazas cibernéticas para ello se propone el desarrollo de ejercicios conjuntos de simulación y manejo de incidentes cibernéticos que pongan en riesgo la aviación civil.

3.1.4 Crear un programa de concientización y capacitación del personal técnico, operativo y directivo en ciberseguridad orientado al sector aéreo, mediante el desarrollo de un programa de capacitación en ciberseguridad que abarque todos los niveles de las organizaciones del sector aéreo, incluyendo:

- Personal operativo: Concientizar y capacitar a los controladores aéreos y demás personal operativo en la identificación de amenazas cibernéticas, las mejores prácticas de seguridad y los procedimientos a seguir en caso de incidentes cibernéticos.
- Personal técnico: Impartir cursos especializados a Inspectores de Seguridad de la aviación civil, personal técnico de TI y TO en seguridad de sistemas, redes y aplicaciones, así como en la

implementación de los controles de ciberseguridad de los sistemas tecnológicos que soportan las operaciones aéreas.

- Personal directivo: Ofrecer concientización y cursos básicos en Ciberseguridad, gobernanza y políticas de Ciberseguridad exclusivas al sector aéreo.
- Desarrollar capacidades humanas: La capacitación del personal en ciberseguridad es esencial para garantizar que el sector cuente con los conocimientos y habilidades necesarios para prevenir, detectar y responder a los ciberataques.

4. Acción Sugerida

4.1 Se invita a la reunión a:

a) Desarrollar un framework o plan de acción de ciberseguridad que contemple los aspectos relacionados en esta nota de estudio que sirva como referencia para los Estados y las partes interesadas del sector aéreo.

— FIN —