



ASAMBLEA — 42º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 13: Seguridad de la aviación — Política

ESTRATEGIA DE CIBERSEGURIDAD AERONÁUTICA BAJO UN PLAN DE TRABAJO COLABORATIVO PARA LA PROTECCION DE LA AVIACIÓN CIVIL

(Nota presentada por Colombia y apoyada por 16 Estados miembros de la CLAC²)

RESUMEN

La aviación está experimentando una transformación digital sin precedentes. Tecnologías como las comunicaciones digitales, la integración de sistemas inteligentes, el análisis de datos, la vigilancia avanzada, los sistemas ATM predictivos y la computación en la nube; están redefiniendo el sector. Sin embargo, esta creciente interconexión aumenta la superficie de ataque y la vulnerabilidad a ciberamenazas. Los ataques, cada vez más sofisticados, ponen en riesgo la seguridad operacional, la privacidad de los datos y la confianza en el sistema.

Para contrarrestar este desafío, es crucial fortalecer la ciberseguridad del sector. Los Estados miembros deben implementar las recomendaciones de la OACI, como la Estrategia de Ciberseguridad y el Plan de acción de ciberseguridad, y adaptarlas a sus contextos nacionales, fortaleciendo su cultura organizacional, su infraestructura tecnológica y sus regulaciones en la materia para afrontar los retos específicos de la ciberseguridad en la aviación civil.

Además, la transaccionalidad del ciberespacio obliga también a generar mecanismos de diálogo y cooperación técnica y operativa en el área entre los estados miembros.

Decisión de la Asamblea: Se invita a la Asamblea a:

- Solicitar al Consejo de la OACI que como parte del plan estratégico 2026 – 2050 se desarrolle una herramienta de autoevaluación para que los Estados midan su nivel de madurez en ciberseguridad aeronáutica.

Objetivos estratégicos:

Esta nota de estudio se relaciona con los Objetivos estratégicos:

- Seguridad operacional.
- Capacidad y eficiencia de la navegación aérea.
- Seguridad de la aviación y facilitación.
- Cada vuelo es seguro (Safety and Security)
- La aviación proporciona movilidad fluida, accesible y confiable para todos
- Ningún País se queda atrás.

¹ La versión en español fue proporcionada por Colombia

² Belice, Bolivia (Estado Plurinacional de), Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela (República Bolivariana de).

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

1. INTRODUCCIÓN

1.1 La aviación mundial ha experimentado una transformación digital sin precedentes, impulsada por el uso de tecnologías avanzadas. Sin embargo, esta digitalización aumenta la vulnerabilidad a ciberataques, que pueden comprometer la seguridad y la confianza en el sistema. Por ello, fortalecer la ciberseguridad es esencial para proteger la información y garantizar la continuidad de las operaciones aéreas.

1.2 Los Estados han desarrollado estrategias integrales nacionales de ciberseguridad que incluyen la capacitación del talento humano, el fortalecimiento de tecnologías de seguridad, la creación de un marco regulatorio, la cooperación público-privada y la colaboración internacional. Su objetivo es mejorar la infraestructura tecnológica, la gestión de riesgos y la formación del personal de manera integral en el Estado.

1.3 La cooperación internacional es clave para fortalecer la aviación frente a las ciberamenazas. Compartir información, coordinar respuestas y establecer mecanismos de colaboración permite mitigar riesgos y garantizar la seguridad operacional, como ocurrió en el incidente del 19 de julio de 2024, que afectó sistemas administrativos de aerolíneas a nivel global.

1.4 La digitalización de la aviación civil ha aumentado su vulnerabilidad a ciberataques, que ponen en riesgo la seguridad operacional y la infraestructura del sector. Fortalecer la ciberseguridad es una prioridad estratégica para garantizar su continuidad y resiliencia.

1.5 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, como catalizador de los objetivos estratégicos de la organización 2026-2050

2. DISCUSIÓN

2.1 La digitalización ha optimizado la aviación civil, mejorando procesos y competitividad. Sin embargo, la interconexión de sistemas ha aumentado los riesgos de ciberseguridad, desde el acceso no autorizado a datos hasta la manipulación de sistemas críticos. Por ello, los Estados deben fortalecer sus capacidades individuales y cooperar para mejorar la seguridad operacional y la confianza en el sector.

2.2 La aviación civil se enfrenta al reto de mantener los beneficios de la digitalización y al mismo tiempo, garantizar la ciberseguridad. Esto implica la implementación de tecnologías de seguridad

digital, la capacitación del personal, el intercambio de experiencias y el desarrollo de políticas y estrategias de seguridad de la información y seguridad digital para las empresas que hacen parte con el sector.

2.3 La OACI considera la ciberseguridad una responsabilidad compartida que requiere cooperación internacional. Dado que las ciberamenazas evolucionan rápidamente y trascienden fronteras, es fundamental que los Estados respondan de manera ágil y coordinada, intercambiando información, mejores prácticas y recursos técnicos.

2.4 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

2.5 La aviación civil enfrenta a riesgos cibernéticos como el robo de datos, la manipulación de sistemas, la interrupción de servicios críticos y la pérdida de confianza del público. Fortalecer la ciberseguridad es esencial para garantizar operaciones seguras y proteger la estabilidad del sector.

2.6 Ante la creciente amenaza de ciberataques, es esencial adoptar un enfoque integral y colaborativo para fortalecer la ciberseguridad en la aviación civil mediante la creación de un marco de referencia sólido que sirva de guía a los Estados y partes interesadas para aplicar medidas de seguridad efectivas. Este marco de trabajo debe incluir el compromiso de la alta dirección, una gobernanza eficaz y políticas de ciberseguridad claras que regulen la protección de los sistemas críticos de TI/TO.

2.7 Es necesario iniciar una estrategia para fortalecer sus capacidades de ciberseguridad en la aviación civil. Su estrategia debe considerar cuatro ejes: (i) capacitación del personal; (ii) fortalecimiento de la infraestructura tecnológica interna; (iii) desarrollo de un marco regulatorio que promueva la ciberseguridad en todo el sector aeronáutico civil; y (iv) cooperación entre entidades.

2.8 Esta estrategia busca garantizar la seguridad de la aviación civil mediante la gestión de la integridad, disponibilidad y confidencialidad de la información en sistemas críticos, asegurando la prestación eficiente de servicios y la protección de datos sensibles con talento altamente capacitado. Además, se implementará un marco regulatorio sólido que reforzará la ciberseguridad en aerolíneas, aeropuertos, proveedores y fabricantes, promoviendo prácticas de seguridad robustas y una respuesta coordinada ante incidentes cibernéticos, lo que permitirá fortalecer la resiliencia del sector y mantener la confianza de los usuarios frente a las crecientes amenazas digitales.

2.9 Además, resulta fundamental desarrollar talento especializado mediante formación continua en ciberseguridad. La capacitación de profesionales cualificados es clave para garantizar la seguridad del sector y reducir riesgos asociados a la rotación de personal. También es necesario consolidar un Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT) exclusivo para la aviación civil, permitiendo una reacción rápida y coordinada a los incidentes cibernéticos. Este centro debe centralizar la gestión de incidentes, articular esfuerzos con otros actores del sector y garantizar la capacitación de su equipo.

2.10 La cooperación internacional es otro elemento esencial facilitando el compartir información y desarrollar ejercicios conjuntos de simulación para responder eficazmente a amenazas cibernéticas transfronterizas. Una plataforma tecnológica única facilitaría el intercambio de conocimientos y mejores prácticas.

2.11 También es necesario establecer un dialogo constante con autoridades y empresas del sector con el fin de establecer un frente de respuesta frente a amenazas cibernéticas. Sin embargo, el ciberespacio no conoce fronteras y es por esto por lo que este dialogo debe extenderse a los Estados que deben generar mecanismos eficientes y robustos con el fin de intercambiar experiencias y recomendaciones frente a las estrategias nacionales de ciberseguridad.

2.12 Es fundamental que las estrategias nacionales de ciberseguridad se basen en las legislaciones y regulaciones de cada Estado, pero que también sean interoperables para garantizar la seguridad operacional a nivel global. Es necesario fomentar la colaboración y el intercambio de información entre expertos para identificar y abordar vulnerabilidades y fortalecer la resiliencia del sector frente a ciberataques. También es importante abrir un espacio continuo en el que los expertos de las entidades puedan retroalimentarse frente a las estrategias locales con el fin de trabajar conjuntamente en cerrar brechas que puedan ser aprovechadas por los ciberdelincuentes o ciber terroristas que afecten al sector.

2.13 En este sentido, se considera necesario que la OACI promueva acciones que fortalezcan la gestión de la ciberseguridad en la aviación civil. La creación de una herramienta de autoevaluación integrada en el Plan Estratégico 2026–2050 se justifica en la medida en que permitiría a los Estados identificar de manera temprana brechas normativas, operativas y técnicas, facilitando una planificación proactiva de medidas de mitigación y el desarrollo de capacidades nacionales. Esto contribuiría a garantizar un nivel más homogéneo de protección entre los Estados, reduciendo asimetrías que hoy generan vulnerabilidades en la red global de aviación.

2.14 De igual manera, resulta esencial que la OACI impulse lineamientos técnicos y políticos más específicos en materia de ciberseguridad que orienten a los Estados en la adopción de mejores prácticas y estándares internacionales. Con ello, se favorecería la construcción de un marco común que permita enfrentar las amenazas digitales con mayor eficacia, fortalecer la resiliencia del sistema aeronáutico y preservar la seguridad y continuidad de las operaciones aéreas a nivel global.

3. CONCLUSIÓN

3.1 La ciberseguridad en la aviación civil es un desafío que requiere una respuesta global y coordinada. La OACI, en colaboración con los Estados miembros, debe liderar el camino hacia un sector más resiliente y seguro frente a las ciberamenazas. La seguridad de millones de pasajeros y la estabilidad del sistema de aviación global dependen de ello.