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

NOTA DE ESTUDIO

NACC/WG/10 — NE/33
20/08/25

Décima Reunión del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/10)
Tulum, Quintana Roo, México, del 8 al 12 de septiembre de 2025

Cuestión 5 del Orden del Día: **Sesión de trabajo colaborativa de Grupos de Tarea NACC/WG**

PRÁCTICAS ACTUALES Y MEJORAS EN CIBERSEGURIDAD PARA LA AVIACIÓN CIVIL

(Presentada por la Corporación Centroamericana de Servicios de Navegación Aérea/COCESNA)

RESUMEN EJECUTIVO

La tecnología desempeña un papel vital en el sector aeronáutico, facilitando el turismo, el comercio y la conectividad global, lo que impulsa el crecimiento económico y mejora la calidad de vida. Los avances en aviónica han permitido mejoras significativas en la gestión de la navegación, la seguridad de las aeronaves y la eficiencia operativa. La innovación tecnológica en el sector es esencial para mantener la competitividad y responder a las demandas crecientes del transporte aéreo.

La ciberseguridad en la aviación civil se ha convertido en un pilar fundamental para garantizar la seguridad operacional y la eficiencia de la navegación aérea. Actualmente, la industria enfrenta un entorno dinámico con amenazas cibernéticas en constante evolución, lo que requiere de un enfoque estratégico y coordinado para proteger infraestructuras críticas.

Esta nota de estudio presenta un análisis de las prácticas actuales de ciberseguridad en el sector aeronáutico y propone aspectos clave a considerar para su mejora e implementación futura, con el objetivo de fortalecer la resiliencia de los sistemas de aviación ante amenazas cibernéticas emergentes

Acción:	Acciones sugeridas en el inciso 6 de la nota de estudio.
Objetivos Estratégicos:	• Seguridad Operacional • Capacidad y eficiencia de la navegación aérea • Desarrollo económico del transporte aéreo • Protección del medio ambiente
Referencias:	• Marco Normativo NIST. • OACI Documentos 9985, 10161, 10075. • OACI- Anexo 17.

1. Introducción

1.1 La tecnología desempeña un papel vital en el sector aeronáutico, la provisión de servicios de navegación aérea se ha beneficiado enormemente de los avances tecnológicos. Sistemas como la navegación basada en el rendimiento (PBN), la vigilancia dependiente automática (ADS-B) y los sistemas de gestión del tráfico aéreo (ATM) han transformado la manera en que se gestionan los vuelos, mejorando la precisión, seguridad y eficiencia. Estos sistemas permiten una mejor planificación de rutas, reducción de demoras y optimización del espacio aéreo.

1.2 La ciberseguridad en la aviación civil se ha convertido en un aspecto fundamental, ya que las operaciones dependen cada vez más de sistemas digitales interconectados, donde los recursos tecnológicos son críticos para la operación segura y eficiente de la aviación civil. La evolución tecnológica ha traído consigo desafíos significativos, incluyendo ataques cibernéticos dirigidos a sistemas de control del tráfico aéreo, aeropuertos y operadores aéreos, resulta estratégico y fundamental protegerlos de ciber amenazas. La integridad y disponibilidad de estos sistemas deben ser garantizadas para evitar interrupciones que puedan afectar la seguridad operacional y la continuidad del transporte aéreo. La ciberseguridad en este contexto no solo protege los datos y sistemas, sino que también asegura la confianza en la infraestructura de navegación aérea global.

1.3 En respuesta a estas amenazas, los Estados han implementado una variedad de medidas de ciberseguridad basadas en estándares internacionales, como los desarrollados por la OACI, la IATA y la EASA. Sin embargo, aún existen brechas que deben abordarse para garantizar una protección integral del ecosistema aeronáutico.

1.4 Esta nota se desarrolla en línea a las resoluciones: A39-19 de la Asamblea de la OACI que reconoce por parte de la comunidad internacional que la Ciberseguridad es una prioridad Urgente para la Aviación Civil., resolución A40-10 sobre la Estrategia de la Ciberseguridad de la Aviación de la OACI con un enfoque colaborativo y multidisciplinario, la resolución A41-19 que reafirma la urgencia de atender la ciberseguridad y Ciberresilencia,

2. Prácticas actuales de Ciberseguridad en COCESNA

2.1 Implementación de Marco Normativo y Regulatorio por medio de la aplicación de la Circular 350 de la OACI sobre ciberseguridad en la aviación. Se ha tomado en cuenta la importancia de implementar un Marco de Ciberseguridad de la OACI para la identificación, protección, detección, respuesta y recuperación ante incidentes cibernéticos. Asimismo, se ha coordinación con organismos internacionales dentro y fuera de la región como ser IATA, EUROCONTROL y EASA para compartir mejores prácticas.

2.2 Para la gestión de riesgos cibernéticos, COCESNA se encuentra en proceso de establecer las bases para aplicación de metodologías de análisis de riesgo (ISO 27001, NIST, MITRE ATT&CK). Las implementaciones nos permitirán realizar evaluaciones continuas de vulnerabilidades en sistemas aeronáuticos, integración de ciberseguridad en los sistemas que brindan el servicio de Navegación Aérea a nivel de la región Centroamericana.

2.3 COCESNA pretende implementar un SOC – Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés), que permitirá a la organización fortalecer su postura de seguridad mediante la vigilancia continua, el análisis avanzado de amenazas y la respuesta rápida ante incidentes. A través de este servicio, se busca implementar un enfoque estratégico y eficiente para la protección de los sistemas, datos y usuarios, minimizando riesgos y garantizando la continuidad del negocio y el cumplimiento normativo.

2.4 En el área de capacitación y concienciación, actualmente se está desarrollando una capacitación básica de ciberseguridad a ser impartida a todo el personal de la Corporación, así como también se desarrollarán capacitaciones para especializar a personal específico en las mejores prácticas y tendencias de ciberseguridad.

3. Aspectos por considerar para mejorar la Ciberseguridad en la Aviación

3.1 Cooperación y el intercambio de información con otros proveedores de servicios de navegación aérea por medio de la creación de plataformas seguras para compartir información sobre amenazas y vulnerabilidades en tiempo real. Esto se puede lograr fortaleciendo la colaboración regional en seguridad cibernética a través de acuerdos multilaterales.

3.2 Definir y aplicar un marco normativo que regule la ciberseguridad. Este marco debe proporcionar directrices claras y estándares que las organizaciones puedan seguir para proteger sus activos digitales y salvaguardar la confidencialidad de los datos. La implementación de un marco normativo robusto ayuda a mitigar riesgos, prevenir incidentes de seguridad y asegurar la continuidad operativa.

3.3 Programas de formación en ciberseguridad deben incluir aspectos técnicos y prácticos, como la gestión de incidentes, el análisis de riesgos y la implementación de medidas de protección. Además, es importante fomentar habilidades de comunicación y colaboración para que el personal pueda trabajar en equipo y compartir conocimientos sobre ciberseguridad. La inversión en formación es una estrategia rentable que fortalece la resiliencia de la organización frente a ciber amenazas.

3.4 Promover la concienciación sobre ciberseguridad entre el personal permite reducir los errores humanos, que son una de las principales causas de incidentes de seguridad. Según estudios como el informe "*The Global Risks Report* 2022" del Foro Económico Mundial señala que el 95%. de los problemas de ciberseguridad tienen su origen en errores humanos. La sensibilización sobre las amenazas y las mejores prácticas de ciberseguridad ayuda a crear una cultura organizacional centrada en la seguridad digital.

3.5 Desarrollar un plan de resiliencia cibernética que nos permita incorporación de la ciberseguridad en los Planes Nacionales de Seguridad de la Aviación (NASP). Esto deberá incluir estrategias de recuperación ante ataques cibernéticos para minimizar el impacto operativo.

3.6 Identificar y tratar estas vulnerabilidades de manera proactiva para proteger la infraestructura tecnológica y garantizar la seguridad de los datos.

3.7 Cooperación con expertos en ciberseguridad de diversas industrias, como la tecnología, la banca y otros sectores, puede proporcionar conocimientos valiosos y recursos especializados que mejoren la protección de los sistemas aeronáuticos.

3.8 La adopción de tecnologías emergentes como la inteligencia artificial y la computación en nube ofrece oportunidades para mejorar la eficiencia y seguridad en la aviación civil. Sin embargo, es crucial que estas tecnologías se implementen con medidas de ciberseguridad robustas para proteger contra posibles vulnerabilidades y amenazas. La integración segura de estas tecnologías puede transformar el sector, pero requiere una planificación cuidadosa y una gestión de riesgos adecuada.

4. Conclusiones

4.1 La ciberseguridad es un elemento clave para la seguridad operacional y la eficiencia en la aviación civil. Proteger estos sistemas de ciber amenazas es esencial para garantizar la seguridad operacional y la continuidad del transporte aéreo. Si bien se han logrado avances importantes en la implementación de medidas de protección, aún existen desafíos que requieren atención inmediata.

4.2 Es fundamental fortalecer la cooperación internacional y el intercambio de información entre organizaciones del sector aeronáutico mediante plataformas seguras y acuerdos multilaterales es vital para mejorar la ciberseguridad, integrando tecnologías avanzadas y adoptando enfoques proactivos en la gestión de riesgos cibernéticos en la aviación civil internacional.

4.3 Implementar normas internacionales como ISO/IEC 27001 y NIST CSF proporciona directrices claras para proteger los activos digitales y asegurar la confidencialidad de los datos, ayudando a mitigar riesgos y prevenir incidentes.

4.4 Capacitar al personal y promover la concienciación sobre ciberseguridad reduce los errores humanos, mejorando la capacidad de respuesta ante amenazas y fortaleciendo la resiliencia organizacional.

4.5 Identificar y tratar vulnerabilidades de manera proactiva mediante evaluación de riesgos, actualizaciones, pruebas de penetración y monitoreo continuo es crucial para proteger la infraestructura tecnológica.

4.6 Colaborar con expertos en ciberseguridad de diversas industrias y contratar servicios especializados como SOC y MSSP proporciona monitoreo continuo y respuesta rápida a incidentes, mejorando la protección de los sistemas aeronáuticos.

4.7 Integrar tecnologías como IA y computación en nube con medidas de ciberseguridad robustas ofrece oportunidades para mejorar la eficiencia y seguridad en la aviación civil, asegurando una adopción segura y efectiva.

5. Recomendaciones

5.1 Se recomienda someter a consideración de los diferentes grupos de trabajo de la OACI la propuesta para fortalecer la ciberseguridad en la aviación civil, basada en:

- Evaluar y fortalecer las estrategias de ciberseguridad adoptando enfoques basados en mejores prácticas internacionales, intercambio de información y nuevas tecnologías.
- Implementar un marco normativo robusto que regule la ciberseguridad, proporcionando directrices claras y estándares que las organizaciones puedan seguir para proteger sus activos digitales y salvaguardar la confidencialidad de los datos.
- Promover la cooperación y el intercambio de información.
- Colaborar con expertos en ciberseguridad de diversas industrias y contratar servicios especializados como SOC y MSSP para proporcionar monitoreo continuo y respuesta rápida a incidentes.
- Integrar tecnologías emergentes como la inteligencia artificial y la computación en nube con medidas de ciberseguridad robustas para mejorar la eficiencia y seguridad en la aviación civil.

6. Acciones sugeridas

6.1 Se invita a la Reunión a:

a) Tomar nota de la información presentada;
b) que la OACI en el marco de los grupos de trabajo regionales que corresponda evalúe y fortalezca las estrategias de ciberseguridad, adoptando enfoques basados en mejores prácticas internacionales, intercambio de información y nuevas tecnologías;
c) que OACI en el marco de los grupos de trabajo regionales que corresponda continue apoyando a los estados en la definición y aplicación de los marcos normativos para regular la ciberseguridad, así como en la formación y fortalecimiento de competencias del personal sobre este tema y a la creación de planes de resiliencia cibernética que incorporen la ciberseguridad en los planes Nacionales de Seguridad de la Aviación NASP.

— FIN —