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

NOTA DE ESTUDIO

NACCWG10 — NE/24
01/09/2025

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

Cuestión 5 del Orden del Día: **Sesión de trabajo del NACC/WG/10**

Ciberseguridad en los Servicios de Navegación Aérea

(Presentada por la Secretaría)

RESUMEN EJECUTIVO

La OACI ha reconocido la ciberseguridad como un pilar esencial para garantizar la seguridad operacional y la continuidad de los servicios de navegación aérea, especialmente ante la creciente digitalización e interconexión de sistemas ATS, aeropuertos y aeronaves. En la AN-Conf/14 de 2024 se destacó que los ciberataques son una amenaza constante y en evolución, lo que exige a los Estados implementar mecanismos de gestión de riesgos, planes de recuperación, capacitación especializada y marcos normativos sólidos, alineados con la Estrategia de Ciberseguridad de OACI (2019) y el Plan Global de Seguridad de la Aviación (GASeP).

Como respuesta regional, la Oficina NACC lanzó en 2025 el proyecto piloto NACC-2, que incluye el desarrollo de un Plan de Asistencia en Ciberseguridad en Trinidad y Tobago y COCESNA, con el objetivo de expandirlo a otros Estados del Caribe. El proyecto busca fortalecer la resiliencia de los sistemas ANS mediante un enfoque multidisciplinario que involucre a ATCO, ATSEP, ANSPs, aerolíneas y fabricantes, promoviendo la cooperación internacional. En conclusión, la ciberseguridad es clave para proteger la aviación frente a amenazas digitales, garantizar la confianza del público y cumplir con los estándares globales de OACI.

Acción:	Acciones sugeridas bajo el ítem 4 de la presente nota de estudio.
Objetivos Estratégicos:	• Seguridad Operacional • Capacidad y eficiencia de la navegación aérea • Desarrollo económico del transporte aéreo • Protección del medio ambiente
Referencias:	• NACC/WG/09 • La catorceava conferencia de navegación aérea AN-Conf/14

1. Introducción

1.1 La creciente digitalización y conectividad de los sistemas de navegación aérea, aeropuertos y aeronaves ha incrementado la exposición del sector a riesgos cibernéticos. La OACI reconoce la ciberseguridad como un pilar esencial para garantizar la seguridad operacional, la continuidad del negocio y la confianza del público. Documentos estratégicos como la Estrategia de Ciberseguridad de OACI (2019) y el Plan Global de Seguridad de la Aviación (GASeP), orientan a los Estados y a la industria en la adopción de medidas de prevención, detección, respuesta y recuperación frente a incidentes cibernéticos.

1.2 En la AN-Conf/14 de 2024, la OACI subrayó que la ciberseguridad es un componente esencial de la seguridad operacional, especialmente ante la creciente hiper-conectividad de los sistemas de navegación aérea. Varios documentos de trabajo, como el WP-125 presentado por Estados de LACAC, destacaron la necesidad de establecer mecanismos de gestión de riesgos cibernéticos, desarrollar procedimientos de recuperación y definir competencias específicas para enfrentar incidentes que afecten los sistemas de tránsito aéreo (ATS). La conferencia también reconoció que los ciberataques son una amenaza constante que requiere un enfoque global y coordinado, alineado con la estrategia de ciberseguridad de OACI.

1.3 El debate estuvo marcado por la discusión sobre los roles de los distintos profesionales frente a incidentes cibernéticos: mientras algunos planteaban que los controladores de tránsito aéreo (ATCO) debían estar preparados para responder, la Federación Internacional del Personal Técnico (IFATSEA) enfatizó que la responsabilidad técnica inmediata corresponde a los especialistas en sistemas electrónicos (ATSEP). En conclusión, la conferencia reforzó que la ciberseguridad debe abordarse de forma multidisciplinaria, fortaleciendo la formación del personal, clarificando responsabilidades y promoviendo la cooperación internacional para garantizar la resiliencia de los sistemas de navegación aérea.

2. Análisis

2.1 Se identifican los siguientes ítems que afectan los servicios de navegación aérea en cuanto a ciberseguridad:

- Amenazas: ataques de denegación de servicio (DDoS) a sistemas de gestión de tráfico aéreo, manipulación de datos de navegación, malware en redes aeroportuarias y vulnerabilidades en la cadena de suministro.
- Impacto: interrupción de servicios ANS/ATM, pérdida de datos críticos y degradación de la seguridad operacional.
- Brechas normativas: fragmentación en marcos regulatorios; no todos los Estados han desarrollado normas específicas de ciberseguridad en aviación.
- Colaboración: OACI promueve un enfoque coordinado e interoperable entre Estados, ANSPs, aerolíneas y fabricantes.

3. Resumen de la Actividad OACI – Plan de Asistencia

3.1 En 2025, el Programa de Movilidad de Talento de OACI incluyó la asignación NACC-2 “Desarrollo de un Plan de Asistencia en Ciberseguridad para los Estados de la Región NACC”. Esta iniciativa contempla:

- Elaboración de un Plan Estatal de Asistencia en Ciberseguridad siguiendo la guía global de OACI.
- Análisis de ciberseguridad aplicado a los servicios de navegación aérea (ANS).
  - Evaluación en dos Estados del Caribe mediante misiones de campo.
  - Entrega de un informe técnico con hallazgos y recomendaciones.
- El proyecto piloto responde a solicitudes expresas de los Estados del Caribe, que han modernizado sus sistemas ANS, pero carecen aún de mecanismos robustos de protección cibernética.

3.2 La Oficina realizara este proyecto piloto en el Estado de Trinidad y Tobago y en la Organización de COCESNA. Los resultados de este proyecto piloto impulsan un proyecto mucho mas grande que cubra los demás Estados CAR.

3.3 Además es importante contar con el apoyo de los Estado que ya están trabajando en el tema y que respalden este tipo de proyectos innovadores en la región.

4. Recomendaciones

4.1 Se recomienda que los proveedores de navegación aérea trabajen arduamente para asegurar:

- Integrar la ciberseguridad en los Programas Nacionales de Seguridad de la Aviación Civil.
- Aplicar metodologías de gestión de riesgos cibernéticos en sistemas críticos.
- Fortalecer capacitación y simulaciones para personal ANS/ATM.
- Implementar monitoreo y redundancias técnicas (ej. autenticación en GNSS/ADS-B).

4.2 Promover cooperación internacional en foros regionales (NACC/WG, GREPECAS).

5. Conclusión:

5.1 La ciberseguridad en la aviación requiere marcos normativos sólidos, medidas técnicas resilientes y fortalecimiento del factor humano. Las amenazas son persistentes y en evolución, lo que exige un enfoque proactivo y coordinado.

5.2 La ciberseguridad en los servicios de navegación aérea es fundamental porque protege la seguridad operacional, garantiza la continuidad del servicio y preserva la confianza del público en la aviación. Los sistemas de gestión del tránsito aéreo, comunicaciones, navegación y vigilancia dependen de redes digitales vulnerables a ataques que pueden alterar datos críticos, interrumpir operaciones y generar riesgos directos para la seguridad de los vuelos.

5.3 Además, las amenazas cibernéticas son intencionales, dinámicas y en constante evolución, lo que exige una vigilancia permanente, cooperación internacional y cumplimiento de las normas establecidas por OACI. Integrar la ciberseguridad en los programas nacionales no solo fortalece la resiliencia de los servicios de navegación aérea, sino que también asegura que los Estados y proveedores cumplan con los estándares globales, evitando consecuencias técnicas, económicas y reputacionales graves.

6. Acciones sugeridas

6.1 Se invita a la reunión:

a) Trabajar con sus organizaciones nacionales para desarrollar un Plan Nacional de Ciberseguridad en Aviación.

b) Realizar evaluaciones periódicas de vulnerabilidades en CNS/ATM y aeropuertos.

c) Establecer un Centro Regional de Coordinación de Ciberseguridad.

d) Implementar programas de concienciación y entrenamiento en todos los niveles.

e) Miembros del MCAAP solicitar la solicitud de fondos para el desarrollo de proyecto que cubran esta necesidad.

f) Incluir ejercicios de ciber-incidentes en planes de contingencia.

g) Fortalecer la cooperación internacional para compartir alertas y lecciones aprendidas.

h) Asignar personal de contacto para trabajar en esta área.

— FIN —