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

NOTA DE ESTUDIO

NACC/WG/6 — NE/20
23/08/21

Sexta Reunión del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/6)
En línea, 25 – 27 de agosto de 2021, 09:00 a 13:00 (UTC -5)

Cuestión 4 del Orden del Día: **Implementación de asuntos de Navegación aérea**
4.8 Tecnologías emergentes y nuevos retos regionales

LA CIBERSEGURIDAD EN LAS ACTIVIDADES DE NAVEGACIÓN AÉREA

(Presentada por la Secretaría)

RESUMEN EJECUTIVO	
Esta nota de estudio presenta información acerca de un reto importante y emergente que debe ser tomado en cuenta, como parte integral de las actividades de Navegación Aérea.	
Acción:	Las acciones sugeridas se presentan en la Sección 4.
Objetivos Estratégicos:	• Capacidad y eficiencia de la navegación aérea • Desarrollo económico del transporte aéreo
Referencias:	• Plan Mundial de Navegación Aérea versión 6, octubre de 2019. • Resolución Asamblea A40-10: Formas de abordar la ciberseguridad en la aviación civil, octubre de 2019.

1. Introducción

1.1 La tecnología y los ciber-sistemas se han convertido en algo esencial para la sociedad moderna, dependemos aún más de la tecnología, que proporcionan mayor eficiencia a todas las actividades que se realizan día a día. Junto con el beneficio de las tecnologías cibernéticas, surgen inseguridades que afectan a todos los sistemas e infraestructuras. La ciber-amenaza y el ciber-ataque tienen un componente y un efecto transnacional, ya que los sistemas mundiales están interconectados. Además, la complejidad de la acción tiene implicaciones para diversos actores a nivel nacional, regional e internacional.

1.2 La Estrategia de Ciberseguridad de la Aviación desarrollada por OACI indica que el sector de la aviación civil depende cada vez en mayor medida de la disponibilidad de sistemas de tecnología de información y comunicaciones, así como de la integridad y confidencialidad de los datos. La amenaza de posibles incidentes cibernéticos para la aviación civil evoluciona de forma constante, con unos perpetradores que actúan maliciosamente para perturbar las operaciones y robar información por razones políticas, financieras y de otra índole.

1.3 Personal operativo, de tripulaciones aéreas, controladores de tránsito aéreo, infraestructuras CNS, dependerán cada día más de la gestión y capacidad técnica para afrontar las amenazas en cuanto a los ciber-ataques con el objetivo de garantizar la seguridad operacional.

1.4 La obligación de los Estados de identificar infraestructuras críticas y establecer mecanismos adecuados para afrontar estos nuevos retos, así como establecer los mecanismos de restablecimiento ante un ciber-ataque y los mecanismos de continuidad del negocio.

2. Análisis

2.1 La OACI a través de la Resolución ***A40-10: Formas de abordar la ciberseguridad en la aviación civil***, de la Asamblea 40, desarrollada en el 2019, estableció las recomendaciones necesarias para que el tema de ciberseguridad se establezca parte integrante de las operaciones de aviación. La Resolución A40-10 se encuentra bajo el **Apéndice** de esta nota de Estudio.

2.2 La OACI ha establecido la estrategia de ciberseguridad basada en siete pilares importantes para la implementación de ciberseguridad:

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf

2.3 Las operaciones de Navegación Aérea están soportadas por tecnología de punta, tanto a nivel de los equipos en tierra como de la aviónica a bordo de las aeronaves. Facilidades como intercambio de información aeronáutica, los protocolos automatizados entre los centros de control, ATFM, A-CDM, entre otros requieren que los datos cuenten con medidas de calidad, disponibilidad y certificación, esta información es base para la toma de decisiones en tiempo real.

2.4 La aviación incluye usuarios del espacio aéreo, proveedores de navegación aérea, explotadores de aeropuertos, autoridades de aviación civil y fabricantes de equipo, entre otros. En ese sentido se requiere realizar un análisis del sistema de aviación integrando todas las partes interesadas que forman parte del sistema.

2.5 La ciberseguridad requiere un enfoque holístico, las interfaces entre los componentes de seguridad de la aviación merecen una atención espacial, como por ejemplo la seguridad de la Gestión de tránsito aéreo (ATM), la seguridad de los componentes y operaciones de Comunicación, Navegación y Vigilancia (CNS) (ADS-B, GNSS, data Link), la seguridad del espacio aéreo y la seguridad de los aeropuertos. La seguridad de la gestión del tránsito aéreo debe ser parte integrante del sistema de seguridad de la aviación.

2.6 La Oficina Regional NACC de la OACI, a través de la iniciativa de ciberseguridad para los servicios de tránsito aéreo en colaboración con la industria y organizaciones, tal y como lo recomienda la Resolución A40-10 de la OACI, ha desarrollado en colaboración con CANSO y AIRBUS el Proyecto para la región CAR que tiene como objetivo apoyar a los Estados en el establecimiento de su primer *Manual de Políticas de Ciberseguridad.*

2.7 El proyecto ha desarrollado satisfactoriamente las siguientes actividades:

a) Taller básico de ciberseguridad: que abarco los lineamientos generales de ciberseguridad, documentación de la OACI y mejores prácticas.
https://www.icao.int/NACC/Pages/meetings-2020-aci.aspx

b) Taller del formato del Manual de Ciberseguridad para la navegación aérea, que contempla un documento desarrollado dentro de esta iniciativa, por OACI/NACC, CANSO y AIRBUS que brinda las recomendaciones para que los Estados puedan comenzar a trabajar en su Manual de Políticas de Ciberseguridad.
https://www.icao.int/NACC/Pages/meetings-2021-canso02.aspx

c) Tercera etapa en desarrollo, donde dentro de la iniciativa se le apoya a los Estados de forma directa en el desarrollo de su manual de políticas de ciberseguridad acorde con su sistema de aviación, su infraestructura ATM/CNS y a sus operaciones.

3. Conclusiones

3.1 Los retos de ciberseguridad, requieren un trabajo en conjunto de todas las aéreas del sistema de Aviación Civil, integrando tanto las áreas internas y partes del sistema, como las partes interesadas externas a las operaciones de aviación civil.

3.2 Los ciber-ataques se han venido incrementando en los últimos años, la aviación no pensó que podía ser blanco de este tipo de amenazas, pero el uso de tecnología de punta, la interconectividad regional y mundial, además como otros intereses hacen a nuestro sector vulnerable a esta amenaza.

3.3 La ciberseguridad necesita un trabajo que incluye todas las disciplinas de la aviación y requieren ver el sistema como un todo y no por partes.

4. Acciones sugeridas

4.1 Se invita a la Reunión a:

a) tomar nota de la información presentada en esta nota de estudio;

b) considerar la adopción de enfoques multidisciplinarios para el enfoque de ciberseguridad para todas las operaciones de navegación aérea.

c) la adopción de tareas correspondiente para todos los Grupos de Tareas parte del ANI/WG (NACC/WG)

d) tomar ventaja de la iniciativa de ciberseguridad OACI/NACC-CANSO-AIRBUS para el apoyo puntual a las actividades propias de sus Estados.

e) cualquier otra actividad que aplique.

— — — — — — — — — — —

Apéndice

A40-10: Formas de abordar la ciberseguridad en la aviación civil

Considerando que el sistema de aviación mundial es un sistema altamente complejo e integrado que comprende tecnología de la información y las comunicaciones de carácter crítico para la seguridad y protección de las operaciones de aviación civil;

Observando que el sector de la aviación depende cada vez más de la disponibilidad de sistemas de tecnología de la información y las comunicaciones, así como de la integridad y confidencialidad de los datos;

Consciente de que la amenaza planteada por los incidentes que afectan a la ciberseguridad en la aviación civil evoluciona rápida y continuamente, que los autores de esas amenazas tienen la intención de causar daño, buscando interrumpir las actividades y robar información por razones políticas, económicas o de otra índole, y que la amenaza puede mutar fácilmente hasta llegar a afectar sistemas críticos de la aviación civil en todo el mundo;

Reconociendo que no todos los problemas de ciberseguridad que afectan a la seguridad operacional de la aviación civil se relacionan con actos ilícitos y/o intencionales, y que en consecuencia deberían resolverse aplicando sistemas de gestión de la seguridad operacional;

Reconociendo la naturaleza polifacética y multidisciplinaria de los problemas de ciberseguridad y sus soluciones, y observando que los riesgos cibernéticos pueden afectar simultáneamente una amplia gama de áreas y propagarse con rapidez;

Reafirmando las obligaciones estipuladas en el Convenio sobre Aviación Civil Internacional (Convenio de Chicago) de velar por la seguridad operacional, la seguridad y la continuación de la aviación civil;

Considerando que el Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional (Convenio de Beijing) y el Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves (Protocolo de Beijing) mejorarían el marco jurídico mundial para tipificar los ciberataques contra la aviación civil internacional como delitos, por lo que la ratificación de ambos instrumentos por un amplio número de Estados garantizaría la disuasión y el castigo de dichos ataques en cualquier parte del mundo donde se produzcan;

Reafirmando la importancia y urgencia de proteger de ciberamenazas a los sistemas de infraestructura de la aviación civil y los datos críticos;

Considerando la necesidad de trabajar en colaboración para crear un marco mundial eficaz y coordinado que permita a las partes interesadas de la aviación civil abordar los retos de la ciberseguridad, junto con medidas de corto plazo para aumentar la resiliencia del sistema de aviación mundial ante las ciberamenazas que atenten contra la seguridad operacional de la aviación civil;

Reconociendo la labor del Grupo de estudio de la Secretaría sobre Ciberseguridad, que contribuyó sobremanera al formato de la Estrategia de ciberseguridad al vincular las características de la seguridad operacional y la seguridad de la aviación a la ciberseguridad;

Reconociendo que es necesario armonizar la ciberseguridad en la aviación a nivel mundial, regional y nacional con miras a promover la coherencia en todo el mundo y asegurar la plena interoperabilidad de las medidas de protección y los sistemas de gestión de riesgos; y

Destacando el valor de las iniciativas, los planes de acción, las publicaciones y demás medios concebidos para abordar los problemas de ciberseguridad en colaboración y de forma integral.

La Asamblea:

1. Insta a los Estados miembros y a la OACI a promover la adopción universal e implementación del Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional (Convenio de Beijing) y el Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves (Protocolo de Beijing) como instrumentos para hacer frente a los ciberataques contra la aviación civil;

2. Exhorta a los Estados y las partes interesadas de la industria a adoptar las medidas siguientes para contrarrestar las ciberamenazas a la aviación civil:

   a) implantar la estrategia sobre ciberseguridad;
   b) identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y los sistemas críticos de la aviación civil y las graves consecuencias que pueden resultar de tales incidentes;
   c) definir las responsabilidades de los organismos nacionales y las partes interesadas de la industria con respecto a la ciberseguridad en la aviación civil;
   d) fomentar una interpretación común entre los Estados miembros de las ciberamenazas y riesgos y la formulación de criterios comunes para determinar qué bienes y sistemas son de carácter crítico y es preciso proteger;
   e) fomentar la coordinación entre gobierno e industria con respecto a las estrategias, políticas y planes de ciberseguridad de la aviación, así como el intercambio de información para ayudar a identificar las vulnerabilidades críticas que sea necesario resolver;
   f) formar y participar en asociaciones y mecanismos entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación;
   g) sobre la base de una interpretación común de las ciberamenazas y riesgos, adoptar un enfoque flexible y basado en el riesgo para proteger los sistemas de aviación críticos mediante la implantación de sistemas de gestión de la ciberseguridad;
   h) fomentar una sólida cultura de ciberseguridad en todos los aspectos dentro de los organismos nacionales y en todo el sector de la aviación;
   i) promover la elaboración y aplicación de normas internacionales, estrategias y mejores prácticas para proteger los sistemas críticos de tecnología de la información y las comunicaciones que se usan en la aviación civil de interferencias que puedan atentar contra la seguridad operacional de la aviación civil;
   j) establecer políticas y destinar recursos cuando sea necesario para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura; que sean resilientes; que tengan métodos seguros de transferencia de datos que garanticen su integridad y confidencialidad; que tengan métodos de vigilancia, detección y notificación de incidentes y que se lleven a cabo análisis forenses de los incidentes; y

k) colaborar en el desarrollo del marco de ciberseguridad de la OACI adoptando un enfoque horizontal, intersectorial y funcional que integre la navegación aérea, las comunicaciones, la vigilancia, las operaciones de aeronaves, la aeronavegabilidad y demás disciplinas pertinentes.

3. Encarga a la Secretaria General que:

a) formule un plan de acción para ayudar a los Estados y la industria a adoptar la Estrategia de ciberseguridad; y
b) continúe asegurándose de que los asuntos de ciberseguridad se examinen y coordinen de forma transversal por medio de los mecanismos apropiados conforme se estipula en la estrategia

— FIN —