Organización de Aviación Civil Internacional

AN-Conf/14-WP/124[1]
29/06/24

**NOTA DE ESTUDIO**

# DECIMOCUARTA CONFERENCIA DE NAVEGACIÓN AÉREA

**Montreal, Canadá, 26 de agosto al 6 de septiembre de 2024**

**Cuestión 4: Hiperconectividad del sistema de navegación aérea**
**4.2: Ciberseguridad y resiliencia de los sistemas de información**

## LINEAMIENTOS NORMATIVOS SOBRE LA CIBERSEGURIDAD PARA LOS SERVICIOS DE TRÁNSITO AÉREO

(Nota presentada por Argentina con el apoyo de 19 Estados miembros de la Comisión Latinoamericana de Aviación Civil (CLAC[2]))


**RESUMEN**

En esta nota se presentan consideraciones para armonizar disposiciones relativas a la normativa ATS, con el objetivo de incluir especificaciones, métodos y procedimientos relacionados con posibles escenarios de ataques de malware en los ATS, garantizando una supervisión continua de la capacitación y actualización del personal.

**Medidas propuestas a la Conferencia:**

a) Apoyar las iniciativas presentadas en esta NE, solicitando que se analice la pertinencia de incorporar, al marco global de la aviación, la regulación y métodos relativos a ciberseguridad para el ATS.

b) Alentar a los Estados a integrar sus estrategias nacionales de ciberseguridad con las estrategias de la aviación civil impulsadas por la OACI, en función de emprender una cultura de la ciberseguridad en los ATS, incorporando políticas, estrategias y mecanismos tendientes al resguardo de esta, mediante el desarrollo de las provisiones regulatorias sugeridas.


## 1. INTRODUCCIÓN

1.1 El creciente uso de tecnología de vanguardia y de interconexión global en la aviación civil ha provocado un incremento notable en el riesgo de amenazas cibernéticas.

[1] La versión en español fue proporcionada por Argentina.
[2] Aruba (Reino de los Países Bajos), Belice, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay, Venezuela (República Bolivariana de).

1.2 La 41° Asamblea de la Organización de Aviación Civil Internacional (OACI) dio relevancia al tema, incorporando en la PARTE VII: *Interferencia Ilícita; Otras cuestiones relativas a la interferencia ilícita* del Documento OACI 10184 "Resoluciones vigentes de la Asamblea", publicado el 7 de octubre de 2022, la ***Resolución Permanente A41-19: Formas de abordar la ciberseguridad en la aviación civil.*** En ella se exhorta a los Estados a una serie de acciones, algunas de las cuales deben ser abordadas mediante herramientas normativas, y de ese modo enfrentar las actuales dudas generadas en la comunidad de la aviación con respecto a la eficacia de las normas, procedimientos y procesos existentes al momento de mantener un nivel aceptable de riesgo en un entorno conectado digitalmente.

1.3 Según el artículo publicado en 2019 por el Grupo ALLIANZ denominado "Risk Barometer: Top Business Risks" (citado en la séptima edición del GANP) las *Business Interruption* (BI) más temidas son los ciberataques de *ransomware*[3]. *WannaCry* y *Petya* son dos ejemplos de *ransomware*, que han atacado sistemas digitales en la Unión Europea. Sin embargo, es interesante destacar que el artículo observa que el 12% de los ciber BI se producen debido a actos delictivos de ciberataques, mientras que el 88% se producen debido a fallas técnicas o errores causados por la interacción humana con los sistemas.

1.4 Todas las partes interesadas de la aviación civil han emprendido un gran esfuerzo de colaboración para proteger y asegurar el sistema de navegación aérea contra actos de interferencia ilícita, priorizando la gestión de los riesgos y la ciber resiliencia del sistema. En este contexto, los organismos reguladores de la aviación civil desempeñan un papel fundamental, que debería evolucionar. Es decir, junto con las regulaciones vigentes, sería propicio ofrecer innovación escalable y flexible, especialmente al considerar los nuevos modelos de negocios en curso, donde el enfoque debe ser de empresa a empresa y/o de empresa a cliente[4]. Consecuentemente, las regulaciones deberían establecer los estándares de desempeño que son necesarios en este nuevo contexto, en lugar de mantener su función de especificar con gran detalle los componentes técnicos individuales.

1.5 Asimismo, deberían facilitar y fomentar la innovación, cumplir con los requisitos de desempeño y apoyar la evolución del sistema de navegación aérea, al tiempo que proporcionan monitoreo y supervisión. Desde esta óptica, el nuevo paradigma regulatorio representa en muchos sentidos una transición de un sistema centralizado conformado solo por dos actores (organismo regulador estatal y proveedor de servicios de navegación aérea - ANSP) a un sistema regulatorio distribuido y coordinado y que ofrece servicios adaptados a las necesidades de una infraestructura ciber resiliente y a las necesidades determinadas por los usuarios.

## 2. ANÁLISIS

2.1 Considerando lo expuesto, se presentan una serie de consideraciones que propenden a la alineación y armonización de disposiciones, relativas a la normativa ATS, con el objetivo de analizar la propuesta de inclusión de especificaciones y procedimientos relacionados con posibles escenarios de ataques de *malware* en sus sistemas de información, abordando las necesidades de todas las partes involucradas y garantizando una supervisión continua de la capacitación y actualización para mantener las competencias necesarias del personal.

2.1.1 De acuerdo con la ***Resolución 41-19*** de la Asamblea, y debido a su naturaleza delictiva, el escenario de un ciberataque en la aviación civil es catalogado como una interferencia ilícita.

---

[3] *El ransomware es un tipo de malware que cifra los archivos de un usuario y solicita un rescate para devolverlos.*

[4] *GANP Online; Modelo de negocios emergentes, nuevos y adaptados, ICAO:* https://www4.icao.int/ganpportal/GanpDocument#/lessons/WWfUWzbj1hwCVRRkMTd9NRWaFjpHfZxp

2.1.2 El avance tecnológico y la interconexión de los sistemas de navegación aérea apuntan a la seguridad operacional, sin embargo, potencialmente se crean condiciones para que la interferencia ilícita pueda afectar, no solo a las aeronaves, sino también a las dependencias de los ATS.

2.1.3 Las SARPS del Anexo 11, así como los métodos del PANS ATM - Documento 4444, consideran a la interferencia ilícita a través de acciones o procedimientos en caso de que una aeronave sea, o se sospeche que sea, objeto de interferencia ilícita.

2.1.4 Los mencionados documentos no abordan el caso de un potencial ataque a los sistemas de las dependencias ATS. Por lo tanto, puede ser fundamental incorporar normativa u orientación técnica de la OACI para las dependencias ATS que sean afectadas por ciberataques, con el propósito de disponer de procedimientos adecuados para reaccionar de manera adecuadamente tales eventos. Se propone estudiar el escenario de interferencia ilícita en el ATS, de modo tal que se desarrollen métodos específicos ante ciber ataques.

2.1.5 En este sentido, y conforme al Plan de Acción para la Ciberseguridad de la OACI, se sugiere que se analice la viabilidad de incorporar, especificaciones y/o procedimientos con el objeto de informar a la autoridad competente designada por el Estado en aquellos casos donde se sospecha o haya confirmación de ciberataque a una dependencia de los ATS, permitiendo el intercambio oportuno de información relevante entre todas las partes interesadas pertinentes, y especialmente con los explotadores aéreos.

2.1.6 Asimismo, se considera que podría ser esencial establecer mecanismos para el intercambio de información sobre ciberseguridad entre las autoridades militares y los ATS, de modo tal que compartan información relevante. Este enfoque colaborativo se estima que contribuiría a mitigar los riesgos de ciberataques en el ámbito ATS.

2.2 Por otra parte, y en base a lo descrito en el Plan de Acción para la Ciberseguridad respecto a la necesidad de *"procurar la armonización de la reglamentación a nivel mundial, regional y nacional con el objeto de promover la coherencia en todo el mundo y mantener la interoperabilidad de las medidas de protección"*[5], se advierte la necesidad de incorporar provisiones regulatorias específicas - sin perjuicio de adoptar otras disposiciones afines a la materia -que incluyan:

a) procedimientos que aborden los escenarios de ciberamenazas y ciberataques a nivel regional, ya que proporcionaría una forma de enfrentar las diferencias económicas y tecnológicas que algunos Estados no podrían abordar por sí solos, considerando que el impacto de un ciberataque o ciberamenaza suele trascender las fronteras estatales;

b) instrumentos adecuados para proporcionar un enlace entre la estrategia de ciberseguridad adoptada por el Estado y los lineamientos establecidos por la OACI en el documento *"Estrategia de ciberseguridad de la aviación"*, estableciendo de este modo la incorporación de una política, estrategia, formación y costos asociados a la implantación de esta, en el ámbito de la aviación civil nacional, contemplando, además, la designación de la autoridad competente en materia de ciberseguridad de la aviación civil y cuál sería su interacción con los organismos nacionales y demás partes interesadas;

c) disposiciones respecto a la seguridad del sistema de navegación aérea de los Estados, con una arquitectura que asegure su integridad y protección. Esto podría considerar la implementación

[5] *Plan de Acción para la Ciberseguridad, Capítulo 3, Plan de acción estratégico, Pilar 1: Cooperación Internacional, OACI, Ed.2022.*

de métodos para el reporte, la supervisión e incluso, la realización de análisis forenses[6] de incidentes cibernéticos, específicos para el ámbito de la aviación civil;

d) disposiciones respecto a la capacitación para promover una cultura de ciberseguridad en los ATS y proporcionar una formación adecuada a todo el personal involucrado en el sistema de navegación aérea. En este sentido, la inclusión de proyectos que contemplen la capacitación de dicho personal resultaría imprescindible;

e) medidas específicas de contingencia ATS diseñadas para afrontar estas situaciones y garantizar una rápida recuperación de las operaciones, que contemple acciones de recuperación de incidentes cibernéticos, y la identificación de partes interesadas clave para la comunicación y coordinación efectiva durante una crisis; y

f) protocolos de detección y notificación de ciber incidentes, en el cual se establezcan procedimientos claros para la detección temprana y la notificación oportuna de cualquier incidente de ciberseguridad que afecte a las dependencias ATS. El mismo, aseguraría una respuesta rápida y coordinada ante cualquier amenaza, minimizando así el impacto potencial de los ciberataques en la seguridad y la continuidad de las operaciones aéreas.

## 3. CONCLUSIÓN

3.1 La ciberseguridad en los Servicios de Tránsito Aéreo (ATS) es una preocupación que demanda acciones concertadas a nivel nacional, regional y global. La incorporación de las propuestas expuestas en este documento representa un paso significativo hacia el fortalecimiento de la seguridad del servicio y la mitigación de los riesgos asociados a los ciberataques en las dependencias ATS. Al adoptar estos enfoques, los Estados estarían mejor preparados para abordar los desafíos emergentes en el ámbito de la ciberseguridad, garantizando al mismo tiempo la continuidad y la integridad de las operaciones aéreas. Además, la colaboración internacional y la armonización de las regulaciones contribuirían a promover una cultura de ciberseguridad sólida y resiliente en toda la comunidad aeronáutica global.

3.2 Por lo tanto, se proponen que la Conferencia apruebe las siguientes medidas:

a) apoyar las iniciativas presentadas en esta NE, solicitando que se analice la pertinencia de incorporar, al marco global de la aviación, la regulación y métodos relativos a ciberseguridad para el ATS; y

b) alentar a los Estados a integrar sus estrategias nacionales de ciberseguridad con las estrategias de la aviación civil impulsadas por la OACI, en función de emprender una cultura de la ciberseguridad en los ATS, incorporando políticas, estrategias y mecanismos tendientes al resguardo de esta, mediante el desarrollo de las provisiones regulatorias sugeridas.

— FIN —

[6] *El análisis forense en ciberseguridad es una disciplina que se utiliza para investigar y analizar incidentes de seguridad informática. Esto incluye ciberataques, robos de datos e intrusiones.*