



NOTA DE ESTUDIO

DECIMOCUARTA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 26 de agosto - 6 de septiembre de 2024

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

IMPLEMENTACIÓN DE LOS ELEMENTOS BÁSICOS DE UN MARCO DE CIBERSEGURIDAD DE LA AVIACIÓN

(Nota presentada por la Secretaría)

RESUMEN

La transformación digital del sector de la aviación civil en todos los ámbitos de la aviación está acelerando la necesidad de abordar la cuestión de la ciberseguridad en la aviación civil para garantizar la seguridad operacional, la protección, la capacidad y la eficacia del sector. En esta nota de estudio se presentan una serie de elementos básicos de alto nivel que deben ser tenidos en cuenta por los Estados y las partes interesadas para abordar la ciberseguridad de la aviación de manera holística y armonizada en todos los ámbitos pertinentes. También se establece la necesidad de orientaciones adicionales de la OACI para ayudar a los Estados y a las partes interesadas a mejorar la protección y la resiliencia del sector frente a las ciberamenazas y los ciberriesgos. Además, contiene recomendaciones que permiten una mayor armonización y coherencia a nivel regional.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a convenir en la recomendación 4.2/x — Ciberseguridad de la aviación, que figura en el párrafo 3.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los objetivos estratégicos de <i>Seguridad operacional, Capacidad y eficiencia de la navegación aérea, y Seguridad de la aviación y facilitación</i> .
Repercusiones financieras:	<i>Para la comunidad de la aviación:</i> La implementación de las áreas de las que trata esta nota supone un costo. No obstante, brindará la oportunidad de aplicar un enfoque claro a la ciberseguridad de la aviación, que incluya funciones y responsabilidades bien definidas de todas las partes interesadas. <i>Para la OACI (con relación a los niveles de recursos existentes en el actual presupuesto del Programa regular):</i> Las actividades de la OACI a las que se hace referencia en la presente nota de estudio continuarán durante el próximo trienio. Se necesitarán recursos adicionales para sustentar el desarrollo de estas actividades, así como para llevar a cabo campañas de concienciación y prestar apoyo a la implementación.
Referencias:	<i>Manual de seguridad de la aviación</i> (Distribución limitada) (Doc 8973) <i>Global Air Navigation Plan</i> (Plan mundial de navegación aérea, Doc 9750) <i>Plan global para la Seguridad Operacional de la Aviación</i> (Doc 10004) <i>Plan global para la seguridad de la aviación</i> (Doc 10118) <i>Resoluciones vigentes de la Asamblea (al 7 de octubre de 2022)</i> (Doc 10184) Estrategia de Ciberseguridad de la Aviación Plan de Acción de Ciberseguridad Orientación sobre política de ciberseguridad Cultura de ciberseguridad en la aviación civil

1. INTRODUCCIÓN

1.1 Durante su 40º período de sesiones, la Asamblea de la OACI reafirmó la importancia y urgencia de un compromiso mundial de todas las partes interesadas consistente en la toma de medidas para ocuparse de la ciberseguridad en la aviación civil de manera colaborativa mediante la adopción de la resolución A40-10: *Formas de abordar la ciberseguridad en la aviación civil*, y la aprobación de la Estrategia de Ciberseguridad de la Aviación¹. En el 41º período de sesiones de la Asamblea de la OACI se reiteró la importancia de abordar la ciberseguridad en la aviación civil a través de la resolución A41-19 actualizada.

1.2 La Asamblea también pidió a la OACI que elaborase un plan de acción para apoyar la implementación de la Estrategia de Ciberseguridad de la Aviación por parte de los Estados y las partes interesadas. La segunda edición del Plan de Acción de Ciberseguridad², publicado en enero de 2022, proporciona las bases para que la OACI, los Estados y las partes interesadas trabajen juntos, y propone una serie de principios, medidas y acciones para lograr los objetivos de los siete pilares de la Estrategia de Ciberseguridad³.

1.3 En consonancia con el Plan de Acción de Ciberseguridad, la OACI ya ha publicado textos de orientación sobre temas relacionados con la ciberseguridad de la aviación. La labor de la OACI también incluye iniciativas relacionadas con la investigación sobre la idoneidad de los instrumentos jurídicos internacionales para hacer frente a los ciberataques contra la aviación civil, la investigación acerca de la necesidad de normas y métodos recomendados sobre ciberseguridad de la aviación en los anexos del Convenio sobre Aviación Civil Internacional (Convenio de Chicago), la elaboración de textos para fomentar la confianza en cuanto a la interoperabilidad en diferentes ámbitos de la aviación, la sensibilización sobre la importancia de abordar las ciberamenazas y los ciberriesgos para la aviación civil, el desarrollo de iniciativas de creación de capacidad en materia de ciberseguridad de la aviación y la realización de ejercicios de simulación sobre ciberseguridad de la aviación internacional.

2. ANÁLISIS

2.1 Mientras el sector de la aviación civil sigue beneficiándose de las innovaciones tecnológicas para mejorar su capacidad y eficacia, manteniendo al mismo tiempo los niveles acordados de seguridad operacional y protección, la ciberseguridad se ha considerado en cada ámbito de la aviación por separado. A lo largo de los años, esto ha llevado a que la aviación se convierta en un sistema de sistemas (SoS) en el que los controles y procesos para la ciberprotección y la resiliencia no se diseñaron, ni se implementaron, de manera holística, lo que generó posibles brechas a nivel macro.

2.2 En ese sentido, es importante que la ciberseguridad de la aviación se integre en los ámbitos de la aviación civil a nivel nacional, regional e internacional de manera coordinada, armonizada y holística. Esto ayudaría a hacer frente a las ciberamenazas y los ciberriesgos para la aviación civil, sin poner en peligro los requisitos de seguridad operacional, protección, capacidad y eficiencia.

2.3 Se han logrado avances significativos en el tratamiento de la cuestión de la ciberseguridad en la aviación civil, pero se necesitan orientaciones adicionales para apoyar la integración de la ciberseguridad de la aviación por parte de los Estados en sus sistemas de reglamentación y de vigilancia en vigor, así como en sus planes regionales y nacionales relacionados con los ámbitos pertinentes de la aviación civil, principalmente la seguridad operacional, la seguridad de la aviación y la facilitación, y la navegación aérea.

¹ <https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx>

² <https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx>

³ Los pilares de la Estrategia de Ciberseguridad de la Aviación son los siguientes: cooperación internacional; gobernanza; leyes y reglamentos eficaces; política de ciberseguridad; intercambio de información; gestión de incidentes y planificación ante emergencias, y creación de capacidad, instrucción y cultura de ciberseguridad.

2.4 Además, tanto en la resolución 2341 (2017) del Consejo de Seguridad de las Naciones Unidas, relativa a la protección de la infraestructura vital contra los actos terroristas, como en la resolución A/RES/77/298 de la Asamblea General de las Naciones Unidas, relativa al octavo examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo (A/RES/60/288), se subraya la importancia de una cooperación intersectorial de múltiples partes interesadas en el tratamiento de la ciberseguridad, entre las organizaciones internacionales, regionales y subregionales, el sector privado y la sociedad civil.

2.5 Como tal, y en consonancia con las resoluciones de la Asamblea de la OACI vigentes, la Estrategia de Ciberseguridad de la Aviación, su Plan de Acción y los diversos textos de orientación elaborados por la OACI, en esta nota se proponen elementos básicos de referencia que deben ser considerados por los Estados y las partes interesadas al abordar las ciberamenazas y los ciberriesgos para la aviación civil. Estos elementos básicos deberían incluir:

a) Aspectos de reglamentación a nivel estatal:

- 1) **Gobernanza de la ciberseguridad de la aviación a nivel estatal:** Este elemento incluye, entre otros, aspectos relacionados con el establecimiento de una autoridad competente para la ciberseguridad de la aviación, la integración de la ciberseguridad de la aviación en los programas de seguridad operacional y los programas nacionales de seguridad de la aviación civil de los Estados, la determinación de las funciones y responsabilidades de las autoridades aeronáuticas y no aeronáuticas (por ejemplo, las autoridades nacionales de ciberseguridad) y la coordinación de sus actividades en relación con la reglamentación y la vigilancia de la ciberseguridad en la aviación civil, aprovechando los recursos nacionales de ciberseguridad para ayudar a las organizaciones en la vigilancia, la detección, la respuesta y la recuperación en el ámbito de los ciberincidentes.
- 2) **Marco jurídico nacional:** Este elemento incluye aspectos relacionados con los marcos jurídicos nacionales de los Estados para permitir el enjuiciamiento de los ciberataques contra la aviación civil. Además, incluye aspectos relacionados con la ratificación del *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* (Beijing, 2010) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves* (Beijing, 2010) como instrumentos para hacer frente a los ciberataques contra la aviación civil.
- 3) **Política de ciberseguridad de la aviación:** Este elemento incluye aspectos relacionados con la política de ciberseguridad de la aviación a nivel estatal.
- 4) **Funciones de vigilancia:** Este elemento incluye aspectos relacionados con las capacidades de vigilancia de los Estados en materia de ciberseguridad de la aviación, que pueden implementarse a través de los mecanismos existentes de vigilancia de la seguridad operacional y la seguridad de la aviación de manera coordinada.

b) Aspectos relacionados con los Estados y con las partes interesadas:

- 1) **Gestión de los ciberriesgos:** Este elemento incluye aspectos relacionados con la determinación de la infraestructura crítica de la aviación y la integración de la evaluación de los ciberriesgos en las evaluaciones existentes de riesgos de seguridad de la aviación y seguridad operacional de esa infraestructura.

- 2) **Notificación de incidentes de ciberseguridad:** Este elemento incluye aspectos relacionados con la implementación de un mecanismo de notificación de incidentes de ciberseguridad por parte de las entidades a sus autoridades, que puede hacerse por separado o a través de los mecanismos de notificación existentes para la seguridad operacional o la seguridad de la aviación.
- 3) **Intercambio de ciberinformación:** Este elemento incluye aspectos relacionados con la implementación de mecanismos de intercambio de información entre los Estados y las partes interesadas a nivel nacional, regional e internacional.
- 4) **Respuesta y recuperación en materia de ciberincidentes:** Este elemento incluye aspectos relacionados con la implementación de capacidades y de planes de respuesta y recuperación en materia de ciberincidentes. También incluye aspectos relacionados con la integración de esos planes en los planes de gestión de crisis y respuesta a emergencias en la aviación.
- 5) **Gestión de los ciberriesgos de las cadenas de suministro:** Este elemento incluye aspectos relacionados con la gestión de los ciberriesgos de las cadenas de suministro de la aviación y ajenas a la aviación. Esto incluye varios tipos de cadena de suministro, por ejemplo, sistemas/equipos de aviación certificados, servicios de sistemas de aviación (por ejemplo, sistemas de planificación de vuelo, redes aeroportuarias), proveedores de servicios ajenos a la aviación (por ejemplo, proveedores de servicios en la nube, proveedores de comunicaciones por satélite).
- 6) **Cultura de ciberseguridad:** Este elemento incluye aspectos relacionados con la implementación de una cultura de ciberseguridad sólida en la aviación civil, que aproveche la experiencia del sector en la implementación de las culturas de seguridad operacional y seguridad de la aviación.
- 7) **Programas de instrucción en ciberseguridad de la aviación:** Este elemento incluye aspectos relacionados con el desarrollo y la implantación de programas de instrucción sobre ciberseguridad de la aviación que se dirigen a los diferentes tipos de público (por ejemplo, la concienciación general frente a la instrucción basada en las funciones).

2.6 Dado que el sector de la aviación se considera como una infraestructura crítica nacional en muchos Estados, es necesario un enfoque progresivo y de múltiples niveles para abordar la protección de la ciberseguridad y la resiliencia del sector. El objetivo es implementar una estrategia de defensa en profundidad que incluya, ya sea directa o indirectamente, a todas las partes interesadas que se ocupan de las ciberamenazas y ciberriesgos de la aviación civil⁴. Los elementos descritos anteriormente no son la lista completa de las esferas que deberían abordarse en el ámbito de la ciberseguridad de la aviación; no obstante, proporcionan una base que permite una gestión sólida y eficaz de la ciberseguridad de la aviación, incluidas la protección y la resiliencia de los activos de la aviación gestionados por los Estados y las partes interesadas.

2.7 Se están estableciendo grupos de ciberseguridad en las regiones de la OACI para apoyar los debates regionales sobre la ciberprotección y la resiliencia en los diferentes ámbitos de la aviación. Esas actividades son sumamente relevantes para abordar áreas específicas relacionadas con cada región en materia de ciberamenazas y ciberriesgos, pero existe un riesgo potencial de duplicación, e incluso de conflicto si esas actividades no se coordinan entre los diferentes grupos y planes regionales. Esa

⁴ La defensa en profundidad es la aplicación de múltiples contramedidas de manera estratificada o escalonada para lograr los objetivos de seguridad. El método implica la superposición de tecnologías de seguridad heterogéneas en los vectores de ataque comunes a fin de que los ataques que se escapan a una tecnología sean detectados por otra (referencia ISO/IEC 62443 1-1).

coordinación permitirá un enfoque holístico, armonizado y coordinado para hacer frente a las ciberamenazas y los ciberriesgos en las diferentes regiones, y garantizará la coherencia y complementariedad de los planes regionales para la navegación aérea, la seguridad operacional, la protección y la facilitación de la ciberseguridad de la aviación, lo que repercutirá aún más positivamente en las actividades de planificación e implementación de los Estados miembros a nivel nacional. Los Estados también pueden utilizar esos foros para informar a la OACI sobre los desafíos a los que se enfrentan para ocuparse de la ciberseguridad en la aviación civil, lo que serviría de base para las actividades de la OACI relacionadas con la elaboración de disposiciones y textos de orientación.

3. CONCLUSIÓN

3.1 La transformación digital del sector de la aviación civil en todos los ámbitos de la aviación pone de relieve la necesidad de abordar la cuestión de la ciberseguridad en la aviación civil para garantizar la seguridad operacional, la protección, la capacidad y la eficacia del sector. Si bien se reconocen los desafíos asociados con la ciberseguridad de la aviación, los Estados y las partes interesadas deben tener en cuenta los elementos básicos de referencia en los reglamentos y las operaciones.

3.2 A la luz de lo anterior, se invita a la Conferencia a convenir en la siguiente recomendación:

Recomendación 4.2/x — Ciberseguridad de la aviación

Que los Estados:

- a) elaboren y apliquen un plan nacional para hacer frente a las ciberamenazas y los ciberriesgos de la aviación civil de forma holística en todos los ámbitos de la aviación, y en coordinación con las partes interesadas pertinentes ajenas a la aviación, utilizando los elementos básicos como referencia;
- b) alineen las actividades de ciberseguridad de la aviación en los planes regionales de navegación aérea, seguridad operacional, protección y facilitación a través de los procesos de coordinación de los Grupos Regionales de Planificación y Ejecución (PIRG), los Grupos Regionales de Seguridad de la Aviación (RASG) y los Grupos Regionales de Seguridad de la Aviación y Facilitación (AVSEC/FAL);
- c) informen a la OACI de su experiencia en la aplicación de las disposiciones y los textos de orientación de la OACI relacionados con la ciberseguridad de la aviación, a través de los grupos de expertos competentes o a través de los procesos de los PIRG, los RASG y los Grupos Regionales AVSEC/FAL; y

que la OACI:

- d) proporcione orientación sobre los elementos básicos para ayudar a los Estados y a las partes interesadas a ocuparse de la cuestión de la ciberseguridad de la aviación, e integre de forma holística todas las actividades de ciberseguridad de la aviación en un modo coherente y coordinado.