Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A42-WP//165[1]
EX/83
24/7/25

ASAMBLEA — 42º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 13: Seguridad de la aviación — Políticas

FORTALECIMIENTO DE LA GOBERNANZA Y LA GESTIÓN DE LAS AMENAZAS DIGITALES Y DE CIBERSEGURIDAD A LA AVIACIÓN CIVIL

(Nota presentada por el Consejo Coordinador Internacional de Asociaciones de la Industria Aeroespacial (ICCAIA) y la Federación Internacional de Asociaciones de Pilotos de Línea Aérea (IFALPA))

RESUMEN

La aviación civil depende cada vez más de las tecnologías y los sistemas digitales interconectados, incluidos aquellos que controlan o influyen de manera directa en los procesos físicos y operativos. Pese a que estas tecnologías aportan grandes beneficios, también exponen al sector a amenazas digitales deliberadas, accidentales y naturales, así como a vulnerabilidades que pueden intensificar dichas amenazas y poner en peligro operaciones críticas.

La mayoría de los marcos de la OACI —ya sea en los ámbitos de la seguridad operacional, la seguridad de la aviación o las operaciones— no se concibieron inicialmente para abordar la índole sistémica y transversal de las amenazas digitales que actualmente se extienden por todas las capacidades e interdependencias digitales emergentes. La carencia que hay que suplir con más urgencia atañe a los actos deliberados y malintencionados que traspasan los límites de la seguridad operacional y la seguridad de la aviación.

En la presente nota se invita a la OACI a establecer, como primera medida, un marco interno y coordinado de gobernanza y gestión de las amenazas digitales que armonice sus ámbitos de seguridad operacional, seguridad de la aviación y operaciones y que se centre, en un principio, en las amenazas deliberadas y malintencionadas. Como medida complementaria, se alienta a la OACI a acelerar el desarrollo de los textos orientativos y normas mundiales necesarios para lograr un nivel coherente y eficaz de actuación en materia de seguridad en todo el ecosistema de la aviación.

Decisión de la Asamblea: Se invita a la Asamblea a:

a) reconocer que todas las categorías de amenazas digitales, ya sean deliberadas, accidentales o naturales, conllevan riesgos para la aviación civil y deben abordarse mediante un enfoque de gobernanza integral que se establezca, en primer lugar, en el seno de la OACI a fin de garantizar la coherencia y el apoyo efectivo a los Estados y al sector;

b) solicitar al Consejo de la OACI que inicie el establecimiento de un marco de gobernanza interno, que abarque varios ámbitos y disciplinas, para las amenazas digitales dentro de la OACI;

c) alentar a la OACI a acelerar la elaboración de textos orientativos y, cuando proceda, de normas y métodos recomendados (SARP) a fin de establecer un punto de referencia sistémico, armonizado y adaptable de seguridad digital para todos los Estados y partes interesadas; y

[1] Las versiones en árabe, chino, español, francés, inglés y ruso fueron proporcionadas por ICCAIA y la IFALPA.

d) recomendar a la OACI que refuerce la concienciación y la comunicación relativas al tratamiento coordinado de las amenazas digitales a través de sus redes regionales, con el fin de favorecer la adopción de medidas armonizadas y una actuación en materia de seguridad eficaz a escala mundial.	
Objetivos estratégicos:	Esta nota de estudio se relaciona con el objetivo estratégico *Todos los vuelos son seguros y protegidos.*
Repercusiones financieras:	Ninguna
Referencias:	A41-19 Formas de abordar la ciberseguridad en la aviación civil Anexo 17 — *Seguridad de la aviación* Anexo 19 — *Gestión de la seguridad operacional*

1. INTRODUCCIÓN

1.1 La transformación digital ha mejorado el rendimiento de la aviación civil. Pese a ello, la mayor dependencia digital revela —y crea— vulnerabilidades derivadas del aumento de la interconexión y la complejidad sistémica.

1.2 Esta evolución plantea retos organizativos y de gobernanza debido a las responsabilidades comunes a todos los ámbitos de la OACI, incluidas la seguridad operacional, la seguridad de la aviación, la capacidad y la eficiencia, evidenciando una necesidad general de gobernanza integral y coordinada.

1.3 De entre las diversas categorías de amenazas digitales, es especialmente urgente abordar los actos deliberados y malintencionados, comúnmente denominados ataques a la ciberseguridad, debido a su potencial para interrumpir los sistemas críticos de la aviación y a la incertidumbre imperante en cuanto a las responsabilidades en los ámbitos de la seguridad operacional y la seguridad de la aviación.

1.4 Este cambio también pone de relieve la inexistencia de un marco mundial para aplicar sistemáticamente un enfoque de «seguridad desde el diseño» y basado en las amenazas mediante textos orientativos y normas específicas en todos los ámbitos. Ante la falta de enfoques armonizados, podrían necesitarse mecanismos provisionales de coordinación para facilitar la adopción anticipada de medidas, especialmente en contextos operativos de alto riesgo.

1.5 Las amenazas digitales -—definidas como todo suceso potencial o realmente perjudicial originado o facilitado por las capacidades digitales— han empezado a ser el centro de atención en los grupos de expertos y de trabajo de la OACI. Sin embargo, muchas de estas amenazas siguen sin abordarse suficientemente, sobre todo cuando no se ajustan a las definiciones convencionales de interferencia ilícita o peligro para la seguridad. Esto es especialmente cierto en el caso de las amenazas deliberadas y malintencionadas que se encuentran en la intersección de los ámbitos de la OACI, lo cual genera incertidumbre en torno a la rendición de cuentas, la supervisión y la respuesta coordinada.

2. ANÁLISIS

2.1 Las amenazas digitales para la aviación civil abarcan una amplia variedad de supuestos. Dichas amenazas pueden ser deliberadas (malintencionadas o no), accidentales (error humano, configuración errónea) o naturales (fenómenos medioambientales). Pueden tener su origen en vectores digitales, físicos o híbridos y afectar tanto a los elementos digitales como a los sistemas físicos que dependen de ellos, poniendo así en riesgo la seguridad operacional, la seguridad de la aviación y la

continuidad operativa. Conocer a fondo estas categorías generales es tan solo el primer paso: el sector también debe afrontar la manera en que la transformación digital permanente intensifica su complejidad.

2.2 La transformación digital está remodelando el ecosistema de la aviación, ya que no solo introduce nuevas tecnologías, sino también nuevas modalidades de fallos, exposición y dependencia. Muchos de estos riesgos no se captan adecuadamente en los marcos tradicionales de los ámbitos de la OACI —empezando por los relacionados con la seguridad operacional y la seguridad de la aviación, entre otros. La ausencia de una estructura mundial da lugar a respuestas dispares, responsabilidades fragmentadas y falta de consenso, condiciones estas que menoscaban la protección y la resiliencia.

2.3 Además de aumentar la exposición a actos malintencionados, la transformación digital añade complejidades estructurales que ponen en cuestión los marcos existentes de gobernanza y gestión de riesgos/incidentes. Crea interdependencias opacas entre la tecnología de la información (IT) y la tecnología operativa (OT), riesgos en la cadena de suministro y un ritmo de cambio más rápido que el de los ciclos de certificación. La aviónica preexistente depende ahora de la nube, la inteligencia artificial (IA) y enlaces de protocolo de Internet (IP) cuyos componentes, suministrados por terceros, se actualizan mensualmente, introduciendo vulnerabilidades que escapan a los controles tradicionales. Dado que la innovación avanza en cuestión de meses, mientras que la normativa evoluciona a lo largo de los años, las medidas de mitigación se quedan obsoletas y aumentan las divergencias entre los Estados. Al carecer de una taxonomía común y de un mecanismo de intercambio de información sobre incidentes, la comunidad percibe solamente fragmentos del problema y esto retrasa la implantación de protecciones proporcionadas.

2.4 La falta de textos orientativos y SARP mundiales específicos fundamentados en una filosofía de «seguridad desde el diseño» y basados en las amenazas se traduce en la inexistencia de un enfoque armonizado y sistémico para hacer frente a las amenazas digitales en todos los ámbitos. Dicha falta de un punto de referencia común para los Estados crea un contexto sistémico vulnerable que allana el camino a las amenazas diseñadas de forma deliberada para explotar esta misma complejidad.

2.5 En esta situación, las amenazas deliberadas y malintencionadas merecen especial atención. A menudo complejas, dinámicas y difíciles de atribuir, dichas amenazas están diseñadas para explotar las dependencias digitales con el fin de provocar una degradación o interrupción de las operaciones. Sus características singulares pueden situarlas dentro, a través o al margen de las clasificaciones tradicionales de la aviación, lo cual dificulta la detección, notificación y respuesta.

2.6 La experiencia práctica demuestra que algunas interferencias digitales malintencionadas no se corresponden claramente con los marcos de los ámbitos existentes. Un ejemplo destacado es la suplantación deliberada de señales del GNSS, consistente en la difusión de señales de posicionamiento falsas que desorientan a los sistemas de navegación de las aeronaves sin necesidad de acceso físico o intrusión visible. Aunque deliberadas y capaces de afectar directamente a las operaciones de vuelo, es posible que tales acciones no se ajusten a los criterios sobre interferencia ilícita definidos en el Anexo 17 ni den lugar a la presentación obligatoria de un informe de notificación de incidente de seguridad operacional con arreglo al Anexo 19.

2.7 Esta laguna reglamentaria no solo limita la comprensión de la situación y la respuesta coordinada, sino que, más importante aún, demuestra la imperiosa necesidad de contar con un marco de gobernanza y gestión que integre estos nuevos tipos de interferencia digital, establezca umbrales de notificación claros y defina sin ambigüedades las funciones institucionales entre los ámbitos de la seguridad operacional y la seguridad de la aviación.

2.8 Actualmente, ante la ausencia de un marco internacional coordinado, los Estados y las autoridades regionales han empezado a adoptar enfoques reglamentarios diferentes. Esta creciente divergencia añade complejidad para las partes interesadas de la aviación como, por ejemplo, los fabricantes (OEM), los proveedores y los prestadores de servicios, quienes se ven obligados a desenvolverse en contextos de cumplimiento normativo heterogéneos.

Para sortear estos obstáculos, se necesita un planteamiento doble:

- Una estrategia exhaustiva e integral capaz de abarcar todo tipo de amenazas digitales: deliberadas, accidentales y naturales.
- Medidas que se centren de manera prioritaria en las amenazas deliberadas y malintencionadas dada su urgencia, su posible gravedad y la discordancia normativa existente en la actualidad.

3. CONCLUSIÓN

3.1 Reforzar la protección frente a las amenazas digitales es esencial para mantener la seguridad operacional y la seguridad de la aviación civil, así como su capacidad y eficiencia. A medida que las dependencias digitales siguen aumentando en todos los sistemas y ámbitos, también aumenta la necesidad de una gobernanza coordinada y con visión de futuro.

3.2 Para hacer frente a este reto, la OACI y sus partes interesadas deben perseguir un objetivo doble y claro:

- Adoptar una perspectiva integral que abarque todos los tipos de amenazas digitales, ya sean deliberadas, accidentales o naturales.
- Dar prioridad al tratamiento de las amenazas deliberadas y malintencionadas, que son las que actualmente conllevan el mayor riesgo de incertidumbre en cuanto a las funciones y la coordinación entre los respectivos ámbitos de la OACI.

3.3 La OACI puede contribuir de manera decisiva a garantizar una respuesta coherente, adaptable y uniforme a nivel mundial ante la evolución de los riesgos digitales, fomentando la coordinación entre los distintos ámbitos, promoviendo los instrumentos provisionales y creando una concepción común.

3.4 Esta iniciativa podría ser dirigida por el actual Comité ad hoc de coordinación de la ciberseguridad (AHCCC) asignándole un mandato de gobernanza específico, ya que actualmente carece de tal función.

— FIN —