Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A40-WP/395[1]
EX/161
30/7/19
(Nota de información)

ASAMBLEA — 40º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 12: Seguridad de la aviación — Política

CIBERSEGURIDAD EN LA AVIACIÓN – NUEVOS PLANTEAMIENTOS

(Presentado por la Asociación de Transporte Aéreo Internacional)

RESUMEN

El documento presenta las opiniones de la Asociación de Transporte Aéreo Internacional (IATA) sobre la necesidad de una evolución palpable, proactiva y coordinada en la adquisición de visibilidad tanto de los riesgos en ciberseguridad, como en su gestión, dentro de la aviación.

Objetivos estratégicos:	Este documento informativo se refiere a Objetivos estratégicos de Seguridad de la aviación y Facilitación.
Implicaciones financieras:	Ninguna
Referencias:	

[1] Las versiones en español, árabe, chino, francés, inglés y ruso fueron proporcionadas por la Asociación de Transporte Aéreo Internacional.

1. INTRODUCCIÓN

1.1 La ciberseguridad en aviación (la ciberseguridad que atañe al mantenimiento seguro, fiable y efectivo de las operaciones aéreas) sigue siendo una prioridad clave para el sector. El aumento de la digitalización y la conectividad está ayudando a transformar el servicio disponible para los clientes, aparte de mejorarlo todo: desde la eficiencia hasta la fiabilidad con respecto a los operadores regulados. Sin embargo, esta transformación, aunque ofrece una oportunidad para el sector de la aviación, también significa una oportunidad potencial para aquellos que desearían crear un perjuicio. A nivel básico, el sector de la aviación se encuentra paradójicamente en mejor situación que muchos otros sectores, gracias a su interés en una cultura de la seguridad, una visibilidad del riesgo, además de un diseño y una formación orientados a la redundancia o los fallos. No obstante, la complejidad del servicio y del sistema, junto con su interdependencia, a menudo internacionalmente, está afectando potencialmente a la capacidad para entender y gestionar el riesgo en ciberseguridad.

1.2 La IATA apoya firmemente la posición de la OACI como la organización mejor dispuesta para dirigir un diálogo global coherente y una dinámica en la ciberseguridad de la aviación. Sin un liderazgo internacional claro en lo referente a ciberseguridad en la aviación, nos arriesgamos a la fragmentación de los estándares globales, un régimen normativo complejo que reprime el crecimiento y la innovación además de a restringir la capacidad de evaluación y gestión de los riesgos de la ciberseguridad en la aviación, dentro y fuera de nuestras fronteras.

1.3 La producción de la Estrategia de Ciberseguridad de la Aviación de la OACI supone un avance encomiable y ya finalizado que tiene el apoyo total de la IATA. En la actualidad, el liderazgo, la dinámica y la gobernanza adecuada serán útiles para respaldar dicha estrategia a través de una enmienda de la existente Resolución A39-19 de la Asamblea: Cómo abordar la ciberseguridad en la aviación civil (*Addressing Cybersecurity in Civil Aviation*) para incorporar la referencia correspondiente. En consecuencia, es necesario garantizar una apropiada dotación de recursos, tiempos y esfuerzos junto a todas las partes interesadas, donde se incluyan seguridad y protección. Además, según lo expresado anteriormente, es importante que la ratificación por parte de los Estados del *Convenio para la supresión de actos ilícitos relacionados con la Aviación Civil internacional*, así como del *Protocolo suplementario al Convenio para la supresión del apoderamiento ilícito de aeronaves*, sea firmemente instada. Este compromiso colaborativo debería llevar al desarrollo de mejores prácticas y materiales de orientación a partir de lo cual la IATA, en principio, apoya la generación de ciberseguridad relacionada con las SARP y su consiguiente implementación y vigilancia.

1.4 Más ampliamente, en nuestros esfuerzos por afianzar el sector, no podemos olvidar la verdadera esencia de nuestra industria, la cual está formada por nuestros pasajeros y clientes. Debemos asegurarnos de que durante todo el viaje de nuestros clientes, toda su ciberseguridad, privacidad, datos y derechos, se encuentren protegidos. Es más, con la garantía de que nosotros somos un sector transparente en esta materia, se asegurará la creación y el afianzamiento de una relación de confianza con aquellos que la defienden.

1.5 La IATA ha sido proactiva a la hora de crear concienciación y diálogo entre las partes interesadas en relación con los retos globales sobre ciberseguridad en la aviación. La IATA cuenta con un Grupo operativo de ciberseguridad en aeronaves (*Aircraft Cyber Security Task Force*, ACSTF) que trabaja para aumentar el conocimiento, dirigir el diálogo y captar las mejores prácticas en las partes interesadas del sector de la aviación. La madurez del ACSTF ha generado un entorno de alta confianza donde se ha intercambiado y explorado información palpable que ha sido compartida en una multitud de temas relacionados. Adicionalmente, la IATA también dirigió una innovadora mesa redonda sobre ciberseguridad en la aviación, celebrada en Singapur (en abril de 2019), con las partes interesadas que representan todos los ámbitos de posibilidades dentro del sector de la aviación. Durante esta mesa

redonda, esas partes exploraron los retos actuales a los que se enfrenta el sector de la aviación, cómo debería ser el futuro de la ciberseguridad y cuál sería el camino de llegada. Las conclusiones destacaron que, a pesar de que hay mucho hecho, todavía queda bastante por hacer.

1.6 Además, la IATA ha iniciado el proceso para el desarrollo de una Estrategia de Ciberseguridad de la Aviación del sector, junto con una hoja de ruta para presentarla. El objetivo de esta estrategia es permitir que la IATA, en representación de sus miembros y el sector al completo, dedique mayor atención tanto a los retos como a las oportunidades de los temas en ciberseguridad a los cuales nos enfrentamos, sobre la palpable actividad que supondrá como diferencia, y en referencia a las colaboraciones que la materializarán.

2. DEBATE

2.1 Con las cifras actuales de crecimiento, para 2037 se podría esperar el doble de pasajeros, teniendo mucho que ver en ese crecimiento la región Asia-Pacífico[2]. Existen muchos riesgos y presiones en este crecimiento y la ciberseguridad en la aviación debe añadirse como uno de esos riesgos. La criticidad de afianzar la seguridad, la protección y la efectividad de la tecnología de la que depende este crecimiento se basa en no subestimar aquella.

2.2 Un evento cibernético en aviación no solo supone un impacto de riesgo en la seguridad, protección, servicios operativos, en las pérdidas económicas o el crecimiento. Pone en riesgo de forma importante la confianza e integridad que deposita el pasajero en el mismo servicio que suministramos. Durante muchos años, el sector de la aviación ha demostrado ser sólido ante incidentes de seguridad o protección, y ha sido capaz de devolver la confianza al pasajero a través de medidas y compromisos evidentes. Después de un evento cibernético adverso, la recuperación de la confianza será una misión más complicada a la experimentada previamente por el sector de la aviación, por ello, necesitamos no solo mejorar esta ciberseguridad, sino también, mantener un diálogo abierto sobre los retos a los que nos enfrentamos en paralelo a los esfuerzos que realizamos.

2.3 En nuestro camino hacia el avance tecnológico, también debe encontrarse un equilibrio entre fomentar eficiencias y un servicio definido por una mayor aplicación de tecnologías conectadas con la ciberseguridad de la vida diaria, y la misma protección y solidez de esa tecnología. Ya no podemos permitir la aceptación de ninguna nueva tecnología dentro del sector de la aviación, si no cuenta con seguridad cibernética en su diseño, implementada con una gestión ante vulnerabilidades que sea ágil y proactiva, junto con una relación de riesgo cibernético transparente entre el proveedor y el usuario final.

2.4 Además de los esfuerzos de los diversos sectores con objeto de mejorar la ciberseguridad, también deben intentar disminuirse los costes en dicha seguridad. Como sector internacional compuesto por un amplio espectro de organizaciones, todo lo que pueda hacerse para reducir la complejidad, costes o el reto de gestionar de forma adecuada el riesgo en ciberseguridad, garantizará que ningún país (o empresa) se quede en el camino.

2.5 El sector también debe trabajar más para buscar visibilidad, de una forma proactiva, en la vulnerabilidad y los riesgos de la ciberseguridad. Esto significa estar dispuestos y proactivos a una colaboración entre las partes interesadas, lo que incluye compañeros, naciones, organizaciones multinacionales, otros sectores, así como la comunidad investigadora. Como sector, debemos ser muy precisos para saber quiénes son nuestros adversarios y quiénes no; es decir, aquellos que desean

[2] Nota de prensa de la IATA del 24 de octubre de 2018. Las predicciones de la IATA esperan 8 200 millones de pasajeros aéreos para 2037. Puede consultarse enhttps://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx

ayudarnos a entender nuestros riesgos no serán nuestros adversarios. La investigación privada, jurídica e intersectorial sobre las vulnerabilidades cibernéticas de hardware y software ha originado una comunidad de investigación activa y próspera, compuesta por aquellos que actúan de buena fe para ayudar a diversos sectores a poseer mejor ciberseguridad.

2.6 El sector de la aviación tiene el deber de escuchar, evaluar y tomar las medidas apropiadas respecto a cualquier incidente potencial en seguridad, comoquiera que sea notificado; debemos tratar la notificación de potenciales vulnerabilidades en ciberseguridad del mismo modo. El sector de la aviación debe avanzar para generar confianza y construir relaciones con la comunidad investigadora, siempre con el objetivo de que ambas partes generen un conocimiento colaborativo. La IATA también respalda este esfuerzo, junto con la generación de medidas y una legislación que fomente y proteja la capacidad que reside en la buena fe de los investigadores para respaldar el sector de la aviación.

2.7 Durante la Mesa Redonda sobre Ciberseguridad en Aviación de la IATA que se celebró en Singapur en abril de 2019, los asistentes internacionales, provenientes del sector relacionado, destacaron tanto dónde se está realizando el desarrollo, como dónde se necesita incidir más. Los puntos principales se exponen a continuación.

2.7.1 Las perspectivas ofrecidas sobre el estado actual de la ciberseguridad en la aviación fueron:

a) La escala y complejidad del riesgo en la ciberseguridad en la aviación no están siendo nada favorables para que algunas organizaciones entiendan, prioricen y tomen medidas.

b) Debido a la naturaleza global e interdependiente del sector de la aviación, se entiende que los incidentes en ciberseguridad probablemente podrían aumentar con rapidez y causar impactos a nivel internacional.

c) Quedan incoherencias e insuficiencias en todo el sector de la aviación a la hora de hallar, gestionar y comunicar en lo referente a las vulnerabilidades en ciberseguridad, lo que conlleva una mala visibilidad del riesgo actual en ciberseguridad.

2.7.2 Las perspectivas sobre lo que los asistentes consideraron como «una visión de futuro» ideal para la ciberseguridad en aviación en 2030 y cómo lograrla, fueron propuestas como;

a) Cultura de ciberseguridad. Más que una cultura de seguridad y una cultura de seguridad física, el sector de la aviación al completo necesita una cultura de ciberseguridad.

b) Transparencia y confianza. Entre todas las partes interesadas del sector de la aviación, existe la necesidad de aumentar la transparencia y, por consiguiente, la confianza, respecto a las incidencias en ciberseguridad, las cuales van desde el acceso a datos relevantes de ciberseguridad hasta afianzar prácticas de desarrollo y gestionar la vulnerabilidad. Para ello, el sector de la aviación puede aplicar enfoques similares a lo que ya se está haciendo en toda la cultura de seguridad y protección, aportando homogeneidad de enfoque y unos valores que sean entendidos por todos.

c) La creación de consenso y consistencia. Necesitamos además construir consistencia, estándares y gobernabilidad en la ciberseguridad, en todo el sector de la aviación y a

nivel mundial. Esto llevará al liderazgo individual y organizativo, parejo de una voluntad, a crear un diálogo abierto entre todas las partes interesadas.

d) Comunicaciones y colaboración. Para gestionar mejor el riesgo en la ciberseguridad de la aviación a nivel global, deben construirse relaciones más firmes por todo el sector de la aviación además de con aquellos, ajenos al sector, que puedan ayudar. De este modo, se acogerá una colaboración estrecha en todo ámbito desde el desarrollo de las mejores prácticas hasta la gestión de vulnerabilidades potenciales.

e) Personal laboral. A través del diálogo sobre los retos en ciberseguridad y sobre las oportunidades a las que se enfrenta el sector de la aviación, debemos inspirar a una nueva generación de individuos y organizaciones para que sean capaces de reaccionar a las cuestiones que supone el reto de la ciberseguridad en la aviación. Además, se debe enseñar al personal de la aviación con objeto de que sepa reconocer y gestionar los riesgos de ciberseguridad, logrando un aumento en su solidez y vigilancia.

2.8 Se trataron dos temas adicionales en la Mesa Redonda sobre Ciberseguridad en Aviación de la IATA.

2.8.1 La investigación de los aspectos en ciberseguridad de accidentes e incidentes. Dentro de la investigación de los accidentes e incidentes en aviación, existe en la actualidad muy poca visibilidad en cuanto a las preocupaciones potenciales sobre ciberseguridad. En una época en la que muchos sistemas de aviación están conectados y digitalizados, se consideró que era necesario esforzarse más por entender el cómo adquirir, proteger y analizar firmemente los datos relevantes en ciberseguridad. No hacerlo significa que el sector tendrá muy poca capacidad para garantizarse a sí mismo y a sus clientes el tener la capacidad de gestión del riesgo en ciberseguridad.

2.8.2 En resumen, hay mucho que hacer para aumentar la ciberseguridad, la protección y la solidez del sector de la aviación. Pero, al lado de este reto, existe mucho potencial para tomar medidas y colaborar intersectorialmente, en asociación estrecha con todas las partes interesadas. Lo que se necesita ahora es: compromiso, liderazgo y dinamismo.

— FIN —