Organización de Aviación Civil Internacional

A39-WP/99
EX/45, TE/26
26/07/16

NOTA DE ESTUDIO

ASAMBLEA — 39º PERÍODO DE SESIONES

COMITÉ EJECUTIVO
COMISIÓN TÉCNICA

Cuestión 16: Seguridad de la aviación — Política
Cuestión 36: Seguridad operacional de la aviación y navegación aérea – Apoyo a la implantación

CIBERRESILIENCIA EN LA AVIACIÓN CIVIL

(Nota presentada por Estados Unidos y por Eslovaquia en nombre de la Unión Europea y sus Estados miembros[1], y los demás Estados miembros de la Conferencia Europea de Aviación Civil[2]; y por EUROCONTROL)

RESUMEN

El sistema de aviación consiste en un conjunto de componentes, sistemas y redes interconectados. En los últimos años se ha registrado un aumento en el potencial de ciberincidentes que podrían poner en peligro el intercambio de comunicaciones e información entre las diversas partes interesadas de la aviación, así como repercutir en la seguridad operacional y en la seguridad de la aviación y perjudicar la continuidad de las actividades del sector de la aviación. Si bien la OACI reconoce la importancia de definir un enfoque de ciberseguridad en la aviación civil, aún se requieren mayores esfuerzos para elevar el grado de sensibilización en el mundo y elaborar enfoques de ciberresiliencia para el sistema de aviación que sean coherentes a escala mundial.

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

a) pedir que la OACI aborde la cuestión de la ciberresiliencia en la aviación civil de manera integral;
b) pedir que la OACI y sus Estados contratantes promuevan la sensibilización sobre las ciberamenazas y las vulnerabilidades en la aviación civil, especialmente mediante la inclusión de la dimensión de la ciberresiliencia en los procesos y actividades pertinentes tales como el diseño de sistemas, de procedimientos ATM y la gestión de la seguridad operacional y de la seguridad de la aviación;
c) pedir que la OACI facilite, de manera segura, el intercambio de información entre Estados y partes interesadas pertinentes sobre ciberamenazas, vulnerabilidades y medidas de mitigación;
d) pedir que la OACI examine las medidas que se requieren para elaborar los principios rectores aplicables a la gestión de ciberamenazas y vulnerabilidades actuales y futuras, desde la identificación hasta la mitigación, teniendo en cuenta las medidas existentes adoptadas por los Estados y las normas de la industria; y
e) pedir que la OACI de instrucciones a los grupos de expertos y grupos de especialistas para que tengan en cuenta, de ser pertinente, esas directrices al llevar a cabo su trabajo.

[1] Alemania, Austria, Bélgica, Bulgaria, Croacia, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumania y Suecia.

[2] Albania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Georgia, Islandia, La ex República Yugoslava de Macedonia, Mónaco, Montenegro, Noruega, República de Moldova, San Marino, Serbia, Suiza, , Turquía y Ucrania.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos: Seguridad operacional, Capacidad y eficiencia de la navegación aérea, Seguridad, y Facilitación.
Repercusiones financieras:	Las actividades mencionadas en esta nota de estudio de la Asamblea se llevarán a cabo con sujeción a la disponibilidad de recursos en el Presupuesto del Programa regular para 2017 – 2019 y/o con contribuciones extrapresupuestarias.
Referencias:	*Resoluciones vigentes de la Asamblea (al 4 de octubre de 2013)* (Doc 10022) Anexo 17 — *Seguridad — Protección de la aviación civil internacional contra los actos de interferencia ilícita*

1. INTRODUCCIÓN

1.1 El sistema de aviación consiste en un conjunto de componentes, sistemas y redes interconectados. Los nuevos avances, tales como la introducción progresiva de los RPAS y la continua evolución del sistema ATM (p. ej., SWIM), refuerzan esta interconectividad e integración de sistemas. Pese a las medidas preventivas de seguridad que se han adoptado hasta la fecha, el riesgo de ciberincidentes en el sistema de aviación ha aumentado.

1.2 En todo el mundo se reconoce la importancia de disponer de un enfoque de ciberseguridad adecuado en el campo de la aviación. No obstante, aún es necesario realizar esfuerzos adicionales para elevar el grado de conciencia en el mundo y elaborar enfoques de ciberresiliencia para el sistema de aviación que sean coherentes a nivel mundial.

1.3 Los ciberincidentes pueden afectar a la comunidad de aviación mundial o a sistemas individuales a muchos niveles. Estos incidentes pueden poner en peligro el intercambio de comunicaciones e información entre las diversas partes interesadas de la aviación, lo cual repercute en la seguridad operacional y en la seguridad de la aviación y perjudica la continuidad de las actividades de aviación. La posibilidad de compartir información ligada a lo cibernético, así como la aplicación de sólidos métodos normalizados para proteger el intercambio de datos e información aumentaría la capacidad de la comunidad de la aviación de protegerse y limitar las repercusiones de los ciberincidentes.

2. ANÁLISIS

2.1 Si bien se han emprendido varias iniciativas a escalas local, nacional, regional y mundial, un enfoque más uniforme, sistemático y coherente podría ser ventajoso para hacer frente a los riesgos que plantea el cambiante entorno de las ciberamenazas.

2.2 Promover la sensibilización a escala mundial sobre la ciberresiliencia en la aviación

2.2.1 En ciertos sectores económicos como el sector bancario, se tiene un amplio conocimiento sobre las ciberamenazas y las vulnerabilidades y se toman medidas para contrarrestar y mitigar los riesgos identificados. Sin embargo, en el ámbito de la aviación no todos los Estados y partes interesadas tienen un buen conocimiento de los riesgos relacionados con lo cibernético, ni éstos se abordan de manera coherente y sistemática.

2.2.2 Es necesario elevar el nivel de sensibilización sobre las ciberamenazas y vulnerabilidades en el sector de la aviación a nivel mundial a fin de garantizar que todos los Estados y las partes interesadas identifiquen posibles riesgos y puedan mitigarlos.

2.2.3 Dicha mayor sensibilización podría formalizarse, en especial, mediante la adaptación de los procesos existentes, p. ej., mediante la elaboración de un enfoque de seguridad en el diseño o la implantación de instrucción específica. Además, y en coordinación con las iniciativas relacionadas con la seguridad (p. ej., sistemas de gestión de la seguridad operacional – SMS, cuando se dispone de éstos, o programas nacionales de seguridad de la aviación civil), debería tenerse en cuenta el aspecto de la ciberresiliencia en el contexto de las actividades de gestión de la seguridad operacional, a nivel organizativo (dentro del Programa estatal de seguridad operacional – SSP) y, cuando sea pertinente, en el contexto de un Programa regional de seguridad operacional de la aviación.

2.3 Promover el intercambio de información sobre ciberincidentes, amenazas y enfoques normalizados

2.3.1 Ninguna organización o parte interesada podrá protegerse por sí sola de la interferencia electrónica intencional no autorizada. Además, las ciberamenazas evolucionan constantemente y nadie puede pretender estar a salvo de todos los posibles riesgos conexos. Por consiguiente, para hacer frente a los ciberincidentes de manera eficaz es necesario que los Estados y las partes interesadas compartan toda información pertinente y armonicen los medios que se utilizarán para proteger y preservar la integridad de los datos y el intercambio de información. El intercambio de información ayudaría a los Estados y a las partes interesadas a prepararse mejor para hacer frente a los ciberincidentes y a tomar medidas adecuadas para mitigarlos. La información compartida puede incluir casos de incidentes, vulnerabilidades, amenazas, tendencias y patrones observados, evaluaciones de riesgos compartidos, planes para el manejo de riesgos, medios de mitigación eficaces (de índole técnico, operacional u organizativo) o actividades de aseguramiento de la seguridad que hayan probado ser protecciones eficaces.

2.3.2 Ya existen varias iniciativas en el sector de la aviación que tienen por objeto promover el intercambio de información relacionada con la seguridad, incluso a escala regional y mundial; no obstante aún es necesario desarrollarlas más a fondo y complementarlas para apoyar la ciberresiliencia del sistema de aviación global. Dichas iniciativas pueden basarse en las plataformas existentes para el intercambio de información tales como el ISAC (centro de intercambio y análisis de información) o CERT (equipo de respuesta a emergencias informáticas) y pueden requerir el establecimiento de protocolos comunes para el intercambio de información sobre ciberincidentes, conforme a reglamentos nacionales y regionales relativos a la protección de información de carácter confidencial.

2.3.3 También existe la necesidad de mejorar los métodos para proteger los datos y el intercambio de información entre todas las partes interesadas pertinentes. Debería alentarse la normalización de los controles técnicos que facilitarán la creación de métodos más sólidos de autenticación y autorización de datos para la comunidad de aviación mundial.

2.4 Promover un "enfoque conjunto para la gestión de riesgos de aviación”

2.4.1 En la aviación existen muchas metodologías para evaluar riesgos, la mayoría de las cuales se centra en la caracterización y evaluación de amenazas y vulnerabilidades. Si bien se puede coincidir con respecto a los elementos que se necesitan para caracterizar riesgos (p. ej., probabilidad que ocurra un suceso y la magnitud de las repercusiones), las evaluaciones de detalles específicos son demasiado diversificadas como para poder lograr resultados comparables, coherentes o sistemáticos. Sin embargo, cuando se hace frente a ciberincidentes recurrentes que pueden tener patrones similares, resulta ventajoso definir "principios comunes " y métodos para identificar, evaluar y mitigar los riesgos.

2.4.2 Dichos "principios comunes " deberían facilitar la identificación de amenazas y vulnerabilidades, permitir una evaluación de los riesgos y proporcionar herramientas para su mitigación. A título de ejemplo, la definición formal del ámbito de seguridad, mediante una descripción del contexto

en que se realizan las evaluaciones de riesgos y la delimitación de dicho ámbito ayudaría a identificar los sistemas de información de la aviación que son críticos conforme a lo previsto en las disposiciones del Anexo 17 de la OACI. Otro ejemplo sería el análisis de extremo a extremo de los "escenarios de amenazas" lo cual incluye las amenazas, la arquitectura del sistema que es objeto de examen y los recursos que ocasionan los efectos no deseados. Esto también incluye las vulnerabilidades conocidas dentro del escenario de amenaza que podrían necesitar una mitigación acorde con la gravedad de las repercusiones.

2.4.3 Una vez definidos y adoptados los “principios comunes " de la evaluación de riesgos en la aviación, idealmente, éstos también se aplicarían en el marco de la OACI al elaborar o enmendar normas y métodos recomendados (SARPS)

— FIN —