Organización de Aviación Civil Internacional

A41-WP/74
EX/36
26/7/22

**NOTA DE ESTUDIO**

# ASAMBLEA — 41º PERÍODO DE SESIONES

## COMITÉ EJECUTIVO

**Cuestión 14: Seguridad de la aviación - Política**

## DESARROLLO DE UN MARCO PARA LA CIBERSEGURIDAD

(Nota presentada por Chequia en nombre de la Unión Europea y sus Estados miembros[1] y los demás Estados miembros de la Conferencia Europea de Aviación Civil[2], los Estados miembros de la Comisión Africana de Aviación Civil[3], y EUROCONTROL)

**RESUMEN**

La importancia de la ciberseguridad sigue aumentando a medida que las nuevas tecnologías y una mayor dependencia de la aviación de la tecnología de la información y los sistemas operativos digitales crean nuevas vulnerabilidades, así como nuevas oportunidades. Una mayor comprensión del ámbito cibernético apunta además a una serie de dificultades específicas, lo que hace más evidente la necesidad de promover y avanzar hacia un enfoque distinto para la mitigación del riesgo. Su creciente importancia pone aún más de relieve la necesidad crítica de que los Estados y la OACI incrementen sus esfuerzos en apoyo del desarrollo de un marco para la ciberseguridad, así como de la cultura y la instrucción en materia de ciberseguridad.

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

[2] Albania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Georgia, Islandia, Macedonia del Norte, Moldova, Mónaco, Montenegro, Noruega, Reino Unido, San Marino, Serbia, Suiza, Türkiye y Ucrania.

[3] Angola, Argelia, Benin, Botswana, Burkina Faso, Burundi, Camerún, Cabo Verde, Chad, Comoras, Congo, Cote d'Ivoire, Djibouti, Egipto, Eritrea, Eswatini, Etiopía, Gabón, Gambia, Ghana, Guinea, Guinea-Bissau, Guinea Ecuatorial, Kenya, Lesotho, Liberia, Libia, Madagascar, Malawi, Malí, Marruecos, Mauritania, Mauricio, Mozambique, Namibia, Níger, Nigeria, República Centroafricana, República Democrática del Congo, República Unida de Tanzania, Rwanda, San Tomé y Príncipe, Senegal, Seychelles, Sierra Leona, Somalia, Sudáfrica, Sudán, Sudán del Sur, Togo, Túnez, Uganda, Zambia y Zimbabwe.

| | |
|---|---|
| **Decisión de la Asamblea**: Se invita a la Asamblea a:<br>a) Pedir a la OACI que considere los pasos necesarios para avanzar hacia una orientación sobre la evaluación de los ciberriesgos en la aviación, teniendo en cuenta las partes involucradas, la necesidad de una perspectiva transversal holística y los factores característicos descritos en esta nota de estudio;<br>b) pedir a la OACI que culmine la recopilación de las normas y métodos recomendados (SARPS) pertinentes que están vigentes y otros documentos jurídicos internacionales en los que los Estados y las organizaciones puedan basarse para incluir los ciberriesgos en sus marcos relativos a la aviación;<br>c) solicitar que la OACI y sus Estados contratantes intensifiquen los esfuerzos para promover una cultura y actividades de ciberseguridad dedicadas a apoyar el desarrollo de suficientes recursos humanos y la capacidad para gestionar la ciberseguridad y la resiliencia cibernética en la aviación civil; y<br>d) solicitar que la OACI considere la organización de ejercicios de ciberseguridad a nivel regional y mundial. | |
| *Objetivos estratégicos:* | Esta nota de estudio se relaciona con el objetivo estratégico de *Seguridad de la aviación y facilitación*. |
| *Repercusiones financieras:* | |
| *Referencias:* | |

## 1. INTRODUCCIÓN

1.1 El 40º período de sesiones de la Asamblea de la OACI adoptó la Resolución de la Asamblea A40-10 – *Formas de abordar la ciberseguridad en la aviación civil*. Dicha resolución aborda la ciberseguridad a través de un enfoque horizontal, transversal y funcional, que reafirma la importancia y la urgencia de proteger los sistemas y datos de infraestructura crítica de la aviación civil contra las ciberamenazas y alienta a los Estados a aplicar la Estrategia OACI de Ciberseguridad de la Aviación (octubre 2019). La estrategia se pone en práctica a través del Plan de Acción de Ciberseguridad (CyAP) y con el apoyo del recién creado Grupo Experto en Ciberseguridad, que se basará en la labor del Grupo de Estudio de la Secretaría sobre Ciberseguridad.

1.2 A medida que la digitalización repercute profundamente en las economías y reconfigura el sector de la aviación, la cuestión de la ciberseguridad se vuelve cada vez más crítica. La ciberseguridad también sigue suponiendo una dificultad para todos los sectores durante la fase de recuperación de la pandemia de COVID-19. Las empresas están empleando más medios de trabajo virtuales, lo que puede aumentar su vulnerabilidad a las ciberamenazas. Esto requiere intensificar esfuerzos para el desarrollo de un marco para la ciberseguridad teniendo en cuenta sus especificidades.

## 2. EL PANORAMA DE LA CIBERSEGURIDAD PRESENTA ELEMENTOS CARACTERÍSTICOS PARA DEFINIR UN ENFOQUE DE GESTIÓN DEL RIESGO

2.1 El ámbito de la ciberseguridad presenta un panorama de amenazas único. Debe centrarse no solo en los grupos terroristas que buscan ataques directos y víctimas en masa, sino también en una serie de otros posibles actores y motivaciones. Entre ellos se encuentran los grandes grupos de delincuencia organizada, los activistas y los ciberdelincuentes, que buscan, por ejemplo, la interrupción, la coerción, demostrar su fuerza, la atención de los medios de comunicación o un beneficio económico. Los ataques

pueden afectar intencionadamente, o no, a la aviación civil, pudiendo incluso poner en peligro la seguridad operacional y repercutir en el sector de manera directa o indirecta.

2.2 Otros elementos que habría que tener en cuenta en la gestión de los ciberriesgos son el importante número de proveedores de servicios no específicos de la aviación para el sistema aeronáutico, y que pueden entender de una manera diferente las necesidades y los riesgos de ciberseguridad.

2.3 El entorno de la ciberseguridad se caracteriza además por una reglamentación estatal que puede operar en todos los sectores, sin un elemento característico de la aviación.

2.4 Lo anterior apunta a la necesidad de definir un enfoque específico para la evaluación de los riesgos de ciberseguridad en el que:

a) los conocimientos necesarios, particularmente en relación con las vulnerabilidades y las medidas de mitigación, tienen que combinar los conocimientos y la experiencia en materia de aviación y tecnologías de información;

b) el alcance de la evaluación tiene que estar claramente definido, centrándose en la seguridad operacional, la seguridad de la aviación y la resiliencia de las funciones críticas que afectan a los explotadores/entidades individuales y a los dominios; y

c) la evaluación de riesgos puede identificar posibles puntos únicos de falla desde la perspectiva de la seguridad de la información (global) con el fin de abordarlos de la manera adecuada.

## 3. DESARROLLAR UN MARCO PARA LA CIBERSEGURIDAD QUE TENGA EN CUENTA LAS ESPECIFICIDADES

3.1 A la hora de desarrollar un marco para la ciberseguridad, el sector de la aviación debe establecer enfoques que no solo crucen los límites tradicionales de los dominios aeronáuticos (como la necesidad de una perspectiva macro (por ejemplo, la ATM) y una perspectiva de vuelo individual), sino que también tengan en cuenta dónde se ubican los sectores no relacionados con la aviación y las reglamentaciones estatales horizontales (no específicas de la aviación), como se describe en 2.2 y 2.3. En la implementación de un marco para la ciberseguridad es necesario garantizar la coherencia, así como evitar la duplicación, las brechas y la carga reglamentaria o de vigilancia innecesaria para los Estados y los explotadores.

3.2 El sector de la aviación está bien posicionado para aprovechar y seguir consolidando las funciones, responsabilidades y procedimientos actuales de la aviación internacional. Los SARPS de la OACI en materia de seguridad de la aviación y seguridad operacional proporcionan una base firme sobre la que se puede trabajar, tanto a nivel gubernamental como organizacional. Lo mismo ocurre con los mecanismos de intercambio de información y notificación. También existen instrumentos de derecho aeronáutico internacional para la penalización de los actos que ponen en peligro la seguridad operacional y que deberían utilizarse en la medida de lo posible.

3.3 Se alienta a los Estados y a las organizaciones a que examinen y consideren los documentos pertinentes de la OACI sobre ciberseguridad y a que apliquen los SARPS existentes que se relacionan con la ciberseguridad. Asimismo, es importante que los Estados y las organizaciones se replanteen sus estructuras existentes de seguridad operacional y seguridad de la aviación, así como las estructuras de

derecho penal aeronáutico, desde una perspectiva digital para asegurarse de que las funciones y responsabilidades sigan siendo pertinentes y estén debidamente coordinadas.

## 4. LA IMPORTANCIA DEL ELEMENTO HUMANO EN LA CIBERSEGURIDAD

4.1 El elemento humano es el corazón de la ciberseguridad, como se reconoce en la Estrategia de Ciberseguridad de la Aviación de la OACI (2019).

4.2 La creciente digitalización e interconectividad del sistema de aviación exige que se redoblen los esfuerzos para satisfacer las crecientes necesidades de concienciación, instrucción, actualización de los planes de estudios académicos y un personal debidamente instruido que además cuente con conocimientos en materia de aviación y ciberseguridad.

4.3 La Secretaría de la OACI ha puesto en marcha un primer curso OACI sobre ciberseguridad y ciberresiliencia, "Gestión técnica y fundamentos de liderazgo en ciberseguridad de la aviación", así como un curso sobre "Gestión del riesgo de seguridad en la ATM", diseñado en colaboración con EUROCONTROL. Bien valdría la pena aprovechar estos bien recibidos esfuerzos y las lecciones que los mismos puedan aportar.

4.4 Como se señala en la Estrategia de Ciberseguridad de la Aviación de la OACI, los ejercicios de ciberseguridad constituyen una herramienta útil para poner a prueba la ciberresiliencia existente e identificar los avances, y por eso se recomienda altamente su conducción. Además de los ejercicios a nivel de cada Estado europeo. Europa cuenta con experiencia regional en este ámbito que puede compartir en beneficio de la comunidad de la aviación internacional[4]. Se alienta a la OACI a explorar las posibilidades de acoger tales ejercicios.

4.5 Como se destacó durante el *Año de la Cultura de la Seguridad* (YOSC) de la OACI, es vital ampliar la noción de cultura de la seguridad operacional y de la aviación más allá del ámbito físico. Se alienta a los Estados y a las organizaciones a basarse en los logros del YOSC promoviendo una cultura de ciberseguridad y a compartir las prácticas más idóneas. La OACI debería fomentar los esfuerzos en este sentido, incluida la elaboración de textos de orientación adecuados.

— FIN —

[4] "Ciber Europa 2018" organizado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), estaba dirigido principalmente al público de profesionales y organizaciones que participan en actividades de seguridad de la información en el sector de la aviación; la Célula de Coordinación de Crisis de la Aviación (EACCC) de la Unión Europea organizó un ejercicio de gestión de crisis en 2018 como resultado de un ciberataque al software de seguimiento de la vigilancia y está preparando un ejercicio de gestión de crisis en 2022 para simular una interrupción a gran escala de la infraestructura de red digital europea como resultado de un ciberataque; la Agencia de la Unión Europea para la Seguridad Aérea también ha organizado ejercicios de ciberseguridad.