Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A40-WP/243[1]
EX/95
5/8/19

ASAMBLEA — 40º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 12: Seguridad de la aviación — Política

CIBERSEGURIDAD

[Nota presentada por el Consejo Internacional de Aeropuertos (ACI)]

RESUMEN

Las amenazas de ciberseguridad se han transformado en riesgos reales para el sector de la aviación y se estima que estos riesgos aumentarán en cantidad y consecuencias en el futuro previsible. Entonces, resulta esencial que las partes interesadas de la aviación establezcan un programa de ciberresiliencia y mantengan defensas de ciberseguridad robustas y eficientes. Todos los negocios, incluyendo los aeropuertos, están expuestos al riesgo de ciberamenazas, desde las empresas con un conjunto de sistemas sencillo a aquellas con los programas más avanzados de transformación digital de tecnología de la información (IT).

Existe una clara necesidad de cooperación internacional y de contar con un enfoque de gobernanza conjunto, así como políticas coherentes y viables para abordar la ciberseguridad, conjuntamente con soluciones prácticas para compartir información, vigilancia, creación de capacidad e instrucción. El actual enfoque compartimentado no aborda eficazmente el problema; se requiere una visión y una estrategia claras por parte de la OACI así como una labor conjunta en todas las disciplinas que considere la seguridad operacional, la seguridad de la aviación, las operaciones y la resiliencia.

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

a) apoye la estrategia de ciberseguridad de la OACI y pida que esta Organización trabaje junto a los Estados y la industria para elaborar un plan de acción que respalde dicha estrategia;
b) reconozca la inmediata necesidad de establecer un enfoque multidisciplinario de la ciberseguridad;
c) pida que la OACI realice rápidamente una evaluación de la actual estructura de gobernanza en materia de ciberseguridad, considerando seriamente establecer un grupo de expertos responsable de la ciberseguridad que examine en conjunto los aspectos de seguridad de la aviación, seguridad operacional, resiliencia y continuidad de las operaciones. El grupo de expertos debe estar integrado por elementos adecuadamente capacitados de los Estados y la industria para avanzar en la tarea identificada en la "Estrategia de ciberseguridad" y debería depender conjuntamente de la Comisión de Aeronavegación y del Comité sobre interferencia ilícita o el Comité de transporte aéreo; y
d) pida al Consejo que involucre a la industria, así como a los Estados, al definir una política, una estrategia, planes y normas en materia de ciberseguridad de la aviación.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos: Seguridad operacional, Capacidad y eficiencia de la navegación aérea y Seguridad de la aviación y facilitación.
Repercusiones financieras:	Las actividades que se mencionan en la presente nota se llevarán a cabo con sujeción a la disponibilidad de recursos en el presupuesto del Programa regular de 2020 - 2022 y/o con contribuciones extrapresupuestarias.
Referencias:	A40-WP/28 EX/13 *Estrategia de ciberseguridad de la OACI* Anexo 17 — *Seguridad* *Manual de seguridad de la gestión del tránsito aéreo* (Doc 8973)

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

1. INTRODUCCIÓN

1.1 Los sistemas de aviación están cada vez más conectados; los sistemas de aeropuertos, explotadores de aeronaves, ANSP, servicios de escala y sistemas de pasajeros dependen mutuamente para el intercambio de información digital.

1.2 Las amenazas de ciberseguridad se han materializado en riesgos reales para el sector de la aviación y es probable que estos riesgos continúen creciendo en cantidad y consecuencias en el futuro previsible. Entonces, resulta de vital importancia que las partes interesadas en la aviación establezcan defensas de ciberseguridad robustas y eficientes y mantengan un programa de ciberresiliencia. Todos los negocios, incluyendo los aeropuertos, están expuestos a amenazas de ciberseguridad, desde aquellos con un conjunto de sistemas sencillo a los que cuentan con programas de transformación digital IT más avanzados.

1.3 Más importante aún, debe hacerse hincapié en que la seguridad no constituye "solamente" un problema de tecnología de la información y las comunicaciones (ICT). La ciberseguridad es responsabilidad de toda la organización de que se trate y la ciberresiliencia eficaz se basa en el apoyo de todos, con sólido aseguramiento de la calidad y la vigilancia, marcos de política claros y colaboración efectiva entre las partes interesadas. Es fundamental que en el sector de la aviación se desarrolle una sólida cultura de seguridad de la información.

1.4 Las amenazas e incidentes relacionados con la informática pueden afectar a todo el sistema de transporte aéreo y también provocar preocupaciones de seguridad operacional, seguridad de la aviación, interrupción de operaciones y pérdidas financieras, con consecuencias que pueden rápidamente trascender fronteras y afectar a todo el mundo.

1.5 La comprensión de las amenazas de ciberseguridad será crítica para entender y gestionar los riesgos. Es necesario que todos los involucrados en la industria de la aviación colaboren a efectos de promover un diálogo que valore múltiples perspectivas y arribe a un conjunto de medidas comunes.

1.6 La industria de la aviación cuenta con décadas de experiencia en el tratamiento de problemas de seguridad operacional y seguridad de la aviación, pero el reto de la ciberseguridad es comparativamente nuevo. Las industrias de la aviación y de los aeropuertos están obteniendo experiencia en cuanto a abordar los riesgos de ciberseguridad. Como tal, la industria debería colaborar igualmente con los Estados en la toma de decisiones, pero también en la elaboración de políticas y normas por los órganos apropiados de la OACI. El desarrollo y sustitución de sistemas de aviación puede insumir más tiempo que el dedicado por los perpetradores a desarrollar sus capacidades, de modo que se requiere un enfoque que permita a la industria continuar implementando mejores prácticas con arreglo a las normas internacionales existentes como las ISO, promoviendo al mismo tiempo una mayor implementación con carácter mundial.

1.7 Es necesario contar con un enfoque completo que abarque la seguridad de la aviación, la seguridad operacional, la resiliencia del sistema de transporte aéreo, medidas de protección, mecanismos de respuesta, compartición de información, creación de capacidad y vigilancia.

2. ANÁLISIS

2.1 Durante los últimos años, la OACI ha abordado la ciberseguridad y la resiliencia frente a los ciberataques en diferentes foros.

2.2 El Grupo de expertos AVSEC considera actualmente la ciberseguridad desde una perspectiva de seguridad de la aviación y se ha concentrado principalmente en la utilización de la ciberseguridad con intenciones terroristas de perjudicar a la aviación. Tres grupos de trabajo de dicho Grupo de expertos han abordado el tema con cierto detalle.

2.3 El Grupo de trabajo sobre amenazas y riesgos realizó (en 2015) un análisis del riesgo de un ataque de ciberseguridad deliberado que pudiera afectar a las compañías aéreas, los aeropuertos y los sistemas de navegación aérea. En particular, por lo que respecta a los aeropuertos, la atención se concentró en la manipulación deliberada de los sistemas de seguridad como los sistemas de control de accesos y el equipo de inspecciones de seguridad.

2.4 El Grupo de trabajo sobre textos de orientación (WGGM) del Grupo de expertos AVSEC ha producido un capítulo sobre ciberseguridad destinado al *Manual de seguridad* de la OACI (Doc 8973). Dicho capítulo abarca, a alto nivel, información de antecedentes para los Estados, orientación para la creación de una evaluación de riesgos y política correspondiente, un marco sugerido, gobernanza, instrucción, prácticas de diseño, adquisición, detección, respuesta a incidentes y recuperación de los mismos y notificación.

2.5 El Grupo de trabajo sobre el Anexo 17 del Grupo de expertos AVSEC ha analizado en profundidad los SARPS pertinentes culminando en el apoyo inicial por parte de dicho Grupo de expertos para que dos métodos recomendados en la Enmienda 15 del Anexo 17, sean remplazados por una norma y un método recomendado incluidos en la Enmienda 16 de dicho Anexo, con fecha noviembre 2018.

2.6 Para investigar la posibilidad de una red fiable de navegación aérea, la Secretaría de la OACI estableció el equipo “INNOVA” dentro de la Dirección de navegación aérea, dirigido a definir un medio de facilitar un intercambio seguro, resiliente y continuo de información en un entorno conectado en forma digital en apoyo de las operaciones actuales y futuras. Con este fin, se constituyó en el ámbito de dicha Dirección el Grupo de estudio sobre el Marco de confianza (TFSG) para elaborar un conjunto común de principios, políticas y orientación, así como la estrategia de transición para un marco armonizado mundialmente que permitirá el intercambio fiable de datos e información tierra-tierra, aire-tierra y aire-aire entre las partes interesadas pertinentes de la aviación con el nivel de resiliencia e interfuncionamiento necesario a efectos de apoyar una mayor capacidad y eficiencia para la operación continua del sistema de aviación civil en condiciones de seguridad.

2.7 La OACI estableció el Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC) dirigido por el Director adjunto de seguridad de la aviación y facilitación (DD/ASF). Este grupo ha estado trabajando sobre recomendaciones para la OACI relativas a estrategia, política jurídica y necesidades generales de los Estados y la industria en el ámbito de la ciberseguridad, pero tiene alcance y participación limitadas.

2.8 El Grupo de expertos sobre sistemas de aeronaves pilotadas a distancia (RPAS) ha elaborado normas para intercambio de información entre las aeronaves pilotadas a distancia y las estaciones de pilotaje a distancia para minimizar la posibilidad y las consecuencias de cualquier tipo de mando y control no autorizado y mitigar las mismas.

2.9 El Comité Jurídico considera la pertinencia de los instrumentos de derecho aeronáutico internacional existentes en el tratamiento de las ciberamenazas contra la aviación civil.

2.10 ACI reconoce que la OACI es la organización más apropiada para impulsar medidas sobre ciberseguridad para la aviación. No obstante, la división actual de las actividades de ciberseguridad dentro de la propia OACI, descrita anteriormente, no permite contar con un enfoque eficiente y holístico.

2.11 ACI opina que sería necesario introducir normas detalladas o prescriptivas sobre ciberseguridad. En verdad, esto podría resultar contraproducente dado que se trata de un problema de rápida evolución y volátil para el cual las respuestas deben ser flexibles y ágiles. Diferentes Estados también tienen enfoques diferentes, con responsabilidades diferentes entre sus múltiples órganos. Esto hace que la implementación de un conjunto de normas específicas para la aviación sea difícil y complicada.

2.12 No obstante, existe la clara necesidad de cooperación internacional, criterios comunes de gobernanza y políticas coherentes y prácticas para abordar estos asuntos. Conjuntamente con soluciones prácticas para la compartición de información, vigilancia, creación de capacidad e instrucción, existe la urgente necesidad de contar con una estrategia y un plan de acción para la aviación civil.

2.13 Este plan de acción debería promover y facilitar la elaboración de directrices, normas y métricas comunes, así como la concientización e intercambio de conocimientos sobre ciberseguridad para el ecosistema de aviación. Además, las iniciativas de concientización y el intercambio de conocimientos y prácticas entre las partes interesadas en la aviación deberían estar sustentado por el aprovechamiento de las enseñanzas obtenidas y de las buenas prácticas existentes.

3. CONCLUSIÓN

3.1 ACI apoya plenamente la nota de estudio de la Secretaría de la OACI respecto de una estrategia de ciberseguridad y continuará desempeñando una función activa en el ulterior desarrollo e implementación de esta.

3.2 Resulta crítico que la OACI, los Estados y la industria aceleren la labor en este ámbito y trabajen conjuntamente en todas las disciplinas para abordar la ciberseguridad. No se trata de un problema que puede separarse naturalmente en sus aspectos de seguridad operacional, seguridad de la aviación, operaciones, navegación aérea y facilitación dado que abarca todos estos sectores; la evaluación de riesgos, los textos de orientación, la elaboración de políticas y la vigilancia se aplicarán también a todas esas áreas.

3.3 Un grupo de expertos sobre ciberseguridad, si cuenta con recursos adecuados, podría abordar algunos de los aspectos identificados anteriormente gracias a:

a) una mayor gama de conocimientos y experiencias en los integrantes del grupo, específicamente sobre el tema de la ciberseguridad;

b) un enfoque holístico de la evaluación de riesgos con metodologías convenidas y mutuamente comprendidas por todas las partes interesadas, sobre la base de la experiencia regional y nacional;

c) la capacidad de crear grupos de trabajo para dedicar más tiempo y recursos a la elaboración de textos de orientación, programas, creación de capacidad, asistencia e instrucción, según se requiera; y

d) la consideración de los aspectos de navegación aérea, seguridad operacional y seguridad de la aviación en un único ámbito.

— FIN —