Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A39-WP/187[1]
EX/72
10/8/16

ASAMBLEA — 39º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 16: Seguridad de la aviación — Política

ESTRATEGIA DE DEFENSA DE CIBERSEGURIDAD

(Nota presentada por CANSO)

RESUMEN

La ciberseguridad es uno de los temas más relevantes y uno de los más debatidos en la aviación civil. La evolución de los sistemas de aviación introduce riesgos nuevos, relevantes para el impacto y la continuidad de la seguridad debido a la dependencia cada vez mayor en la tecnología de la información. Los sistemas de Gestión de Tráfico Aéreo (ATM), pero también los sistemas de aeronaves, sistemas de gestión de aeropuertos, sistemas de reservas, información aeronáutica e información climática podrían verse igualmente afectados por los incidentes cibernéticos, que no solo se relacionan con la confidencialidad, sino principalmente con la disponibilidad y continuidad.

Decisión de la Asamblea: Se invita a la Asamblea a: aceptar la recomendación contenida en el párrafo 5.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el Objetivo Estratégico C: *Seguridad y su Facilitación*
Implicancias financieras:	Reducción de costos de seguro; mitigación de amenazas y peligros a la luz de resistencia y seguridad (?) y reducción al mínimo de costos relacionados con la gestión de crisis y las implicancias sociales.
Referencias:	Anexo 17 — *Seguridad* del Convenio de Chicago; Doc. 8973; Doc. 9985; Doc 9854; Guía de Evaluación de Riesgos de Seguridad Cibernética de CANSO

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

1. INTRODUCCIÓN

1.1 La aviación civil sigue siendo un objetivo potencial de nivel alto para los criminales y terroristas. La obligación de proteger la aviación civil contra actos de interferencia ilegales debe comprender lidiar con amenazas sofisticadas, incluyendo aquellas de naturaleza tecnológica. La sociedad siempre esperará una ocurrencia de cero incidentes y accidentes debido a brechas de seguridad para la industria de la aviación en su totalidad. Esta perspectiva establecerá la confianza del cliente final en el transporte aéreo. La red de transporte aéreo es esencial para la economía mundial y fundamental para el comercio internacional, el turismo, la inversión y la prosperidad. Todo trastorno en su eficiencia puede resultar en un trastorno significativo económico y social en todo el mundo. El desarrollo de sistemas complejos, por su naturaleza interoperable, en un entorno mundial e internacional, exige un enfoque metodológico de las reglas de seguridad para que sea posible el control constante de recursos, la integración de procesos entre la Tecnología de la Información (TI), la seguridad física y lógica. Esto debe hacerse mediante la evaluación continua del nivel de amenaza y la vulnerabilidad potencial, con el objetivo de prevenir y responder a actos de interferencia ilegal. Esto además exige una coordinación directa entre todos los actores del sistema de aviación, los estados y las partes interesadas relevantes. El simple cumplimiento de las reglamentaciones no es suficiente, pero es siempre necesario para demostrar la diligencia debida para la protección de vidas humanas en aire y tierra y para garantizar la seguridad, continuidad, resistencia y regularidad del sistema. El Grupo de Trabajo de Riesgos y Amenazas (TRWG) de ICAO también destacó que el sistema de aviación mundial en su complejidad de información y comunicación es ciertamente un objetivo potencial para ataques cibernéticos graves. El objetivo de interoperabilidad y la apertura de redes para un concepto de operación céntrica de redes habilitado por datos operativos e intercambio de información en tiempo real están abriendo el sistema a más vulnerabilidades.

1.2 ICAO ya ha planteado la preocupación de que la seguridad cibernética podría ser un impedimento para la implementación del Plan de Navegación Aérea Internacional (GANP) y apoyó la iniciativa conjunta con las principales partes interesadas del mundo de la aviación para evaluar sistemáticamente el marco cibernético actual (Grupo de trabajo de alto nivel sobre la industria Cíber [IHLG] firmado en Montreal el 5 de diciembre de 2014).

1.3 Durante el Panel de Seguridad de la Aviación de ICAO (AVSECP/27) llevado a cabo en marzo de 2016, un amplio número de miembros de los estados destacaron la necesidad de actualizar la práctica recomendada actual en el Apéndice 17 (Seguridad) sobre la seguridad cibernética a una norma. Sin embargo, la mayoría de los miembros sostuvieron la visión de que la ciberseguridad no está limitada al sistema de seguridad de la aviación. Los miembros subrayaron la gran necesidad de asegurar la coordinación apropiada, incluyendo la alienación con otros Apéndices, específicamente el Apéndice 3, 6, 10, 11, 14 y 15. Además, la coordinación con otros paneles relevantes es necesaria antes de actualizar las prácticas recomendadas actuales a normas, y hay una clara necesidad de consultar a ANC de ICAO.

1.4 CANSO quiere destacar la importancia de la protección de toda la información digital y los sistemas dentro del sistema de aviación. Esto es vital para asegurar la protección y seguridad del público en general, los pasajeros, la tripulación, el personal de tierra, las instalaciones de aviación y aeronaves contra actos de interferencia ilegales perpetrados en tierra o en vuelo. Se podría requerir de acciones específicas para mejorar este concepto en estados menos desarrollados, como se abarca bajo la iniciativa de ICAO “Ningún país se deja de lado (NCLB)”.

2. NECESIDAD DE UNA ACLARACIÓN SOBRE CIBERSEGURIDAD

2.1 CANSO destaca que hay un cierto grado de confusión en relación al término "Ciberseguridad". Se usa para hablar sobre la amenaza impuesta por antagonistas, además de la necesidad de evaluar y fijar vulnerabilidades en sistemas de TI. Además se usa para describir cómo implementar una planificación efectiva de contingencia en caso de resistencia.

2.2 CANSO enfatiza que una estrategia sólida de seguridad para la aviación civil debería considerar no solamente el nivel tecnológico de madurez, sino principalmente un enfoque metodológico protector para alcanzar el objetivo primario de la seguridad de la aviación. Esto puede lograrse sólo mediante un enfoque ascendente, incluyendo a toda la organización, teniendo en cuenta factores humanos.

2.3 El objetivo está claramente especificado en el *Concepto Operacional de Gestión de Tráfico Aéreo Mundial* (ICAO Doc. 9854) en el que el rol de la seguridad está bien descrito como esencial y presentado de una forma muy innovadora:

> *"Seguridad hace referencia a la protección contra amenazas que derivan de acciones intencionales (por ej. terrorismo) o acciones no intencionales (por ej. error humano, desastre natural) que pueden afectar a las aeronaves, personas o instalaciones en tierra. La seguridad adecuada es una expectativa importante en la comunidad del sistema de ATM. El sistema de ATM debe por lo tanto contribuir a la seguridad y el sistema de ATM, además de la información relacionada con la ATM, debe protegerse contra las amenazas de seguridad".*

2.4 Desde esta perspectiva, relacionada con las normas principales en la seguridad de la TI, el objetivo de brindar disponibilidad, integridad y confidencialidad hace referencia a la obligación general de los estados contratantes de garantizar la protección de los principales elementos de la aviación civil, de acuerdo a la Convención de Chicago y específicamente en el Apéndice 17 de ICAO (Seguridad).

3. UN NUEVO ENFOQUE

3.1 CANSO destaca que la protección de los activos relevantes, esenciales para la seguridad de la aviación civil puede diferir entre las partes interesadas de la aviación de acuerdo a sus metas; por ej. los gobiernos, los ANSP, las aerolíneas, los aeropuertos, los fabricantes, los militares, etc. Es posible identificar algunos de los temas de la ciberseguridad para la aviación, comunes para todos los miembros de la comunidad, definidos con necesidades específicas:

a) garantizar que la información importante sea accesible solamente para aquellos autorizados, para prevenir actos de interferencia ilegales de parte de amenazas internas, independientemente del servicio central del operador;

b) cumplir con la obligación, dependiendo del sentido común y *bona fide*, para identificar y abordar vulnerabilidades sobre sistemas críticos, para identificar la prudencia y la diligencia ordinaria;

c) extender la gestión de riesgos, al riesgo que deriva de la dependencia cada vez mayor de los recursos de TI de propiedad de un solo operador;

d) tener una gestión apropiada de respuesta para el manejo de incidentes y la gestión de crisis, incluyendo la planificación de contingencia;

e) evaluar impactos que derivan de brechas de (ciber) seguridad no sólo en el único operador sino también en la industria en general, en el marco del Programa Nacional de Seguridad de la Aviación Civil.

3.2 En otros términos, la ciberseguridad no es diferente del enfoque tradicional de la seguridad de la aviación, pero es una extensión natural de los principios básicos contenidos en el Apéndice 17 (Seguridad) y el material de guía, abordando las amenazas más comunes y las vulnerabilidades relacionadas con la seguridad física.

3.3 La amenaza cibernética a la aviación será probablemente uno de los principales temas de seguridad en cualquier programa nuevo de modernización, ya sea el Cielo Único Europeo (SES/Single European Sky), el proyecto de ATM Cielo Único Europeo (SESAR/Single European Sky ATM Research), Próxima Generación (NEXTGEN) y otros que se están desarrollando a nivel regional. Parece ser uno de los impulsores más relevantes en otras partes de la industria de la aviación. Como fuente crítica, la información debe ser tratada como cualquier otro activo esencial para la capacidad de supervivencia y el éxito de los sistemas de ATM. Todos estos programas, no limitados a la ATM sino también los que involucran operadores de aeronaves, aeropuertos, militares y otros, se basarán en el concepto de la Gestión de Información de Todo el Sistema (SWIM), facilitando el intercambio operacional de red centralizada de información y servicios en todo el sistema. El concepto SWIM mejorará la toma de decisiones colaborativa, ofreciendo mejor calidad de la información requerida sobre la necesidad de conocer la base en el momento oportuno para el receptor correcto. SWIM es el facilitador clave para el entorno tecnológico futuro de la aviación y su infraestructura crítica para la cual la seguridad debe ser considerada como un requisito clave por diseño.

3.4 En este sentido, mientras la seguridad general sigue siendo una obligación para los estados contratantes con implicancias sobre la soberanía nacional, la defensa, la inteligencia y el cumplimiento de la ley, la necesidad de considerar el carácter específico del entorno de la aviación necesita de una acción más efectiva.

3.4.1 Las iniciativas relevantes a nivel regional están en proceso o ya fueron implementadas. Solo para mencionar algunos resultados recientes: La posición de la Unión Europea sobre la ciberseguridad en el sistema de ATM expone claramente en la edición publicada de Reglamentación de la EC (Reg. 1035/2011) una clara relación entre las vulnerabilidades de la seguridad y prescribe requisitos obligatorios para la ciberseguridad. La Administración Federal de Aviación de Estados Unidos (FAA) en su oferta presentada al Senado de EE. UU. declara un objetivo relevante para la ciberseguridad (Sec. 4109) con el fin de desafiar objetivos, incluyendo un amplio conjunto de acciones para abordar temas de seguridad cibernética. Otros estados se están centrando también en su esfuerzo reglamentario sobre la ciberseguridad de la aviación en un modo similar.

3.4.2 Debido a la importancia de la ciberseguridad para la aviación civil, CANSO apoya totalmente toda iniciativa con el fin de llevar a cabo una integración total del tema de la ciberseguridad dentro de los programas de seguridad de la aviación nacional y regional y declara su disponibilidad total para participar de manera activa.

4. CONCLUSIÓN

4.1 La ciberseguridad en aviación es un tema a ser abordado metodológicamente y en modo realista, considerando implicancias e impactos en la industria general y en la confianza del público en general.

4.2 CANSO promueve una iniciativa internacional renovada bajo el liderazgo de ICAO y en un modo efectivo y sostenible bajo el principio “Ningún país se deja de lado”.

4.3 La iniciativa del grupo de trabajo de alto nivel sobre la industria (Cíber), siguiendo el Plan de Acción de Ciberseguridad firmado en diciembre de 2014, está desarrollando un marco para mejorar la cooperación voluntaria en este campo. Este programa liderado de la industria debe complementarse y apoyarse a través de aprobaciones reglamentarias y una consideración más profunda del tema interrelacionado en la aviación civil representado por la ciberseguridad.

5. RECOMENDACIONES

5.1 Se invita a la Asamblea a convocar a la Secretaría de ICAO como un tema de urgencia para hacer que la ciberseguridad sea una parte actual de la seguridad de la aviación en un modo efectivo y sostenible. Se solicita a la Asamblea que acepte las siguientes recomendaciones:

Que la Asamblea:

a) considere el contenido del informe y lo apruebe, reconociendo la relevancia y el impacto posible en la aviación civil;

b) acuerde en que ICAO desarrolle una estrategia nueva sobre la ciberseguridad en la aviación como un dominio vertical dentro de la seguridad de la aviación y emita material de guía, con el fin de armonizar las iniciativas actuales a nivel nacional y regional;

c) recomiende a los estados miembros centrar su atención en las vulnerabilidades en los sistemas y redes en lugar de en amenazas y considerar las implicancias en toda la industria de la aviación civil en su totalidad;

d) recomiende que se establezca un foro para que las firmas de aviación compartan mejores prácticas en un entorno seguro/confiado para que se puedan compartir las herramientas y técnicas efectivas que mejoran la seguridad en la tecnología futura y actual;

e) recomiende a los estados miembros que revisen las iniciativas presentadas durante AVSECP/27 para elevar a una norma las prácticas actuales recomendadas 4.9.1 y 4.9.2 del Apéndice 17.; y

f) Tenga en cuenta *la “Guía de evaluación de riesgos y ciberseguridad” de CANSO*[2].

— FIN —

[2] https://www.canso.org/canso-cyber-security-and-risk-assessment-guide