Cuestión 8 del Orden del Día: **Otros asuntos**

Concientización e instrucción sobre seguridad informática (ciberseguridad) de aviación civil

(Presentada por la Secretaría)

RESUMEN

Esta nota de estudio presenta información sobre las acciones que debieran considerarse adoptar para la protección de los datos que gestiona el AIM, de los ciberataques

REFERENCIAS

- Doc 8973/10ma Edición - Manual de Seguridad de la Aviación, Capítulo 18, *Amenaza de ciberataques contra sistemas críticos de tecnología de la información y las comunicaciones aeronáuticas.*
- Doc 9985 - Manual de seguridad de la gestión del tránsito aéreo, Capítulo 5, *Sistema de seguridad de la Tecnología de la Comunicación e Información (ICT) (incluida la ciberseguridad*).
- Resolución A39-19 de la Asamblea: *Formas de abordar la ciberseguridad en la aviación civil*

1. Introducción

1.1 La 39ª Asamblea de la OACI adoptó la Resolución 19, relacionada a la forma de abordar la ciberseguridad.

1.2 Mientras el progreso de la tecnología y la tecnología informática se mueven a muy alta velocidad, el crimen cibernético e informático se ha incrementado a nivel mundial afectando diferentes áreas vitales de organizaciones, empresas, instituciones financieras, y hasta las redes sociales, ataques a los cuales no escapa el sector aeronáutico. Por lo tanto, los ciberataques se han tornado como una más de las amenazas emergentes a los sistemas de tecnología de la información y las comunicaciones y datos críticos, así como otros involucrados en la aviación civil.

1.3 Los servicios de información aeronáutica/gestión de información aeronáutica funcionan como el centro de concentración, verificación y distribución de la información aeronáutica de los Estados, siendo por tanto sujetos a amenazas de ataques cibernéticos que podrían afectar la seguridad operacional de las operaciones aeronáuticas.

2 **Discusión**

2.1 La 39ª Asamblea de la OACI, a través de la Resolución A39-19: *Formas de abordar la ciberseguridad en la aviación civil*, exhortó a los Estados, entre otras cosas, a:

- Identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y los sistemas críticos de la aviación civil, y las graves consecuencias que pueden resultar de tales incidentes.

- Fomentar una interpretación común entre los Estados miembros de las ciberamenazas y riesgos y la formulación de criterios comunes para determinar cuáles bienes y sistemas son de carácter crítico y es preciso proteger.

- Fomentar la coordinación entre gobierno e industria con respecto a las estrategias, políticas y planes de ciberseguridad de la aviación, así como el intercambio de información para ayudar a identificar las vulnerabilidades críticas que sea necesario resolver.

- Formar y participar en asociaciones y mecanismos público-privados entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación.

- Establecer políticas y destinar recursos cuando sea necesario para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura; que sean resilientes; que tengan métodos seguros de transferencia de datos que garanticen su integridad y confidencialidad; que tengan métodos de vigilancia, detección y notificación de incidentes y que se lleven a cabo análisis forenses de los incidentes.

2.2 La industria aeronáutica, los proveedores de servicios de navegación aérea (ANSP) y las autoridades de aviación civil (AAC) dependen cada vez más de las comunicaciones y de las operaciones basadas en redes, por lo que los Estados deben esforzarse para modernizar la infraestructura informática y de red, conectando a los usuarios, los sistemas y los datos para brindar un acceso transparente y seguro, protegido de los incidentes de ciberseguridad.

2.3 Los incidentes cibernéticos pueden afectar a la comunidad aeronáutica mundial o a los sistemas individuales en muchos niveles. Estos incidentes pueden poner en peligro las comunicaciones y los intercambios de información entre las diversas partes involucradas de la aviación, afectando la seguridad operacional y la seguridad de la aviación, y perjudicando la continuidad del negocio aeronáutico.

2.4 Es importante que los Estados desarrollen material de instrucción sobre ciberseguridad y que la información sea compartida entre los actores involucrados en la aviación tales como las autoridades reguladoras, los proveedores de servicios a la navegación aérea, explotadores aéreos y de aeropuertos, especialistas de soporte en Tecnología Informática (IT) y otros colaboradores de la industria de aviación con la concientización básica sobre los riesgos de ciberseguridad.

2.5 Hay que reconocer que no todos los problemas de ciberseguridad que afectan a la seguridad operacional de la aviación civil se relacionan con actos ilícitos y/o intencionales, y que en consecuencia deberían resolverse aplicando sistemas de gestión de la seguridad operacional, pero es importante proteger de ciberamenazas a los sistemas de infraestructura de la aviación civil y los datos

críticos. El AIS/AIM, como gestor de información y datos de la aeronáutica de todo el Estado, debiera de comenzar unos procesos de concientización del personal sobre medidas que pudieran implementarse en la gestión de la información para mitigar las amenazas.

2.6 Se debe trabajar muy de cerca con el personal de redes e IT para proteger la información e implementar otras medidas de contingencias que pudieran ayudar en caso de ciberataques.

2.7 El Grupo Regional sobre Seguridad de la Aviación y Facilitación NAM/CAR y SAM OACI/CLAC (AVSEC/FAL/RG) comenzó a trabajar sobre este tema desde 2014. Sería importante identificar los puntos de contacto de este grupo en sus Estados, y comenzar a diseñar un trabajo en conjunto con ellos para acordar acciones de mitigación de los ciberataques a un área tan sensible como es el AIM.

3. **Acciones sugeridas;**

3.1 Se invita a la Reunión a:

a) tomar conocimiento el contenido de la presente nota de estudio; y

b) ubicar a la ciberseguridad en la agenda de trabajo del AIM

- FIN -