Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE ESTUDIO

DGAC/CAP/98 — NE/18
23/02/15

98ª Reunión de Directores Generales de Aeronáutica Civil de Centroamérica y Panamá (DGAC/CAP/98)

Ciudad de México, México, 2 al 4 de marzo de 2015

Cuestión 4 del Orden del Día: **Asuntos de Navegación Aérea**
4.5 Otros asuntos de navegación aérea

SEGURIDAD CIBERNÉTICA EN EL ÁMBITO DE LA NAVEGACIÓN AÉREA

(Presentada por CANSO)

RESUMEN EJECUTIVO	
La industria aeronáutica está evolucionando de una manera dinámica y sistemática, lo cual proporciona ventajas en el uso e intercambio de información digital para ofrecer un servicio de navegación aérea más eficiente y eficaz. Dicho cambio es muy positivo, sin embargo, existen riesgos relacionados al mismo, por tal motivo, es de mayor importancia vigilar e implantar planes de mitigación relacionados al riesgo cibernético.	
Acción:	CANSO desarrollo el documento de seguridad cibernética y evaluación de riesgos como un documento guía para los Proveedores de Servicios de Navegación Aérea y Estados. CANSO insta a los proveedores de servicios de navegación aérea y Estados en utilizar la guía de seguridad cibernética y evaluación de riesgos como un documento guía y educacional.
Objetivos Estratégicos:	• Seguridad Operacional • Capacidad y eficiencia de la navegación aérea • Seguridad de la aviación y facilitación
Referencias:	• Doc 9854 – *Concepto operacional de gestión del tránsito aéreo mundial* • CANSO Cyber Security and Risk Assessment guide

1. Introducción

1.1 La tendencia dentro del ámbito de la gestión de tránsito aéreo es el incremento del intercambio de la información digital y el conocimiento situacional proporcionado un espectro muy amplio para los interesados en la aviación. Mientras crece la eficiencia y productividad bajo el esquema de información digital, también aumenta la probabilidad de un ataque cibernético.

1.2 Las vulnerabilidades crecen por la demanda de intercambio de información correspondiente a la disponibilidad de información comercial digital, sistemas compartidos, infraestructuras de computación más avanzadas, arquitecturas de redes céntricas y operaciones.

1.3 Se estima que el intercambio de información de los futuros sistemas de gestión de tránsito aéreo no estarán limitados a comunicaciones de punto a punto, al contrario, se utilizaran sistemas abiertos e información de flujo basada en Internet. Estamos siendo testigos de un estilo hacia el aumento de tecnologías existentes, incremento de la interoperabilidad entre sistemas y el uso de automatización para optimizar la productividad. Lo anterior no es único en la industria de la aviación; otras industrias están aplicando información tecnológica para mejorar la eficiencia de operaciones reales permitiendo el diseño de nuevos métodos operativos.

1.4 Los beneficios se obtienen al permitir el intercambio y uso de la información de una forma expedita e ininterrumpida entre los usuarios y los sistemas, no obstante, el crecimiento en el uso de información tecnológica significa una mayor exhibición a los ataques cibernéticos.

1.5 Los riesgos son muy reales y serios, por tal motivo, los proveedores de servicios de navegación aérea deben desarrollar y ejecutar estrategias de seguridad y planes para asegurar la continuidad de las operaciones independientemente del riesgo.

2. Conclusiones

2.1 Entendiendo la importancia, se ha catalogado la seguridad cibernética como prioridad y un tema a tratar por medio del grupo de alto nivel de la industria de la OACI (IHLG). ACI, CANSO, IATA, ICCAIA y OACI están trabajando conjuntamente en una visión, estratégica y alineamientos para mitigar las amenazas que conlleve un conflicto con la seguridad cibernética.

2.2 CANSO colectivamente con sus afiliados, desarrollaron la guía de seguridad cibernética y evaluación de riesgos, misma que explica sobre las amenazas, métodos, motivos, seguridad cibernética en la gestión de tránsito aéreo, estándar globales de seguridad cibernética y metodología de riesgo, por mencionar algunos puntos de la guía. La guía se puede descargada por medio del siguiente enlace: https://www.canso.org/canso-cyber-security-and-risk-assessment-guide

2.3 La visión, estrategia y trabajos a desarrollar bajo el IHLG y el programa de trabajo del grupo de seguridad ATM (ASWG), comprenden una serie de entregables y tareas que están en línea y bajo el marco de la guía de CANSO sobre seguridad cibernética y evaluación de riesgos.

3. Acción sugerida

3.1 Se invita a la reunión a:

a) tomar nota de la información contenida en esta nota de estudio; y

b) en la medida de lo posible, utilizar la guía como un documento educativo y de conocimiento para las respectivas unidades de trabajo.

— FIN —