Organización de Aviación Civil Internacional
Oficina Regional Sudamericana
Décimo Cuarta Reunión de Autoridades de Aviación Civil de la Región Sudamericana (RAAC/14)
(Santiago, Chile, 27, 28 y 30 de Octubre de 2015)

RAAC/14-NE/16
06/10/15

Cuestión 3 del Orden del Día: **Análisis de los resultados obtenidos en la seguridad de la aviación en la Región SAM**

GUÍA DE SEGURIDAD CIBERNÉTICA Y EVALUACIÓN DE RIESGOS

(Presentada por CANSO)

RESUMEN

Mientras que la gestión de tránsito aéreo entra a un esquema más directo de estándares y sistemas, los proveedores de servicios de navegación aérea (ANSP) precisan de mayor entendimiento sobre los riesgos que enfrentan y tener mayor flexibilidad y receptividad en acciones para contrarrestarlas.

A medida que la amenaza cibernética continúa evolucionando, la gestión de tránsito aéreo (ATM) debe evaluar la vulnerabilidad de los procesos y de los ataques, ya sea a partir de fuentes internas o externas, y poner en marcha las medidas de mitigación necesarias.

Para apoyar a los ANSP´s, CANSO publicó la Guía de seguridad cibernética y Evaluación de Riesgos, misma que recomienda la elaboración de una evaluación como un primer paso para la comprensión y la gestión de los riesgos de seguridad cibernética en los sistemas, activos, datos y capacidades del ATM.

Referencias:

- OACI DOC. 9854
- CANSO - Guía de Seguridad Cibernética y Evaluación de Riesgos

***Objetivos Estratégicos de la OACI*:**	*A - Seguridad* *D - Desarrollo económico del Transporte Aéreo* *E - Protección de medio Ambiente*

1. Introducción

1.1 En respuesta a la creciente amenaza de ataques cibernéticos en los sistemas de gestión del tráfico aéreo (ATM), CANSO publicó la guía de seguridad cibernética y Evaluación de Riesgos el pasado junio 2014, como una guía práctica que apoya a incrementar el conocimiento de seguridad cibernética en todo el sector ATM. La Guía ofrece a los afiliados de CANSO una introducción a la seguridad cibernética en ATM e incluye una visión general de las amenazas, riesgos y las motivaciones de los actores que amenazan el sistema; al igual que algunas consideraciones para la gestión de riesgos cibernéticos y sugerencias para la ejecución de un programa de seguridad cibernética. Los apéndices incluyen además

información sobre las normas; un marco para la seguridad cibernética; y algunas orientaciones prácticas para la realización de una evaluación de riesgos cibernéticos - un primer paso que se recomienda para el conocimiento y la gestión de los riesgos de seguridad cibernética en los sistemas, activos, datos y capacidades de ATM.

2. Discussion

2.1 Históricamente, la información y las comunicaciones (ICT, por sus siglas en Inglés) en los sistemas ATM han estado utilizando enlaces punto a punto para intercambiar información entre los sistemas dentro de un ANSP. Estas soluciones han funcionado, pero son costosas, con tiempos de desarrollos extensos y generalmente no son flexibles. Esto está cambiando con la adopción de las normas internacionales (IT) de redes estándares arquitectónicos, así como el uso de sistemas comerciales (COTS) de software, hardware y servicios. Programas de modernización ATM como SESAR, NextGen y acciones de colaboración de Japón para la renovación de los sistemas de tránsito aéreo (CARATS) han sido diseñados con esto en mente.

2.2 Mientras los sistemas del ATM evolucionan hacia normas y sistemas abiertos, los ANSPs tendrán que adquirir mayores conocimientos sobre las amenazas que enfrentan, deben ser más flexible y receptivos en sus acciones para contrarrestarlos. La amenaza cibernética es en continua evolución y cada vez más sofisticados. La difusión de los conocimientos de los expertos que desarrollan los virus está incrementando y se distribuye a través de herramientas que pueden ser utilizadas por cualquier persona. Por ejemplo, una vez que se identificó Stuxnet[1] fue adoptado y alteró a nivel de código y redistribuido por los creadores de virus de alto nivel rápidamente. Luego se incorpora a kits de herramientas de ciber-delincuentes y vendió en la "red oscura" - redes privadas donde las conexiones se hacen sólo entre compañeros de confianza. El mundo cibernético es de creciente interés para los delincuentes que están creando un nivel profesional y una cadena de suministro global para llevar a cabo la guerra cibernética. El potencial de un ataque cibernético contra la aviación utilizando el sistema ATM también es muy real.

2.3 La gestión de tránsito aéreo debe hacer frente a la amenaza cibernética mediante la evaluación de la vulnerabilidad de los procesos y activos con mayor riesgo, si éstas implican personal interno o terceros. La amplia gama de posibles amenazas cibernéticas y la integración de los sistemas moderna ATM, exigen un enfoque integral y la participación de todos los participantes en el entorno ATM. Es importante destacar que las evaluaciones de riesgos de los sistemas ATM deben tener en cuenta, no sólo ataques relacionados con el terrorismo, sino que también incluyen los ataques perpetrados por hackers que deseen tener acceso a los sistemas y causar la interrupción, o los ataques llevados a cabo con fines de espionaje o comerciales por parte de actores estatales. Estos pueden ser igualmente perjudiciales y poner en peligro la seguridad operacional y la integridad del sistema de aviación.

2.4 En Junio 2014 y como herramienta de apoyo, CANSO publico la Guía de Seguridad Cibernética y Evaluación de Riesgos, misma que está disponible en https://www.canso.org/canso-cyber-security-and-risk-assessment-guide. La guía tiene como intención proporcionar a los ANSP una introducción a la seguridad cibernética en ATM e incluye una visión general de las amenazas, los riesgos y las motivaciones de los actores que amenazan el sistema; algunas consideraciones para la gestión de riesgos cibernéticos; y sugerencias para la implementación de un programa de seguridad cibernética. Entre las conclusiones de la Guía, se identifica que la seguridad cibernética debe ser considerada como parte de la seguridad ATM y, en general, de la seguridad de la aviación en general, con el fin de cumplir con las expectativas sociales de protección y seguridad del sistema de aviación.

[1] Stuxnet es un virus de computadora que fue descubierto en junio de 2010, diseñado para atacar controladores industriales de lógica programable (PLC). Habría había arruinado casi una quinta parte de Irans centrifugadoras nucleares.

2.5 La guía recomienda realizar evaluaciones como como primer paso para comprender y gestionar el riesgo cibernético dentro de los sistemas, datos y capacidades ATM.

3. Acciones sugeridas

3.1 Se invita la reunión a:

a) Tomar nota de la información presentada en esta nota de estudio; y
b) Recomendar y utilizar la guía como documentación de apoyo y adicional.

- FIN -