Organización de Aviación Civil Internacional
Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS)
Decimoctava Reunión del Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS/18)
Punta Cana, República Dominicana, 9 al 14 de abril de 2018

Cuestión 3 del Orden del Día: **Actividades de navegación aérea a nivel global, inter e intrarregionales**
3.2 Seguimiento en la implantación de las actividades a nivel global, inter e intrarregionales

CONCIENCIACIÓN E INSTRUCCIÓN SOBRE SEGURIDAD INFORMÁTICA (CIBERSEGURIDAD) DE AVIACIÓN CIVIL

(Presentada por la Secretaría)

RESUMEN

Esta Nota de estudio presenta información relevante sobre las acciones adoptadas por el Programa de Seguridad Informática (cibersecurity) del Grupo Regional sobre Seguridad de la Aviación y Facilitación NAM/CAR y SAM OACI/CLAC (AVSEC/FAL/RG). La acción sugerida se presenta en la Sección 4 de esta Nota de Estudio.

REFERENCIAS

- Anexo 17, Método Recomendado 4.9.
- 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).
- Carta a los Estados NACC71408 de fecha 24 de enero de 2018, sobre la invitación al Taller sobre Ciberseguridad de la aviación civil, (Montego Bay, Jamaica, 20 al 23 de marzo de 2018.

1. Introducción

1.1 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. Por lo tanto los ciber-ataques se han tornado como una más de las amenazas emergentes a los sistemas de tecnología de la información y las comunicaciones y datos críticos, y otros involucrados en la aviación civil.

1.2 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, y finalmente de acuerdo a la Conclusión 7/4 del AVSEC/FAL/RG/7, que se reunió en la Oficina Regional de la OACI para Sudamérica, del 4 al 6 de octubre de 2017, el Grupo de trabajo sobre ciberseguridad liderado por Jamaica, completó el desarrollo de un material de instrucción guía sobre esta materia para los Estados Miembros del AVSEC/FAL/RG; y en colaboración con el Comité Inter-Americano contra el Terrorismo (CICTE) de la Organización de estados Americanos (OEA), y gracias a la Autoridad de Aviación Civil de Jamaica que fue el anfitrión, se llevó a cabo un Taller sobre Ciberseguridad de la aviación civil en Montego Bay, Jamaica, del 20 al 23 de marzo de 2018.

2 Discusión

2.1 El propósito de este taller fue el de validar el material de instrucción para el taller de Ciberseguridad y proveer a los entes reguladores de la aviación civil, a 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 concienciación básica sobre los riesgos de ciberseguridad. 17 participantes de 14 Estados de las Regiones Norteamérica, Centroamérica, el Caribe y Sudamérica participaron en este taller, y apreciaron el desarrollo de dicha guía para contrarrestar esta forma de ataque que se viene incrementando, y como un potencial riesgo a la aviación civil.

2.2 El CICTE de OEA apoyo con 12 becas consistentes en pasajes aéreos y alojamiento. La Administración federal de Aviación, y la Administración de Seguridad del Transporte de los estados Unidos participaron en el evento, mientras que el representante de *Transport Canada* evaluó el material como parte de la validación del material de instrucción para futuros ajustes.

2.3 El taller incluyó la identificación de ciber amenazas y riesgos, los motivos para los ciber ataques, así como una metodología para gestionar y mitigar los ciber ataques. Este taller de concienciación ayudó a los participantes a estar mejor preparados para conducir evaluaciones de riesgo y preparar el plan de la gestión del riesgo sobre ciber ataques. El material del taller está diseñado para ayudar a los estados en alcanzar la propuesta de cambio del actual Método Recomendado 4.9 (según lo previsto, será una Norma aplicable en noviembre de 2018) del Anexo 17 de la OACI, que requiere que los Estados identifiquen sus sistemas de tecnología de la información y las comunicaciones y datos críticos que se empleen para los fines de la aviación civil, y que en función de una evaluación de riesgos elaboren y lleven a la práctica las medidas que correspondan para protegerlos de interferencia ilícita.

2.4 La Segunda Fase de este Proyecto incluye la realización de un taller similar para los estados de habla hispana, usando los mismos instructores de Jamaica con interpretación simultánea, en el último trimestre de 2018. Se llevaron a acabo conversaciones con la representante de OAS-CICTE para puedan continuar apoyando con este Proyecto de Ciberseguridad en la región. En la Tercera Fase de este Proyecto se considerará la traducción del material de instrucción al español para realizar un taller junto con un ejercicio de mesa, o si posible un simulacro, para el beneficio de los estados Miembros del AVSEC/FAL/RG.

3 Conclusión

3.1 Será importante que los estados eleven la concienciación sobre este delicado asunto, y designar recursos para considerar la instrucción de personal idóneo de todos los niveles de aviación, incluyendo sus especialistas en Tecnología de la Información y Comunicaciones (ICT), tomando ventaja del desarrollo del taller arriba mencionado. Esto ayudará a establecer Equipos de respuesta a incidentes cibernéticos/informáticos (CSIRT) al nivel de aviación, y para desarrollar procedimientos bajo los criterios nacionales para que sean implementados por Equipos de respuesta a emergencias cibernéticos/informáticos (CSERT) para gestionar y contrarrestar potenciales ataques a la aviación civil.

3.2 Una vez que los criterios y los procedimientos sean establecidos, y se hayan conformado los CSIRT y CSERT, debería de considerarse la realización de ejercicios como parte de sus planes de contingencia.

4 Acciones sugeridas

3.1 Se invita a la Reunión a:

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

b) asegurar la concienciación de la comunidad aeronáutica sobre este delicado asunto, y enviar a sus participantes a futuros eventos de instrucción sobre ciberseguridad.

— END —