



Organización de Aviación Civil Internacional
Comisión Latinoamericana de Aviación Civil
Grupo Regional sobre Seguridad de la Aviación y
Facilitación NAM/CAR/SAM OACI/CLAC (AVSEC/FAL/RG)

NOTA DE ESTUDIO

AVSEC/FAL/RG/7 — NE/09
05/09/17

**Séptima Reunión del Grupo Regional sobre Seguridad de la Aviación y Facilitación
NAM/CAR y SAM OACI/CLAC (AVSEC/FAL/RG/7)
Lima, Perú, del 4 al 6 de octubre de 2017**

**Cuestión 4 del
Orden del Día:**

**Programas y proyectos - Seguridad de la Aviación (AVSEC)
4.4 Ciberseguridad de la aviación civil**

AVANCE SOBRE EL PROYECTO CONCIENCIA DE LA CIBERSEGURIDAD

(Presentada por Jamaica)

RESUMEN EJECUTIVO

En 2014 el Secretario General de la OACI pidió a los Estados miembros ser más proactivos y promover una fuerte cultura de la ciberseguridad. Esto fue nuevamente enfatizado en el Plan global sobre seguridad de la aviación 2017 de la OACI, que la identificó como uno de los tres riesgos emergentes que enfrenta la aviación civil internacional. El Grupo de Trabajo (WG) sobre conciencia de la ciberseguridad desarrollo un Curso sobre conciencia de la ciberseguridad para ser impartido en la región con la ayuda de la Organización de Estados Americanos (OEA). Esta Nota de estudio proporciona una actualización del avance sobre el proyecto e informa a los Estados la cooperación entre organizaciones internacionales y regionales para promover la impartición de un Taller Regional sobre conciencia de la ciberseguridad.

Acción:	La acción sugerida se presenta en la Sección 4.
Objetivos Estratégicos:	• Seguridad de la aviación y facilitación
Referencias:	• Plan global sobre seguridad de la aviación de la OACI 2017 • Resolución A39-19 de la Asamblea — Formas de abordar la ciberseguridad en la aviación civil • Informe Final de la Reunión AVSEC/FAL/RG/6, 2016 • "Estrategia para la Ciberseguridad Nacional", Gobierno de Jamaica, 2015 • "Tendencias de Ciberseguridad en América Latina y el Caribe", Informe de la Organización de los Estados Americanos, junio de 2014 • "Uniendo a la aviación ", Comunicado de Prensa de la OACI, 2014 • Doc 9941 <i>Guía para la preparación de programas de instrucción TRAINAIR Plus</i>, 2011

1. Introducción

1.1 La cambiante naturaleza de la amenaza a la aviación civil se ha tornado cada vez más evidente en tanto el mundo se sumerge profundamente en la era tecnológica. La gran sofisticación con la que se realizan ataques calculados en nuestra industria, justifica un nuevo paradigma en el modo en el que abordamos estos nuevos desafíos. Esto también requiere trabajar en conjunto como Estados para implementar planes coherentes para abordar el riesgo emergente. El ciberterrorismo y otros crímenes cibernéticos, así como nuestra habilidad para responder adecuadamente a incidentes críticos de esta naturaleza, son una preocupación mundial creciente.

1.2 La Resolución A39-19 de la Asamblea, “*Formas de abordar la ciberseguridad en la aviación civil*”, reafirma y expande el acuerdo inicial de diciembre de 2017, cuando la OACI firmó un acuerdo inicial con cuatro organizaciones internacionales para alinear sus acciones sobre amenazas cibernéticas. La meta común del acuerdo firmado por las cinco organizaciones internacionales de aviación civil, como subrayó el entonces Secretario General de la OACI, fue “*trabajar más eficientemente en conjunto para establecer y promover una cultura y estrategia fortalecidas sobre ciberseguridad para el beneficio de todas las acciones de la industria*”. El Plan global sobre seguridad de la aviación (GASeP) de la OACI diseminado en mayo de 2017, ahora hace eco del acuerdo inicial y reitera y apoya la preocupación creciente que identificaron las regiones de Norteamérica, Centroamérica, Caribe y Sudamérica (NAM/CAR/SAM) en la Quinta Reunión del Grupo Regional AVSEC/FAL celebrada en Lima, Perú, en junio de 2015.

2. Resumen de actividades

2.1 Como parte del Plan estratégico 2016/2017 del AVSEC/FAL/RG, los países miembros acordaron incluir el desarrollo de un taller sobre conciencia de la ciberseguridad. El objetivo del grupo de trabajo es reportar sobre el avance del proyecto e informar a los Estados sobre la cooperación entre organizaciones internacionales y regionales para promover la impartición de un Taller regional sobre conciencia de la ciberseguridad.

2.2 El grupo de trabajo identificó tres tareas principales: revisión de documentación existente, consultas con expertos en ciberseguridad dentro de la región y otras agencias regionales, y la identificación y el uso de Desarrolladores de cursos para Conjuntos de materiales didácticos (STP).

2.3 La revisión de la documentación existente realizada por CANSO, AIAA, la Unión Europea, OEA y otras agencias, a la base de datos electrónica de la literatura actual, se llevó a cabo en agosto de 2015 y se mantuvo con la adición de la literatura de 2016-2017. La participación en conferencias sobre ciberseguridad regionales e internacionales proporcionaron una plataforma para presentar el trabajo realizado por el grupo de trabajo, principalmente en la Conferencia regional de la OEA sobre ciberseguridad, llevada a cabo en Bogotá en septiembre de 2016, así como la Cumbre y exhibición inaugural de la OACI sobre ciberseguridad llevada a cabo en Dubai en abril de 2017.

2.4 Se solicitó y recibió orientación técnica a través del Instituto de Instrucción de Aviación Civil de Jamaica, miembro Trainair Plus de la OACI, sobre cómo desarrollar el Taller sobre conciencia de la ciberseguridad para la industria. Como parte de los miembros del equipo de desarrollo se incluyó a un consultor de crímenes cibernéticos y seguridad de la aviación y al jefe del equipo de respuesta de ciberseguridad de Jamaica.

2.5 El primer borrador del taller se completó en enero de 2017 y se realizaron consultas iniciales con la OEA para recibir financiamiento y apoyo en la traducción para el Taller regional sobre ciberseguridad 2017/2018. En junio de 2017, el Secretario Ejecutivo del Comité Interamericano contra el Terrorismo (CICTE) de la OEA indicó formalmente que ellos apoyarían la impartición se una serie de talleres sobre ciberseguridad para la región, iniciando en el primer trimestre de 2018.

3. Discusión

3.1 Se acordó que los Estados dentro de la región deberán continuar adoptando acciones que vayan de acuerdo con el Plan global sobre seguridad de la aviación de la OACI 2017 y la Resolución A39-19 de la Asamblea para abordar adecuadamente los desafíos de las amenazas cibernéticas al sistema de aviación civil. Se anticipa que la impartición y la implementación del Taller sobre Conciencia de la ciberseguridad será parte del marco de trabajo para mejorar la capacidad regional para la identificación del riesgo y para la aplicación de medidas apropiadas para mitigarlas.

4. Acciones sugeridas

4.1 Se invita a la Reunión a:

- a) Promover la cultura de ciberseguridad entre el personal de la Autoridades de Aviación Civil, y la comunidad nacional de aviación civil nacional;
- b) Tomar provisiones para insertar dentro sus presupuestos, la participación en el futuro Taller sobre ciberseguridad 2018/2019
- c) Compartir información sobre ciberseguridad a través de la Secretaría del AVSEC/FAL/RG y utilizando la red de puntos de contacto (PoC) de la OACI; e
- d) Incluir preocupaciones sobre ciberseguridad en la conducción de sus evaluaciones de riesgos de la seguridad de la aviación, y adoptar las medidas que correspondan.

APÉNDICE
CALENDARIO DEL INSTRUCTOR

Guía del instructor				Código del taller: Ciberseguridad en la aviación civil	
Calendario				Duración: 3 días laborales	
Título del curso: Ciberseguridad en la aviación civil				Publicado en: Abril de 2017	
				Publicado por: Autoridad de Aeronáutica Civil de Jamaica	
Día	Sesiones	Módulo Núm.	Título del Módulo	Material del aprendizaje	Ayudas visuales
1	1-3	1	Introducción al curso	H1.1 – 1.3	Diapositivas 1.1 – 1.10
1	3-8	2	Aspectos fundamentales en ciberseguridad para sistemas de aviación	H2.1 – 2.5	Diapositivas 2.1 – 2.37
1-2	9 - 14	3	Identificación de infraestructura crítica y las motivaciones / métodos sobre ataques cibernéticos	H3.1 – 3.2 Apéndice 3.1 – 3.3	Diapositivas 3.1 – 2.28
2 - 3	15-17	4	Protección de información crítica y de sistemas de tecnologías de la comunicación	H 4.1 – 4.24	Diapositivas 4.1 – 2.37
3	17-24	5	Mejora en la planeación de estrategias para infraestructura crítica y sistemas aeronáuticos de información y tecnologías de la comunicación	H 5.1 Apéndice 5.1 – 5.2b	Diapositivas 5.1 – 5.58
3	24-26	6	C-SIRT Respondiendo a incidentes de ciberseguridad	H 6.1	Diapositivas 6.1 -
3	27	7	Actividades de clausura	H 7.1	Diapositivas 7.1 – 7.5