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/9 — NE/23 Rev.1
27/03/19

Novena Reunión del Grupo Regional sobre Seguridad de la Aviación y Facilitación NAM/CAR y SAM OACI/CLAC (AVSEC/FAL/RG/9)

Santo Domingo, República Dominicana, del 25 al 29 de marzo de 2019

Cuestión 7 del Orden del Día: **Instrucción, cooperación y asistencia**

7.1 Actualización de la Sección de apoyo a la implementación y desarrollo – Seguridad de la aviación (ISD-SEC)

LECCIONES APRENDIDAS EN CIBERSEGURIDAD

(Presentada por la Secretaría)

RESUMEN EJECUTIVO	
Esta Nota de Estudio presenta los avances de la OACI en ciberseguridad y las iniciativas realizadas en este campo en las regiones NAM, CAR y SAM. La nota también presenta conclusiones y recomendaciones extraídas de las actividades en ciberseguridad realizadas para su consideración por el Grupo Regional y para su posible presentación al Panel de Expertos en Seguridad de la Aviación (AVSECP).	
Acción:	La acción sugerida se presenta en la Sección 5.
Objetivos Estratégicos:	• Seguridad de la aviación y facilitación
Referencias:	• Resoluciones adoptadas por la Asamblea - 39ª Sesión • Plan de Acción de Ciberseguridad en la Aviación Civil – 5 de diciembre de 2014

1. Introducción

1.1 En la 39ª Sesión de la Asamblea de la OACI hubo dos resoluciones principales en Seguridad de la Aviación Civil (AVSEC). La primera fue la Resolución de la Asamblea de la OACI A39-18 "Política AVSEC Consolidada", que establecía las áreas AVSEC prioritarias para el trienio actual (2017–2019) y sentaba las bases para el desarrollo del Plan Global de Seguridad de la Aviación (GASeP).

1.2 La segunda fue la Resolución A39-19, "Direccionamiento de la Ciberseguridad en la Aviación Civil" en donde se reconocía que *"… el sistema global de aviación es un sistema altamente complejo e integrado que comprende información y tecnologías de comunicación críticas para la seguridad (safety y security) de las operaciones de aviación civil"*. El sector de la aviación depende de *"la*

disponibilidad de la información y de los sistemas tecnológicos de comunicaciones, así como de la integridad y confidencialidad de los datos".

1.3 El rápido desarrollo de nuevas tecnologías en un mundo cada vez más digitalizado y conectado no solo ha creado oportunidades, sino también nuevas áreas de amenaza. Los ciberincidentes o ciberataques representan nuevas amenazas que, en caso de un mayor desarrollo, pueden fácilmente afectar sistemas críticos de aviación civil en todo el mundo. La declaración de ciberseguridad invita a los Estados e Industria a desarrollar un entendimiento común de la amenaza y una estrategia común para combatir dicha amenaza. Esta es también un llamado para una aproximación global a un problema global, que solo puede ser mitigado uniendo esfuerzos y colaborando.

2. Avances de la OACI en Ciberseguridad

2.1 El año 2018 ha supuesto un importante avance para promover la cultura en ciberseguridad y la colaboración entre Estados e industria. Tras el trabajo en ciberseguridad coordinado por el Panel de Expertos en Seguridad de la Aviación (AVSECP), la Enmienda 16 al Anexo 17, aplicable desde el 16 de noviembre de 2018, contiene la primera norma relacionada con ciberseguridad (4.9.1): *"Cada Estado contratante se asegurará de que los explotadores o entidades definidos en el programa nacional de seguridad de la aviación civil u otra documentación nacional pertinente 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".*

2.2 Asimismo, la Práctica Recomendada 4.9.2 ha sido reformulada como se lee ahora: "*Cada Estado contratante debería asegurarse de que las medidas en aplicación protejan, según corresponda, la confidencialidad, integridad y disponibilidad de los sistemas y/o datos críticos identificados. Las medidas deberían incluir, entre otras cosas, características de seguridad en el diseño, seguridad de la cadena de suministro, separación de redes y protección o limitación de las capacidades de acceso remoto, según corresponda y de acuerdo con la evaluación de riesgos efectuada por las autoridades nacionales correspondientes".*

2.3 Más aún, la OACI estableció el Grupo de Estudio de la Secretaría en Ciberseguridad (SSGC), siguiendo las instrucciones de la Asamblea, para guiar hacia un plan de trabajo integral en este campo. Entre los principales trabajos de este grupo está el borrador de la "Estrategia en Ciberseguridad de la OACI" y el estudio de viabilidad de un Panel de Ciberseguridad, ambos en consideración durante la 216ª Sesión del Consejo de la OACI (Montreal, del 18 de febrero al 15 de marzo 2019).

2.4 Dentro del SSGC se ha formado además el Subgrupo de Investigación en Aspectos Legales de Ciberseguridad, cuyos objetivos son la categorización de ciberamenazas y el análisis del marco legal internacional actual y provisiones legales de los Estados en este campo.

3. Iniciativas en ciberseguridad en las regiones NAM, CAR y SAM

3.1 Durante el año 2018 y este año 2019, en las regiones NAM, CAR y SAM se han organizado distintas actividades en ciberseguridad para promover un entendimiento común de las ciberamenazas y sus riesgos; compartir experiencias y buenas prácticas entre Estados e industria; y, en definitiva, aplicar consistentemente mecanismos de coordinación, reporte y gestión de riesgos en ciberseguridad.

3.2 La Autoridad de Aviación Civil de Jamaica (JCAA), en coordinación con el Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos (OAS-CICTE) y el Grupo Regional AVSEC/FAL, organizó el Taller sobre Ciberseguridad en Aviación, en Montego Bay, del 20 al 23 de marzo de 2018, cuyo objetivo fue concienciar a autoridades e industria de aviación civil de las ciberamenazas basándose en ejemplos reales ocurridos en los últimos años.

3.3 La Administración Federal de Aviación de los Estados Unidos (FAA), por su parte, organizó un ejercicio de simulación sobre ciberseguridad en Washington, D.C. del 17 al 19 de julio de 2018, orientado a los Estados del Caribe. El ejercicio incluyó dos escenarios y un recorrido del Centro de Control de Tráfico Aéreo de la FAA y del Centro de Ciberseguridad e Integración de Comunicaciones (NCCIC) del Departamento de Seguridad Nacional (DHS), para observar cómo Estados Unidos maneja la ciberseguridad y cómo coordina entre las entidades gubernamentales.

3.4 Del 4 al 6 de diciembre de 2018 se celebró en la Oficina Regional NACC de la OACI un Taller de Ciberseguridad en Aviación, en donde participaron Estados, industria y organizaciones internacionales. La primera sesión del Taller se enfocó en las iniciativas y buenas prácticas internacionales aplicadas no solo en aviación; el resto de las sesiones abarcaron la ciberseguridad para proveedores de servicios de navegación aérea (ANSPs), aerolíneas y aeropuertos.

3.5 Con el material del Taller de Jamaica traducido al español, se organizó un nuevo Taller sobre Ciberseguridad de la Aviación Civil en Buenos Aires, del 19 al 22 de febrero de 2019, orientado a la concienciación en ciberseguridad de las autoridades y la industria.

4. Lecciones aprendidas y recomendaciones en ciberseguridad

4.1 Tras los conocimientos adquiridos y las experiencias compartidas en las actividades antes mencionadas, la presente nota de estudio intenta resumir las principales conclusiones y lecciones aprendidas por los Estados a la hora de implementar la Norma 4.9.1 y la Práctica Recomendada 4.9.2 para su consideración por el Grupo Regional sobre Seguridad de la Aviación y Facilitación NAM/CAR y SAM OACI/CLAC (AVSEC/FAL/RG):

- Las ciberamenazas a las que se ve expuesta la aviación civil y los desafíos a los que se enfrenta su industria (ej. confidencialidad e integridad de datos, disponibilidad de los sistemas, amenazas internas) son, en gran parte, similares a los que se ven expuestos otros sectores (banca, seguros, gobierno, entretenimiento). Por tanto, muchas de las medidas que explotadores y entidades de aviación civil deberían aplicar son las mismas ya aplicadas en sectores con mayor experiencia y recursos (sector financiero).
- Al ser la ciberseguridad una materia transversal a varios sectores e infraestructuras críticas de los Estados, las políticas y regulación aplicables a la protección de datos críticos y de sistemas de tecnología de la información y las comunicaciones son establecidas por autoridades especializadas (ej. autoridades estatales competentes en telecomunicaciones) con poca relación con aviación civil, por lo que es conveniente verificar qué lineamientos generales en ciberseguridad ya existen en cada Estado.

- Varias organizaciones internacionales y regionales desarrollan material guía en ciberseguridad y ofrecen información contrastada sobre el nivel de madurez de los Estados en ciberseguridad (ej. política y estrategia; marcos legales; tecnologías):

  - La Unión Internacional de Telecomunicaciones (UIT) estableció en 2007 la Agenda Global de Ciberseguridad (GCA) que abarca cinco pilares: medidas legales; medidas técnicas y procedurales; estructura organizacional; desarrollo de capacidad; y cooperación internacional. ITU también ofrecen asistencia técnica para la protección de infraestructuras críticas, instrucción y organización de simulacros. Desde el año 2014, publican el Índice Global de Ciberseguridad (GCI) que muestra el grado de compromiso de los Estados con la GCA (http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx).

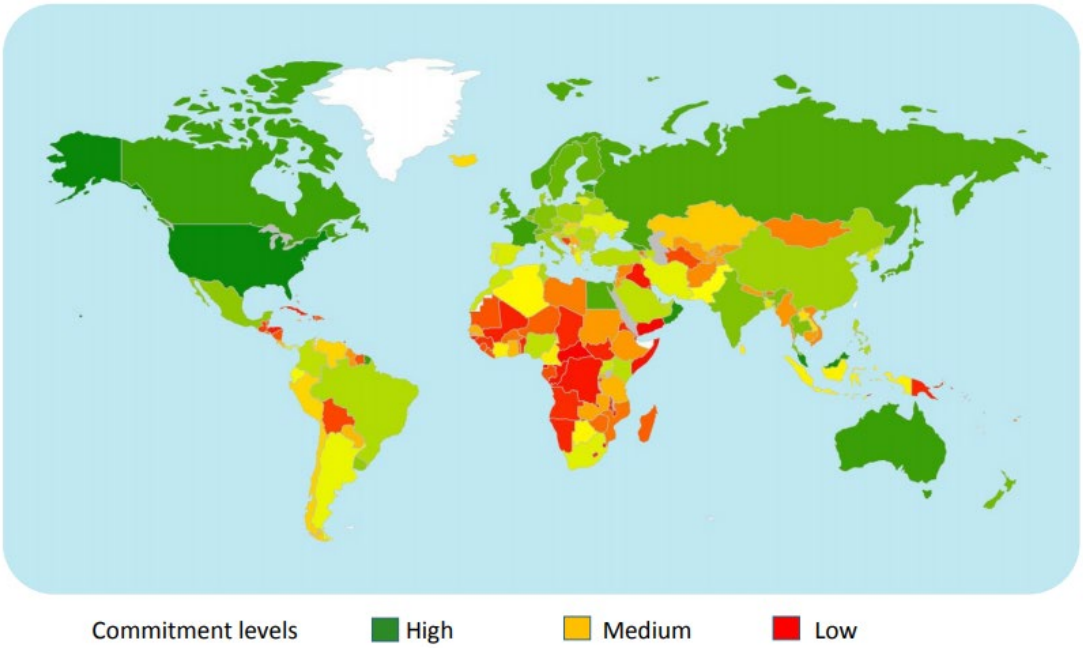

Figura 1. Resultados del Índice Global de Ciberseguridad (GCI) en 2017

  - La Organización de Estados Americanos (OEA) mantiene un observatorio de la ciberseguridad en América Latina y el Caribe (http://observatoriociberseguridad.org), donde se ofrecen estadísticas y un resumen de las iniciativas en ciberseguridad de cada uno de los Estados miembros de la OEA. Además, en su página web dedicada a la ciberseguridad (www.sites.oas.org/cyber/EN/Pages/Directory/Default.aspx) mantiene un repositorio de documentos guía (ej. manual para el manejo de incidentes en ciberseguridad) y un listado actualizado de CERT/CIRT/CSIRT (Equipos de Respuesta a Emergencias Informáticas/Equipos de Respuesta a Incidentes Informáticos/Equipos de Respuesta a Incidentes de Seguridad Informática) por Estado.

- Tanto los inspectores AVSEC nacionales como los auditores AVSEC de la OACI deberían ser conscientes y hacer uso del material y herramientas ya disponibles para hacer una primera evaluación de los Estados en ciberseguridad. La información recabada debería servir para determinar si un Estado ha dictaminado normativa y/o recomendaciones en materia de ciberseguridad aplicables a los explotadores o entidades de aviación civil que manejan datos críticos y/u operan infraestructuras y sistemas de tecnología de la información y comunicaciones vitales para el correcto funcionamiento del transporte aéreo.
- En general, a los Estados que tienen un CERT/CIRT/CSIRT nacional establecido se les presupone una capacidad básica para identificar, defender, responder y manejar ciberamenazas. Los CERT/CIRT/CSIRT no solo ofrecen servicios reactivos, sino que pueden involucrarse en servicios proactivos como evaluaciones de riesgos y auditorías de ciberseguridad. Sin embargo, hay que tener en cuenta que existen muchas tipologías de CERT/CIRT/CSIRT: gubernamentales (dan servicio solo a entidades del sector público), sectoriales (atienden a las entidades de un sector crítico como salud o banca), académicos, militares.
- Los explotadores y entidades de aviación civil conscientes de la criticidad de los datos que manejan y sistemas que operan suelen confiar el monitoreo de la infraestructura de red y la protección de sus datos a un Centro de Operaciones de Red/Centro de Operaciones de Seguridad (NOC/SOC) externo, normalmente especializado en el sector (ej. Indra, Thales, SITA), aunque los grandes operadores también pueden invertir en equipos y capacitación de personal para tener su propio NOC/SOC. Los NOC/SOC realizan un estudio de las necesidades del cliente y ofrecen una arquitectura y tecnología de seguridad con base en sus necesidades operativas, cumpliendo casi de forma automática con la Práctica Recomendada 4.9.2.
- Las actuales Normas y Métodos Recomendados (SARPS) en ciberseguridad contenidos en el Anexo 17 tienen en cuenta la preparación de la industria y sus avances en este terreno. En este sentido, la OACI firmó el Plan de Acción de la Aviación Civil en Ciberseguridad en diciembre de 2014, junto al Consejo Internacional de Aeropuertos (ACI), la Organización Civil de Proveedores de Servicios de Navegación Aérea (CANSO), la Asociación del Transporte Aéreo Internacional (IATA) y el Consejo Coordinador Internacional de Asociaciones de la Industria Aeroespacial (ICCAIA), con una clara hoja de ruta y objetivos que, al día de hoy, deben estar plenamente alcanzados.

5. Acciones sugeridas

5.1 Se invita a la Reunión a:

a) Revisar el contenido de las lecciones aprendidas y recomendaciones en ciberseguridad y decidir sobre la posibilidad de elevar la presente nota de estudio al Panel de Expertos de Seguridad (AVSECP) para recabar la opinión de otros Estados en la implementación de los SARPS en ciberseguridad y su verificación.

— FIN —