Organización de Aviación Civil Internacional
Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS)

NOTA DE ESTUDIO

CRPP/5 — NE/26
11/07/19

**Quinta Reunión del Comité de Revisión de Programas y Proyectos (CRPP/5)**
Ciudad de México, México, 16 al 18 de julio de 2019

**Cuestión 7 del Orden del Día:** **Análisis de los retos emergentes en navegación Aérea**
**7.1 Perspectiva de la OACI en Ciber-seguridad y Ciber-resiliencia**

# ACTIVIDADES DE LAS REGIONES CAR/SAM DE LA OACI SOBRE SEGURIDAD CIBERNÉTICA Y RESISTENCIA CIBERNÉTICA

(Presentada por la Secretaría)


**RESUMEN EJECUTIVO**

La presente Nota de Estudio refleja las actividades realizadas por la Regiones CAR y SAM en cuanto a proveer a sus Estados de información para que ellos puedan desarrollar una correcta implementación de mecanismos que apoyen la seguridad de la información aeronáutica.

| | |
|---|---|
| **Acción:** | La acción sugerida se presenta en la Sección 3. |
| *Objetivos Estratégicos:* | • Capacidad y eficiencia de la navegación aérea |
| *Referencias:* | • Resolución A39-19 de la Asamblea sobre Ciberseguridad en la Aviación Civil.<br>• Reunión NAM/CAR/SAM para la implementación del AIDC, Lima, Perú, abril 2018.<br>• Taller NAM/CAR/SAM de la OACI sobre Ciberseguridad en la aviación, Ciudad de México, del 4 al 6 de diciembre de 2018. |


## 1. Introducción

1.1 La presente Nota de Estudio presenta un resumen de las actividades que las regiones CAR/SAM realizó durante 2018 para apoyar los resolución A39-19 de la Asamblea dirigida a los Estados para que estos promuevan disposiciones legales en materia de ciberseguridad que sean de aplicación en sus Estados.

1.2 El tema de ciberseguridad se venía tratando desde la perspectiva de seguridad de la aviación sin embargo durante la reunión NAM/CAR/SAM para la implementación del AIDC, que se realizó en Lima, Perú en abril del 2018, los Estados indicaron la necesidad de que se ampliara la visión de seguridad cibernética a los sistemas de navegación aérea, teniendo en cuenta que los sistemas como el ADS-B, los sistemas de información aeronáutica y los sistemas de control de tránsito aéreo puedan ser vulnerables a ataques cibernéticos.

1.3 Dentro de la reunión se analizó que además de la protección de la información existen otros aspectos que los Estados deben asegurar su protección a nivel interno y externo a sus operaciones por lo cual es necesario implementar mecanismos de seguridad en todos los aspectos.

1.4 En virtud de la solicitud de los Estados, las Oficinas Regionales NACC y SAM de la OACI organizaron un taller de Ciberseguridad en la Ciudad de México en diciembre del 2018 en el cual se desarrollaron las siguientes sesiones:

1. Sesión I: Iniciativas internacionales y disposiciones legales sobre Ciberseguridad Esta sesión se centró en el trabajo realizado sobre ciberseguridad por parte de organizaciones internacionales, y presentó las estructuras existentes para la coordinación de cuestiones de ciberseguridad y material de orientación y disposiciones sobre la materia que afectan a la aviación civil.
2. Sesión II: Ciberseguridad de Servicios de Navegación Aérea (ANS) Esta sesión se centró en ANS, el área donde probablemente el concepto de operaciones y la tecnología de soporte están cambiando más rápidamente y donde el marco de recomendaciones de ciberseguridad está más desarrollado.
3. Sesión III: Ciberseguridad y aerolíneas La industria de las aerolíneas reposa extensivamente en sistemas informáticos para sus operaciones en tierra y de vuelo. Esta sesión se centró en cómo las compañías aéreas implementan la automatización y las nuevas tecnologías, y cómo protegen sus sistemas contra amenazas cibernéticas.
4. Sesión IV: Ciberseguridad en aeropuertos: Esta sesión se centró en asegurar los sistemas de los aeropuertos y en la protección de la creciente cantidad de información y datos que estos sistemas manejan.
5. Finalmente se tuvo una sesión en grupos con el objetivo de fomentar el intercambio de ideas y discutir sobre el marco regulatorio actual sobre ciberseguridad, iniciativas potenciales en las regiones NAM/CAR y SAM y en el papel que la OACI podría jugar.

2 **Discusión**Como resultado de las discusiones se concluyó que la ciberseguridad es un tema que debe ser incluido en la cultura de seguridad a través de instrucción impartida al personal del ecosistema de transporte aéreo (Proveedores de Servicios de Navegación Aérea [ANSP], aerolíneas, y aeropuertos). La tecnología y el internet de las cosas están afectando a todo tipo de equipamiento no sospechoso. La aplicación de unas buenas prácticas básicas puede dificultar los ciberataques, que, aunque representasen riesgos mínimos en seguridad, afectarían la confianza pública.

2.2 Si bien los equipos nuevos podrían estar mejor preparados frente a ataques cibernéticos, hay equipos más antiguos que siguen en uso en aeropuertos, aerolíneas y ANSP. La ciberseguridad es un tema interrelacionado que no debe considerarse solamente bajo el Anexo 17, ya que afecta a los aeródromos, la aeronavegabilidad o la navegación aérea.

2.3 Las Oficinas Regionales de la OACI juegan un papel clave en la promoción de la ciberseguridad entre los Estados. Pueden facilitar la interacción de los Estados con programas e iniciativas en ciberseguridad de otras organizaciones internacionales, que puedan ayudar a construir capacidad (ej. desarrollo de una estrategia nacional de ciberseguridad); coordinar la participación de los Estados en ejercicios de ciberseguridad; o ayudar en la realización de análisis de riesgos en ciberseguridad.

2.4 La reunión también proporciono una serie de recomendaciones “Recomendaciones sobre Servicios de Navegación Aérea (ANS)” que se encuentran en el **Apéndice A** de esta nota de Estudio.

2.5 En ese sentido las Oficinas Regionales NACC y SAM han incorporado estas actividades de la siguiente forma:

1. Región NAM/CAR: ha integrado todo el desarrollo y temas de ciberseguridad en todos los grupos de trabajo del ANI/WG, como una tarea complementaria a los términos de referencia de los Grupos. Además, el MEVA/TMG está trabajando en el desarrollo de una nueva fase del MEVA donde integra los requisitos de seguridad en las comunicaciones, interconexión de bases de datos aeronáuticos y seguridad de la información.

2. Región SAM: abordó este tema de forma más puntual para los Estados SAM durante la Vigesimosegunda Reunión del Comité de Coordinación del Proyecto Regional RLA/03/901 (RCC/22) en Lima, Perú, del 5 al 7 de marzo de 2019, en la cual se adoptó la siguiente conclusión:

<table>
<tr><td colspan="2">Conclusión<br>RCC/22-4 ADQUISICIÓN DE LOS EQUIPOS CORTA FUEGO (FIREWALL) PARA LA REDDIG II</td></tr>
<tr><td>Que la Secretaría:<br>a) Por solicitud de los Estados participantes de la REDDIG, proceda a realizar, junto con el TCB de la OACI, el proceso para adquisición de los equipos corta fuego (firewall) para la REDDIG II;<br>b) El presupuesto inicial asignado para dicha adquisición sería de USD 375,000.00.</td><td>Impacto esperado:<br>☐ Político / Global<br>☐ Inter-regional<br>☒ Económico<br>☐ Ambiental<br>☒ Técnico/Operacional</td></tr>
<tr><td colspan="2">Por qué:<br>Para mejorar la protección de la red contra ataques cibernéticos y accesos no autorizados.</td></tr>
<tr><td>Cuándo:<br>2019/2020.</td><td>Estatus:<br>Actividad en progreso.</td></tr>
<tr><td colspan="2">Quién:<br>Secretaría de la RCC/22.</td></tr>
</table>

2.6 Ambas Regiones han adoptado mayormente la realización de actividades a través de sus Grupos de Comunicaciones aeronáuticas, pero es necesario impulsar la seguridad operacional en cada una de las áreas que forman parte de la cadena de información y servicios aeronáuticos.

2.7 La necesidad de que los Estados implementen mecanismos que permitan asegurar las operaciones aeronáuticas son ahora mayormente necesarios y se requiere que los Estados de nuestras regiones comiencen a trabajar en estos temas de forma de enfrentar las actuales amenazas y estar preparados para las futuras, de forma de asegurar siempre la operación continúa de sus actividades. En ese sentido las Regiones NAM/CAR/SAM proponen el Proyecto Regional indicado en el **Apéndice B** de esta Nota de estudio.

**3** **Acciones sugeridas:**Se invita a la Reunión a:

a) tomar nota esta información;

b) analizar las recomendaciones brindadas en el Apéndice A de esta Nota de Estudio; y

c) revisar y aprobar la propuesta de proyecto presentada en el Apéndice B de esta Nota de Estudio.

— — — — — — — — — — —

**APÉNDICE A**
**RECOMENDACIONES SOBRE SERVICIOS DE NAVEGACIÓN AÉREA (ANS)**

1. Los Estados necesitan identificar su infraestructura de comunicaciones, navegación y vigilancia que soporta sus servicios de tránsito aéreo y, así, identificar su infraestructura crítica vulnerable a ataques cibernéticos. La protección de infraestructura crítica debe ser una prioridad para los Estados.

2. Los sistemas automáticos como los centros de Control de Tráfico Aéreo (ATC) o sistemas de información aeronáutica, entre otros, para sus operaciones dependen de bases de datos que permiten tomar decisiones informadas con datos recibidos en tiempo real. Estos sistemas deberían ser adecuadamente protegidos para asegurar la confidencialidad, integridad y disponibilidad de la información.

3. El análisis de riesgos sobre ciberseguridad debería abarcar los servicios de tránsito aéreo y ser continuo para que los Estados puedan tener una perspectiva completa de los riesgos y las amenazas acerca de ciberseguridad para las operaciones de transporte aéreo.

4. Las nuevas tecnologías implementadas en los servicios de tránsito aéreo proveen mayor eficiencia y simplifican la gestión de operaciones. Sin embargo, podrían ser vulnerables a nuevas amenazas cibernéticas y, para mitigar esto y asegurar la redundancia, los Estados deberían revisar y actualizar las especificaciones técnicas y operacionales de sus sistemas.

5. La supervisión y el análisis del intercambio de información y las conexiones son esenciales para detectar ataques cibernéticos y para establecer medidas de protección adecuadas para los sistemas de tránsito aéreo.

6. Los Estados y la industria deberían colaborar para adaptar los requisitos técnicos al ritmo de desarrollo de las nuevas tecnologías y asegurar que el hardware y el software de los sistemas de tránsito aéreo estén actualizados y preparados contra las amenazas cibernéticas Asimismo, todas las partes interesadas (Estados, ANSP y la industria) necesitan colaborar en el diseño de Procedimientos operacionales normalizados (SOP), que aseguren una adecuada protección de las operaciones.

7. La cualificación y formación adecuada del personal a cargo de las áreas técnicas y operacionales de ANS son esenciales para un correcto suministro de los servicios. El personal debería tener conocimiento y necesita tener las habilidades para llevar a cabo los planes de recuperación en caso de incidentes cibernéticos.

— — — — — — — — — — —

**PROPUESTA DE PROYECTO CAR/SAM PARA CIBERSECURITY**

| **Región CAR/SAM** | **DESCRIPCIÓN DEL PROYECTO (DP)** | **DP N° C** | |
|---|---|---|---|
| ***Programa*** | **Título del Proyecto** | **Fecha inicio** | **Fecha término** |
| Nuevo Programa<br><br>(Coordinador OACI:<br>Región CAR:<br>Mayda Ávila<br>Región SAM:<br>Francisco Almeida) | **Implementación de Mecanismos de Ciber-seguridad y Ciber-resiliencia para los Servicios de Navegación Aérea.**<br><br>**Propuesta de Proyecto**<br><br>Coordinadores del proyecto: Por definir<br><br>Expertos contribuyentes al proyecto: Por definir | Septiembre 2019 | Agosto 2020 |
| **Objetivos del Proyecto** | 1. Establecer el estado de implementación de medidas de **Ciber-seguridad y Ciber-resiliencia de los servicios** de Navegación Aérea en los diferentes Estados.<br>2. Establecer un enfoque Regional para atender este tema.<br>3. Desarrollar un mecanismo de análisis e implementación de medidas de **Ciber-seguridad y Ciber-resiliencia de los servicios** de Navegación Aérea. | | |
| **Alcance** | El alcance del proyecto contempla la evaluación e identificación de los niveles principales de servicios, establecimiento de bases de datos y de todos los equipos y servicios que son vulnerables a los ataques cibernéticos a nivel interno y externo de las instituciones y que son parte de la cadena de servicios de navegación aérea de los Estados CAR/SAM.<br><br>Establecer un mecanismos regional de análisis que proporcione a los Estados información para poder identificar riesgos y establecer los mecanismos necesarios para minimizar o liminar estos riesgos y asegurar la continuidad del servicio. | | |
| **Métricas** | • El análisis de 20 Estados de la región CAR en cuanto a sus servicios de navegación aérea. 14 Estados de la región SAM.<br>• Establecer un plan de acción para cada Estado.<br>• Establecer un plan de acción regional. | | |
| **Metas** | • Identificación de las amenazas en cuanto a ciber-seguridad y Ciber-seguridad y Ciber-resiliencia para los Servicios de Navegación Aérea de los Estados de las regiones CAR/SAM.<br>• Obtener estadísticas regionales de las amenazas identificadas.<br>• Establecer necesidades de entrenamiento regional.<br>• Establecer un plan de acción regional que apoye los planes de acción nacional en cuanto a este tema.<br>• Identificar los requisitos técnicos y operativos en cuanto al funcionamiento de las redes de comunicación MEVA y REDDIG. | | |

| Región CAR/SAM | DESCRIPCIÓN DEL PROYECTO (DP) | DP N° C | |
|---|---|---|---|
| *Programa* | Título del Proyecto | Fecha inicio | Fecha término |
| **Estrategia** | • La ejecución de las actividades del Proyecto será coordinada entre miembros del proyecto, el coordinador del proyecto y el coordinador del programa, principalmente a través de teleconferencias, así como eventuales reuniones que se puedan realizar según las actividades del programa de trabajo.<br>• El coordinador de Proyecto coordinará según sea necesario, con el Coordinador del Programa, los requerimientos de otros proyectos y de las informaciones de los Grupos de trabajo de implementación NAM/CAR. Se incorporaron expertos adicionales según las tareas y trabajos especializados. | | |
| **Justificación** | • Los servicios de control de tráfico aéreo hoy en día exigen que se comparta mayor cantidad de información, no solo entre centros específicos de control, sino a través de una nube de información a la cual puede acceder un sin número de usuario para obtener o proporcionar información entre un número ilimitado de conexiones virtuales. Aunque al aumentar la información se proporciona mayor conciencia situacional, al mismo tiempo incrementa el riesgo de ataques cibernéticos. Incrementar el uso de la tecnología es proporcionar a incrementar el riesgo a ataques cibernéticos.<br>• Los Estados requieren hoy en día asegurarse que sus sistemas que proporcionan servicios de navegación aérea, ya sea equipos, sistemas, bases de información, entre otros cuentas con los mecanismos necesarios para asegurar su continuo funcionamiento basado en correcto funcionamiento, calidad de la información, interoperabilidad acorde a los requerimientos de funcionamiento. Para asegurar esto los Estados deben realizar análisis de riesgo identificando las posibles amenazas tanto interna y externa a sus operaciones y tener desarrollados mecanismos que afronten estas amenazas y reduzcan los riesgos. En este análisis los Estados deben incorporar su recurso humano, desastres naturales, vulnerabilidades y otras amenazas propios de los Estados.<br>• Acorde con el Doc 9854 “Concepto Operacional de gestión del tránsito aéreo mundial”, se requiere que los Estados tomen acciones en cuanto a la seguridad de la aviación y la seguridad operacional con el objetivo delimitar amenazas intencionales o no, hackers, actos criminales, errores de recursos humanos, interrupciones físicas de los servicios y otras posibles amenazas.<br>• Los Estados requieren analizar e identificar sus amenazas, implementar procesos de protección y respuesta ante estas amenazas y definir procesos de contingencia para asegurar la continuidad de sus operaciones.<br>• Ante todo este proceso de amenazas, este proyecto busca apoyar a los Estados en el proceso de identificación y análisis de sus amenazas, riesgos y apoyarlos a desarrollar los planes de acción requeridos para eliminar o minimizar su impacto. | | |
| **Proyectos relacionados** | Este proyecto está relacionado con el Programa D (ATN y sus Aplicaciones Tierra- Tierra y Aire- Tierra de la ATN), Fase IV de la red MEVA. | | |

— FIN —