Organización de Aviación Civil Internacional
Oficina Regional Sudamericana

CIAC/20-NE/09
20/10/22

Vigésima Reunión de Directores de los Centros de Instrucción de Aviación Civil de la Región Sudamericana (CIAC/19)
(Brasilia, Brasil, 24 al 28 de octubre de 2022)

Cuestión 4 del Orden del Día: **Seguimiento de la implementación de las actividades de capacitación en materia de navegación aérea, seguridad operacional, seguridad de la aviación, medio ambiente, y otras áreas de la aviación en la Región**

RESULTADOS DE LA PRIMERA REUNIÓN DE CIBERSEGURIDAD EN LOS ANS Y SU IMPACTO EN LA INSTRUCCIÓN DEL PERSONAL TECNICO ANS

(Presentada por la secretaria)

RESUMEN

Esta nota de estudio presenta un resumen de los resultados de la primera reunión de ciberseguridad en los servicios de navegación aérea, y el impacto que tendrá la implementación de la estrategia de ciberseguridad en los ANS, específicamente en lo que se refiere a la formación de los técnicos de las distintas especialidades.

La educación y el entrenamiento se reconocen como un elemento conductor para el establecimiento de una estrategia solida de ciberseguridad, y aunque la OACI ha desarrollado varios programas de instrucción, será necesario la cooperación de toda la comunidad para lograr el objetivo buscado.

Referencias:

- Sumario de la primera reunión de ciberseguridad en los ANS

Objetivos estratégicos de la OACI:	• A – Seguridad operacional B – Capacidad y Eficiencia de la Navegación Aérea

1. Introducción

1.1. La primera reunión sobre ciberseguridad en los servicios de navegación aérea se llevó a cabo en línea del 31 de agosto al 2 de septiembre de 2022, asistiendo representantes de las Autoridades y proveedores de servicios de navegación aérea de la región de Sudamérica; así como representantes de organizaciones internacionales incluyendo CANSO, EUROCONTROL y COCESNA. Los siguientes objetivos fueron definidos para la primera reunión de ciberseguridad en ANS:

a) Mejorar el conocimiento de los participantes sobre la importancia de la ciberseguridad en los servicios de navegación aérea.
b) Familiarizar a los participantes con la estrategia de seguridad operacional de la OACI.
c) Familiarizar a los participantes con el Plan de acción sobre seguridad Operacional de la OACI.
d) Fomentar la cooperación entre todas las partes interesadas en lo que se refiere a la ciberseguridad en los servicios de navegación aérea.

2. Análisis

2.1 Según los datos de las organizaciones especializadas, los ataques cibernéticos se han multiplicado exponencialmente después de la pandemia del COVID-19, los métodos de ataque evolucionan constantemente, haciendo cada vez más complejo el establecimiento de defensas frente a estos ataques.

2.2 El nivel de automatización de los servicios de navegación aérea de la región sudamericana ha alcanzado niveles importantes; la gestión de los datos que apoya la prestación de los servicios de tránsito aéreo, incluyendo la mensajería, comunicaciones y la vigilancia cada vez es más dependiente de los aspectos digitales. Esta automatización puede generar vulnerabilidades que impacten la correcta prestación de los servicios de navegación aérea, afectando la seguridad operacional y la eficiencia.

2.3 El establecimiento de una estrategia que promueva la identificación y gestión de los riesgos relacionados con la ciberseguridad es indispensable en el ANS. Uno de los componentes esenciales de la estrategia se relaciona con la **educación e instrucción** del personal técnico ANS, dependiendo de las funciones y responsabilidades que este tenga dentro de los servicios.

2.4 En el caso específico de los controladores de tránsito aéreo y de los especialistas AIS/ MET la educación y entrenamiento relacionados con los asuntos de ciberseguridad se podría limitar a los aspectos relacionados con la utilización de los sistemas automatizados dentro de los servicios de navegación aérea; sin embargo, en lo que se refiere a los especialistas CNS, esta educación e instrucción abordaría temas más especializados como lo relacionado a la identificación de riesgos de ciberseguridad, segregación de redes, identificación de activos críticos en las redes, entre otros aspectos técnicos.

2.5 Adicional a lo mencionado en el párrafo anterior, la ciberseguridad incluye elementos puntuales relacionados con aspectos de seguridad operacional y de seguridad de la aviación (safety and security), esta mezcla de elementos requiere un proceso especial de educación e instrucción para el personal técnico del ANS

2.6 Otro aspecto resaltado en la reunión es la necesidad de la colaboración entre todas las autoridades y partes interesadas, incluyendo las relacionadas a seguridad de la aviación, seguridad operacional, proveedores de servicios, centros de instrucción entre otros.

2.6 La oficina SAM de la OACI busca liderar la estrategia regional para el establecimiento de la ciberseguridad en los servicios de navegación aérea. Esta estrategia está enmarcada dentro de la documentación guía desarrollada por la OACI para la ciberseguridad. Esta documentación está disponible en la página de la primera reunión de ciberseguridad en el ANS:

https://www.icao.int/SAM/Pages/MeetingsDocumentation.aspx?m=2022-CIBER

3. Conclusiones

3.1 Los datos muestran que después de la pandemia del COVID-19 los ataques a los sistemas informáticos se han incrementado exponencialmente; las redes bancarias, de salud y de comunicación se han convertido en foco de atención de los piratas informativos. Con los niveles alcanzados de automatización en la aviación los riesgos de sufrir un ataque se incrementan exponencialmente por lo que es necesario el establecimiento de una estrategia que ayude a reducir los riesgos de los ataques cibernéticos.

3.2 La educación y el entrenamiento se reconoce como un elemento conductor para el establecimiento de una estrategia solida de ciberseguridad, y aunque la OACI ha desarrollado varios programas de instrucción, será necesario la cooperación de toda la comunidad para lograr el objetivo buscado.

3.3 Una de las conclusiones principales de la primera reunión de ciberseguridad en el ANS fue la siguiente:

“La OACI y los Estados deben fomentar la educación en ciberseguridad dependiendo de las funciones y responsabilidades del personal, es recomendable la revisión de los programas y planes de capacitación del personal técnico a todo nivel, para esto la oficina trabajara en coordinacion con los Estados para llevar a cabo esta tarea”

3.4 Para lograr implementar la conclusión anterior será necesaria la cooperación de las todas las partes interesadas, incluyendo los centros de instrucción que son elementos fundamentales de la estrategia de ciberseguridad.

4. Acción sugerida:

4.1 Se invita a la Reunión a:

a) Tomar nota de la información presentada en esta nota de estudio.
b) Considerar incluir dentro de los programas de instrucción de los especialistas de navegación aérea (controladores de tránsito aéreo y los especialistas AIS/MET); los aspectos relacionados a la ciberseguridad.
c) Que los centros de instrucción se sumen a la estrategia regional para el establecimiento de la ciberseguridad en los servicios de navegación aérea.

— FIN —