Organización de Aviación Civil Internacional

A41-WP/122[1]
TE/37
1/8/22

NOTA DE ESTUDIO

ASAMBLEA — 41º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 31: Seguridad operacional de la aviación y navegación aérea – Normalización

ACTUALIZAR LOS OBJETIVOS DE FORMACIÓN EN CIBERSEGURIDAD EXISTENTES DE ATSEP CYBER Y EL DESARROLLO DE NUEVOS OBJETIVOS DE FORMACIÓN EN CIBERSEGURIDAD DE ATSEP

[Nota presentada por International Federation of Air Traffic Safety Electronics Associations (IFATSEA)]

RESUMEN

Este documento describe una propuesta para actualizar los objetivos existentes de capacitación en ciberseguridad de ATSEP y desarrollar nuevos objetivos de capacitación en ciberseguridad en el Manual de la OACI sobre seguridad del tráfico aéreo Electrónica Capacitación y evaluación basada en competencias personales (Doc10057).

Se invita a la Conferencia a que:

a) tenga en cuenta los crecientes roles y responsabilidades de ATSEP como parte de la defensa cibernética en las interfaces con las áreas adyacentes de responsabilidad y las nuevas arquitecturas y modelos de negocio de ATM;
b) tenga en cuenta la naturaleza siempre cambiante y dinámica de las amenazas cibernéticas; y
c) priorice y tome todas las medidas necesarias dentro del proceso PANS-TRG para actualizar los Objetivos de Capacitación en Ciberseguridad existentes, y desarrolle nuevos Objetivos de Capacitación en Ciberseguridad de ATSEP para los Objetivos de Capacitación Básica y de Calificación en el Doc 10057, Apéndice B.

Objetivos estratégicos:	El presente documento de trabajo se refiere a los objetivos estratégicos: Seguridad operacional, capacidad y eficiencia de la navegación aérea, seguridad física, y facilitación.
Implicaciones financieras:	Habrá algún costo asociado con la actualización y el desarrollo de los Objetivos de Capacitación en Ciberseguridad en el Doc 10057. Las *unidades* de formación responsables de la formación básica y de cualificación de la ATSEP pueden tener que adaptar el contenido de los cursos de formación para incorporar los objetivos actualizados o nuevos.
Referencias:	A39-WP/370 UN ENFOQUE ARHCITECTURAL DE CIBERSEGURIDAD PARA SISTEMAS CNS/ATM TRADICIONALES Y BASADOS EN SWIM Anexo 10 — Telecomunicaciones aeronáuticas, volúmenes I, II, III y IV Manual sobre instrucción y evaluación básicas en competencias de los especialistas en sistemas electrónicos para la seguridad del tránsito aéreo (Doc 10057) Procedimientos para los servicios de navegación aérea — Formación (PANS-TRG) (Doc 9868)

[1] Las versiones en español, árabe, chino, francés, inglés y ruso fueron proporcionadas por IFATSEA.

1. INTRODUCCIÓN

1.1 Los sistemas CNS/ATM están experimentando un cambio de paradigma con la implementación de nuevas tecnologías, conceptos y modelos de negocio. El modelo ANS integrado va a ser reemplazado por una Arquitectura Orientada a Servicios (SOA) que se define como distribuida, y la información se intercambia a través de redes como SWIM. Los Servicios de Sistemas de Navegación Aérea existirán en el terreno y en el espacio, e incluso el procesamiento de datos ATM puede estar en sistemas desplegados en arquitecturas distribuidas y geográficamente separadas (por ejemplo, Proveedores de Servicios de Datos para la Navegación Aérea ADSP europeos y centros virtuales). Las configuraciones de sistemas CNS híbridos están entrando rápidamente en funcionamiento en todo el ecosistema de la aviación. Si las interfaces de interconexión del sistema de transporte aéreo entre las partes implicadas no se abordan adecuadamente en términos de ciberseguridad, las vulnerabilidades pueden ocurrir en un sistema o elemento de un sistema en una parte implicada. Aunque estas vulnerabilidades no representan un riesgo importante para el sistema en sí, pueden escalar fácilmente a una amenaza que representa un riesgo para el sistema de otra parte implicada con consecuencias negativas. Se requiere la creación de una capa de datos ATM entre las partes implicadas de ANS y las partes implicadas externas.

1.2 ICAO, en la Estrategia de Ciberseguridad de la Aviación, octubre de 2019 Capítulo 7. La creación de capacidad, la capacitación y la cultura de ciberseguridad, establece que "*se debe proporcionar capacitación adecuada relacionada con el trabajo de manera continua para apoyar al personal en sus funciones diarias"* y "La ciberseguridad *podría incluirse en la estrategia para la próxima generación de profesionales de la aviación, ya que la OACI está bien situada para trabajar con los Estados y la industria para desarrollar competencias basadas en roles. requisitos para los profesionales de la aviación*". Al igual que en el proyecto de informe de la OACI A40-WP/577, párrafo 30.36, se afirma que se podría considerar una orientación específica sobre capacitación en ciberseguridad para futuras actualizaciones del Doc 10057".

1.3 Los ATSEP son los primeros especialistas dentro de un ANSP en abordar tácticamente la seguridad cibernética de los vectores de ataque, ya sea a través de la red o combinados con la señal en el espacio. Son responsables en este caso de distinguir entre fallos técnicos y ciberataques. Algo que estos servicios CNS/ATM tienen en común es la autorización para poner en servicio, fuera de servicio, comisionar y desmantelar hardware y software por parte de ATSEP. Para asegurar mejor el sistema funcional ATM como se describió anteriormente, estos especialistas apropiados que también tienen acceso legal a los sistemas técnicos ATM / ANS deben desplegarse en las interfaces.

1.4 Las ATSEP desempeñan un papel cada vez más importante en la protección de estas interfaces críticas (OACI A39. WP17 EX / 5). Por ejemplo, la mayoría de los países han desarrollado o están comenzando a desarrollar equipos de respuesta a emergencias informáticas (CERT), que son responsabilidad de ATSEP. Sin embargo, la capacitación de ATSEP contenida en la versión actual de ICAO Doc 10057 se aborda principalmente como requisitos de seguridad física, mientras que la referencia a la Ciberseguridad, especialmente para abordar los cambios de paradigma presentados por SESAR y NextGen, incluida la visión CANSO ATM no se aborda. Por las razones anteriores, existe una clara necesidad de ampliar la capacitación para ATSEP dentro de un contexto de Ciberseguridad para que adquieran la competencia para abordar táctica y estratégicamente los Eventos Cibernéticos.

1.5 Como se sabe desde Europa, la seguridad física no solo requiere que los proveedores de ATS tengan un sistema de gestión de la seguridad, como es el caso de la seguridad operacional, sino que el NPA 2019/07 requiere un SGSI (Sistema Integrado de Gestión de la Seguridad) para todos los servicios ATM / ANS y servicios habilitadores, ya que hay muchas interfaces adicionales, lo que también es correcto, ya que se trata de diferentes disposiciones y actividades de servicio. Sin embargo, la incursión y

el tratamiento de la seguridad cibernética en la capacitación de ATSEP a nivel mundial dentro de los ANSP es, en el mejor de los casos, inconsistente, y en el peor, ad hoc.

1.6 Para comprender el impacto de un ciberataque en las partes individuales de la red ATM, no es suficiente tener un muy buen conocimiento de la tecnología de la Información (TI) y las redes IP. Dado que las diferentes redes no son solo conexiones físicas, sino información, controles y señales desencadenadas por diferentes factores y utilizando diferentes rutas de transmisión como radio, VoIP, redes, comandos humanos, signos y señales ópticas, sonidos, etc., también se requiere una comprensión profunda de las acciones de mitigación de ciberseguridad y su impacto en la seguridad operacional ATM. También es necesario tener una formación aeronáutica.

1.7 Por lo tanto, se propone reorientar y ampliar el contexto de capacitación de ATSEP en el Doc 10057, en Ciberseguridad desde dentro de ATM/ANS Services, que tienen suficiente formación aeronáutica y cultura de seguridad, así como los conocimientos necesarios en tecnología de redes e informática, para abordar las amenazas de seguridad cibernética táctica y estratégicamente.

2. DISCUSIÓN

2.1 Los objetivos de formación existentes contenidos en el Manual de Formación de la ATSEP (DOC OACI 10057 Segunda edición 2020) en materia de Ciberseguridad deben revisarse, actualizarse y, cuando sea necesario, crearse nuevos Objetivos de Formación tanto en objetivos básicos como en objetivos de cualificación, con un enfoque hacia la cobertura los elementos de ciberseguridad de la propia información y los sistemas TIC (Tecnologías de la Información y la Comunicación), basados en el estado actual de la técnica y, en algunos casos, en el tratamiento de ataques combinados con vectores de ataque de TI y Señal en el Espacio.

2.2 IFATSEA está dispuesta a contribuir con su asistencia a la OACI para el desarrollo de la formación en ciberseguridad para ATSEP.

— FIN —