Organización de Aviación Civil Internacional

AN-Conf/14-WP/113[1]
28/6/24

NOTA DE ESTUDIO

DECIMOCUARTA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 26 de agosto - 6 de septiembre de 2024

Cuestión 4: Hiperconectividad del sistema de navegación aérea
4.2: Ciberseguridad y resiliencia de los sistemas de información

CIBERSEGURIDAD
GESTIÓN DEL RIESGO E INVENTARIO DE CIBER-ACTIVOS DE INFORMACIÓN EN LOS SERVICIOS DE NAVEGACIÓN AÉREA (ANS)

[Nota presentada por Chile con el apoyo de 20 Estados miembros de la Comisión Latinoamericana de Aviación Civil (CLAC[2])]

RESUMEN

La presente nota propone lineamientos generales de ciberseguridad que, en los Servicios de Navegación Aérea (ANS), debieran considerarse para hacer frente a las amenazas actuales para los sistemas tecnológicos utilizados en dicho ámbito. El constante intercambio de información transforma dichos sistemas en focos potenciales para un ciberataque.

La condición es atingente a la estructura funcional del sistema de aviación, tales como, las autoridades de aviación civil, los proveedores de servicios de navegación aérea (ANSP), explotadores de aeropuertos, y cualquier otra organización pertinente.

Medidas propuestas a la conferencia: Se invita a la conferencia a convenir la siguiente propuesta:

a) promover el desarrollo de un plan de gestión del riesgo en los ANS, que permita identificar y mitigar cualquier amenaza de ciberseguridad durante el diseño, instalación y operación de las redes y sistemas requeridos;
b) promover elementos que faciliten la gestión del riesgo, como, por ejemplo, la implementación de un registro único integrado por cada ciberactivo identificado en los ANS; que permita determinar amenazas, en rangos prioritarios de acción, mantención y recuperación rápida del sistema, en caso de ser necesario; y
c) renovar el compromiso de realizar mejoras continuas a diversos procesos, y dentro de ellos a aquellos denominados como críticos, con el objetivo de alcanzar niveles óptimos de ciberseguridad en los (ANS).

[1] La versión en español fue proporcionada por Chile.
[2] Argentina, Aruba, Belice, Brasil, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela (República Bolivariana de).

1. INTRODUCCIÓN

1.1 La evolución tecnológica implementada en las diferentes organizaciones de la sociedad, hace que éstas queden cada día más expuestas a la ciberdelincuencia. La provisión de los Servicios de Navegación Aérea (ANS) no escapa a lo anterior, lo cual impulsa desarrollar estrategias y levantar barreras de protección frente a esta amenaza latente y en crecimiento, la que, eventualmente, podría afectar los niveles de seguridad operacional óptimos.

1.2 La necesidad de desarrollar una gestión del riesgo que permita identificar y mitigar cualquier amenaza de ciberseguridad sobre el sistema ANS, renuevan el compromiso de realizar mejoras continuas a diversos procesos, y dentro de ellos, aquellos denominados como críticos para la organización.

1.3 Una política de ciberseguridad desarrollada para los ANS debiese considerar el ciclo de vida completo del sistema de aviación e incluir elementos tales como: cultura de ciberseguridad, promoción de la seguridad por diseño, seguridad de la cadena de suministros de programas y equipos informáticos, integridad de datos, control apropiado del acceso, gestión proactiva de vulnerabilidades, mejoras en los tiempos de actualización de sistemas, incorporar sistemas y procesos para vigilar los datos.

2. ANÁLISIS

2.1 El objetivo de alcanzar un sistema de navegación mundialmente interoperable considera redes compartidas e infraestructuras informáticas, arquitecturas y operaciones centradas en redes. El intercambio de información futuro, no se limitará a las comunicaciones punto a punto, sino que también utilizará la arquitectura de sistemas abiertos y el flujo de información basado en Internet. Todo lo anterior, aumenta la vulnerabilidad de los sistemas frente a un ciberataque.

2.2 La implementación de la Ciberseguridad en los ANS debe considerar el resguardo y resiliencia de las redes, sistemas y su continuidad operacional, confidencialidad, integridad y disponibilidad de la información. Lo anterior requiere el análisis de impacto operacional, así como del ciclo de vida de los sistemas.

2.3 Se entiende como ciberincidencia a todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por los sistemas de información y su infraestructura, que puedan afectar al normal funcionamiento de estos.

2.4 Los ANS, están expuestos a una serie de ciberamenazas, tales como, inundación de información, interceptación pasiva de información, interceptación activa de información, modificación de la configuración o los datos del sistema, destrucción de la configuración de los sistemas, ataques de interrupción o denegación de servicio, entre otros.

2.5 Los ANSP, deberían determinar los soportes lógicos y físicos de los sistemas críticos de información utilizados en sus operaciones, y considerar el grado de afectación en caso de que éstos se vean dañados o suspendidos.

2.6 Las medidas de protección de los sistemas críticos de información debiesen realizarse en la etapa de diseño o lo antes posible, para asegurarse de que sean lo más resilientes a ciberataques. Lo anterior, debiera considerar controles administrativos, virtuales o lógicos y materiales.

2.7 Las medidas de seguridad de infraestructura, debiera considerar seguridad mediante el diseño, separación entre redes, acceso remoto.

2.8 Las medidas de seguridad en la cadena de suministro para soportes físicos y lógicos, debiera considerar la actualización de los sistemas de tecnología de la información y las comunicaciones (ICT) aeronáuticos periódicamente debido a los cambios en los requisitos operacionales o la modernización de soportes lógicos.

2.9 La implementación de un plan de gestión del riesgo para los ANS requiere, al menos, la identificación de la gestión del tránsito aéreo (ATM), definir una clasificación de incidentes, nivel de peligrosidad, nivel de impacto en el sistema.

DESCRIPCIÓN DE PROCESOS									
Producto Estratégico	Proceso	Subproceso	Etapa relevante	Nombre Activo	Identificador o código	Tipo	Ubicación	Responsable / dueño	Soporte

				ANÁLISIS DE CRITICIDAD			
Medio de almacenamiento	Tiempo de retención	Disposición	Criterio de Busqueda	Confidencialidad	Integridad	Disponibilidad	Criticidad

Figura núm. 1. Planilla de Identificación e inventario de Ciberactivos ATM

Figura núm. 2. Mapa de Gestión de Riesgos

		Susceptibilidad						Riesgo																	
								Probabilidad de ocurrencia									Impacto								
								Factores de Agente Amenazante				Factores de Vulnerabilidad					Factores técnicos					Factores de		
ID ACTIVO	Vulnerabilidad	Suplantación de identidad (Autenticidad)	Manipulación (Integridad)	Repudio (No Repudio)	Divulgación de información (Confidencialidad)	Denegación de servicio (Disponibilidad)	Elevación de privilegios (Autorización)	Nivel de habilidad	Motivación	Oportunidad	Tamaño	Facilidad de descubrimiento	Facilidad de explotación	Conocimiento	Detección de intrusión	Total Probabilidad de ocurrencia	Pérdida de Confidencialidad	Pérdida de Integridad	Pérdida de Disponibilidad	Pérdida de responsabilidad	Total Impacto técnico	Daño financiero	Daño a la reputación	No cumplimiento
ACT17	descripción de la vulnerabilidad	S	T	R	I	-	E	9	4	4	3	4	3	3	4	4,25	2	2	2	2	2	6	3	3
ACT17		S	T	-	I	D	E	4	4	7	4	4	4	7	4	4,75	4	4	3	3	3,5	3	4	4
ACT17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	6,75	7	7	0	0	3,5	0	0	0
ACT 16 Y 17		S	T	R	I	D	E	4	4	7	9	9	9	9	3	6,75	2	2	2	2	2	2	2	2
ACT17		S	T	-	I	D	E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ACT 16 Y 17		S	T	-	I	D	E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figura núm. 3. Planilla de Análisis de Riesgo y Vulnerabilidades para activos identificados

2.10 La formulación de un plan de gestión del riesgo debiera permitir la anticipación a las consecuencias derivadas de amenazas tales como ciberataques y ciberincidencias no hostiles, en base a un análisis y evaluación de los riesgos a los cuales se exponen sus redes y sistemas, con el objetivo de evitar o reducir la ocurrencia de tales contingencias. Mitigar los eventuales efectos, indicando acciones inmediatas y medidas progresivas de mejoras, con sus respectivos indicadores, controles y documentación.

2.11 Como un elemento facilitador en la gestión del riesgo, se debiera considerar un *registro único* por cada ciberactivo ATM identificado. Lo anterior, permitirá:

a) reunir los ciberactivos, del mismo género y/o ciclo vital;

b) asegurar la integridad de los datos;

c) potenciar el acierto de las acciones para mantener la resiliencia del sistema;

d) evitar que los elementos se dupliquen o desactualicen; y

e) reducir los esfuerzos del equipo para el análisis y toma de decisiones.

3. CONCLUSIÓN

3.1 La necesidad de implementar estrategias de ciberseguridad contra amenazas digitales en la provisión de los ANS, requiere que los proveedores de estos definan planes y protocolos de trabajo, de manera de proteger y garantizar que los sistemas y la infraestructura relacionada, tengan la resiliencia necesaria que permita mantener la *confidencialidad, integridad y disponibilidad* de la información.

3.2 A la luz de lo expuesto, y en el contexto del *Plan de Acción de Ciberseguridad* de la OACI, se propone a la Conferencia convenir en la siguiente recomendación:

Que los ANSP:

a) desarrollen un Plan de gestión del riesgo ante ciberamenazas, en el que se considere, al menos, la identificación de los ciberactivos ATM, una clasificación de incidentes, una clasificación de nivel de peligrosidad, nivel de impacto en el sistema y protocolos de recuperación del mismo;

b) dentro de la gestión del riesgo, consideren elementos facilitadores tales como el diseño de un registro único por cada ciberactivo ATM interoperable; y

c) renovar el compromiso de realizar mejoras continuas a diversos procesos, y dentro de ellos a aquellos denominados como críticos, con el objetivo de alcanzar niveles óptimos de ciberseguridad en los Servicios de Navegación Aérea (ANS).

— FIN —