Organización de Aviación Civil Internacional

AN-Conf/14-WP/125[1]
29/6/24

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

LA CIBERSEGURIDAD EN EL SUMINISTRO DE LOS SERVICIOS DE TRÁNSITO AÉREO (ATS)

[Nota presentada por Argentina con el apoyo de 19 Estados miembros de la Comisión Latinoamericana de Aviación Civil (CLAC[2])]

RESUMEN

En esta nota se presentan consideraciones que propician el diseño de mecanismos que orienten a los ATSP respecto de la gestión de ciberamenazas y cibersucesos en la prestación de los servicios de tránsito aéreo (ATS) y la elaboración de estrategias de mitigación eficientes.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a:
a) desarrollar mecanismos de orientación para el ATSP respecto de la gestión de riesgos de seguridad operacional en materia de ciberseguridad en el SMS del ATSP;
b) desarrollar y/o implementar el uso de tecnologías, procedimientos y dispositivos necesarios para que el Controlador preste los servicios de tránsito aéreo (ATS) de manera segura y, ante un *cibersuceso*, contribuya a la pronta recuperación de las operaciones; y
c) definir competencias y habilidades que los ATCO requieren para interpretar y actuar ante la ciberseguridad y su impacto en la prestación de los ATS, logrando ciberresiliencia.

1. INTRODUCCIÓN

1.1 En virtud del creciente número de ciberamenazas y ciberataques a la industria de la aviación y, teniendo en cuenta que uno de los siete pilares de la "Estrategia de ciberseguridad de la aviación" impulsada por la OACI - la "*política de ciberseguridad*" - insta a contemplar la *ciberseguridad* en la gestión de riesgos de la aviación, resulta cada vez más relevante identificar y medir el impacto de tales sucesos en la provisión de los Servicios de Tránsito Aéreo (ATS), aun cuando las tecnologías emergentes que la navegación aérea adopta estén mejor preparadas para hacer frente a un *cibersuceso.*

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

1.2 Los *cibersucesos* - en virtud de la hiperconectividad existente entre los sistemas de la aviación y también entre éstos y otros sistemas externos a la misma - cobran mayor magnitud, tanto en su alcance como en su impacto, pudiéndose convertir en un *suceso perturbador*[3] de envergadura global. Por lo tanto, es importante considerar que tales *cibersucesos* deberían ser concebidos como peligros de seguridad operacional o, al menos, como precursores y factores contribuyentes a las categorías mundiales de sucesos de alto riesgo (G-HRC), descritas en el "Plan Global para la Seguridad Operacional de la Aviación 2023-2025" (Doc 10004, GASP), más aún cuando el concepto operacional ATM (Doc 9854 de OACI) advierte que muchas veces se adoptan decisiones basadas en diversos criterios, incluido en materia de seguridad operacional, lo que insta, en consecuencia, a adoptar las acciones necesarias para alcanzar uno de los beneficios citados en su Apéndice E: " *(...) la ampliación de la definición de peligros permitirá trayectorias de usuarios más estables*."

1.3 Los ATS se prestan, entonces, en un entorno de mayor automatización, digitalización e interconectividad, lo que hace que esa prestación sea más vulnerable ante las *ciberamenazas* y los *ciberataques*. El uso de comunicaciones por enlace de datos controlador-piloto (CPDLC), la creciente coexistencia de aeronaves y vehículos aéreos no tripulados (VANTs) en espacios aéreos controlados, la instalación de torres remotas digitales (TRD) y la implantación de Servicios de Información de Vuelo de Aeródromo Automatizados (A-AFIS) para el suministro de ATS, entre otros desarrollos, ponen de relieve la necesidad de tomar mayor conciencia y actuar sobre el impacto de los *cibersucesos* en esa prestación.

1.4 Por otra parte, si bien se han observado importantes avances en la adopción de acciones que prevén y/o mitigan la incidencia de *cibersucesos*, los mismos tienen que ver - naturalmente - con los sistemas de comunicaciones, navegación y vigilancia/gestión del tránsito aéreo (ATM/CNS) y de información, en los cuales dicha incidencia es directa. No obstante, se requiere continuar trabajando al respecto, resultando imperioso considerar el impacto de dichos sucesos en la ATM.

1.5 Si las dependencias ATS no disponen de barreras defensivas y sistemas de control de riesgos suficientes y apropiados, podrían verse sometidas, en consecuencia, a una interrupción parcial de los servicios que suministran, a una condición de "ATC ZERO" o, incluso, a la ocurrencia de eventos de seguridad operacional tales como pérdidas de separación entre aeronaves en vuelo (MAC: *Mid Air Collision)*, uno de los cinco (5) sucesos de alto riesgo (G-HRC).

1.6 La sección 4 – *Elaborar unan política de ciberseguridad* del "Plan de Acción de Ciberseguridad (CyAP)" - propiciado por el Grupo de Estudio de la Secretaría sobre Ciberseguridad (SSGC) de la OACI - establece acciones vinculadas a la gestión de ciberriesgos, por lo que resulta pertinente repensar la manera en que se gestionan los riesgos de seguridad operacional en la prestación de los ATS, advirtiéndose que dicha prestación se desarrolla en un entorno mundial descrito como volátil, incierto, complejo y ambiguo, evolucionando hacia un contexto, además, frágil y no lineal[4].

2. ANÁLISIS

2.1 Conforme a lo expuesto, resulta menester, entonces, identificar las oportunidades de mejora en cuanto a previsiones y acciones que promuevan la *ciberseguridad* en la prestación de los ATS.

---

[3] Suceso perturbador: eventos anómalos - de gran importancia a nivel mundial, regional o nacional - que afectan negativamente las actividades de la aviación. No suelen devenir de actividades de la aviación, sin embargo, tienen un impacto considerable en sus operaciones.

[4] Las características citadas proceden de los abordajes VUCA (volatile, uncertain, comple, ambiguous) y BANI (brittle, anxious, non linear, incomprehensible) que son modelos mediante los cuales se intenta explicar - desde las ciencias sociales - el actual escenario mundial y que son transversales a todas las disciplinas humanas.

2.2 Primeramente, es importante reexaminar el contexto operacional - caracterizado por su creciente complejidad - en el que actualmente se suministran los ATS, y redefinir el rol y las funciones de las dependencias ATS, en especial, en la intersección resultante de las relaciones y acciones entre cuatro (4) sistemas de gestión que son transversales a dichos servicios: gestión de ciberriesgos, gestión de riesgos de seguridad operacional (safety), gestión de la seguridad (security) y gestión de la seguridad de la información.

2.3 Por otra parte, se advierten tres (3) aspectos vinculados a la prestación de los ATS en los que se requiere diseñar e implementar medidas que contribuyan a mitigar las consecuencias de *cibersucesos*:

a) La gestión de riesgos de seguridad operacional en relación con la prestación de los ATS;

b) Las herramientas técnico-operativas[5] utilizadas por las dependencias ATS para prestar los servicios pertinentes; y,

c) Las competencias y habilidades necesarias de los controladores de tránsito aéreo (ATCO) que cumplen funciones en las dependencias ATS para lograr la *ciberresiliencia*.

2.4 Con respecto a la gestión de riesgos de seguridad operacional de los ATS, resulta necesario que las *ciberamenazas* y los *ciberataques* sean contemplados en el sistema de gestión de riesgos de seguridad operacional (SMS) del proveedor de servicios de tránsito aéreo (ATSP). En ese sentido, claro está, adopta especial relevancia el componente 2 de dicho sistema y, a fin de gestionar los riesgos, es necesario, naturalmente, identificar los peligros. Por lo tanto, comprender que las *ciberamenazas* y los *ciberataques* requieren ser identificados como tales, es fundamental para comenzar a registrar su ocurrencia, medir su impacto en la prestación de los ATS, y evaluar los riesgos asociados a los mismos.

2.5 En tal sentido, se pone de relieve la necesidad de adoptar tal abordaje sin circunscribirse a la identificación de peligros que, convencionalmente, se asocian a los ATS, sino contemplando a aquellos vinculados con tecnologías de la información (IT) (Ej. la red que alimenta a los sistemas ATM/CNS de la dependencia ATS; los software, servidores y ordenadores utilizados, etc.) y a otros aspectos de ciberseguridad. Es primordial considerar que - al tratarse de tecnología, la cual evoluciona, como ya se citó, de forma exponencial y a velocidades significativas - dicho abordaje no tiene que revestir un carácter estático sino, más bien, ha de ser dinámico y adaptativo, lo que implica llevar a cabo tareas de revisión y ajuste constantes en virtud de los rápidos cambios que se producen, no sólo en el contexto operativo, sino también en el entorno en general. Es necesario entender, entonces, que tanto un suceso como un incidente de ciberseguridad se puede transformar en un suceso de seguridad operacional en la prestación de los ATS y las operaciones de vuelo.

2.6 En cuanto a las herramientas de carácter operativo utilizadas por las dependencias ATS para prestar los servicios pertinentes, se entiende que alcanzan a aquellas tecnologías, procedimientos y dispositivos que el Controlador requiere para prestar los ATS de manera segura y, ante un *cibersuceso*, lograr *ciberesiliencia* y la pronta recuperación de las operaciones. Por lo tanto, cobra vital importancia el desarrollo de dispositivos que coadyuven al Controlador a identificar rápidamente las ciberamenazas y actuar en consecuencia.

2.7 El rol del Controlador de Tránsito Aéreo ha cambiado, y su interacción con los elementos que componen al "Modelo SHELL" se va transformando a la nueva realidad. La integración entre la persona, el hardware y el software es cada vez más simbiótica y, en consecuencia, está más expuesta a los *cibersucesos*. Es necesario, entonces, desarrollar las competencias y habilidades necesarias para que los ATCO, en las dependencias ATS, logren *ciberresiliencia*, contemplando diversos escenarios potenciales, contribuyendo, así, a una mejor preparación de estos ante un *cibersuceso*.

[5] Se consideran como tales los procedimientos operacionales; los sistemas informáticos y otras TICs; los sistemas de vigilancia ATS y de comunicaciones; etc.

3. CONCLUSIÓN

3.1 Conforme a lo precedentemente expuesto y teniendo en cuenta la transversalidad de la ciberseguridad en la prestación de los ATS, se necesita, entonces, de mecanismos que orienten a los ATSP en la inclusión de *ciberamenazas* y *cibersucesos* y su gestión, en la gestión de riesgos de seguridad operacional de su SMS, como también, de herramientas de análisis que conduzcan a diseñar estrategias de mitigación eficientes; procedimientos de detección temprana de ciberamenazas; e instrumentos de apoyo que faciliten a los ATCO la toma de decisiones inmediata ante este tipo de ocurrencias.

3.2 Asimismo, sería propicio definir competencias y habilidades que el controlador de tránsito aéreo ha de detentar, a fin de interpretar y actuar en consecuencia ante la ciberseguridad y su impacto en la prestación de los ATS, y que, además, contribuyan a incrementar la conciencia situacional de los ATCO con relación a la incidencia de estos eventos en la prestación de los ATS y el impacto de estos en materia de factores humanos.

3.3 En virtud de lo manifestado, se invita a la Conferencia a considerar:

a) desarrollar mecanismos de orientación para el ATSP respecto de la gestión de riesgos de seguridad operacional en materia de ciberseguridad en el SMS del ATSP;

b) desarrollar y/o implementar el uso de tecnologías, procedimientos y dispositivos necesarios para que el Controlador preste los servicios de tráfico aéreo (ATS) de manera segura y, ante un *cibersuceso*, contribuya a la pronta recuperación de las operaciones; y

c) definir competencias y habilidades que los ATCO requieren para interpretar y actuar ante la ciberseguridad y su impacto en la prestación de los ATS, logrando ciberresiliencia.

— FIN —