Organización de Aviación Civil Internacional

A41-WP/64[1]
EX/33
22/7/22

NOTA DE ESTUDIO

ASAMBLEA — 41.º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 14 : Política de seguridad de la aviación

INTEGRACIÓN Y COORDINACIÓN DE LOS PLANES DE TRABAJO Y LAS ESTRATEGIAS DE CIBERSEGURIDAD DE LA OACI

(Nota presentada por la Asociación de Transporte Aéreo Internacional [IATA])

RESUMEN

La ciberseguridad en la aviación civil continúa recibiendo cada vez más interés por parte de la OACI, los estados y el sector. El enfoque no solo se centra en identificar y mitigar las ciberamenazas y riesgos que pretendan alterar los sistemas digitales, sino también definir un marco internacional para la provisión de innovaciones tecnológicas seguras que adopten principios clave tales como la seguridad por diseño para la cadena de suministro aeroespacial.

Este informe destaca la necesidad de adoptar un enfoque integrado y coordinado en la provisión de ciberseguridad por el recién creado Comité Ad Hoc de Coordinación de la Ciberseguridad (AHCCC). Señalamos que las propuestas proceden de subgrupos y paneles técnicos, que pueden afectar a los Estándares y Prácticas Recomendadas (SARP), así como otros requisitos, que reflejen la transversalidad de esta disciplina en los múltiples anexos, documentos y manuales de la OACI.

Medidas propuestas a la Conferencia: Se invita a la Asamblea a:

a) solicitar al Consejo que se asegure de que todos los grupos de trabajo de la OACI adoptan conjuntamente un enfoque concertado multidisciplinar y de múltiples fases para la integración de las disposiciones de ciberseguridad y otros requisitos basado en los principios de la seguridad por diseño; y

b) solicitar al Consejo que reconozca y tenga en cuenta las potenciales repercusiones de la introducción de una nueva generación de tecnologías interconectadas e innovadoras, con sus cadenas de suministro asociadas, que no estén sujetas a las normas de la aviación civil ni a los SARP.

Objetivos estratégicos:	Esta nota de estudio se refiere a los siguientes objetivos estratégicos: seguridad, seguridad y facilitación y capacidad y eficiencia de la navegación aérea.
Repercusiones financieras:	El coste de desarrollar, coordinar y procesar nuevas disposiciones y materiales de orientación que el sector entregaría a la OACI.
Referencias:	*Resoluciones vigentes de la Asamblea (al 4 de octubre de 2019) (Doc. 10140)* *Declaración sobre el contexto de riesgo global para la seguridad de la aviación* (Doc. *10108)* *Resolución A40-10 – Abordar la ciberseguridad en la aviación civil* *Estrategia de ciberseguridad* *Plan de acción de ciberseguridad para la aviación de la OACI*

[1] Las versiones en español, árabe, chino, francés e inglés fueron proporcionadas por la IATA.

1. INTRODUCCIÓN

1.1 En la sesión n.º 40 de la Asamblea General de la OACI (2019) se adoptó la Resolución A40-10, *Abordar la ciberseguridad en la aviación civil*. Básicamente, la Resolución permitía a la Secretaría General continuar garantizando que las cuestiones de ciberseguridad se consideran y se coordinan de manera transversal mediante mecanismos apropiados según el espíritu de la Estrategia de Ciberseguridad de la Aviación de la OACI (2019).

1.2 La Estrategia de Ciberseguridad de la Aviación de la OACI propone una serie de principios, medidas y actividades, e identifica acciones de coordinación claramente identificadas mediante el Plan de Acción de Ciberseguridad de la OACI (CyAP) (2019) para abordar las ciberamenazas y los elementos necesarios para aumentar la posición de resiliencia de la aviación civil internacional hacia la seguridad y la confianza digital.

1.3 En 2022, el Consejo de la OACI resolvió la creación del Comité Ad Hoc de Coordinación de la Ciberseguridad (AHCCC) y dos paneles separados, bajo dos comités diferentes. Esto subraya la importancia de la ciberseguridad de la aviación estratégica para la OACI y el Consejo. El nuevo Panel de Ciberseguridad (CYSECP), creado tal como lo aprobó el Comité de Seguridad de la Aviación en la 225ª sesión, del 24 de enero de 2022, celebró su primera reunión en mayo de 2022. El CYSECP señaló los logros anteriores del SSGC y propuso un plan de trabajo que destacaba la necesidad de coordinación interna e internacional. Además, la Comisión de Navegación Aérea (ANC) creó el Panel de Sistemas de Confianza (TSP) para reforzar la perspectiva de coordinación entre los grupos de trabajo, comités y paneles técnicos de la OACI.

2. DISCUSIÓN

Coordinación en ciberseguridad de la OACI

2.1 Se señala que la ciberseguridad en la aviación es una disciplina de naturaleza transversal e integrada. Por este motivo, la función del AHCCC en lo sucesivo será fundamental para garantizar la dirección estratégica coordinada que integre los planes de trabajo y las actividades de los distintos esfuerzos relacionados de la OACI para proteger la aviación ante cualquier forma de interferencia digital, además de promover la innovación tecnológica segura.

2.2 De manera inherente, las SARP y las directrices derivadas de los documentos suelen dirigirse a que los estados cumplan las obligaciones internacionales establecidas en el Anexo 19. Por lo tanto, es fundamental que la AHCCC garantice la coordinación mediante una gobernanza estructurada y eficiente.

2.3 A continuación se señalan una serie de esfuerzos en relación con la AHCCC:

a) Las actividades del Panel de Sistemas de Confianza sientan las bases para la próxima generación de movilidad aérea y abordan el desarrollo de un concepto de operaciones y gobernanza para dicho marco;

b) El Panel de Ciberseguridad establece actividades que incluyen la presentación de propuestas para actualizar/modificar los anexos, documentos y manuales existentes en la provisión de ciberseguridad;

c) El Panel de Gestión de la Información en sus Procedimientos para Servicios de Navegación Aérea – Gestión de la Información (PANS-IM), expresa ciertos requisitos

de seguridad de la información, así como otros esfuerzos, como la actual redacción de la revisión 3 del documento 9896, sobre la implementación de los servicios de protocolo de internet en la red de telecomunicaciones aeronáuticas, que también introduce requisitos de ciberseguridad en su manual;

d) También se proponen modificaciones en el Manual de gestión de la seguridad (doc. 9859);

e) Se señala la coordinación de los resultados del Programa Universal de Auditoría de Seguridad (USAP) para las SARP relacionadas con la ciberseguridad en el Anexo 17 mencionados en la nota A41-WP/22 presentada por el Consejo de la OACI; y

f) Se señala el trabajo del Subgrupo de Investigación sobre Asuntos Legales (RSGLA) y la coordinación de la Secretaría con el Comité Legal, como se menciona en la nota A41-WP/22 presentada por el Consejo de la OACI.

2.4 Con el tiempo, la integración de los requisitos y las disposiciones de ciberseguridad entre los diferentes anexos y documentos se hará más compleja. Por este motivo, podría ser necesario evaluar la creación de un nuevo Anexo para reducir la complejidad de dicha integración y garantizar el desarrollo transversal de SARP para abordar medidas que mitiguen los eventos intencionados o no y, sobre todo, las amenazas que puedan provocar efectos de seguridad secundarios/acumulativos que no necesariamente se identifiquen de inmediato como una forma de interferencia digital.

Integración de la transformación digital

2.5 La continua evolución de la transformación digital en diversos ámbitos produce tecnologías más conectadas, como el mantenimiento predictivo de los aparatos, la toma de decisiones basada en inteligencia artificial y/o en aprendizaje automático, la computación perimetral, la arquitectura abierta y las actualizaciones «por el aire» de sistemas de telecomunicaciones críticos.

2.6 Los últimos conceptos de movilidad aérea dan como resultado tecnologías nuevas y eficientes. No obstante, las cadenas de suministro aeroespacial no se rigen necesariamente por las reglas y normas tradicionales de la aviación civil nacional. Las nuevas cadenas de suministro crean oportunidades ocultas para introducir posibles vulnerabilidades en un entorno operativo ya de por sí complejo, donde la superficie de ataque, que antes se reducía a los sistemas heredados, se amplía ahora hasta tecnologías vinculadas desconocidas. En general, la mayor interconectividad y el aumento de las dependencias requieren una clara estructura normativa aeroespacial que respalde la certificación continua de las aeronaves y la aeronavegabilidad.

2.7 Los principios de la seguridad por diseño forman parte de un enfoque de políticas de ciberseguridad que se señaló en la Estrategia de Ciberseguridad de la Aviación de la OACI. A tal efecto, los planes de trabajo dirigidos a proteger digitalmente al sector y respaldar tecnologías de última generación, productos y servicios innovadores deben ser agnósticas y abordar la totalidad del sistema de la aviación civil. No solo se limita a respaldar un concepto de marco de confianza ni a sugerir modificaciones de los anexos y documentos, sino también un completo plan de trabajo multidisciplinar mediante un enfoque en múltiples fases.

3. CONCLUSIÓN

3.1 Las políticas y obligaciones de ciberseguridad de la aviación internacional que permitan a los operadores regulados y a sus cadenas de suministro obtener un retorno de la inversión eficiente son críticas para la sostenibilidad del sector de la aviación. Además, también lo es la necesidad de que la OACI y los estados apoyen los esfuerzos internacionales para permitir al sector innovar y aumentar la resiliencia de la aviación civil con nuevas cadenas de suministro. Es fundamental promover un enfoque basado en la seguridad por diseño, con una naturaleza multidisciplinar y en varias fases que integre las disposiciones y los requisitos en un plan de trabajo universal, bajo la competencia del AHCCC, en todos los paneles, grupos de trabajo y de estudio de la OACI.

3.2 Este plan de trabajo centrado en la seguridad por diseño deberá establecer la referencia básica para un ecosistema integrado, ciberresiliente, ágil e innovador, para así reducir la frecuencia y las consecuencias de los ciberataques contra los estados y el sector que podrían afectar a la seguridad y a todo el sector de la aviación civil internacional en su conjunto.

— FIN —