



ASAMBLEA — 42º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 24: Iniciativas prioritarias de seguridad operacional de la aviación y navegación aérea

ESTRATEGIA DE SEGURIDAD DE LOS DATOS AERONÁUTICOS DEL ADS-B

(Nota de estudio presentada por Colombia y apoyada por Estados miembros²
de la Comisión Latinoamericana de Aviación Civil (CLAC))

RESUMEN

La vigilancia dependiente automática – radiodifusión (ADS-B) ha transformado la gestión del tránsito aéreo al ofrecer alta precisión, disponibilidad de datos en tiempo real y una mayor eficiencia en la administración del espacio aéreo. Sin embargo, su diseño basado en protocolos no cifrados lo hace vulnerable a ataques cibernéticos, electrónicos y riegos frente a la privacidad de la información y protección de datos, lo que puede degradar la calidad de la información usada para el control de tránsito aéreo (ATC) y generar amenazas en el uso y la privacidad de la información reportada por las aeronaves que usan esta tecnología.

Para mitigar estos riesgos, se deben generar estrategias integrales que combinen el uso de múltiples datos de vigilancia tanto de sistemas colaborativos como no colaborativos, correlacionando información y generando una medida de confianza en los datos, aumentando la resiliencia y robustez tecnológica. Adicional la incorporación de prácticas avanzadas de ciberseguridad y el desarrollo de técnicas de detección de anomalías basadas en big data e inteligencia artificial, que permitan evaluar y garantizar la confianza de la información transmitida y el desarrollo de leyes y/o regulaciones nacionales que definan claramente el límite entre el uso público/privado de los datos transmitidos por estos sistemas y el nivel de afectación en la privacidad de usuarios de aeronaves privadas o de Estado.

El desarrollo de esta estrategia integral permitirá aumentar la calidad y la confianza de los datos aeronáuticos provistos por esta tecnología, identificar patrones inusuales y discrepancias de altitud o posición, e incluso mensajes falsos garantizando información de calidad para el servicio de ATC, y al mismo tiempo garantizar la protección de datos personales y privados de acuerdo con la legislación de cada país.

Este último aspecto, es de especial importancia ya que genera un nuevo reto para los Estados, la comunidad aeronáutica, y algunas empresas privadas, que tendrán que definir los límites y efectos que puede causar el uso indebido de datos aeronáuticos ADS-B en la privacidad de la información frente a la legislación de cada país.

Decisión de la Asamblea: Se invita a la Asamblea a:

- a) solicitar a la OACI que se avance en conjunto en regulaciones nacionales, estableciendo normas y mecanismos que regulen el acceso, publicación y uso de la información aeronáutica ADS-B, por parte de privados, con el fin de proteger la privacidad y la seguridad de la aviación, sin comprometer los beneficios que ofrece esta tecnología;

¹ La versión en español fue proporcionada por Colombia.

² Belice, Bolivia (Estado Plurinacional de), Chile, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela (República Bolivariana de)

	b) solicitar que se analice el uso de tecnologías de big data e inteligencia artificial como mecanismo predictivo de supervisión automática de la calidad de la información ADS-B y el establecimiento de un valor de confianza derivado del uso y medición de la precisión de la información ADS-B frente a la correlación de otros sistemas dentro un programa multisensorial como parte de los planes de navegación aérea regionales para mitigar los riesgos descritos del ADS-B; c) reconociendo que la integridad de los datos es esencial, ya que cualquier modificación en la información transmitida (por ejemplo, la altitud o posición de una aeronave) podría generar graves consecuencias, incluir la verificación de la integridad de los datos a través de controles de consistencia, como algoritmos de hash y uso de protocolos de protección de la integridad que aseguren que los datos no han sido alterados en tránsito, como el HMAC (Hashed Message Authentication Code); d) el hecho de que el ADS-B transmite datos en frecuencias de radio abiertas genera vulnerabilidades en cuanto a la confidencialidad de la información. A pesar de que actualmente el ADS-B no utiliza cifrado, evaluar la posibilidad de introducirlo, particularmente en áreas sensibles. La encriptación aseguraría que solo los sistemas autorizados pudieran descifrar y utilizar los datos; e) implementar sistemas redundantes de vigilancia (como radar primario o secundario) que puedan complementar los datos de ADS-B en caso de fallos y desarrollar mecanismos para identificar y mitigar el jamming o la interferencia; f) proporcionar capacitación a los operadores, técnicos y pilotos sobre los riesgos asociados al ADS-B y las mejores prácticas para mitigar esos riesgos. La concienciación es clave para detectar y reaccionar adecuadamente ante posibles amenazas.
<i>Objetivos estratégicos:</i>	Esta nota de estudio se relaciona con los Objetivos estratégicos: <i>Todos los vuelos son seguros, La aviación brinda movilidad fluida, accesible y confiable para todo el mundo; y Ningún país se queda atrás.</i>
<i>Repercusiones financieras:</i>	
<i>Referencias:</i>	Anexo 17 — <i>Seguridad de la aviación</i> Documento OACI: <i>Estrategia de Ciberseguridad de la Aviación</i> Documento OACI: <i>Orientación sobre la política de Ciberseguridad</i> Documento OACI: <i>Plan de acción de Ciberseguridad</i> FAA website - PIA and LADD NBAA website Ali, B. S., Ochieng, W. Y., Schuster, W., Majumdar, A., & Chiew, T. K. (2015). A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. <i>Safety Science</i>, 78, 91–100. https://doi.org/10.1016/J.SSCI.2015.04.011 Jeon, D., Eun, Y., & Kim, H. (2015). Estimation fusion with radar and ADS-B for air traffic surveillance. <i>International Journal of Control, Automation and Systems</i>, 13(2), 336–345. https://doi.org/10.1007/s12555-014-0060-1 Jamming and Spoofing Protection for ADS-B Mode S Receiver Through Array Signal Processing. <i>Lecture Notes in Electrical Engineering</i>, 555, 184–204. https://doi.org/10.1007/978-981-13-7086-1_13 Smith, A., Cassell, R., Breen, T., Hulstrom, R., & Evers, C. (2006). Methods to provide system-wide ADS-B back-up, validation and security. <i>AIAA/IEEE Digital Avionics Systems Conference - Proceedings</i>. https://doi.org/10.1109/DASC.2006.313681

1. INTRODUCCIÓN

1.1 El sistema de vigilancia dependiente automática – radiodifusión (ADS-B) ha transformado la gestión del tráfico aéreo, ofreciendo mayor precisión, eficiencia y disponibilidad de datos en tiempo real (actualización cada segundo) y menores costes en su instalación y mantenimiento. Esta tecnología permite una mejor gestión del espacio aéreo, optimizando rutas, mejorando la predicción de congestiones, contribuye a la gestión de flujos de tránsito aéreo (ATFM) y facilita la toma de decisiones en operativas en tiempo real. Sin embargo, el ADS-B basado en protocolos de transmisión no cifrados lo hace vulnerable presentando riesgos de seguridad que deben ser abordados para garantizar la integridad de la información y evitar efectos en la seguridad operacional.

1.2 El diseño del ADS-B, al basarse en protocolos de transmisión no cifrados, lo expone a diversos riesgos cibernéticos y electrónicos. Entre las amenazas más relevantes se encuentran la inyección de mensajes falsos, la suplantación de identidades y la interferencia deliberada con las señales. Estas vulnerabilidades comprometen la integridad del sistema y representan un riesgo significativo para la seguridad y protección del espacio aéreo y de las aeronaves.

1.3 La privacidad de los datos transmitidos por el sistema ADS-B constituye un aspecto crítico que requiere especial atención, particularmente en lo que respecta a la protección de datos personales, la identidad de los pasajeros, la seguridad nacional y la confidencialidad operativa. La publicación, explotación privada o exposición pública de datos aeronáuticos puede afectar la intimidad de las personas especialmente en vuelos de aviación general o aeronaves privadas, así como comprometer la seguridad de vuelos estatales, en especial en contextos internacionales. En este sentido, resulta fundamental establecer regulaciones claras sobre los niveles de acceso y autorización para el uso, difusión o comercialización de la información generada por el ADS-B.

1.4 Todo esto, evidencia la necesidad de desarrollar una estrategia para asegurar la seguridad de la información aeronáutica que proviene del ADS-B. Este desafío reside en encontrar el equilibrio entre la necesidad de utilizar esta data para mejorar la seguridad y la eficiencia de las operaciones, y la obligación de proteger los datos personales y privados de acuerdo con la legislación de cada país y la explotación comercial de privados de estos datos, en donde se requiere de un estándar global de protección.

1.5 Para mitigar estos riesgos, es necesario implementar una estrategia integral de seguridad que abarque diferentes aspectos, desde el fortalecimiento de la infraestructura tecnológica hasta el desarrollo de herramientas de análisis de datos y la implementación de marcos legales y regulatorios sólidos. La cooperación internacional y el intercambio de información entre los Estados son cruciales para abordar los desafíos de seguridad que plantea el ADS-B y garantizar la seguridad y eficiencia del espacio aéreo global.

1.6 Para mitigar de manera efectiva los riesgos, es necesario desarrollar estrategias integrales que combinen datos provenientes de sistemas de vigilancia colaborativos (como los radares secundarios) y no colaborativos (como los radares primarios). Al correlacionar la información generada por estos sistemas, se puede verificar de forma más precisa los blancos emitidos por las aeronaves, tanto hacia las estaciones en tierra como hacia los sistemas satelitales de baja órbita que envían datos a los centros de control. Este enfoque contribuye a aumentar la resiliencia y robustez tecnológica del sistema de vigilancia aérea, mejorando su capacidad para enfrentar amenazas y garantizar la seguridad en tiempo real.

2. ANÁLISIS

2.1 La tecnología ADS-B ha transformado la gestión del tráfico aéreo al proporcionar datos más precisos y en mayor cantidad, lo que permite una mayor flexibilidad en el espacio aéreo y optimiza

procesos como la facturación y la gestión de rutas. La tecnología cuenta con parámetros de calidad que son evaluados por los sistemas ATM y que contribuyen a la toma de decisiones. Sus beneficios incluyen la optimización del espacio aéreo, la mejora de la seguridad, especialmente en áreas con control limitado, la integración con tecnologías como big data e inteligencia artificial, y la transmisión de datos de alta calidad para la toma de decisiones en los sistemas ATM. En resumen, ADS-B no solo mejora la eficiencia y la seguridad, sino que también impulsa la modernización del espacio aéreo.

2.2 La tecnología ADS-B, depende de la transmisión de los datos propios de la aeronave y de otras tecnologías como los sistemas de posicionamiento global. Además, transmite la información mediante protocolos abiertos (no cifrados), lo que la hace vulnerable a: Primero, ciberataques (ataques a datos e información digital); segundo, perturbaciones electrónicas (susceptibilidad a interferencias electromagnéticas en la capa de radio), que podrían comprometer la integridad de la información generada y por ende la seguridad tanto safety como security y por último el uso no autorizado de la información aeronáutica transmitida.

2.3 En el primer aspecto se refiere a riesgos en el ciberespacio, podrían existir ataques de inyección de datos, suplantación de identidad, manipulación de los datos y denegación del servicio. En el segundo, bloqueos de las señales, ruido electromagnético, suplantación de fuentes de posicionamiento, y jamming dentro de la esfera de ciberseguridad.

2.4 El tercer aspecto, que es relevante, es que podría suponer riesgos para la privacidad de las personas, uso o publicación no autorizada de datos privados, en particular sobre la aviación general y exponer la aviación de estado a riesgos de seguridad de la aviación. Todo esto, esto podría suponer situaciones de riesgo para aeronaves, a los propios sistemas ATC, credibilidad sobre las aerolíneas y efectos sobre la privacidad de los usuarios del sistema.

2.5 En relación con la privacidad de los datos personales, la Administración Federal de Aviación (FAA) ha desarrollado Programa de Limitación de Datos de Aeronaves (LADD) y el Programa de Dirección de Privacidad de OACI (PIA) para abordar preocupaciones sobre la privacidad en el sistema ADS-B. Este programa permite a los propietarios de aeronaves registradas en EE.UU. solicitar una dirección ICAO alternativa y temporal, evitando que su identificación esté vinculada directamente al registro civil de aeronaves.

2.6 La National Business Aviation Association (NBAA) ha expresado preocupaciones sobre la privacidad en el sistema ADS-B, especialmente en el caso de los operadores de aeronaves privadas y corporativas, en el mismo sentido que esta nota de estudio, evidenciando que se expone información sensible de vuelos privados, lo que puede facilitar el rastreo no autorizado y la explotación de los datos, abogando por regulaciones que equilibren la transparencia con la protección de la privacidad de los propietarios, viajeros o usuarios.

2.7 Algunos fabricantes han indicado que el programa PIA tiene ciertas limitaciones que pueden hacer que algunos operadores duden en utilizarlo. En el caso en comento, su uso está restringido exclusivamente al espacio aéreo de EE.UU., lo que significa que no es válido para vuelos internacionales, incluidos los que cruzan el Golfo de México o el Caribe. Además, revertir la dirección ICAO de privacidad a la dirección permanente requiere un proceso técnico de mantenimiento, que en algunos casos implica la reprogramación del sistema de la aeronave. Esto hace que el cambio no pueda realizarse de manera inmediata. Otra limitación importante es que la aeronave podría perder acceso a ciertos servicios provistos por ARINC y SITA que no reconocen la dirección temporal.

2.8 Los Estados vienen fortaleciendo sus sistemas de vigilancia aérea mediante una estrategia integral que combina infraestructura tecnológica avanzada y el desarrollo de software basado en big data e

inteligencia artificial. En donde estrategias como la implementación de un sistema multisensor con sensores primarios, secundarios y ADS-B en áreas de alta densidad de vuelos, junto con medidas de seguridad y ciberseguridad en las redes de comunicación contribuyen al problema técnico. A nivel de software, se desarrollan herramientas para caracterizar el tráfico aéreo y detectar anomalías automáticamente, mejorando la confianza en la información utilizada por los servicios de ATC. Este enfoque optimiza la seguridad y eficiencia para la aviación del país y debe hacer parte del plan de navegación aérea de cada región.

2.9 Con respecto al tercer aspecto, la privacidad de la información, se plantea a nivel de los Estados una discusión, sobre la limitación del uso de la información aeronáutica generada por el ADS-B desde una perspectiva regulatoria o legislativa de acuerdo a cada norma de protección de datos de cada Estado, que permita discernir frente a la privacidad de los datos aeronáuticos y el derecho a ser explotados por terceros o visibles al público en general y los efectos que esta explotación pueda causar sobre la privacidad y seguridad de las aeronaves, tanto física como operacional, en el caso de vuelos de aviación general, privados o de aviación de estado y la subsecuente protección legal de acuerdo a esta definición y alcance del derecho a la privacidad, en cada país (regulatoria).

2.10 Esto, motivado en la creciente explotación de datos aeronáuticos, como los proporcionados por ADS-B a través de plataformas comerciales lo que plantea serias preocupaciones sobre los efectos de estas prácticas sobre la privacidad y seguridad de usuarios de aeronaves privadas y de Estado. La falta de cifrado y la naturaleza de radiodifusión de ADS-B; hacen que la información de vuelo, incluyendo posición e identificación única de la aeronave, sea accesible al público, lo que puede comprometer la seguridad de las operaciones y la privacidad de los pasajeros. Es crucial que la comunidad aeronáutica, los Estados y las empresas privadas trabajen en conjunto para establecer normas y mecanismos que regulen el acceso y uso de esta información, con el fin de proteger la privacidad y la seguridad de la aviación, sin comprometer los beneficios que ofrece la tecnología ADS-B.

2.11 Frente a este aspecto regulatorio, un estándar global actualizado sería importante, se propone una discusión entre los Estados, los explotadores y empresas privadas que publican los datos, con el fin de tomar medidas para desde las legislaciones nacionales y a través de la autoridad de aviación civil, garantizar la protección de datos personales y privados que puedan ser afectados por la publicación no autorizada de datos aeronáuticos, de acuerdo con las leyes de cada país.

2.12 Es fundamental abordar el impacto en la seguridad y privacidad de los pasajeros que podría resultar de la divulgación y el uso comercial no autorizados de información aeronáutica en plataformas web. Solo a través de un diálogo constructivo con las empresas que gestionan dichos datos y una regulación efectiva del uso de información aeronáutica, se podrá mitigar la explotación en línea de estos datos. De esta forma, se garantiza el derecho a la privacidad y seguridad tanto de los vuelos como de sus ocupantes, especialmente en el ámbito de la aviación privada y de estado.

2.13 En conclusión, si bien ADS-B es una herramienta esencial para la gestión del tráfico aéreo, también presenta vulnerabilidades que exigen la atención de los Estados. Es crucial una estrategia integral que combine mejoras tecnológicas, análisis de datos y marcos legales para proteger la información y la privacidad. Además, se deben desarrollar mecanismos que regulen el uso de la información ADS-B, especialmente la divulgación comercial de datos de aeronaves privadas o de Estado, para proteger la privacidad de los usuarios y prevenir posibles riesgos a la seguridad de los Estados.