



ASAMBLEA — 42º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 13: Seguridad de la aviación — Política

**ENFOQUE HOLÍSTICO DE LA CIBERSEGURIDAD EN LA AVIACIÓN:
DEL CONCEPTO A LA REALIDAD**

(Nota presentada por Dinamarca en nombre de la Unión Europea y sus Estados miembros¹, los demás Estados miembros de la Conferencia Europea de Aviación Civil² y por EUROCONTROL, y con la coautoría del Brasil, Kazajstán y el Perú)

RESUMEN

A medida que la aviación está cada vez más interconectada, las ciberamenazas presentan mayores riesgos para la seguridad, la seguridad operacional y la eficacia de la aviación. En la presente nota se destaca la necesidad de un enfoque holístico de la ciberseguridad para superar la fragmentación de los esfuerzos dirigidos a la mitigación de los riesgos relacionados con la ciberseguridad.

Dicho enfoque holístico debería aplicarse a los principios clave de la ciberseguridad, como el establecimiento de marcos de gobernanza, la integración de características de seguridad en el diseño de los sistemas, la gestión proactiva de los ciberriesgos en consonancia con los protocolos de seguridad operacional y seguridad de la aviación y la instrucción basada en competencias sobre ciberseguridad en todos los ámbitos de la aviación. El enfoque prioriza la resiliencia durante el ciclo de vida, la coordinación mundial y la integración con las estrategias existentes. Se insta a la OACI a poner al día sus políticas, fomentar la colaboración y promover iniciativas de creación de capacidad para armonizar las prácticas de ciberseguridad en todo el mundo.

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

- a) alentar a la OACI a que siga fortaleciendo sus políticas y normas y métodos recomendados con el fin de apoyar un enfoque holístico de la ciberseguridad, y a que vele por que todos sus órganos de trabajo colaboren para integrar la ciberseguridad en otros marcos de reglamentación, promoviendo así una incorporación integral y coordinada de las medidas de ciberseguridad en la aviación civil;
- b) exhortar a los Estados miembros y a las partes interesadas pertinentes a que adopten un enfoque holístico de la ciberseguridad en todo el ecosistema de la aviación civil con el fin de aplicar un enfoque armonizado, proactivo y basado en el ciclo de vida para gestionar y mitigar los riesgos relacionados con la ciberseguridad;

¹ Alemania, Austria, Bélgica, Bulgaria, Chequia, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumanía y Suecia.

² Albania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Georgia, Islandia, Macedonia del Norte, Mónaco, Montenegro, Noruega, Reino Unido, República de Moldova, San Marino, Serbia, Suiza, Türkiye y Ucrania.

c) alentar a la OACI a que promueva iniciativas de creación de capacidad para ayudar a los Estados miembros a adoptar un enfoque holístico de ciberseguridad, aprovechando al máximo las actividades de creación de capacidad y sus recursos propios; y d) reconocer en la resolución A42-XX, propuesta para poner al día la resolución A41-19 de la Asamblea sobre las formas de abordar la ciberseguridad en la aviación civil, la necesidad de atender las ciberamenazas y ciberriesgos de la aviación civil de manera holística.	
<i>Objetivos estratégicos:</i>	Esta nota de estudio se relaciona con el objetivo estratégico: Todos los vuelos son seguros y protegidos.
<i>Repercusiones financieras:</i>	<i>Las acciones mencionadas en esta nota estarán sujetas a la disponibilidad de recursos en el Presupuesto del programa regular y/o de contribuciones extrapresupuestarias.</i>
<i>Referencias:</i>	Resolución A41-19 de la Asamblea

1. INTRODUCCIÓN

1.1 Como la aviación está cada vez más interconectada y digitalizada, las ciberamenazas presentan mayores riesgos a la seguridad operacional, la seguridad y la eficacia de la aviación. Esto se ve intensificado por la rapidez con que evoluciona el ámbito de los macrodatos y de las funciones y servicios avanzados de procesamiento de datos. Además, la aviación civil se está convirtiendo en un ecosistema sumamente innovador y complejo según se van integrando e interconectando cada vez más los sistemas y aplicaciones, tanto avanzados como tradicionales, mediante las mejoras en las capacidades de red y el uso de componentes «inteligentes».

1.2 Estos vínculos presentan nuevos desafíos para la confidencialidad, la integridad y la disponibilidad de la información. Estos desafíos deben atenderse de forma holística, velando por la seguridad de cada aspecto del ecosistema de la aviación, desde el diseño de los sistemas hasta la gestión estratégica, de manera que se pueda aplicar sistemáticamente en todo el mundo.

1.3 Para evitar esfuerzos fragmentados y aislados, un enfoque holístico extiende los conceptos de ciberseguridad a todos los ámbitos de las prácticas organizacionales, las medidas proactivas y reactivas y las capacidades de las autoridades pertinentes y del sector. Este enfoque integral homogeneiza los esfuerzos de ciberseguridad en todas las actividades de la aviación civil, lo que permite un enfoque sistemático en la gestión de riesgos y la resiliencia. Tal enfoque facilita la integración de las perspectivas tradicionales de seguridad operacional y seguridad de la aviación civil con las cuestiones de ciberseguridad en los sistemas y las estrategias de gestión organizacional, lo que mejora su eficacia y rendimiento.

1.4 El establecimiento del Comité Ad Hoc de Coordinación de la Ciberseguridad (AHCCC) por parte del Consejo de la OACI durante el trienio 2022-2025 representa un paso positivo e importante para tratar la ciberseguridad con mayor coordinación. Esta iniciativa ofrece una gran oportunidad para hacer avanzar aún más un enfoque verdaderamente holístico e integrado de la ciberseguridad. La incorporación sistemática de la ciberseguridad en todas las actividades, marcos de reglamentación y prioridades estratégicas de la OACI servirá para fortalecer la resiliencia en todo el mundo y para que el sector de la aviación cuente con una buena preparación para responder a la complejidad y los cambios constantes de las ciberamenazas.

3. ANÁLISIS

3.1 Un enfoque holístico permite evaluar las ciberamenazas y mitigar los riesgos en todo el ecosistema en lugar de tratarlos en componentes aislados. Integrar la ciberseguridad en todo el desarrollo y las operaciones del sistema puede permitir a los Estados miembros y a las partes interesadas de la aviación consolidar su resiliencia y contribuir a un sector de la aviación seguro, protegido y mejor preparado para el futuro.

El enfoque holístico debería servir de guía para la aplicación de los principios fundamentales de la ciberseguridad, como:

3.1.1 **Gobernanza de la ciberseguridad:** Un enfoque holístico de la gobernanza refuerza la toma de decisiones, la asignación de recursos y la colaboración entre los distintos sectores de la aviación. Una gobernanza eficaz permite ajustar los objetivos de ciberseguridad a los objetivos estratégicos y operacionales, ofreciendo un marco de trabajo estructurado para la gestión de recursos. En su marco se definen las partes interesadas clave, los procesos de toma de decisiones, los marcos jurídicos y las políticas para guiar los esfuerzos en materia de ciberseguridad, lo que ayuda a la determinación de amenazas y riesgos. Además, la gobernanza de la ciberseguridad debería integrarse orgánicamente en los ámbitos de la seguridad operacional y la seguridad de la aviación, así como en la resiliencia del sector.

3.1.2 **Ciberseguridad desde el diseño:** Un enfoque holístico que integra «las características de seguridad en el diseño» considera la ciberseguridad como un elemento fundamental del ecosistema de la aviación, en lugar de considerarla accesorio. Este enfoque tiene sus beneficios ya que permite a las organizaciones la gestión proactiva de sus vulnerabilidades y el fortalecimiento de la resiliencia, incorporando la ciberseguridad en cada etapa del desarrollo. En combinación con una metodología de «seguridad por defecto», refuerza la infraestructura y los procesos de la aviación desde la concepción hasta la puesta en marcha. La implementación efectiva implica una modelización temprana de la amenaza, unos principios de ingeniería seguros y evaluaciones de los riesgos a lo largo del ciclo de vida para tratar las vulnerabilidades de forma preventiva. El monitoreo continuo, las actualizaciones regulares y los mecanismos de respuesta automatizados aumentan aún más la agilidad del sistema frente a ciberamenazas emergentes, lo que contribuye a garantizar una ciberseguridad sólida en todo el ecosistema de la aviación.

3.1.3 **Gestión de los ciberriesgos:** El ámbito de la tecnología y del procesamiento de datos cambia rápidamente dentro de la aviación civil, por lo que es crucial determinar y proteger activos e infraestructuras fundamentales (por ejemplo, la gestión del tránsito aéreo) y hacerlos resilientes a los ciberataques, incluidas las amenazas emergentes como la inteligencia artificial. El carácter interconectado de los sistemas modernos amplía las posibilidades de ciberataques, por lo que se necesita una gestión holística de los ciberriesgos. Al vincular la gestión de los ciberriesgos con otras disciplinas de gestión de riesgo, la aviación puede crear un marco de trabajo integral y resiliente, que permita un equilibrio entre la seguridad operacional, la seguridad de la aviación y la eficacia. Esta estrategia refuerza la capacidad de mitigación de los riesgos y fortalece la resiliencia contra amenazas fluctuantes relacionadas con el ciberespacio.

3.1.4 **Conocimientos y competencias en ciberseguridad:** La elaboración de un enfoque holístico de la instrucción de la ciberseguridad en la aviación es esencial para desarrollar competencias robustas. Esta estrategia integral permite que las personas adquieran las aptitudes necesarias para gestionar eficazmente los riesgos y las medidas de ciberseguridad. La instrucción debe ser pragmática, ajustada a funciones específicas e integrar conocimientos teóricos con experiencias prácticas. Una cultura de aprendizaje continuo ayuda al personal de la aviación a mantenerse al día de las prácticas y tendencias más recientes y a aplicar buenas prácticas, lo que le permite determinar sus vulnerabilidades y aplicar estrategias de mitigación eficaces. Programas, talleres y simulaciones regulares deberían impartirse a todos los niveles e incluir a todas las personas empleadas y no solo al personal informático. Este enfoque de instrucción no

solo fortalece la ciberresiliencia general del ecosistema de la aviación, sino que brinda herramientas a todo el personal para anticipar y responder mejor a la ciberamenazas, mejorando así el nivel de ciberseguridad del sector.

3.2 La OACI, en cuanto líder mundial en la promoción de mejores prácticas en la aviación, desempeña un papel crucial en el fortalecimiento de la ciberseguridad de la aviación. Dados los distintos niveles de madurez y recursos de los países, la OACI debería promover iniciativas de creación de capacidad con el fin de apoyar a los Estados miembros para que adopten enfoques holísticos de ciberseguridad. Al mismo tiempo, la OACI debería hacer un mejor uso de las actividades de creación de capacidad existentes (por ejemplo, los seminarios interregionales sobre innovación y ciberseguridad, organizados en el marco de los proyectos CASE, financiados por la Comisión Europea y llevados a cabo por la Conferencia Europea de Aviación Civil (CEAC), o los cursos de ciberseguridad que imparte la CEAC) y de sus propios recursos. Estas iniciativas deberían promover un enfoque coherente y coordinado para reforzar las capacidades en ciberseguridad, fomentando, a la vez, la colaboración internacional mediante el intercambio de mejores prácticas.

3.3 Además, la OACI debería cerciorarse de que sus normas y métodos recomendados y políticas y herramientas se mantengan al día, proporcionando a los Estados miembros los marcos necesarios para gestionar eficazmente los ciberriesgos y adoptar un enfoque holístico de la ciberseguridad. Asimismo, los órganos de trabajo de la OACI deberían estrechar su colaboración para garantizar la integración efectiva de las disposiciones relativas a la ciberseguridad con otros requisitos de reglamentación. En este contexto, el Comité Ad Hoc de Coordinación de la Ciberseguridad (AHCCC) desempeña un papel de facilitador y guía en esta coordinación, apoyando una estrategia integral y coherente en todo el sector de la aviación.

3.4 Con el fin de hacer progresar este enfoque integral, se propone que la Asamblea de la OACI, en su 42º período de sesiones, reconozca en la resolución A42-XX, que actualiza la resolución A41-19, la necesidad de hacer frente a las ciberamenazas y los ciberriesgos para la aviación civil de forma holística. Incorporar este reconocimiento al nivel de la Asamblea reforzará el compromiso de los Estados miembros con la integración sistemática de la ciberseguridad en todas las actividades de la aviación, propiciando la armonización en todo el mundo y aumentando la resiliencia colectiva del sector.

4. MEDIDAS PROPUESTAS A LA ASAMBLEA

Se invita a la Asamblea a que adopte las medidas expuestas anteriormente.