



**NOTA DE ESTUDIO**

**ASAMBLEA — 40º PERÍODO DE SESIONES**

**COMITÉ EJECUTIVO**

**Cuestión 12: Seguridad de la aviación — Política**

**PROPUESTA REFERENTE A LA ESTRUCTURA DE GOBERNABILIDAD DE LA OACI  
EN MATERIA DE CIBERSEGURIDAD**

(Presentado por el Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales ICCAIA)

**RESUMEN**

La ciberseguridad en la aviación civil representa un campo amplio, complejo y multidisciplinar que abarca aspectos sobre tecnología de la información, seguridad tradicional en aviación, gestión de seguridad e impactos operativos en aviación. Dado que la ciberseguridad es transversal, los paneles y grupos de estudio actuales de la OACI no resultan efectivos al coordinar actividades en relación con esta seguridad. Existe la necesidad de establecer una entidad de la OACI, administrada por los Estados miembro y con apoyo proveniente del sector, que no se vea limitada por la estructura organizativa existente en la propia OACI. Esta entidad debe tener la capacidad de garantizar que todas las actividades de ciberseguridad se coordinan de forma efectiva a través de la OACI, y que las interconexiones de esta seguridad con otras disciplinas son gestionadas adecuadamente. Esta entidad debe ser responsable de una estrategia común de la OACI sobre ciberseguridad, así como de alinear y orientar el trabajo realizado por los paneles y grupos de estudio existentes.

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

- a) solicitar al Consejo el establecimiento de una entidad de ciberseguridad para la aviación civil, administrada por los Estados miembro con apoyo proveniente del sector, que pueda trabajar transversalmente para consolidar y armonizar las actividades relacionadas con ciberseguridad a través de la OACI;
- b) solicitar al Consejo la aprobación de la estrategia de ciberseguridad desarrollada por el Grupo de estudio de la Secretaría sobre cibernética (SSGC), al tiempo que reconoce que el SSGC no fue estructurado para tratar el carácter horizontal y la naturaleza interdisciplinaria de la ciberseguridad;
- c) indicar al Secretario General que se coordine con los Estados y el sector para armonizar los procesos de gestión de riesgos en ciberseguridad, teniendo en consideración el trabajo de armonización ya realizado a nivel regional o nacional; y
- d) solicitar al Consejo que inste a los Estados de diferentes regiones al desarrollo de capacidades de gestión de crisis en ciberseguridad y que se coordine a nivel internacional para impedir la pérdida de confianza de los pasajeros debido a incidentes de ciberseguridad dentro de la aviación local.

<sup>1</sup> Las versiones en español, árabe, chino, francés, inglés y ruso fueron proporcionadas por ICCAIA.

<i>Objetivos estratégicos:</i>	Este documento de trabajo se refiere a objetivos estratégicos relativos a: seguridad operacional; capacidad y eficiencia de la navegación aérea; protección y facilitación
<i>Implicaciones financieras:</i>	Las actividades referidas en este documento dependerán de los recursos disponibles en el Presupuesto del programa regular 2020-2022 o de contribuciones presupuestarias adicionales.
<i>Referencias:</i>	Resoluciones de la Asamblea en vigor (a partir del 6 de octubre de 2016) (Doc 10075)

## 1. INTRODUCCIÓN

1.1 La ciberseguridad en la aviación civil representa un campo amplio, complejo y multidisciplinar que abarca aspectos sobre gestión de tecnología de la información, seguridad tradicional en aviación, gestión de seguridad e impactos operativos en la aviación.

1.2 Las actividades en ciberseguridad se han iniciado habitualmente sobre casos locales y particulares; actualmente existe la necesidad de una coordinación global y reforzada para garantizar que se tienen en cuenta la totalidad de aspectos y que no aparezca ninguna laguna o duplicación. Además, dado que la propia ciberseguridad se entrecruza con muchas actividades dentro de la OACI, resulta necesario garantizar la aplicación de una coordinación adecuada entre todas las disciplinas a fin de hacer cumplir la definición y operación de un proceso de toma de decisiones y diseño integrales que tenga en cuenta, entre otros aspectos, la protección en aviación, así como la seguridad física y cibernética en la misma.

1.3 Dado que la ciberseguridad es transversal, los paneles y grupos de estudio actuales de la OACI no resultan efectivos al coordinar actividades en relación con esta seguridad. Existe la necesidad de establecer una entidad de la OACI, administrada por los Estados miembro y con apoyo del sector, que no se vea limitada por la estructura organizativa y política existente de la propia OACI. Esta entidad debe tener la capacidad de garantizar que todas las actividades de ciberseguridad se coordinan de forma efectiva a través de la OACI, y que las interconexiones de esta seguridad con otras disciplinas son gestionadas adecuadamente. Esta entidad debe ser responsable de una estrategia común de la OACI sobre ciberseguridad, así como de alinear y orientar el trabajo realizado por los paneles y grupos de estudio existentes.

1.4 La intención es minimizar los gastos generales, junto con los impactos en la organización, así como potenciar, en la medida de lo posible, las estructuras existentes que desempeñan el trabajo, para llegar a considerarse como una entidad orientada al establecimiento de una estrategia y visión, además de otorgar liderazgo y orientación. Estaría compuesta tanto por los representantes de los Estados miembros de la OACI como por los expertos en ciberseguridad individual y sectorial que, en común, llevarían a cabo el trabajo y propondrían recomendaciones acordadas de forma conjunta como decisiones.

## 2. ANÁLISIS

2.1 Una entidad de ciberseguridad centralizada posee el potencial de tratar algunos de los asuntos señalados en la introducción, ya que podría ayudar a respaldar la necesidad de una gobernabilidad interdominio dentro de la aviación global y en referencia a actividades de ciberseguridad en la propia OACI. Este tipo de entidad de la OACI necesita tenerse en cuenta con cautela a fin de alcanzar con éxito las necesidades y objetivos de la comunidad de aviación civil a nivel global. Tanto las ventajas como las desventajas de las distintas organizaciones (como el Panel o Comité del consejo) deben sopesarse con cuidado frente a las necesidades y al objetivo aquí descritos.

2.2 Esta entidad de ciberseguridad centralizada, en caso de contar con los recursos correctos, podría aportar:

- una mayor gama de experiencias para la membresía, así como conocimientos propios del sector, en concreto, sobre el tema de la ciberseguridad en la aviación civil;
- un enfoque armonizado para la gestión de riesgos con un conjunto de metodologías acordadas por todas las partes interesadas, que se nutra de la experiencia regional y nacional;
- la capacidad de crear grupos de trabajo o asignar tareas a las entidades existentes con el objetivo de focalizar el esfuerzo en el desarrollo de Estándares y Prácticas Recomendadas, materiales de orientación, programas, desarrollo de capacidad, apoyo y formación, según se necesite;
- la consideración de todos los temas sobre ciberseguridad (ciberseguridad para protección en vuelo, operaciones, mantenimiento, ciberdelitos...) en una única entidad; y
- un equipo de expertos en ciberseguridad mixta y especialistas en operaciones y seguridad que representen a todas las partes interesadas implicadas en todos los gobiernos y el sector. Como mínimo, esto debe incluir aeródromos, compañías aéreas, proveedores y fabricantes de aeronaves, operadores de mantenimiento, así como proveedores de servicios de navegación.

2.3 Dada la naturaleza multidisciplinar y transversal de la ciberseguridad, se recomienda el desarrollo de una coordinación exhaustiva entre las disciplinas de seguridad en aviación y la propia protección en aviación a través de sólidos vínculos entre la Comisión de Navegación Aérea, el Comité de Interferencia Ilícita, los Paneles y los Grupos de estudio. Con el entendimiento de que la ciberseguridad posee una naturaleza en rápida evolución, así como de sus interacciones con las nuevas tecnologías, esta entidad en ciberseguridad debe ser capaz de potenciar la participación de todos los expertos globales, incluidos los individuos y organizaciones que no formen parte de la lista de «organizaciones invitadas» actuales (<https://www.icao.int/about-icao/Pages/Invited-Organizations.aspx>).

2.4 Con el reconocimiento de que los conceptos presentados dentro de la estrategia en ciberseguridad desarrollada por el SSGC representan un punto de partida adecuado sobre el que evolucionar, esta entidad de ciberseguridad debe encargarse de desarrollar y ejecutar un plan de acción para todos los asuntos relacionados con cada dominio de la aviación civil en ciberseguridad, aparte de mantener la visión, ámbito y estrategia en la ciberseguridad de la OACI. Esta entidad de ciberseguridad de la OACI debe sacar provecho de las numerosas y ya desarrolladas iniciativas en ciberseguridad, tanto a nivel regional como nacional, como medio para acelerar la definición y adopción de estándares y orientaciones. Además, esta entidad de ciberseguridad debe, entre otros aspectos:

2.4.1 Consolidar la estrategia del SSGC y armonizar el trabajo que realizan los grupos y paneles (es decir, el Grupo de estudio del marco de confianza o *Trust Framework Study Group*, TFSG; el Panel sobre seguridad en la aviación, AVSEC –*Aviation Security*–, etc.) para desarrollar conjuntos de principios, medidas y acciones en ciberseguridad albergados en un marco sustentado sobre ocho pilares:

- Cooperación internacional
- Gobernabilidad

- Normativas y legislación efectivas
- Políticas
- Distribución de información
- Declaración de riesgos globales en relación con la ciberseguridad en la aviación
- Gestión de incidentes y continuidad e impacto operativos
- Desarrollo de capacidades, formación y cultura para una ciberseguridad sólida

2.4.2 Impulsar el Grupo de trabajo sobre amenazas y riesgos (WGTR), trabajar en la evaluación de los riesgos en ciberseguridad de la aviación civil, posiblemente como un grupo de trabajo de esta nueva entidad o bien tras ser designado de forma adecuada dentro de los departamentos. Existe una gran necesidad de establecer orientaciones y criterios para asegurar resultados de análisis comparables cuando son utilizados por diferentes Estados miembro y organizaciones.

2.4.3 Trabajar con el Grupo de estudio del marco de confianza para ayudar en el desarrollo de los resultados de trabajo y, tras su período de 2 años de existencia, continuar armonizando y desarrollando los resultados, así como asignar de forma adecuada el trabajo continuado dentro de los departamentos, o como se considere apropiado.

### 3. CONCLUSIÓN

3.1 La cooperación y coordinación internacionales son necesarias con objeto de armonizar políticas y normativas que permitan una continuidad e interoperabilidad de la ciberseguridad a nivel mundial, así como una continuidad operativa. Los paneles y grupos de estudio actuales de la OACI no resultan efectivos al coordinar actividades en relación con esta seguridad. Existe la necesidad de establecer una entidad de la OACI, administrada por los Estados miembro y con apoyo proveniente del sector, que no se vea limitada por la estructura organizativa existente en la propia OACI. Esta entidad debe tener la capacidad de garantizar que todas las actividades de ciberseguridad se coordinan de forma efectiva a través de la OACI, y que las interconexiones de esta seguridad con otras disciplinas son gestionadas adecuadamente.