

**NOTA DE ESTUDIO****ASAMBLEA — 39º PERÍODO DE SESIONES****COMITÉ EJECUTIVO****Cuestión 16: Seguridad de la aviación — Política****FORMAS DE ABORDAR LA CIBERSEGURIDAD EN LA AVIACIÓN CIVIL**

(Nota presentada por el Consejo de la OACI)

**RESUMEN**

El funcionamiento eficiente, seguro y protegido de la aviación civil internacional depende en gran medida de la disponibilidad de sistemas de tecnología de la información y las comunicaciones (ICT), así como de la precisión y confidencialidad de los datos. La protección y resiliencia de los sistemas de aviación contra ciberamenazas y vulnerabilidades sólo pueden impulsarse adoptando un enfoque global, colaborativo y armonizado que reúna el saber y la experiencia colectiva de las áreas de seguridad de la aviación, navegación aérea, seguridad informática y otras áreas pertinentes.

En 2013, la OACI, el Consejo Internacional de Aeropuertos (ACI), la Organización de Servicios de Navegación Aérea Civil (CANSO), la Asociación del Transporte Aéreo Internacional (IATA) y el Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales (ICCAIA) establecieron el Grupo de alto nivel de la industria (IHLG) como mecanismo de cooperación de alto nivel sobre cuestiones de interés e importancia común, entre las que se incluye la ciberseguridad. A este respecto, el IHLG determinó que la ciberseguridad en la aviación civil es una cuestión horizontal de alta prioridad que requiere medidas armonizadas y coordinadas de todas las partes interesadas pertinentes.

Para fomentar aún más un enfoque sistemático y coherente en la gestión de amenazas y riesgos contra la ciberseguridad, la OACI y los miembros del IHLG elaboraron el proyecto de resolución que se presenta en el apéndice de esta nota, que se dirige a abordar la ciberseguridad en la aviación civil con un enfoque abarcador, transversal y funcional. Los objetivos son reafirmar la importancia y urgencia de proteger los sistemas de infraestructura y los datos críticos de la aviación civil contra las ciberamenazas y obtener de la OACI, sus Estados miembros y las partes interesadas de la industria el compromiso de actuar a fin de dar respuesta al problema de la ciberseguridad en la aviación civil de forma colaborativa y sistemática y mitigar las amenazas y riesgos que la afectan.

**Decisión de la Asamblea:** Se invita a la Asamblea a adoptar el proyecto de resolución sobre *Formas de abordar la ciberseguridad en la aviación civil* que se presenta en el Apéndice.

<i>Objetivos estratégicos:</i>	Esta nota se relaciona con los objetivos estratégicos A — <i>Seguridad operacional</i> , B — <i>Capacidad y eficiencia de la navegación aérea</i> y C — <i>Seguridad de la aviación y facilitación</i> .
<i>Repercusiones financieras:</i>	Las actividades indicadas en esta nota de estudio se emprenderán en la medida en que se disponga de recursos provenientes del presupuesto del Programa regular para 2017-2019 y/o de contribuciones extrapresupuestarias.
<i>Referencias:</i>	<i>Resoluciones vigentes de la Asamblea</i> (al 4 de octubre de 2013) (Doc 10022)

## APÉNDICE

### PROYECTO DE RESOLUCIÓN DE LA ASAMBLEA FORMAS DE ABORDAR LA CIBERSEGURIDAD EN LA AVIACIÓN CIVIL

#### **Resolución 16/xx: Formas de abordar la ciberseguridad en la aviación civil**

*Considerando* que el sistema de aviación mundial es un sistema altamente complejo e integrado que comprende tecnología de la información y las comunicaciones de carácter crítico para la seguridad y protección de las operaciones de aviación civil;

*Observando* que el sector de la aviación depende cada vez más de la disponibilidad de sistemas de tecnología de la información y las comunicaciones, así como de la integridad y confidencialidad de los datos;

*Consciente* de que la amenaza planteada por los incidentes que afectan a la ciberseguridad en la aviación civil evoluciona rápida y continuamente, que quienes montan esas amenazas lo hacen con la intención de causar daño, buscando interrumpir las actividades y robar información por razones políticas, económicas o de otra índole, y que la amenaza puede mutar fácilmente hasta llegar a afectar sistemas críticos de la aviación civil en todo el mundo;

*Reconociendo* que no todos los problemas de ciberseguridad que afectan a la seguridad operacional de la aviación civil se relacionan con actos ilícitos y/o intencionales, y que en consecuencia deberían resolverse instrumentando sistemas de gestión de la seguridad operacional;

*Reafirmando* la importancia y urgencia de proteger de ciberamenazas a los sistemas de infraestructura de la aviación civil y los datos críticos;

*Considerando* la necesidad de trabajar en colaboración en pro del desarrollo de un marco mundial eficaz y coordinado para que las partes interesadas de la aviación civil aborden los retos de la ciberseguridad, junto con medidas de corto plazo para aumentar la resiliencia del sistema de aviación mundial ante las ciberamenazas que atenten contra la seguridad operacional de la aviación civil;

*Destacando* el valor de las iniciativas, los planes de acción, las publicaciones y demás medios concebidos para abordar los problemas de ciberseguridad en colaboración y de forma integral;

*Recordando* las iniciativas de quienes dirigen el Consejo Internacional de Aeropuertos (ACI), la Organización de Servicios de Navegación Aérea Civil (CANSO), la Asociación del Transporte Aéreo Internacional (IATA), el Consejo Coordinador Internacional de Asociaciones de Industrias Aeroespaciales (ICCAIA) y la OACI, quienes reconocieron la necesidad de trabajar juntos y guiarse por una misma visión, estrategia y hoja de ruta para reforzar el sistema de aviación mundial y hacerlo resiliente ante las ciberamenazas; y

*Reconociendo* la naturaleza polifacética y multidisciplinaria de los problemas de ciberseguridad y sus soluciones;

La Asamblea:

1. *Exhorta* a los Estados y las partes interesadas de la industria a adoptar las medidas siguientes para contrarrestar las ciberamenazas a la aviación civil:

- a) identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y los sistemas críticos de la aviación civil y las graves consecuencias que pueden resultar de tales incidentes;
- b) definir las responsabilidades de los organismos nacionales y las partes interesadas de la industria con respecto a la ciberseguridad en la aviación civil;
- c) fomentar una interpretación común entre los Estados miembros de las ciberamenazas y riesgos y la formulación de criterios comunes para determinar cuáles bienes y sistemas son de carácter crítico y es preciso protegerlos;
- d) fomentar la coordinación entre gobierno e industria con respecto a las estrategias, políticas y planes de ciberseguridad de la aviación, así como el intercambio de información para ayudar a identificar las vulnerabilidades críticas que sea necesario resolver;
- e) formar y participar en asociaciones y mecanismos público-privados entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación;
- f) sobre la base de una interpretación común de las ciberamenazas y riesgos, adoptar un enfoque flexible y basado en el riesgo para proteger los sistemas de aviación críticos mediante la implantación de sistemas de gestión de la ciberseguridad;
- g) fomentar una sólida cultura de la ciberseguridad en todos los aspectos al interior de los organismos nacionales y en todo el sector de la aviación;
- h) determinar las consecuencias jurídicas de los actos que comprometen la seguridad operacional de la aviación explotando vulnerabilidades cibernéticas;
- i) promover la elaboración y aplicación de normas internacionales, estrategias y mejores prácticas para proteger los sistemas críticos de tecnología de la información y las comunicaciones que se usan en la aviación civil de interferencias que puedan atentar contra la seguridad operacional de la aviación civil;
- j) establecer políticas y destinar recursos cuando sea necesario para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura; que sean resilientes; que tengan métodos seguros de transferencia de datos que garanticen su integridad y confidencialidad; que tengan métodos de vigilancia, detección y notificación de incidentes y que se lleven a cabo análisis forenses de los incidentes; y
- k) colaborar en el desarrollo del marco de ciberseguridad de la OACI adoptando un enfoque abarcador, transversal y funcional que integre la navegación aérea, las comunicaciones, la vigilancia, las operaciones de aeronaves, la aeronavegabilidad y demás disciplinas pertinentes.

2. *Encarga a la Secretaria General que:*

- a) ayude y facilite la tarea de los Estados y la industria para la adopción de estas medidas; y
- b) se asegure de que los asuntos de ciberseguridad reciban plena atención y se los coordine en todas las disciplinas pertinentes dentro de la OACI.

— FIN —