Organización de Aviación Civil Internacional

A41-WP/22
EX/10
7/7/22

NOTA DE ESTUDIO

ASAMBLEA — 41º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Asunto núm. 14: Seguridad de la aviación — Política

CIBERSEGURIDAD EN LA AVIACIÓN CIVIL

(Nota presentada por el Consejo de la OACI)

RESUMEN

El sector de la aviación ha ido aumentando de forma constante a lo largo de los años su sensibilización sobre la importancia de hacer frente a las ciberamenazas a la aviación civil, a pesar de algunas dificultades que se atribuyen principalmente, de forma directa e indirecta, a la crisis de la pandemia de COVID-19. Aunque se han producido muchos avances a nivel nacional, regional e internacional, debe trabajarse aún más, especialmente a nivel nacional, para procurar un enfoque holístico, armonizado y coherente de la ciberseguridad de la aviación en todo el sector de la aviación civil.

En esta nota de estudio se presenta un examen de las actividades relacionadas con la ciberseguridad de la aviación, incluidas las actividades encomendadas por la Asamblea, y se propone una actualización de la Resolución A40-10 sobre *Formas de abordar la ciberseguridad en la aviación civil* para resaltar la importancia de mejorar la ciberseguridad y la ciberresiliencia del sector de la aviación civil.

Decisión de la Asamblea: Se invita a la Asamblea a:
a) tomar nota de los desarrollos en actividades de ciberseguridad de la aviación; y
b) adoptar la resolución revisada de la Asamblea sobre *Formas de abordar la ciberseguridad en la aviación civil*, presentada en el apéndice, para sustituir a la resolución A40-10 de la Asamblea.

Objetivos estratégicos:	Esta nota se relaciona con los objetivos estratégicos siguientes: *Capacidad y eficiencia de la navegación aérea, Seguridad operacional y Seguridad de la aviación y Facilitación*.
Repercusiones financieras:	Las actividades mencionadas en esta nota de estudio se espera que se lleven a cabo con los recursos disponibles en el Presupuesto regular para 2023-2025 y/o con contribuciones extrapresupuestarias según el Plan de Actividades 2023-2025 de la OACI.
Referencias:	Doc 10140, *Resoluciones Vigentes de la Asamblea (al 4 de octubre de 2019)* Doc 10118, *Plan Global para la Seguridad Operacional de la Aviación* Doc 9750, *Plan Mundial de Navegación Aérea* *Estrategia de Ciberseguridad de la Aviación* *Plan de Acción de Ciberseguridad*

1. INTRODUCCIÓN

1.1 En el 39º período de sesiones de la Asamblea de la OACI se pidió a la Organización que velase por que las ciberamenazas a la aviación civil se examinen plenamente y se ayude a los Estados y la industria a adoptar las medidas necesarias. El Grupo de Estudio de la Secretaría sobre Ciberseguridad (SSGC) se estableció en 2017 a fin de llevar adelante este trabajo.

1.2 Durante su 40º período de sesiones, la Asamblea reiteró la importancia y urgencia de un compromiso mundial de todas las partes interesadas a tomar medidas para ocuparse de la ciberseguridad de la aviación civil de manera colaborativa y adoptar la Estrategia de Ciberseguridad de la Aviación. También pidió a la OACI que formulara un plan de acción para apoyar la aplicación de la Estrategia de Ciberseguridad de la Aviación, y que continuara asegurándose de que las cuestiones de ciberseguridad se consideren y coordinen de manera transversal. Además, señaló algunas brechas en la estructura que aborda la ciberseguridad en la OACI y debatió un conjunto de criterios que podrían sustentar una estructura revisada de ciberseguridad.

1.3 Cabe señalar que la pandemia de COVID-19 afectó el progreso de la labor de la OACI en materia de ciberseguridad de la aviación debido a la reorientación de los recursos para apoyar las tareas críticas de gestión de la crisis y de asistencia para la reanudación y la recuperación de la aviación civil, así como las restricciones financieras que enfrentó la Organización durante los primeros ocho meses de 2020, lo que provocó la pérdida de recursos de ciberseguridad.

2. ANÁLISIS

2.1 Plan de Acción de Ciberseguridad

2.1.1 En consonancia con la Resolución A40-10 de la Asamblea, la OACI elaboró y publicó en noviembre de 2020 el Plan de acción de ciberseguridad (CyAP) para apoyar a los Estados y a las partes interesadas en la aplicación de la Estrategia de Ciberseguridad de la Aviación. El CyAP proporciona las bases para que la OACI, los Estados y las partes interesadas trabajen juntos, y propone una serie de principios, medidas y acciones para lograr los objetivos de los siete pilares de la Estrategia de Ciberseguridad (cooperación internacional; gobernanza, legislación y reglamentación eficaces; políticas de ciberseguridad; compartición de información; manejo de incidentes y planificación de emergencias; creación de capacidad, instrucción y cultura de ciberseguridad).

2.1.2 Teniendo en cuenta los cambios de prioridades de los Estados miembros debido a la actual pandemia de COVID-19, y la experiencia de los Estados y las partes interesadas en la implementación de iniciativas de ciberseguridad de la aviación en sus Estados y organizaciones, la OACI realizó un examen del CyAP y publicó una segunda edición del documento en enero de 2022. El examen incluyó una optimización del documento para que fuera más conciso y claro y se aclararon los puntos de acción en términos de medidas, indicadores y tiempo de iniciación.

2.2 Fortalecimiento del mecanismo para abordar la ciberseguridad en la OACI

2.2.1 En el 40º período de sesiones de la asamblea de la OACI se tomó nota de los distintos órganos que se ocupaban de la ciberseguridad en la Organización y se expresó preocupación por las posibles deficiencias, duplicaciones, incoherencias y pérdida de transparencia. A fin de atender esas preocupaciones, la Asamblea solicitó a la OACI que incluyera la labor de esos grupos en una estructura general y debatió acerca de una serie de criterios que podrían servir de base para una estructura revisada de gobernanza de la ciberseguridad.

2.2.2 Durante su 218º período de sesiones, el Consejo respaldó la metodología para la elaboración de un estudio de viabilidad y análisis de carencias del mecanismo para abordar las cuestiones de ciberseguridad. Las dos primeras fases del estudio se presentaron durante el 219º periodo de sesiones del Consejo. El Consejo pidió a la Secretaría que considerara aún más el estudio de viabilidad y que lo actualizara, y delegó en el Presidente del Consejo la facultad de establecer un grupo de trabajo reducido formado por representantes en el Consejo y miembros de la Comisión de Aeronavegación (ANC) para la formulación de la fase 3 del estudio de viabilidad, con la asistencia de la Secretaría. El grupo de trabajo reducido se reunió en numerosas ocasiones entre noviembre de 2020 y enero de 2021, consideró varias opciones de gobernanza y recomendó una solución que fue aprobada por el 222º período de sesiones del Consejo. La nueva estructura de gobernanza para la ciberseguridad de la OACI incluye:

a) conversión del Grupo de Estudio de la Secretaría sobre Ciberseguridad en un Grupo Experto en Ciberseguridad que rinda cuentas al Comité de Seguridad de la Aviación del Consejo de la OACI;

b) conversión del Grupo de Estudio sobre el Marco de Confianza para integrarlo a la estructura de Grupo Experto de la ANC; y

c) establecer un Comité *Ad hoc* de Coordinación de la Ciberseguridad (AHCCC) en el marco del Consejo. El Comité se compone de un miembro de cada una de las siguientes instancias: Comité de Transporte Aéreo, Comité de Seguridad de la Aviación, Comisión de Aeronavegación, así como un miembro de cada grupo experto de la OACI y de grupos expertos que abordan los elementos de ciberseguridad en su programa de trabajo. Se espera que el Comité ofrezca al Consejo, y a todos los que participan en actividades de la OACI relacionadas con la ciberseguridad, un único punto de coordinación para todas las actividades de la OACI relacionadas con la ciberseguridad, mejorando así la rendición de cuentas, la transparencia, la eficiencia y la coordinación de la labor de la OACI sobre la ciberseguridad y la ciberresiliencia de la aviación. Durante su 224º período de sesiones, el Consejo aprobó las atribuciones del AHCCC.

2.2.3 Seguidamente de la decisión del Consejo sobre la nueva estructura de gobernanza, el Grupo Experto en Ciberseguridad se estableció en el 225º período de sesiones y celebró su primera reunión en mayo de 2022. La ANC, durante su 219º período de sesiones aprobó la conversión del Grupo de Estudio sobre el Marco de Confianza en un nuevo Grupo Experto de la ANC a fin de que continúe la labor relativa al Marco de Confianza para la Aviación Internacional.

2.3 Elaboración de un Marco de Confianza para la Aviación Internacional

2.3.1 Desde su 223º período de sesiones, el Consejo ha venido examinando la elaboración de un Marco de Confianza para la Aviación Internacional. Seguirá haciendo progresar esta labor, incluido el concepto de operaciones y la gobernanza de ese Marco.

2.4 Suficiencia de los instrumentos de derecho aeronáutico internacional frente a la ciberamenazas a la aviación civil

2.4.1 La Estrategia de Ciberseguridad de la Aviación pide que se analicen los instrumentos jurídicos internacionales pertinentes a fin de identificar las disposiciones jurídicas clave existentes o que hacen falta para la prevención, el enjuiciamiento y la reacción oportuna ante los ciberincidentes. En consecuencia, esta tarea se reflejó en el Plan de Acción de Ciberseguridad como una medida para la OACI. Por esa razón, el SSGC creó el Subgrupo de Investigación sobre Aspectos Jurídicos (RSGLEG). El subgrupo está formado por expertos en derecho y ciberseguridad para disponer de todos los conocimientos que se requieren para

abordar sus objetivos. Según lo acordado por el RSGLEG en su última reunión de enero de 2022, la Secretaría informó sobre la labor realizada por el subgrupo en el 38º período de sesiones del Comité Jurídico, que se celebró en marzo de 2022.

2.5 Textos de orientación

2.5.1 En consonancia con el Plan de Acción de Ciberseguridad, la OACI elaboró textos de orientación para apoyar a los Estados y las partes interesadas en su gestión de la ciberseguridad en la aviación civil. Entre los materiales preparados están los siguientes (publicados en ICAO-NET bajo "Publications" y "Others":

a) Guía sobre el uso del Protocolo del Semáforo (TLP), que proporciona una orientación para los Estados y las partes interesadas sobre el uso del TLP para facilitar el intercambio de información sobre ciberseguridad;

b) Orientación sobre política de ciberseguridad, que trata sobre la protección y resiliencia de la infraestructura crítica de la aviación civil internacional frente a las ciberamenazas, y el requisito de cooperación multilateral en la aviación civil, así como con autoridades externas. La orientación también aborda la necesidad de designar la autoridad competente para la ciberseguridad de la aviación e incluye una plantilla para apoyar a los Estados y a las partes interesadas en la formulación de una política de ciberseguridad; y

c) Cultura de ciberseguridad en la aviación civil, que apoye el diseño y la aplicación de una cultura de ciberseguridad sólida, aprovechando el éxito de la aviación civil en la implementación de las culturas de seguridad operacional y seguridad de la aviación.

2.6 Creación de capacidad

2.6.1 En 2020, la OACI elaboró una hoja de ruta sobre la instrucción en ciberseguridad para apoyar los esfuerzos de la Organización de crear capacidad para proporcionar instrucción en materia de ciberseguridad de la aviación que sea adecuada, coherente y relevante para los Estados y las partes interesadas. La hoja de ruta sobre la instrucción en ciberseguridad apoya la Estrategia de Ciberseguridad de la Aviación y el Plan de Acción de Ciberseguridad. Su creación también apoya la Resolución A40-25 de la Asamblea: *Implementación de estrategias de instrucción y creación de capacidad en la aviación*, que establece cómo la OACI, a través de las actividades de instrucción, ayudará y apoyará a los Estados en el desarrollo de recursos humanos y capacidades suficientes. Siguiendo la hoja de ruta sobre la instrucción, la OACI comenzó a crear una cartera de instrucción en ciberseguridad que incluye hasta la fecha los siguientes cursos:

2.6.1.1 Programa de gestión técnica y fundamentos del liderazgo en ciberseguridad de la aviación: este curso se elaboró en colaboración con la Universidad Aeronáutica Embry-Riddle y comenzó a impartirse en octubre de 2021. Se trata de un curso de conciencia integral que cubre todos los aspectos de ciberseguridad abordados en la Estrategia de Ciberseguridad de la Aviación.

2.6.1.2 Gestión del riesgo de seguridad de la aviación en la gestión del tránsito aéreo (ATM): este curso se elaboró en colaboración con EUROCONTROL. El curso cubre la seguridad de la ATM e incluye tanto los elementos físicos como los elementos de ciberseguridad. La primera sesión del curso se dictará en noviembre de 2022.

2.6.1.3 Vigilancia de la ciberseguridad en la aviación civil: este curso está siendo diseñado en colaboración con la Administración de Aviación Civil del Reino Unido. El curso cubre los aspectos clave que servirían de apoyo a los Estados en el diseño y la implementación de sus obligaciones de vigilancia para la ciberseguridad de la aviación.

2.7 Sensibilización y actividades de divulgación

2.7.1 La sensibilización de los Estados y las partes interesadas sobre la importancia de abordar la ciberseguridad en la aviación civil ha sido una actividad fundamental de la OACI. La Organización sigue estando muy involucrada en la organización y/o participación de conferencias, reuniones y webinarios nacionales, regionales e internacionales con el fin de promover la cooperación entre todas las partes interesadas en el ámbito de la ciberseguridad y la ciberresiliencia, así como promover la aplicación de la Estrategia de Ciberseguridad de la Aviación y el Plan de Acción de Ciberseguridad.

2.8 Auditoría de las obligaciones de ciberseguridad en el marco del CMA del USAP

2.8.1 El objetivo del Enfoque de Observación Continua del Programa Universal de Auditoría de la Seguridad de la Aviación (CMA-USAP) es mejorar la seguridad de la aviación mundial a través de la auditoría y la observación continua del desempeño de los Estados miembros en materia de seguridad de la aviación. El personal auditor identifica la documentación en la que se establece el requisito de que los explotadores o entidades identifiquen sus sistemas de tecnología de la información y las comunicaciones y datos críticos que se utilicen para los fines de la aviación civil. También se asegura de que este requisito incluya la evaluación, elaboración y aplicación de medidas para proteger dicha información y sistemas de cualquier interferencia ilícita. Una vez identificado el requisito, el personal de auditoría se asegura de que las responsabilidades relacionadas con las medidas de ciberseguridad estén claramente asignadas.

2.8.2 De los 136 Estados auditados al 31 de diciembre de 2021, los aspectos relacionados con la documentación en materia de preparación para la ciberseguridad se habían auditado en 54 Estados. Los resultados de las auditorías de esos Estados indican lo siguiente:

a) un 15% de los Estados no había establecido el requisito de que los explotadores o entidades identifiquen sus sistemas de tecnología de la información y las comunicaciones y datos críticos que se utilicen para los fines de la aviación civil, y que de acuerdo con una evaluación de riesgos elaboren e implementen las medidas que correspondan para protegerlos de interferencias ilícitas;

b) un 26% de los Estados no había definido las responsabilidades de los explotadores o entidades con respecto a la ciberseguridad en la aviación civil; y

c) un 41% de los Estados no había elaborado criterios para la protección de los sistemas de tecnología de la información y las comunicaciones y datos críticos que se utilicen para los fines de la aviación civil de interferencias ilícitas.

2.8.3 Estos resultados no son necesariamente indicativos del panorama mundial en relación con la protección de la aviación de las ciberamenazas, ya que algunos Estados fueron auditados a distancia debido a la pandemia y sus resultados son incompletos. Además, el tamaño de la muestra general no es lo suficientemente representativo como para proporcionar un alto grado de confianza. Sin embargo, estos resultados muestran claramente que el sector de la aviación civil necesita mejorar sus esfuerzos para hacer frente a las ciberamenazas hasta alcanzar una base que permita una protección coherente y armonizada ante las ciberamenazas a la aviación civil, su mitigación y su respuesta.

— — — — — — — —

APÉNDICE

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

~~A40-10~~A41-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~~ sistemas que son~~,~~ críticos para la seguridad y protección de las operaciones de aviación civil;

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

Consciente de que las ciberamenazas ~~planteada por los incidentes que afectan~~ a la aviación civil evolucionan rápida y continuamente, que ~~los autores de esas amenazas tienen la intención de causar daño, buscando interrumpir las actividades y robar información por razones políticas, económicas o de otra índole,~~ la aviación sigue siendo un objetivo para los delincuentes, tanto en el ámbito cibernético como en el físico, y que las ciberamenazas pueden mutar ~~fácilmente~~ hasta llegar a afectar sistemas críticos de la aviación civil en todo el mundo;

Reconociendo que no todos los ~~problemas~~sucesos 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 aplicando sistemas de gestión de la seguridad operacional~~;

Reconociendo la naturaleza polifacética y multidisciplinaria de los problemas de ciberseguridad y sus soluciones, y observando que los riesgos cibernéticos pueden afectar simultáneamente una amplia gama de áreas de la aviación y propagarse con rapidez;

Reafirmando las obligaciones estipuladas en el Convenio sobre Aviación Civil Internacional (Convenio de Chicago) de velar por la seguridad operacional, la seguridad y la continuación de la aviación civil;

Considerando que el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* (Convenio de Beijing) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves* (Protocolo de Beijing) mejorarían el marco jurídico mundial para tipificar los ciberataques contra la aviación civil internacional como delitos, por lo que la ratificación de ambos instrumentos por los Estados garantizaría la disuasión y el castigo de dichos ataques en cualquier parte del mundo donde se produzcan;

Reafirmando la importancia y urgencia de ~~proteger~~ abordar la ciberseguridad y la ciberresiliencia ~~a~~ de los sistemas ~~de infraestructura~~ de la aviación civil ~~y~~, los datos e información críticos ~~de~~ frente a las ciberamenazas y peligros, entre ellos las interfaces comunes entre la aviación civil y la militar;

Considerando la necesidad de trabajar en colaboración para crear un marco mundial eficaz y coordinado que permita ~~a las partes interesadas de la aviación civil~~ abordar ~~los retos de~~ la ciberseguridad de la aviación~~, junto con medidas de corto plazo~~ y ~~aumentar~~ apoyar la ciberseguridad y la ciberresiliencia del sistema de

aviación mundial ante las ciberamenazas que atenten contra la seguridad operacional y/o seguridad de la aviación civil;

Reconociendo la labor y el liderazgo de la OACI en los ámbitos de ~~del Grupo de estudio de la Secretaría sobre Ciberseguridad,~~ ciberseguridad y ciberresiliencia de la aviación, ~~que contribuyó sobremanera al formato de la Estrategia de ciberseguridad al vincular las características de la seguridad operacional y la seguridad de la aviación a la ciberseguridad enfoque transversal del tema~~ a lo largo de las distintas disciplinas de la aviación;

Reconociendo que es necesario armonizar la ciberseguridad en la aviación a nivel mundial, regional y nacional con miras a ~~promover la coherencia en todo el mundo y~~ asegurar la coherencia y plena interoperabilidad de las medidas de protección y los sistemas de gestión de riesgos; ~~y~~

Reconociendo la importancia de establecer un plan claro de gobernanza y rendición de cuentas a nivel nacional para la ciberseguridad de la aviación civil, incluida la designación de una autoridad nacional competente encargada de la seguridad de la aviación en coordinación con las autoridades y organismos nacionales interesados; y

Destacando el valor de las importantes iniciativas, planes de acción, publicaciones y demás medios concebidos para abordar los problemas de ciberseguridad en colaboración y de forma ~~integral~~ holística.

La Asamblea:

1. *Insta* a los Estados miembros ~~y a la OACI a promover la adopción universal e implementación~~ a adoptar y ratificar ~~d~~el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* (Convenio de Beijing) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves* (Protocolo de Beijing) como instrumentos para hacer frente a los ciberataques contra la aviación civil;

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

a) implantar la ~~e~~Estrategia ~~sobre~~ de ~~c~~ Ciberseguridad de la Aviación de la OACI, y utilizar el Plan de Acción de Ciberseguridad de la OACI como herramienta para apoyar la implementación de la Estrategia de Ciberseguridad de la Aviación;

b) designar la autoridad competente en materia de ciberseguridad de la aviación y definir la interacción entre dicha autoridad y los organismos nacionales interesados;

c) ~~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;~~

c) definir las responsabilidades de los organismos nacionales y las partes interesadas de la industria con respecto a la ciberseguridad en la aviación civil;

d) elaborar e implementar un marco sólido de gestión de riesgos de ciberseguridad que se base en prácticas pertinentes de gestión de riesgos de seguridad de la aviación y seguridad operacional, y adoptar un enfoque basado en los riesgos para proteger los sistemas, información y datos críticos de la aviación civil de las ciberamenazas;

~~j~~e) establecer políticas e instrumentos y destinar recursos ~~cuando sea necesario~~ para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura; que los sistemas estén protegidos y sean resilientes; que los datos estén seguros y disponibles cuando estén almacenados y mientras sean transferidos ~~tengan métodos seguros de transferencia de datos que garanticen su integridad y confidencialidad~~; que tengan métodos de vigilancia, detección y notificación de incidentes; que se elaboren y se pongan en práctica planes de recuperación de incidentes; y que se lleven a cabo análisis forenses de los ciberincidentes; ~~y~~

~~d) fomentar una interpretación común entre los Estados miembros de las ciberamenazas y riesgos y la formulación de criterios comunes para determinar qué bienes y sistemas son de carácter crítico y es preciso proteger;~~

~~e~~f) 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;

g) fomentar la cooperación civil/militar en lo que respecta a la identificación, protección y vigilancia de las vulnerabilidades y los flujos de datos comunes en las interfaces entre los sistemas de aviación civil y militar, y colaborar en la respuesta a las ciberamenazas comunes y en la recuperación de los ciberincidentes;

~~f~~h) formar y participar en asociaciones y mecanismos entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación;

~~g) 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;~~

~~h~~i) ~~fomentar~~diseñar y aplicar una sólida cultura de ciberseguridad ~~en todos los aspectos dentro de los organismos nacionales y~~ en todo el sector de la aviación civil;

j) alentar a los Estados a que sigan aportando su contribución a la OACI en la elaboración y aplicación de normas, estrategias y mejores prácticas internacionales para hacer que progresen la ciberseguridad y la ciberresiliencia de la aviación;

~~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;~~

~~k~~j) colaborar continuamente en el desarrollo del marco de ciberseguridad de la OACI adoptando un enfoque horizontal, intersectorial y funcional que integre la seguridad operacional de la aviación, la seguridad de la aviación, la facilitación, la navegación aérea, las comunicaciones, la vigilancia, la gestión del tránsito aéreo, las operaciones de aeronaves, la aeronavegabilidad y demás disciplinas pertinentes.

3. *Encarga* a la ~~Secretaría General~~ OACI que:

a) siga promoviendo la adopción y ratificación universal del Convenio para la Represión de Actos Ilícitos relacionados con la Aviación Civil Internacional (Convenio de Beijing) y el Protocolo

Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (Protocolo de Beijing); y

~~a) formule un plan de acción para ayudar a los Estados y la industria a adoptar la Estrategia de ciberseguridad;~~

b) continúe asegurándose de que los asuntos de ciberseguridad y ciberresiliencia se examinen y coordinen de forma transversal por medio ~~de los mecanismos apropiados conforme se estipula en la estrategia~~ del nuevo mecanismo de la OACI que trata el tema de la ciberseguridad.

— FIN —