



NOTA DE ESTUDIO

ASAMBLEA — 42° PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 13: Seguridad de la aviación – Política

CIBERSEGURIDAD EN LA AVIACIÓN CIVIL

(Presentada por el Consejo de la OACI)

RESUMEN

La concienciación y las medidas del sector de la aviación civil para hacer frente a las ciberamenazas y los ciberriesgos a la aviación civil han ido en constante aumento. Durante el último trienio se han producido muchos acontecimientos en la OACI, así como en los Estados a nivel nacional, regional y mundial. Sin embargo, es necesario seguir trabajando, especialmente a nivel nacional, para garantizar un enfoque holístico, armonizado y coherente de la ciberseguridad de la aviación en todo el sector de la aviación civil. En esta nota se hace una reseña general de las actividades relacionadas con la ciberseguridad de la aviación, incluidas las encomendadas por la Asamblea, y se propone una actualización de la resolución A41-19 sobre *Formas de abordar la ciberseguridad en la aviación civil* para hacer hincapié en la importancia de mejorar la protección y la resiliencia del sector de la aviación civil frente a las ciberamenazas y los ciberriesgos, teniendo en cuenta al mismo tiempo el desarrollo de la labor de la OACI sobre este tema.

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

- tomar nota de la evolución de las actividades de ciberseguridad de la aviación; y
- adoptar la resolución de la Asamblea sobre *Formas de abordar la ciberseguridad en la aviación civil* que figura en el apéndice.

<i>Objetivos estratégicos:</i>	Esta nota de estudio se relaciona con las metas estratégicas: <i>Todos los vuelos son seguros y protegidos</i> y <i>Movilidad fluida, accesible y confiable para todo el mundo</i> .
<i>Repercusiones financieras:</i>	Las actividades a que se refiere la presente nota de estudio se llevarán a cabo con sujeción a los recursos disponibles en el presupuesto regular 2026-2028 y/o a contribuciones extrapresupuestarias, según lo previsto en el Plan de Actividades 2026-2028 de la OACI.
<i>Referencias:</i>	<i>Resoluciones vigentes de la Asamblea</i> (al 7 de octubre de 2022) (Doc 10184) <i>Estrategia de Ciberseguridad de la Aviación</i> <i>Plan de Acción sobre Ciberseguridad de la Aviación Civil</i>

1. INTRODUCCIÓN

1.1 El sector de la aviación civil está presenciando una rápida evolución en el uso de la información y las nuevas tecnologías para satisfacer sus necesidades de automatización, interconectividad e interoperabilidad, así como la puesta en práctica de nuevos conceptos operacionales en tierra y en el aire y la integración nuevos participantes, como los sistemas de aeronaves no tripuladas (UAS), en el sistema de transporte aéreo. El objetivo final de estos avances es contribuir al crecimiento del sector de la aviación civil y velar por su seguridad, protección, eficiencia, capacidad y sostenibilidad.

1.2 Sin embargo, esta tendencia generó un aumento de las ciberamenazas a los datos, la información y los sistemas operacionales, agravado por las tensiones geopolíticas que se observan en todo el mundo. Aunque no se han notificado ciberataques que tengan impactos significativos en la seguridad operacional o la protección de la aviación, el sector está presenciando una tendencia al alza en la notificación de incidentes cibernéticos, que hasta la fecha parecen estar motivados principalmente por beneficios económicos, robo de información o intrusiones cibernéticas con fines de activismo¹.

1.3 La creciente complejidad de las ciberamenazas y sus posibles repercusiones en la aviación civil ponen de manifiesto la necesidad de un enfoque mundial sólido y armonizado para mejorar la protección y la resiliencia de la aviación civil frente a las ciberamenazas. En ese sentido, la OACI sigue colaborando con los Estados miembros, las organizaciones internacionales y la industria y prestando apoyo en la mitigación de los ciberriesgos para el sector de la aviación civil.

1.4 La Asamblea de la OACI, en su 41º período de sesiones, tomó nota con satisfacción de la evolución de la labor de la OACI en materia de ciberseguridad de la aviación durante el último trienio (2019-2022), y elogió a la OACI y a sus grupos expertos por su trabajo. En particular, la Asamblea acogió con beneplácito la adopción e implementación de una estructura de gobernanza interna mejorada para la ciberseguridad de la aviación en la OACI, así como el desarrollo continuo de políticas, disposiciones, orientaciones, creación de capacidad e iniciativas de sensibilización sobre la ciberseguridad de la aviación. La Asamblea, en su 41º período de sesiones, también adoptó la resolución A41-19 sobre *Formas de abordar la ciberseguridad en la aviación civil*, que sustituyó a la resolución A40-10 de la Asamblea.

2. ANÁLISIS

2.1 Normas y métodos recomendados para la ciberseguridad de la aviación

2.1.1 En respuesta a la medida CyAP3.4 en el *Plan de Acción sobre Ciberseguridad de la Aviación Civil* (CyAP), que solicita a la OACI que “examine las normas y métodos recomendados (SARPS) de la OACI existentes para identificar la necesidad de posibles actualizaciones de la ciberseguridad”, en 2022, la OACI llevó a cabo un análisis individual exhaustivo de 16 Anexos del *Convenio sobre Aviación Civil Internacional* (Convenio de Chicago), con el objetivo de identificar posibles ámbitos de interés en los SARPS de la OACI relacionados con la ciberseguridad de la aviación, en apoyo de un enfoque holístico y transversal de la ciberseguridad de la aviación en las disposiciones de la OACI.

2.1.2 El análisis fue entregado al Grupo Experto en Ciberseguridad, que creó el Equipo Especial sobre Normas y Métodos Recomendados de Ciberseguridad (TF-CYSARPS) para que continúe estableciendo referencias cruzadas de los posibles ámbitos de interés entre todas las disciplinas de la aviación reflejadas en los Anexos pertinentes. Se creó el equipo especial para examinar si la ciberseguridad de la aviación se trata de manera adecuada (ya sea explícita o implícitamente) en los SARPS existentes,

¹ El documento *Consideraciones de la OACI sobre ciberriesgos mundiales* (Doc 10213 – Distribución limitada) de la OACI contiene más información sobre ciberamenazas y ciberriesgos para el sector de la aviación civil.

detectar posibles lagunas en el marco de los SARPS de la OACI y coordinar con los grupos expertos pertinentes para subsanar esas lagunas, según corresponda. Esta labor está en curso y se espera que continúe a lo largo del próximo trienio.

2.2 Instrumentos jurídicos internacionales

2.2.1 El “Estudio sobre los instrumentos de derecho aeronáutico internacional y su aplicabilidad a las ciberamenazas contra la aviación civil” presentado en el 38º período de sesiones del Comité Jurídico concluyó que el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional*² (Beijing, 2010 – “Convenio de Beijing de 2010”) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves*³ (Beijing, 2010 – “Protocolo de Beijing de 2010”), contienen importantes avances con respecto a los instrumentos más antiguos, proporcionando así una base suficiente para que los Estados aborden los ciberataques contra la aviación civil como delitos.

2.2.2 Al 1 de abril de 2024, 53 Estados miembros han ratificado el Convenio de Beijing de 2010 y 54 Estados miembros han ratificado el Protocolo de Beijing de 2010. Dado que estos instrumentos introducen disposiciones que son pertinentes para tratar los ciberataques contra la aviación civil, se recomienda encarecidamente que los Estados miembros adopten y ratifiquen ampliamente esos instrumentos, como se subraya en las resoluciones de la Asamblea relativas a tratar la ciberseguridad en la aviación civil, a fin de apoyar la disuasión de las ciberamenazas a la aviación civil y el enjuiciamiento de los ciberataques contra el sector.

2.3 Segunda edición del Plan Global para la Seguridad de la Aviación (GASeP)

2.3.1 En consonancia con la acción CyAP 2.5 del Plan de Acción sobre Ciberseguridad, según la cual “la OACI incluirá la ciberseguridad en los planes regionales y mundiales para velar por la seguridad operacional y la seguridad y la resiliencia de la aviación”, y beneficiándose de la actualización del GASeP cuya segunda edición se publicó en junio de 2024 (<https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx>), la OACI incluyó la ciberseguridad de la aviación en las disposiciones del plan en el marco de las prioridades mundiales 1, 2 y 4.

2.4 Textos de orientación

2.4.1 En consonancia con el Plan de Acción sobre Ciberseguridad, la OACI elaboró textos de orientación⁴ para ayudar a los Estados y a las partes interesadas a tratar la ciberseguridad en la aviación civil, que incluyen orientaciones sobre la gobernanza y las políticas de ciberseguridad de la aviación a nivel estatal, la cultura de la ciberseguridad en la aviación civil y la planificación e implementación del intercambio de información cibernética. La OACI también publicó *Consideraciones de la OACI sobre ciberriesgos mundiales* (Doc10213 – Distribución limitada), documento de orientación que proporciona una metodología para integrar la gestión de los ciberriesgos en los procesos de gestión de riesgos para la seguridad operacional de la aviación, la protección de la aviación civil y la eficiencia y la capacidad de la navegación aérea, e incluye una reseña de alto nivel del panorama mundial de las ciberamenazas y los ciberriesgos:

2.4.2 En consonancia con la recomendación 4.2/1 sobre ciberseguridad de la aviación de la Decimocuarta Conferencia de Navegación Aérea, el trabajo en curso sobre los textos de orientación incluye la elaboración de un conjunto completo de documentos de orientación para tratar los diferentes aspectos de la ciberseguridad de la aviación. También incluye un plan para compilar todos los textos de orientación en

² [Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional](#)

³ [Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves](#)

⁴ <https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx>

un manual de ciberseguridad de la aviación que abarque todos los aspectos relacionados con la protección y la resiliencia de las infraestructuras y servicios críticos de la aviación frente a las ciberamenazas y los ciberriesgos.

2.5 Marcos de confianza

2.5.1 Durante su 220º período de sesiones, celebrado en junio de 2022, la Comisión de Aeronavegación aprobó la creación del Grupo Experto en el Marco de Confianza (TFP). Desde entonces, el TFP ha estado apoyando la elaboración de textos de orientación para el establecimiento de marcos de confianza en cuanto a la interoperabilidad:

- a) se han elaborado orientaciones técnicas sobre la confianza en cuanto a la interoperabilidad y la garantía de la identidad, incluidas orientaciones sobre protección de la información (*Manual de información de seguridad de la aviación*, Doc 10204);
- b) se formula una política común de certificados de aviación para respaldar las identidades digitales interoperables, la autenticidad y el aseguramiento de la información en la aviación civil, incluido el respaldo a la autenticación de los sistemas de aumentación basados en satélites (SBAS) para los sistemas mundiales de navegación por satélite (GNSS);
- c) se elabora y mantiene una lista de casos de uso operacional en los que sería conveniente contar con marcos de confianza. Recientemente se ha comenzado a trabajar en la orientación para apoyar a las partes interesadas en la aviación en el establecimiento de instancias de marco de confianza; y
- d) se están ultimando, en estrecha coordinación entre los grupos expertos pertinentes, los textos de orientación para las comunicaciones seguras aire/tierra a través de la red de telecomunicaciones aeronáuticas (ATN) utilizando normas y protocolos de la familia de protocolos de Internet (IPS) en apoyo directo a la Enmienda 93 del Anexo 10 — *Telecomunicaciones aeronáuticas*, Volumen III — *Sistemas de comunicaciones*.

2.6 Programa de trabajo de ciberseguridad de la aviación de la OACI

2.6.1 El Consejo, durante su 228º período de sesiones, celebrado en 2023, aprobó el establecimiento, la composición y las atribuciones del AHCCC, tras identificar los recursos adecuados de la Secretaría para su funcionamiento. El AHCCC se compone de una persona miembro de cada una de los siguientes: Comité de Transporte Aéreo (ATC), Comité de Seguridad de la Aviación (ASC) y Comisión de Aeronavegación (ANC), así como 11 miembros de cada grupo experto que trata con regularidad la ciberseguridad en su programa de trabajo.

2.6.2 Las principales funciones del Comité consisten en coordinar la labor relacionada con la ciberseguridad de la aviación en toda la OACI mediante la elaboración y el mantenimiento de un amplio programa de trabajo sobre ciberseguridad de la aviación. También actúa como principal órgano asesor del Consejo sobre el establecimiento de prioridades entre los elementos de trabajo de conformidad con el programa de trabajo.

2.6.3 El AHCCC se ha reunido tres veces desde su creación y continúa perfeccionando el Programa de Trabajo de Ciberseguridad de la Aviación de la OACI a medida que el trabajo en ciberseguridad evoluciona y actúa como plataforma de colaboración para que los grupos expertos compartan información y contribuyan a un enfoque armonizado y uniforme de la ciberseguridad de la aviación en el contexto de sus respectivas esferas de trabajo.

2.7 Instrucción y creación de capacidad

2.7.1 La cartera de instrucción en ciberseguridad de la OACI incluye hasta la fecha dos cursos de ciberseguridad de la aviación:

- a) Fundamentos del liderazgo y la gestión técnica en el ámbito de la ciberseguridad de la aviación: este curso fue elaborado por la OACI en colaboración con la Universidad Aeronáutica Embry-Riddle y comenzó a impartirse en octubre de 2021. Se trata de un curso de concienciación integral que cubre todos los aspectos de ciberseguridad que se tratan en la Estrategia de Ciberseguridad de la Aviación. Durante el trienio anterior, el curso se dictó a 88 participantes entre septiembre de 2022 y abril de 2025; y
- b) Vigilancia de la ciberseguridad en la aviación civil: El curso fue elaborado por la OACI en colaboración con la Administración de Aviación Civil del Reino Unido y comenzó a impartirse en marzo de 2023. Abarca aspectos clave que ayudarían a los Estados a desarrollar e implementar un marco de supervisión para la ciberseguridad de la aviación, tomando como ejemplo la experiencia del Reino Unido. Durante el trienio anterior, el curso se impartió a 34 participantes entre marzo de 2023 y abril de 2025.

2.8 Actividades de sensibilización y divulgación

2.8.1 En consonancia con los llamamientos formulados en el 41º período de sesiones de la Asamblea para que la OACI intensifique sus campañas de sensibilización y lleve a cabo ejercicios teóricos de ciberseguridad de la aviación, la Organización se benefició de las generosas contribuciones voluntarias de Portugal y Singapur al programa de ciberseguridad de la aviación, lo que permitió que durante el trienio se impartiera una serie de cinco seminarios regionales de ciberseguridad de la aviación.

2.8.2 Los seminarios reunieron a participantes de todas las disciplinas pertinentes de la aviación y también distintas de la aviación (seguridad operacional de la aviación, seguridad de la aviación, navegación aérea, ciberseguridad, CERTS/CSIRTS nacionales, autoridades nacionales de ciberseguridad, fuerzas del orden, fuerzas militares, etc.). En total, los seminarios contaron con la asistencia de más de 450 participantes.

2.8.3 Además de los ejercicios teóricos (TTX) realizados como parte de los seminarios regionales de ciberseguridad de la aviación, la OACI llevó a cabo un TTX en paralelo con la Cuarta Reunión del Grupo experto en Ciberseguridad (CYSECP/4) el 5 de junio de 2025, durante su Semana de la Seguridad en 2023, así como cuatro TTX independientes, lo que eleva el número total de TTX internacionales realizados por la OACI durante el trienio a diez ejercicios de ciberseguridad de la aviación.

3. EXAMEN DE LA RESOLUCIÓN A41-19 DE LA ASAMBLEA

3.1 Tras la adopción de la Declaración de Mascate y teniendo en cuenta los resultados de la decimocuarta Conferencia de Navegación Aérea, las actualizaciones propuestas a la resolución A41-19 de la Asamblea se pueden encontrar en el apéndice adjunto. La resolución actualizada se coordinó con el Grupo Experto en Ciberseguridad de la OACI para alinearla con el contenido de la Declaración y los resultados de la Conferencia en relación con la ciberseguridad de la aviación, así como con las definiciones de términos de ciberseguridad de la aviación aprobadas por la tercera Reunión del Grupo Experto en Ciberseguridad, y con la evolución de la labor de la OACI sobre el tema.

APÉNDICE

Resolución A41-19 A42-XX: Formas de abordar la ciberseguridad en la aviación civil

Considerando que el sistema de aviación mundial es un sistema altamente complejo e integrado interconectado y que comprende datos, información y sistemas que son críticos para la seguridad y, la protección, la eficiencia y la capacidad de las operaciones de aviación civil;

Observando que el sector de la aviación depende cada vez más de la confiabilidad, disponibilidad e integridad y disponibilidad de sistemas, datos e información, y en algunas circunstancias de su confidencialidad;

Reconociendo que la ciberseguridad de la aviación es fundamental para el desarrollo sostenible y eficiente del transporte aéreo y que, por lo tanto, se le debe dar prioridad y asignarle los recursos adecuados;

~~*Reconociendo* que no todos los sucesos ciberincidentes de ciberseguridad que afectan a la seguridad operacional, la protección, la eficiencia o la capacidad de la aviación civil se relacionan con son actos ilícitos o intencionales;~~

Consciente de que las ciberamenazas a la aviación civil evolucionan rápida y continuamente y crecen en escala, sofisticación y frecuencia, que la aviación sigue siendo un objetivo para los delinquentes actores malintencionados, tanto en el ámbito cibernético como en el físico, y que las ciberamenazas pueden llegar a afectar constituir riesgos considerables para la infraestructura crítica de la aviación civil y podrían poner en peligro sistemas críticos la seguridad operacional, la protección, la eficiencia o la capacidad de la aviación civil en todo el mundo;

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

~~*Reconociendo* que no todos los sucesos ciberincidentes de ciberseguridad que afectan a la seguridad operacional, la protección, la eficiencia o la capacidad de la aviación civil se relacionan con son actos ilícitos o intencionales;~~

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 como delitos los ciberataques contra la aviación civil internacional como delitos, por lo que la ratificación e implementación de ambos instrumentos por los Estados miembros garantizaría la disuasión y el castigo de dichos ataques en cualquier parte del mundo donde se produzcan;

Reafirmando la importancia y urgencia de abordar mejorar la ciberseguridad y la ciberresiliencia protección y resiliencia de los sistemas, los datos e información datos, información y sistemas críticos frente a las ciberamenazas y ciberriesgos peligros, entre ellos incluidas las interfaces comunes entre la aviación civil y la militar otros sectores conectados;

Considerando la necesidad de trabajar en colaboración para crear un marco de ciberseguridad de la aviación mundial eficaz y coordinado ~~que permita para abordar la ciberseguridad de la aviación y apoyar la ciberseguridad y la ciberresiliencia del sistema de aviación mundial~~ procurar la protección y resiliencia del sector ante las ciberamenazas y los ciberriesgos de una manera armonizada y coherente ~~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~~ ciberseguridad y ~~ciberresiliencia~~ de la aviación, ~~a lo largo de~~ en todas las distintas disciplinas de la aviación;

Reconociendo que es necesario armonizar la ciberseguridad de la aviación a nivel mundial, regional y nacional con miras a ~~asegurar~~ apoyar la coherencia y plena interoperabilidad de las medidas y los procesos de protección y resiliencia ~~los sistemas de gestión de riesgos;~~

Reconociendo la importancia ~~de que los Estados establecer establezcan e implementen un~~ planes claros y amplios de ciberseguridad de ~~gobernanza y rendición de cuentas a nivel nacional para la ciberseguridad de~~ para la aviación civil, que comprendan leyes, reglamentos, políticas, procedimientos y medidas para la ciberseguridad de la aviación civil, incluida la designación de una autoridad nacional competente encargada de la ciberseguridad de la aviación en coordinación con las autoridades y organismos nacionales interesados; y

Destacando el valor de las importantes ~~disposiciones, textos de orientación e~~ iniciativas, ~~planes de acción, publicaciones y demás medios~~ concebidos para abordar los problemas de ciberseguridad en colaboración y de forma holística; y

Considerando los resultados de la decimocuarta Conferencia de Navegación Aérea celebrada en Montreal del 26 de agosto al 6 de septiembre de 2024, así como las disposiciones de la Declaración de Mascate sobre la seguridad de la aviación y la ciberseguridad de la aviación que se adoptó en Mascate (Omán) el 11 de diciembre de 2024.

La Asamblea:

1. *Insta* a los Estados miembros ~~a adoptar y, ratificar e implementar~~ el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* (Convenio de Beijing de 2010) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves* (Protocolo de Beijing de 2010) 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 abordar las ciberamenazas a la aviación civil:
 - a) implantar la Estrategia de Ciberseguridad de la Aviación de la OACI, y utilizar el Plan de Acción de Ciberseguridad de la OACI como herramienta para apoyar ~~la su implementación de la Estrategia de Ciberseguridad de la Aviación;~~
 - b) desarrollar e implementar planes nacionales de ciberseguridad de la aviación que traten los objetivos estratégicos de ciberseguridad de la aviación, la gobernanza y las responsabilidades, las políticas, las comunicaciones, la gestión de los ciberriesgos, la respuesta a incidentes y la recuperación, la creación de capacidad e instrucción, el cumplimiento de las normas y las auditorías, el monitoreo y la mejora continua, la documentación y el mantenimiento de registros,

- con el objetivo de hacer frente a las ciberamenazas y los ciberriesgos que enfrenta la aviación civil de una manera holística en todas las disciplinas de la aviación;
- c) elaborar e implementar procesos y herramientas que asistan en la implementación y el monitoreo de los planes de ciberseguridad de la aviación;
- d) ~~b)~~ designar la autoridad competente en materia de ciberseguridad de la aviación como parte del plan nacional de ciberseguridad de la aviación, y definir la interacción entre dicha autoridad y los organismos nacionales de aviación y otros organismos interesados;
- e) ~~c)~~ definir las responsabilidades de los organismos nacionales y las partes interesadas de la industria con respecto a la ciberseguridad en la aviación civil;
- f) procurar recursos suficientes para disponer de profesionales con las calificaciones y competencias necesarias en aviación y ciberseguridad y capacitarlas en forma continua para que puedan regular, operar, gestionar, mantener y vigilar la aplicación efectiva de las leyes, reglamentos, políticas, procedimientos y medidas pertinentes de ciberseguridad de la aviación;
- g) ~~d)~~ elaborar e implementar un marco sólido ~~de gestión de riesgos de ciberseguridad que se base~~ integre la gestión de los ciberriesgos con ~~en~~ prácticas pertinentes de gestión de riesgos de ~~seguridad de la aviación y~~ seguridad operacional, seguridad de la aviación, eficiencia y capacidad, y adoptar un enfoque basado en los riesgos para mejorar la protección y la resiliencia ~~de proteger~~ los sistemas, información y datos críticos de la aviación civil ante ~~de~~ las ciberamenazas y los ciberriesgos;
- h) ~~e)~~ establecer leyes, reglamentos ~~y~~, políticas, procedimientos y medidas ~~e instrumentos~~, cuando sea necesario, y destinar recursos adecuados 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 se utilicen o sean transferidos; que tengan métodos de ~~vigilancia~~ monitoreo, detección y notificación de ciberincidentes; que se elaboren y se pongan en práctica planes de respuesta y recuperación ante ciberincidentes en coordinación con los planes de gestión de crisis y respuesta ante emergencias establecidos; y que se lleven a cabo análisis forenses de los ciberincidentes;
- i) ~~diseñar y aplicar~~ elaborar e implementar medidas prácticas para mejorar la ~~una sólida~~ cultura de ciberseguridad en todas las entidades de aviación civil ~~en todo el sector de la aviación civil~~;
- ~~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;~~
- j) ~~h)~~ formar y participar en asociaciones y mecanismos entre ~~gobierno/gobierno y gobierno/~~ e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, vulnerabilidades, indicadores de compromiso, tendencias ~~y~~, acciones de mitigación, mejores prácticas y enseñanzas extraídas;
- k) ~~g)~~ ~~fomentar~~ desarrollar mecanismos de la cooperación civil/militar con las entidades nacionales pertinentes que incluyan, entre otras, las autoridades militares, de policía y de ciberseguridad, en lo que respecta a la identificación, protección y ~~vigilancia~~ monitoreo de las vulnerabilidades comunes y los flujos de datos de información comunes ~~en las interfaces entre los sistemas de aviación civil y militar~~ que puedan afectar a los sistemas de aviación civil, y colaborar en la

respuesta a mitigación y la preparación ante las ciberamenazas comunes y en respuesta y la recuperación de los ciberincidentes;

a. ~~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; y~~

- l) ~~k) continuar colaborando y contribuyendo con la OACI continuamente en el desarrollo del marco de ciberseguridad de la aviación 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 todas las disciplinas de la aviación pertinentes, con el fin de tratar de forma holística las ciberamenazas y los ciberriesgos a la seguridad operacional, la protección, la eficiencia y la capacidad de la aviación.~~

3. Encarga a la 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 de 2010) y el *Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves* (Protocolo de Beijing de 2010); y
- b) continúe asegurándose de que los asuntos de ciberseguridad y ~~ciberresiliencia~~ de la aviación se examinen y coordinen de forma transversal y holística ~~por medio~~ mediante la colaboración entre todos los órganos pertinentes de la OACI ~~el nuevo mecanismo de la OACI que trata el tema de la ciberseguridad.~~