Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A40-WP/28
EX/13
25/6/19

ASAMBLEA — 40º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 12: Seguridad de la aviación — Política

ESTRATEGIA DE CIBERSEGURIDAD DE LA OACI

(Nota presentada por el Consejo de la OACI)

RESUMEN

En esta nota se presenta una Estrategia integral de ciberseguridad y, a fin de destacar la urgencia e importancia de su aplicación, el texto modificado de la Resolución A39-19 de la Asamblea, *Formas de abordar la ciberseguridad en la aviación civil,* para apoyar su implantación por parte de los Estados miembros. La Estrategia se cimienta en la visión que tiene la OACI respecto a la ciberseguridad mundial: que el sector de la aviación debe ser resiliente a los ciberataques y seguir siendo seguro y fiable a escala mundial sin que deje de innovar y crecer, para lo cual es necesario que se apoye en un plan de acción elaborado mediante mecanismos apropiados. La Estrategia es el resultado de las deliberaciones del Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC).

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

a) adopte la Resolución de la Asamblea que figura en el Apéndice A, propuesta para sustituir la Resolución A39-19 de la Asamblea;
b) respalde la Estrategia de ciberseguridad que figura en el Apéndice B; y
c) inste a los Estados a ratificar el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves*.

Objetivos estratégicos:	Esta nota de estudio 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 que se mencionan en esta nota se llevarán a cabo con sujeción a la disponibilidad de recursos en el Presupuesto del Programa regular de 2020 – 2022 y/o con contribuciones extrapresupuestarias.
Referencias:	*Resoluciones vigentes de la Asamblea* (al 6 de octubre de 2016) (Doc 10075)

1. INTRODUCCIÓN

1.1 Durante el 39° período de sesiones de la Asamblea de la OACI se reiteró la importancia y urgencia de proteger los sistemas de infraestructura y los datos que son de importancia crítica para la aviación civil contra los ciberataques y de conseguir que la OACI, sus Estados miembros y las partes interesadas de la industria se comprometan a escala mundial a tomar medidas al respecto, con la intención de ocuparse de la ciberseguridad de la aviación civil de manera colaborativa y sistémica y de mitigar amenazas y riesgos conexos. En la Resolución A39-19, *Formas de abordar la ciberseguridad en la aviación civil*, se identificaron medidas que los Estados y otras partes interesadas deben tomar al respecto. En el 39° período de sesiones de la Asamblea de la OACI también se pidió a la OACI que elaborara un plan de trabajo completo y una estructura de gobernanza en materia de ciberseguridad.

1.2 Para lograr estos objetivos, la OACI estableció el Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC) bajo el liderazgo del Director adjunto de seguridad de la aviación y facilitación (DD/ASF). El SSGC está integrado por 20 Estados, 13 organizaciones internacionales y la Secretaría de la OACI, con la supervisión del Grupo de administración superior de la Secretaría sobre cuestiones comunes de seguridad operacional y seguridad de la aviación, presidido por la Secretaria General de la OACI.

1.3 Desde su creación en agosto de 2017, el SSGC se ha reunido seis veces y elaboró un conjunto de recomendaciones para abordar cuestiones emergentes de ciberseguridad en aviación. El principal resultado fue la elaboración de una Estrategia de ciberseguridad abarcadora, cuyo propósito es orientar la labor de los Estados y la OACI tendente a garantizar la seguridad operacional y la seguridad y continuidad de la aviación civil aplicando un marco de ciberseguridad robusto. El Consejo, en su 217° período de sesiones aprobó en principio la Estrategia de ciberseguridad para la aviación y acordó presentar una versión enmendada de la Resolución A39-19, *Formas de abordar la ciberseguridad en la aviación civil* ante el 40° período de sesiones de la Asamblea de la OACI.

2. ANÁLISIS

2.1 En la Estrategia de ciberseguridad para la aviación se tienen en cuenta otras iniciativas de la OACI relacionadas con la ciberseguridad, estrategia que también complementa esas iniciativas. La estrategia es acorde con las actuales normas y métodos recomendados (SARPS) de seguridad operacional y seguridad de la aviación que se relacionan con la ciberseguridad y la protección de información de importancia crítica para la aviación, en particular con el Anexo 17 — *Seguridad*.

2.2 La Estrategia resalta la importancia de reconocer la ciberseguridad como una cuestión interdisciplinaria que se extiende a todos los campos del sector de la aviación. En ella se sintetizan las disposiciones actuales que se relacionan con cuestiones de ciberseguridad tratadas en varios Anexos, con el propósito de integrarlas en un marco único cuyo objetivo es la gestión de los riesgos cibernéticos y el mejoramiento de la ciberseguridad en su conjunto. La Estrategia proporciona a los Estados una visión que considera que el sector de la aviación civil es resiliente a los ciberataques sin que deje de innovar y crecer.

2.3 La estrategia tiene por objeto:

a) la protección de la aviación civil y del público viajero contra amenazas a la ciberseguridad que puedan afectar a la seguridad operacional y la seguridad de la aviación en el sistema de transporte aéreo y dañar la confianza en dicho sistema;

b) el mantenimiento o mejoramiento de la seguridad operacional y la seguridad de la aviación en el sistema de aviación para preservar la continuidad de los servicios de transporte aéreo;

c) que los Estados reconozcan sus obligaciones, en el marco del *Convenio sobre Aviación Civil Internacional* (Convenio de Chicago), de garantizar la seguridad operacional y la seguridad y continuidad de la aviación civil, teniendo en cuenta las amenazas a la ciberseguridad; y

d) la coordinación entre las autoridades estatales de las medidas de ciberseguridad, a fin de garantizar la gestión eficaz y eficiente de los riesgos de ciberseguridad.

2.4 Los objetivos de la Estrategia se alcanzarán al seguirse una serie de principios, medidas y acciones que figuran en un marco que se apoya en siete pilares que incluyen: cooperación internacional; gobernanza, legislación y reglamentación eficaces; políticas de ciberseguridad; compartición de información; manejo de incidentes y planificación de emergencias; creación de capacidades, instrucción y cultura de ciberseguridad.

2.5 Un prerrequisito para la implantación de la Estrategia es que los Estados miembros se aseguren de que su legislación y reglamentos nacionales se formulen y apliquen de conformidad con las disposiciones de la OACI. Respecto a esto, debería considerarse también si es necesario actualizar la legislación nacional o adoptar una nueva para permitir el enjuiciamiento en caso de ciberamenazas relacionadas con terroristas y ciberataques que tengan un impacto negativo en la aviación civil. El proceso de evaluación y posible actualización de la legislación a escala estatal puede retrasar la implementación efectiva de la Estrategia y plantear dificultades en la armonización de la ciberseguridad a nivel mundial.

2.6 En la Estrategia se aborda la necesidad de crear capacidades y de promover una cultura de ciberseguridad. Para lograrlo, los Estados necesitarán contar con personal capacitado adecuadamente y que cuente con conocimientos especializados interdisciplinarios en aviación y ciberseguridad. Para lograr esta meta, pueden requerirse programas educativos actualizados o nuevos, y será importante considerar el tiempo y los recursos necesarios para elaborarlos.

2.7 Se requerirá un plan de acción integral y multidisciplinario para garantizar la adopción e implantación metódicas de medidas que apoyen los objetivos de la Estrategia. La OACI, en cooperación con los Estados y la industria, debería empezar a elaborar ese plan sin demora a través de mecanismos apropiados que sirvan para tratar cuestiones relacionadas con la ciberseguridad.

2.8 La ciberseguridad es un asunto que avanza a un ritmo acelerado y necesita atenderse de manera urgente dándole la debida importancia. Por lo tanto, y para destacar las responsabilidades y obligaciones de los Estados y la OACI de colaborar para atender el problema de la ciberseguridad, se modificará una resolución de la Asamblea para destacar los logros de los Estados y la OACI en la materia y la necesidad de implantar una Estrategia de ciberseguridad que complementará la actual Resolución A39-19, que fue el punto de partida de la labor de la OACI en materia de ciberseguridad.

2.9 En el proyecto de resolución modificada de la Asamblea que se presenta en el Apéndice de esta nota de estudio se agrega un elemento en la actual resolución sobre ciberseguridad destacando la necesidad de adoptar e implantar de manera universal y global 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), a fin de atender el problema de los ciberataques contra la aviación civil.

2.10 Además, se reconoce la necesidad de proseguir de manera más formalizada con el trabajo del SSGC para permitir la coordinación estructurada con otros grupos de la OACI.

3. CONCLUSIÓN

3.1 En el espíritu del Convenio de Chicago, la Estrategia de ciberseguridad de la OACI a escala mundial sentará bases mutuamente aceptables para todos los Estados a fin de poder avanzar. Permitirá armonizar los marcos internacionales, regionales y nacionales de ciberseguridad y promover mecanismos apropiados de intercambio de información que ofrezcan mayores beneficios en la gestión de los riesgos de ciberseguridad.

3.2 La estrategia en cuestión proporcionará un marco flexible que preparará a la aviación civil para manejar de manera eficaz, en las próximas décadas, la ciberseguridad. Está estructurada de manera modular, por lo que puede adaptarse a ciberamenazas emergentes para tener en cuenta las novedades futuras que tengan lugar en la aviación civil. Garantizará que todos los campos que integran al sector de la aviación se incluyan y permitirá considerar los problemas desde un punto de vista inter y multidisciplinario.

3.3 La Estrategia de ciberseguridad deberá estar respaldada por un plan de acción e incluir fases tangibles, con el fin de lograr un marco de ciberseguridad maduro. El plan de acción se creará a partir de la orientación sobre la manera en que se aplican los actuales SARPS relacionados con la ciberseguridad y, además, profundizará en los SARPS y los sintetizará a fin de ofrecer orientación completa sobre cómo lograr el nivel máximo de ciberseguridad.

3.4 En la Estrategia se tienen en cuenta los actuales planes mundiales y se reconoce, además, la necesidad de contar con personal capacitado y cualificado que posea experiencia en aviación y en ciberseguridad.

— — — — — — — — —

APÉNDICE A

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

Resolución ~~A39-19~~A40-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 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, 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 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 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 un amplio número de 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 de ciberamenazas a los sistemas de infraestructura de la aviación civil y los datos críticos;

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, 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;

Reconociendo la labor del Grupo de estudio de la Secretaría sobre Ciberseguridad, 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;

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 plena interoperabilidad de las medidas de protección y los sistemas de gestión de riesgos; y

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 la protección del sistema de aviación mundial y hacerlo más resiliente ante las ciberamenazas; y~~

La Asamblea:

1. *Insta* a los Estados miembros y a la OACI a promover la adopción universal e implementación 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) como instrumentos para hacer frente a los ciberataques contra la aviación civil;

~~1~~2. *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) implantar la estrategia sobre ciberseguridad que figura en el Apéndice;

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

   ~~c)~~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;

   ~~d)~~e) 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)~~f) 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;

~~f)~~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;

~~g)~~h) fomentar una sólida cultura de ciberseguridad en todos los aspectos dentro 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 horizontal, intersectorial y funcional que integre la navegación aérea, las comunicaciones, la vigilancia, las operaciones de aeronaves, la aeronavegabilidad y demás disciplinas pertinentes.

3. *Encarga* a la Secretaria General que:

a) formule un plan de acción para ayudar a los Estados y la industria a adoptar la Estrategia de ciberseguridad; y ~~ayude y facilite la tarea de los Estados y la industria para la adopción de estas medidas; y~~

b) continúe asegurándose de que los asuntos de ciberseguridad se examinen y coordinen de forma transversal por medio de los mecanismos apropiados conforme se estipula en la estrategia. ~~se asegure de que los asuntos de ciberseguridad reciban plena atención y se coordinen en todas las disciplinas pertinentes dentro de la OACI.~~

— — — — — — — —

APÉNDICE B

ESTRATEGIA DE CIBERSEGURIDAD DE LA AVIACIÓN

VISIÓN DE UNA ESTRATEGIA MUNDIAL DE CIBERSEGURIDAD DE LA AVIACIÓN CIVIL

1.1 El sector de la aviación civil depende cada vez en mayor medida de la disponibilidad de sistemas de tecnología de información y comunicaciones, así como de la integridad y confidencialidad de los datos. La amenaza de posibles incidentes cibernéticos para la aviación civil evoluciona de forma constante, con unos perpetradores que actúan maliciosamente para perturbar las operaciones y robar información por razones políticas, financieras y de otra índole.

1.2 Dada la naturaleza polifacética y multidisciplinaria de la ciberseguridad, y en vista de que los ciberataques pueden afectar de forma simultánea una amplia gama de áreas y propagarse con rapidez, es imperioso concebir una visión común y definir una estrategia de ciberseguridad.

1.3 La visión de la OACI sobre la ciberseguridad mundial es que el sector de la aviación civil sea resiliente a los ciberataques y siga siendo seguro y fiable en todo el mundo, al tiempo que continúa innovando y creciendo.

1.4 Esto puede lograrse mediante:

- el reconocimiento de parte de los Estados de sus obligaciones en virtud del *Convenio sobre Aviación Civil Internacional* (Convenio de Chicago) de velar por la seguridad operacional y la seguridad y continuidad de la aviación civil, incluida la ciberseguridad;
- la coordinación de la ciberseguridad de la aviación entre las autoridades estatales a fin de garantizar una gestión eficaz y eficiente de los riesgos de ciberseguridad a escala mundial; y
- el compromiso de todas las partes interesadas de la aviación de profundizar la resiliencia en este ámbito y protegerse contra los ciberataques que pudieran afectar la seguridad operacional, la seguridad de la aviación y la continuidad del sistema de transporte aéreo.

1.5 La estrategia se alinea con otras iniciativas de la OACI relativas a la ciberseguridad y se coordina con las disposiciones pertinentes sobre gestión de la seguridad operacional y la seguridad de la aviación. La finalidad de la estrategia se cumplirá mediante un conjunto de principios, medidas y actividades contenidos en un marco que descansa sobre siete pilares:

I. Cooperación internacional
II. Gobernanza
III. Leyes y reglamentos eficaces
IV. Política de ciberseguridad
V. Intercambio de información
VI. Gestión de incidentes y planificación ante emergencias
VII. Creación de capacidad, instrucción y cultura de ciberseguridad

2. COOPERACIÓN INTERNACIONAL

2.1 Por naturaleza, la ciberseguridad y la aviación no conocen fronteras. Ambas requieren de la cooperación a nivel nacional e internacional y requieren del mutuo reconocimiento de los esfuerzos desplegados para mejorar la ciberseguridad a fin de proteger el sector de la aviación civil de todos los ciberataques a la seguridad operacional y la seguridad de la aviación.

2.2 La ciberseguridad de la aviación debe armonizarse a nivel mundial, regional y nacional con el objeto de promover la coherencia en todo el mundo y velar por la plena interoperabilidad de las medidas de protección y los sistemas de gestión de riesgos.

2.3 La OACI es el foro mundial idóneo para interactuar con los Estados y abordar la ciberseguridad en la aviación civil internacional. A tal efecto, la OACI organizará, facilitará y promoverá eventos internacionales que sirvan de plataforma para el intercambio de conocimientos entre Estados, organizaciones internacionales e industria. Se alienta a los Estados a participar en las deliberaciones sobre la ciberseguridad en la aviación civil.

3. GOBERNANZA

3.1 Se alienta a todos los Estados miembros de la OACI a apoyar y aprovechar la Estrategia OACI de ciberseguridad de la aviación para velar por la seguridad operacional y la seguridad y continuidad de la aviación civil un mundo cada vez más en peligro ante las amenazas de ciberseguridad.

3.2 Se alienta a los Estados a establecer un plan claro de gobernanza y rendición de cuentas a nivel nacional para la ciberseguridad de la aviación civil. Se invita a las administraciones de la aviación civil a asegurar la coordinación con su autoridad nacional competente en materia de ciberseguridad, dado que la autoridad general en materia de ciberseguridad para todos los sectores puede no ser responsabilidad de la administración de aviación civil. También es esencial establecer los canales apropiados de coordinación entre las diversas autoridades estatales y las partes interesadas de la industria.

3.3 Por último, se alienta a los Estados miembros a incluir la ciberseguridad en sus programas nacionales de seguridad operacional y seguridad de la aviación civil. A tales fines, la OACI debería incluir también la ciberseguridad en sus planes y actividades regionales y mundiales en pro de una base común para normas y métodos recomendados (SARPS) sobre ciberseguridad.

4. LEYES Y REGLAMENTOS EFICACES

4.1 El objetivo principal de las leyes y reglamentos internacionales, regionales y nacionales sobre ciberseguridad para la aviación civil es apoyar la implementación de una estrategia integral de ciberseguridad dirigida a proteger a la aviación civil y a los viajeros de los efectos de los ciberataques.

4.2 Los Estados miembros deben asegurarse de que se formulen y apliquen las leyes y reglamentos pertinentes de conformidad con las disposiciones de la OACI, antes de implantar una política nacional de ciberseguridad para la aviación civil. Es necesario formular nuevas orientaciones apropiadas para ayudar a los Estados y la industria a poner en práctica las disposiciones relacionadas con la ciberseguridad. En ese sentido, la OACI está comprometida a crear, examinar y, de ser el caso, enmendar los textos de orientación relativos a la inclusión de aspectos relacionados con la ciberseguridad en la seguridad operacional y la seguridad de la aviación.

4.3 Deberían analizarse los instrumentos jurídicos internacionales para determinar cuáles son las disposiciones jurídicas que existen o faltan en el derecho aéreo para la prevención, el enjuiciamiento y la reacción oportuna ante los ciberincidentes con el propósito de formar la base para una implementación uniforme y coherente de las leyes y reglamentos de ciberseguridad en el sector de la aviación. Mientras tanto, se alienta a los Estados a ratificar los instrumentos de la OACI, incluidos 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).

4.4 Se alienta a los Estados a considerar si sus respectivas legislaciones nacionales deben ser actualizadas y si debe adoptarse una nueva legislación nacional para permitir el enjuiciamiento de ciberataques relacionados con actos terroristas y aquellos que afectan adversamente a la aviación civil. También se alienta a los Estados a que, de forma paralela, establezcan mecanismos apropiados para cooperar en las investigaciones de seguridad de "buena fe", que es la actividad de investigación que se lleva a cabo en un entorno diseñado para evitar afectar la seguridad operacional y la seguridad y continuidad de la aviación civil.

5. POLÍTICA DE CIBERSEGURIDAD

5.1 La ciberseguridad ha de incluirse en los sistemas de seguridad de la aviación y seguridad operacional de un Estado como parte de un marco integral de gestión de riesgos.

5.2 Habida cuenta de las diferentes metodologías de evaluación de riesgos que existen, debe conferirse prioridad a la enmienda y la posible elaboración de textos de orientación relacionados con las evaluaciones de amenazas y riesgos de ciberseguridad, con el propósito de poder comparar los resultados de dichas evaluaciones.

5.3 En todo el sector de la aviación civil, las políticas de ciberseguridad pueden considerar el ciclo de vida completo del sistema de aviación e incluir elementos como: cultura de ciberseguridad, promoción de la seguridad por diseño, seguridad de la cadena de suministros de programas y equipos informáticos, integridad de los datos, control apropiado del acceso, gestión proactiva de las vulnerabilidades, mejoramiento de la rapidez de las actualizaciones de la seguridad de la aviación sin comprometer la seguridad operacional e incorporación de sistemas y procesos para vigilar los datos pertinentes de ciberseguridad.

6. INTERCAMBIO DE INFORMACIÓN

6.1 El sector de la aviación civil es un sistema global interdependiente con numerosos sistemas comunes, por lo que los ciberataques pueden propagarse fácilmente y tener repercusiones mundiales. El objetivo del intercambio de información es permitir la prevención, detección temprana y atenuación de sucesos relevantes de ciberseguridad antes de que sus efectos se extiendan hacia la seguridad operacional y la seguridad de la aviación. Una cultura de intercambio de información reducirá considerablemente los riesgos cibernéticos sistémicos en todo el sector de la aviación, y su valor ha quedado comprobado en el ámbito de la seguridad operacional y la seguridad de la aviación.

6.2 El intercambio de información sobre aspectos como las vulnerabilidades, amenazas, sucesos y mejores prácticas por medio de relaciones establecidas y fiables pueden reducir el impacto de los ataques en curso. Deben reconocerse los mecanismos apropiados de intercambio de información en consonancia con las disposiciones existentes de la OACI.

7. GESTIÓN DE INCIDENTES Y PLANIFICACIÓN ANTE EMERGENCIAS

7.1 Junto a los mecanismos existentes de gestión de incidentes, es menester contar con planes apropiados y ampliables que aseguren la continuidad del transporte aéreo durante un incidente cibernético. Se recomienda que los Estados y el sector de la aviación enmienden los planes de contingencia existentes para incluir disposiciones relativas a la ciberseguridad.

7.2 Los ejercicios de ciberseguridad son una herramienta útil para someter a prueba la resiliencia ante ciberataques y detectar las áreas que requerirían mejoras, por lo que se recomiendan altamente. Estos ejercicios pueden seguir formatos diferentes (p. ej., ejercicios teóricos, simulaciones o ejercicios en tiempo real) e igualmente variar en escala (internacional, nacional, institucional).

8. CREACIÓN DE CAPACIDAD, INSTRUCCIÓN Y CULTURA DE CIBERSEGURIDSAD

8.1 El elemento humano es el corazón de la ciberseguridad. Es de suma importancia que el sector de la aviación civil dé pasos tangibles para aumentar el número de funcionarios calificados y conocedores tanto de la aviación como de la ciberseguridad. Esto puede hacerse aumentando la conciencia sobre la ciberseguridad, así como con educación, contratación e instrucción. Deberían incluirse planes de estudio pertinentes a la ciberseguridad y – de ser viable – la ciberseguridad específicamente relacionada con la aviación, a todos los niveles del sistema educativo nacional y los programas internacionales de instrucción pertinentes. Deberían buscarse formas innovadoras de fusionar e interconectar las profesiones tradicionales de tecnología de información y cibernética con las profesiones pertinentes de la aviación.

8.2 El apoyo y la estimulación del desarrollo de aptitudes del personal existente y nuevo deberían conducir al fomento de la innovación en materia de ciberseguridad y las debidas investigaciones y diseño en el sector de la aviación. Debería ofrecerse instrucción apropiada y continua en el trabajo para apoyar al personal en sus actividades cotidianas.

8.3 La ciberseguridad podría incluirse en la estrategia para la próxima generación de profesionales de la aviación, ya que la OACI está bien posicionada para trabajar con los Estados y la industria en la formulación de los requisitos de competencias basadas en las funciones de los profesionales de la aviación.

8.4 El sector de la aviación civil tiene una historia envidiable de seguridad operacional con base en una cultura de seguridad operacional que se entiende como responsabilidad de todos. Los principios de esta cultura de seguridad operacional deben seguirse para crear y mantener una cultura de ciberseguridad en todo el sector de la aviación.

— FIN —