



NOTA DE ESTUDIO

DECIMOTERCERA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 9 al 19 de octubre de 2018

COMITÉ A

Cuestión 5 del
orden del día: Cuestiones emergentes
5.4: Ciberresiliencia

CIBERRESILIENCIA

(Nota presentada por la Secretaría)

RESUMEN

En todo el mundo se reconoce la importancia de disponer de un enfoque de ciberresiliencia adecuado para la aviación civil, un asunto crucial que se tratará en la edición de 2019 del *Plan mundial de navegación aérea (GANP)* (Doc 9750). Para manejar bien la ciberresiliencia en un sistema de aviación cada vez más interconectado, se requiere un enfoque mundialmente armonizado entre todas las partes interesadas. Sin un marco de confianza coordinado a nivel mundial para el intercambio seguro de información, aéreo, terrestre y aeroterrestre, y el compromiso de crear un clima de confianza que propicie el intercambio de información sobre ciberincidentes, no puede garantizarse la ciberresiliencia. También se reconoce que, pese a la creciente dependencia de la tecnología de la información, la participación humana es, al mismo tiempo, una de las principales causas de las ciberamenazas y la primera línea de defensa contra ellas y, por este motivo, el personal de operaciones debería recibir instrucción para reconocer las características generales de las ciberamenazas y notificar toda sospecha que tenga de ellas o de ciberincidentes.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a acordar la Recomendación 5.4/x — Ciberresiliencia, que figura en el párrafo 3.

Objetivos estratégicos:	La presente nota de estudio se relaciona con los Objetivos estratégicos de Seguridad operacional y de Capacidad y eficiencia de la navegación aérea.
Repercusiones financieras:	<i>Repercusiones para la comunidad de la aviación:</i> La introducción de políticas, tecnologías y procedimientos a fin de garantizar la ciberresiliencia puede tener repercusiones financieras significativas para algunas partes interesadas. Sin embargo, esto dependerá de la envergadura de la actividad de la aviación y de las infraestructuras de apoyo. También puede haber repercusiones financieras y en materia de seguridad operacional, eficiencia y reputación si no puede garantizarse la ciberresiliencia del sistema de navegación aérea. <i>Repercusiones para la OACI (considerando los niveles actuales de recursos previstos en el presupuesto del Programa regular):</i> Dado que la planificación, creación y ejecución a nivel estatal de un marco mundial de confianza y de otras actividades de concienciación sobre la ciberresiliencia continuarán durante los próximos trienios, son necesarios recursos adicionales, financieros y humanos, para apoyar los esfuerzos realizados por la OACI en las esferas altamente especializadas relacionadas con la ciberresiliencia y el marco de confianza.

Referencias:	Anexo 1 — <i>Licencias al personal</i> Anexo 6 — <i>Operación de aeronaves</i> Anexo 8 — <i>Aeronavegabilidad</i> Anexo 10 — <i>Telecomunicaciones aeronáuticas</i> Anexo 11 — <i>Servicios de tránsito aéreo</i> Anexo 14 — <i>Aeródromos</i> Anexo 15 — <i>Servicios de información aeronáutica</i> Anexo 17 — <i>Seguridad — Protección de la aviación civil internacional contra los actos de interferencia ilícita</i> Anexo 19 — <i>Gestión de la seguridad operacional</i> <i>Concepto operacional de gestión del tránsito aéreo mundial</i> (Doc 9854) <i>Plan mundial de navegación aérea 2016–2030</i> (Doc 9750) <i>Manual para implantar la red de telecomunicaciones aeronáuticas (ATN) utilizando normas y protocolos de la familia de protocolos de Internet (IPS)</i> (Doc 9896) <i>Resoluciones vigentes de la Asamblea (al 4 de octubre de 2013)</i> (Doc 10022) <i>Manual sobre el concepto de gestión de la información de todo el sistema (SWIM)</i> (Doc 10039)
---------------------	---

1. INTRODUCCIÓN

1.1 La aviación es un sistema complejo, compuesto por varias redes y dispositivos cada vez más interdependientes e interconectados para el intercambio de datos e información digitales. Las partes interesadas de la aviación, como los Estados, los explotadores de aeronaves y aeródromos y los proveedores de servicios de navegación aérea (ANSP), entre otros, han terminado dependiendo, para sus operaciones cotidianas, de sistemas de tecnología de la información y las comunicaciones (TIC) interconectados y que operan entre sí, convirtiéndose en parte de un entorno digital de aviación civil. Avances como la gestión de la información de todo el sistema (SWIM), la introducción de sistemas de aeronaves pilotadas a distancia (RPAS) y el surgimiento de futuros usuarios del espacio aéreo y partes interesadas que aún no están operando no hacen sino reforzar esta interdependencia.

1.2 La evolución hacia dichos sistemas de información interconectados y que operan entre sí también trae consigo puntos vulnerables nuevos. Los ciber sucesos pueden repercutir en la aviación a muchos niveles y perjudicar el funcionamiento del sistema de navegación aérea. Pueden influir en los intercambios de información entre las partes interesadas, lo que afecta directamente a la seguridad operacional, la capacidad y la eficiencia, con posibles consecuencias graves.

1.3 En un entorno de aviación totalmente interconectado, la ciberresiliencia se hace indispensable para la seguridad operacional. El sistema de aviación necesita, por tanto, mejorar su resiliencia ante las ciberamenazas. La ciberresiliencia puede definirse como la capacidad del sistema de aviación para resistir ciberamenazas y ciberincidentes y recuperarse de los problemas de funcionamiento que puedan causar, entre ellos, la pérdida o la corrupción de datos y perturbaciones del sistema, como la pérdida de conectividad o de interoperabilidad.

1.4 La ciberresiliencia puede lograrse gracias a una combinación de normas, procedimientos y métodos que ayudan a mitigar las ciberamenazas a las que se enfrentan sistemas críticos para la seguridad operacional y la eficiencia de la aviación.

1.5 La importancia de disponer de un enfoque de ciberresiliencia adecuado para la aviación civil se indicará en la edición de 2019 del *Plan mundial de navegación aérea* (Doc 9750) y constituye un componente fundamental para materializar la visión descrita en el *Concepto operacional de gestión del*

tránsito aéreo mundial (Doc 9854). Por consiguiente, es preciso que las partes interesadas sean más conscientes de las ciberamenazas, los puntos vulnerables y los riesgos del sistema de aviación con el fin de seguir desarrollando un conjunto de enfoques de ciberresiliencia para la aviación civil coherentes a nivel mundial.

1.6 Al tiempo que reconocía la urgencia e importancia de proteger de ciberamenazas los sistemas de infraestructura, información y tecnologías de la comunicación críticos para la aviación civil, la Asamblea de la OACI pidió, en su 39º período de sesiones, la adopción de un enfoque coordinado para lograr un nivel de ciberresiliencia adecuado y aceptable a escala mundial. En este sentido, y a fin de promover la concienciación sobre la ciberresiliencia en toda la comunidad de la aviación, la OACI estableció el Grupo de estudio de la Secretaría sobre ciberseguridad (SSGC) para abordar los aspectos del sistema internacional de la aviación que pueden verse afectados por ciberincidentes.

2. ANÁLISIS

2.1 Para garantizar un entorno rico en información con datos en tiempo real, es necesario un sistema ciberresiliente que posibilite la elaboración de análisis y modelos de predicción. Junto con una serie de herramientas automatizadas de apoyo y para la toma de decisiones, el sistema permitirá que los servicios evolucionen como se prevé en el Doc 9854.

2.2 Interconectividad y ciberresiliencia del sistema mediante un marco de confianza

2.2.1 Para manejar bien la ciberresiliencia, se requiere un enfoque mundialmente armonizado entre todas las partes interesadas. Es preciso acordar cómo deberían operar entre sí los sistemas de información digital para proporcionar a toda la comunidad de la aviación un entorno rico en información que pueda compartirse. El intercambio seguro y resiliente de información necesario para responder a las necesidades cambiantes de las actividades de la aviación puede permitirse gracias a un marco de confianza que consista en normas, procedimientos, métodos y acuerdos coordinados para el intercambio digital de información entre sistemas aéreos, terrestres y aeroterrestres y la regulación de sistemas de identidad.

2.2.2 La mejora de la protección de los intercambios de información entre las partes interesadas y entre sistemas también es necesaria para mejorar la ciberresiliencia. Los modelos adoptados por otras industrias y basados en información abierta y contrastada y en normas de tecnología de la comunicación, como los conceptos de marcos de confianza, certificados digitales y redes privadas virtuales en la infraestructura pública de Internet, pueden servir como ejemplo del modo en que puede protegerse el intercambio de información sobre aviación civil a nivel mundial.

2.2.3 En última instancia, han de desarrollarse sistemas críticos para la seguridad operacional y canales para intercambiar información digital, y someterse continuamente a examen, utilizando un enfoque de seguridad en el diseño que garantice la ciberresiliencia mediante tecnologías y procedimientos.

2.2.4 Un marco mundial de confianza permitiría incrementar la interoperabilidad y la conectividad de los sistemas digitales y, por consiguiente, aumentar la ciberresiliencia. La elaboración de un marco mundial de confianza para la aviación debería centrarse en los requisitos de gobernanza, normativos y de rendimiento técnico general que apliquen las partes interesadas de la aviación que deseen intercambiar información digital. Los enfoques fragmentados y descoordinados a nivel estatal o regional resultarían ineficaces, más costosos para todas las partes interesadas y, a la larga, limitarían la conectividad e interoperabilidad de los sistemas digitales, además de reducir la ciberresiliencia del sistema de aviación.

2.2.5 El marco mundial de confianza solamente puede materializarse con un organismo de normalización que haya ganado la confianza de una mayoría suficiente de partes interesadas de la aviación y con el que, intrínsecamente, se cuente para coordinar a nivel mundial las políticas, procedimientos y métodos destinados a garantizar la seguridad operacional y la eficiencia de la aviación civil.

2.2.6 En la página <https://www4.icao.int/ganportal/trustframework> puede consultarse un proyecto de concepto de operaciones relativas a un marco de confianza para facilitar el intercambio seguro de información. Este proyecto preliminar, en fase de elaboración, proporciona más información sobre dicho marco.

2.3 Intercambio de información y ciberconcienciación

2.3.1 Ninguna parte interesada de la aviación puede protegerse sola de las ciberamenazas. El intercambio de información les ayudaría a estar mejor preparadas para hacer frente a un conjunto mayor de ciberincidentes, y a aumentar su capacidad para reducirlos y paliar riesgos. El intercambio de ciberinformación que afecta a la seguridad operacional crearía asimismo un clima de confianza entre las partes interesadas de la aviación que, a la larga, aumentaría la ciberresiliencia del sistema de aviación y elevaría el nivel de concienciación sobre las ciberamenazas de todas las partes interesadas.

2.3.2 También se insta a las partes interesadas a reconocer que, pese al creciente nivel de dependencia de la tecnología de la información, la participación humana es, al mismo tiempo, una de las principales causas de las ciberamenazas y la primera línea de defensa contra ellas. El personal de operaciones, a todos los niveles, debería recibir instrucción para reconocer las características generales de las ciberamenazas y notificar toda sospecha que tenga de ellas o de ciberincidentes, sin importar cuán triviales sean.

3. CONCLUSIÓN

3.1 Los sistemas de aviación seguirán conectándose a un ritmo cada vez mayor y el sistema digital de aviación continuará expandiéndose. Sin un marco de confianza coordinado a nivel mundial que consista en requisitos de gobernanza, normativos y de rendimiento técnico general para la interconectividad e interoperabilidad de los sistemas, no puede garantizarse la ciberresiliencia. El intercambio de información sobre ciberamenazas y ciberincidentes, junto con la instrucción adecuada del personal, aumenta asimismo la ciberresiliencia. La seguridad operacional y eficiencia continuas de la aviación en un sistema digital de aviación cada vez más conectado e interoperable exige enfoques de ciberresiliencia armonizados a múltiples niveles que beneficien directamente a todas las partes interesadas, ahora y en el futuro.

3.2 Considerando la importancia de hacer frente a las ciberamenazas y reconociendo sus repercusiones en la resiliencia del sistema de aviación, se invita a la Conferencia a acordar la siguiente recomendación:

Recomendación 5.4/x — Ciberresiliencia

Que la Conferencia:

- a) pida a la OACI que trabaje con los Estados, la industria y las organizaciones internacionales con el objetivo de elaborar un marco de confianza para la aviación mundialmente armonizado, que incluya requisitos de gobernanza, normativos y de rendimiento técnico general a fin de permitir la materialización de un sistema de aviación resiliente y rico en información;

- b) pida a la OACI que trabaje con los Estados, la industria y las organizaciones internacionales para promover el marco de confianza, explicar sus ventajas y concienciar sobre el modo en que aumenta la ciberresiliencia; y
- c) inste a los Estados, la industria y las organizaciones internacionales a trabajar con la OACI para elevar el nivel de concienciación sobre las ciberamenazas y los procesos de resiliencia del sistema, así como coordinar las actividades de intercambio de información sobre ciberincidentes y de instrucción conexas.

— FIN —