Organización de Aviación Civil Internacional

AN-Conf/13-WP/62
27/8/18

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**

FOMENTO DE LA CIBERRESILIENCIA MEDIANTE LA TOMA DE CONCIENCIA MUNDIAL Y LOS EJERCICIOS REGIONALES

(Presentada por los Estados Unidos de América)

RESUMEN

De conformidad con la Resolución A39-19 de la Asamblea de la OACI, *Formas de abordar la ciberseguridad en la aviación civil*, la Administración Federal de Aviación (FAA) ha trabajado con asociados de la OACI y regionales para identificar amenazas y riesgos de posibles ciberincidentes que afecten a las operaciones de la aviación civil y a sistemas críticos y alentar la formación de una comprensión común de las ciberamenazas, los riesgos y la mitigación de ciberincidentes por los asociados.

En este sentido, la FAA ha propuesto un modelo de ciberejercicios teóricos regionales basados en el análisis de casos diseñados para fomentar un intercambio abierto de ideas que induzca a la reflexión sobre diversos aspectos de ciberincidentes hipotéticos y simulados. Los ejercicios pueden utilizarse para mejorar el grado de concienciación general, validar los planes y los procedimientos actuales y evaluar los sistemas y las actividades del marco de respuesta a los ciberincidentes y la recuperación de sus efectos.

Medidas propuestas a la Conferencia: Se invita a la Conferencia a aceptar las acciones propuestas:
a) respaldar el concepto de ciberejercicios teóricos regionales realizados en colaboración con las oficinas regionales de la OACI y los Estados miembros, tal como se señala en el párrafo 2.6; y
b) solicitar a la OACI la creación de un repositorio de casos y lecciones aprendidas a disposición de los Estados miembros para la realización de ciberejercicios teóricos regionales.

1. INTRODUCCIÓN

1.1 El aumento de la dependencia de los usuarios del transporte aéreo, la industria de la aviación, los proveedores de servicios de navegación aérea (ANSP) y las autoridades de aviación civil (AAC) con respecto a las comunicaciones y las operaciones basadas en la red, debe estar acompañado del trabajo de los Estados para modernizar la infraestructura de computación y de la red, que conecte a usuarios, sistemas y datos a fin de proporcionar un acceso sin discontinuidades y protegido frente a ciberincidentes.

1.2 Los ciberincidentes pueden afectar a la comunidad mundial de la aviación o a los sistemas individuales a varios niveles. Estos incidentes pueden comprometer las comunicaciones y los intercambios de información entre partes interesadas, al afectar a la seguridad operacional y la seguridad y dañar las actividades de la aviación. La capacidad de compartir ciberinformación y la aplicación de sólidos métodos normalizados de protección de datos y el intercambio de información, refuerza la capacidad de autoprotección del sector de la aviación y limita los efectos de los ciberincidentes.

1.3 Para fortalecer la seguridad de la aviación civil, la Administración Federal de Aviación (FAA) emprendió una serie de actividades para identificar riesgos de ciberseguridad y elaborar estrategias de mitigación en el ecosistema de la aviación que puedan repercutir en la seguridad operacional y causar la interrupción de la operación del sistema del espacio aéreo nacional (NAS). Esta estrategia transversal sobre diversos dominios permite que los componentes del NAS operen conjuntamente como un único sistema para asegurar la prestación de servicios seguros y eficientes a los usuarios del transporte aéreo, las líneas aéreas, el ejército de los Estados Unidos de América, la aviación en general y los aeropuertos.

1.4 Más allá del alcance de las estrategias de mitigación de ciberseguridad doméstica y con arreglo a la Resolución 39-19 de la Asamblea de la OACI, *Formas de abordar la ciberseguridad en la aviación civil*, la FAA ha trabajado con asociados en la OACI así como con asociados regionales para identificar amenazas y riesgos de posibles ciberincidentes que afecten a las operaciones de la aviación civil y a sistemas críticos, y fomentar una interpretación común de los asociados sobre ciberamenazas, riesgos y acciones de mitigación de ciberincidentes.

1.5 La FAA ha propuesto un modelo de ciberejercicios teóricos en los que se analicen casos diseñados para fomentar un intercambio abierto que induzca a la reflexión sobre diversos asuntos relativos a ciberincidentes hipotéticos y simulados, que puedan utilizarse para mejorar la concienciación general, validar los planes y procedimientos actuales y evaluar los sistemas y actividades del marco de la respuesta a los ciberincidentes y la recuperación de sus efectos.

2. ANÁLISIS

2.1 El 39º periodo de sesiones de la Asamblea de la OACI exhortó a los Estados miembros a, entre otras cosas:

a) identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y los sistemas críticos de la aviación civil y las graves consecuencias que pueden resultar de tales incidentes;

b) 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;

c) 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;

d) 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;

e) 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.

2.2 Si bien la labor en el seno de la OACI para establecer métodos comunes y mutuamente acordados de protección del sector de la aviación frente a los riesgos de ciberseguridad a través de un marco federado de requisitos reglamentarios progresa en virtud de los trabajos del Grupo de trabajo INNOVA, los Estados han expresado sus preocupaciones en relación con la creación y ejecución de programas de ciberseguridad.

2.3 Para dar respuesta a estar preocupaciones y dado el importante volumen de comunicaciones y datos compartidos por la FAA y las autoridades de aviación civil y los prestadores de servicios de navegación aérea del Caribe, la FAA organizó un ejercicio teórico de ciberseguridad para impulsar el desarrollo de las mejores prácticas regionales en respuesta a amenazas de ciberseguridad de la aviación. Este ejercicio puede servir de modelo para ciberejercicios teóricos de otras regiones en el futuro.

2.4 El ejercicio teórico de ciberseguridad se estructuró a modo de debate dirigido sobre casos prácticos en un entorno formal relajado. Hubo un intercambio de ideas abierto, que invitaba a la reflexión, sobre diversas cuestiones en torno a un ciberincidente hipotético simulado, que puede ser utilizado para aumentar la concienciación general, validar los planes y procedimientos en vigor y evaluar los sistemas y actividades en el marco de la respuesta a los ciberincidentes y la recuperación de sus efectos en la región del Caribe. El ejercicio también se centró en políticas, planes, contingencias del personal, intercambio de información y coordinación entre gobiernos, así como en identificar lagunas o responsabilidades poco claras o solapadas.

2.5 El ejercicio teórico de ciberseguridad reunió a la FAA y los Estados del Caribe para asegurar la resiliencia de la operación de las redes y los sistemas de información, tanto independientes como compartidos.

2.6 El ciberejercicio teórico fue un análisis de alto nivel centrado en políticas y prácticas. Los objetivos del mismo fueron los siguientes:

a) conformar y fomentar una interpretación común de las ciberamenazas, las vulnerabilidades y el riesgo resultante en el ecosistema de la aviación;

b) identificar lagunas existente en las políticas estatales y las operaciones; y

c) identificar y promover asociaciones y mecanismos regionales para el intercambio de información sobre amenazas emergentes y la respuesta a incidencias.

3. CONCLUSIÓN

3.1 Aunque la OACI sigue trabajando activamente en un marco federado de requisitos reglamentarios para fortalecer la ciberseguridad, es necesario un mayor esfuerzo a nivel estatal y regional. Los Estados pueden iniciar la elaboración de un marco básico que fortalezca la ciberseguridad y mitigue los ciberincidentes a través de un trabajo colectivo en asociaciones regionales, aplicando un modelo exitoso para lograr una interpretación común e identificar lagunas en las políticas y los reglamentos.

— FIN —