Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A41-WP/374
EX/170
2/8/22

ASAMBLEA — 41º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 14: Seguridad de la aviación — Política

PREPARACIÓN DEL PERSONAL PARA LA CIBERSEGURIDAD DE LOS SERVICIOS DE NAVEGACIÓN AÉREA EN TIEMPOS ORDINARIOS Y DE CRISIS

[Nota presentada por la Comisión Africana de Aviación Civil (CAFAC) en nombre de 54 Estados africanos[1]]

RESUMEN

La importancia de la ciberseguridad y la resiliencia cibernética en la aviación ha aumentado considerablemente con el tiempo, algo que se ha puesto de manifiesto una y otra vez debido a los ataques perpetrados antes y durante la pandemia de COVID-19. Además de la repercusión catastrófica de la COVID-19 en la economía mundial en general, y en la aviación en particular, la pandemia ha traído consigo un aumento de los ciberataques. La creación de capacidad, la instrucción y la cultura de ciberseguridad son uno de los principales pilares de la estrategia de ciberseguridad de la OACI, además de que la infraestructura de navegación aérea es esencial para el sector de la aviación. Por tanto, esta nota de estudio destaca la importancia de abordar la creación de capacidad, la instrucción y la cultura de ciberseguridad en tiempos ordinarios y de crisis.

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

a) tomar nota de la información que aquí se presenta; y
b) solicitar a la OACI que incluya, entre las tareas del Grupo Experto en Ciberseguridad, el desarrollo de iniciativas de creación de capacidad, instrucción y cultura de ciberseguridad en tiempos de crisis.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el Objetivo estratégico *Seguridad de la aviación y facilitación*
Repercusiones financieras:	
Referencias:	*Estrategia de Ciberseguridad de la Aviación* *Plan de Acción de Ciberseguridad* Resolución 40-10 de la Asamblea, *Formas de abordar la ciberseguridad en la aviación civil* *Manual de seguridad de la gestión del tránsito aéreo* (Doc 9985)

[1] Angola, Argelia, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Camerún, Chad, Comoras, Congo, Côte d'Ivoire, Djibouti, Egipto, Eritrea, Eswatini, Etiopía, Gabón, Gambia, Ghana, Guinea, Guinea-Bissau, Guinea Ecuatorial, Kenya, Lesotho, Liberia, Libia, Madagascar, Malawi, Malí, Mauritania, Marruecos, Mauricio, Mozambique, Namibia, Níger, Nigeria, República Centroafricana, República Democrática del Congo, Rwanda, Santo Tomé y Príncipe, Senegal, Seychelles, Sierra Leona, Somalia, Sudáfrica, Sudán, Sudán del Sur, Tanzanía, Togo, Túnez, Uganda, Zambia y Zimbabwe.

1. INTRODUCCIÓN

1.1 La tecnología y los sistemas cibernéticos son esenciales para la sociedad contemporánea y forman parte de numerosas actividades que ahora dependen de las tecnologías de la información. La importancia de la ciberseguridad y la resiliencia cibernética en la aviación ha aumentado considerablemente con el tiempo, algo que se ha puesto de manifiesto una y otra vez debido a los ataques perpetrados antes y durante la pandemia de COVID-19.

1.2 Cabe reconocer la naturaleza polifacética y multidisciplinaria de la ciberseguridad y constatar que los ataques cibernéticos pueden afectar simultáneamente a una amplia gama de áreas y propagarse con rapidez, de ahí que es esencial disponer de una visión común y definir una estrategia de ciberseguridad mundial. Así, la OACI desarrolló y publicó la *Estrategia de Ciberseguridad de la Aviació*n para contar con un marco de ciberseguridad sostenible y robusto.

1.3 La *Estrategia de Ciberseguridad de la OACI* cuenta con siete pilares: cooperación internacional; gobernanza; legislación y reglamentación eficaces; política de ciberseguridad; intercambio de información; gestión de incidentes y planificación de emergencias; y **creación de capacidad, instrucción y cultura de ciberseguridad.**

1.4 El 40º período de sesiones de la Asamblea de la OACI adoptó la resolución de la Asamblea 40-10, *Formas de abordar la ciberseguridad en la aviación civil.* La resolución aborda la ciberseguridad con un enfoque horizontal, transversal y funcional, reafirmando la importancia y la urgencia de proteger los sistemas de infraestructuras críticas de la aviación civil y los datos contra las amenazas cibernéticas, y pide a los Estados que implementen la *Estrategia de Ciberseguridad* de la OACI.

1.5 El Plan de Acción de Ciberseguridad (CyAP) de la OACI se ha elaborado con el fin de proponer una serie de principios, medidas y acciones para alcanzar los objetivos de los siete pilares de la estrategia. Proporciona la base para que los Estados, la industria, las partes interesadas y la OACI trabajen juntos para afianzar la capacidad de identificar, prevenir, detectar, responder y recuperarse de los ciberataques a la aviación civil, así como para crear un marco sólido de cooperación.

1.6 Recientemente se ha creado el Grupo Experto en Ciberseguridad, como parte del nuevo mecanismo de gobernanza que se ocupa de la ciberseguridad en la OACI. El mandato del Grupo Experto en Ciberseguridad incluye labores que concuerdan con el programa de trabajo de Ciberseguridad de la Aviación, a fin de elaborar disposiciones que puedan incluir normas y métodos recomendados (SARPS) y/o procedimientos para proteger la aviación civil contra las amenazas cibernéticas, teniendo debidamente en cuenta la repercusión económica y operacional, entre otras, de dichas disposiciones.

1.7 La OACI cuenta con textos de orientación sobre la cultura de la ciberseguridad (*Cultura de ciberseguridad en la aviación civil*).

2. ANÁLISIS

2.1 El estallido de la pandemia de coronavirus en 2019 (COVID-19) ha cambiado nuestro estilo de vida irremediablemente. Los Estados han tomado numerosas medidas para limitar el contacto físico entre las personas y, por tanto, para controlar la propagación de la COVID-19, como el distanciamiento social o el aprendizaje y el trabajo a distancia. Esto supuso el auge del teletrabajo y las videoconferencias, la transformación digital, la innovación y otras tecnologías en línea, lo que dio lugar a la denominada “nueva normalidad”. Además del impacto catastrófico de la COVID-19 en la economía y la sociedad internacionales, durante la pandemia aumentaron los ciberataques, que también afectaron a la sociedad y a las empresas.

2.2 El departamento de navegación aérea se considera una de las infraestructuras esenciales del ámbito de la aviación y, por lo tanto, debe recibir la atención suficiente cuando en las instalaciones correspondientes se pasa de los sistemas analógicos de tierra a los sistemas digitales espaciales para dar cabida al crecimiento ingente de la densidad del tránsito aéreo.

2.3 La creación de capacidad, la instrucción y la cultura de ciberseguridad representan uno de los principales pilares de la estrategia de ciberseguridad que hacen posible la resiliencia del sistema de aviación. Sin embargo, el marco actual de la OACI no aborda la ciberseguridad en tiempos de crisis, como la pandemia COVID-19 u otras pandemias o crisis futuras.

3. CONCLUSIÓN

3.1 La creación de capacidad, la instrucción y la cultura de ciberseguridad representan uno de los principales pilares de la estrategia de ciberseguridad que favorecen la resiliencia del sistema de aviación en tiempos ordinarios y de crisis. Por lo tanto, la resolución de la OACI sobre ciberseguridad debería considerar este aspecto tan importante. Además, el Grupo Experto en Ciberseguridad recientemente creado debería considerar también este asunto en el desempeño de su labor.

— FIN —