



ASAMBLEA — 42º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 18: Desarrollo de capacidad y apoyo a la implementación – Política y actividades

PROPUESTA DE ELABORACIÓN DE UN PROGRAMA DE INSTRUCCIÓN SOBRE CIBERSEGURIDAD QUE SE AJUSTE A NUEVAS ORIENTACIONES

(Nota presentada por la República de Corea)

RESUMEN

Un análisis estadístico reciente sobre incidentes de ciberseguridad en la aviación pone de manifiesto que las ciberamenazas han evolucionado y representan un **peligro real**. Ante esta situación, el Grupo Experto en Ciberseguridad está elaborando para su publicación textos de orientación pertinentes basados en el **Anexo 17 – Seguridad, sección 4.9**. Actualmente, solo se dispone de un curso de instrucción oficial sobre ciberseguridad elaborado por la OACI. Para crear las capacidades que permitan contrarrestar las amenazas reales, se requiere educación e instrucción. Por consiguiente, es necesario que se aliente a los Estados miembros a que elaboren programas de instrucción basados en las orientaciones sobre ciberseguridad y a la OACI, a que **normalice** esas iniciativas.

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

- reconocer la evolución constante de las ciberamenazas a la aviación civil;
- examinar las orientaciones sobre ciberseguridad elaboradas de conformidad con los requisitos del Anexo 17 — *Seguridad de la Aviación*, sección 4.9; e
- iniciar, bajo la dirección de la OACI, la elaboración de nuevos programas de instrucción de la OACI basados en las orientaciones de ciberseguridad.

<i>Objetivos estratégicos:</i>	Esta nota de estudio se relaciona con el objetivo estratégico: <i>Todos los vuelos son seguros.</i>
<i>Repercusiones financieras:</i>	Las actividades de la OACI a las que se hace referencia en esta nota de estudio se llevarán a cabo con los recursos disponibles en el presupuesto regular de 2026-2028 y/o con contribuciones extrapresupuestarias, conforme al Plan de Actividades de la OACI para 2026-2028.
<i>Referencias:</i>	<i>Resoluciones vigentes de la Asamblea (al 7 de octubre de 2022)</i> (Doc 10184) A42-WP/12 <i>Ciberseguridad de la aviación civil</i> A42-WP/13 <i>Resultados del segmento ministerial de alto nivel</i> de la Semana OACI de la Seguridad de la Aviación 2024 celebrada en Mascate (Omán)

1. INTRODUCCIÓN

1.1 Últimamente, los propósitos de los ciberataques han estado cambiando. Antes, quienes atacaban se concentraban en robar la información personal, como los nombres, los números de teléfono y las tarjetas de crédito de los pasajeros y las pasajeras. Actualmente, hay un cambio de objetivo, y lo que se busca es ocasionar interrupciones directas y concretas en la aviación civil; por ejemplo, paralizando los servicios de transporte aéreo o desactivando los sistemas de navegación aérea.

1.2 Según datos publicados por el Equipo de Respuesta a Emergencias Informáticas (EREI-CERT) del Sistema Europeo de Gestión del Tránsito Aéreo (EATMS), recabados durante un período de un año que comprende el primer semestre de 2025, los tipos de ciberataques más comunes son los programas secuestradores, con 15 de un total de 33 incidentes (aproximadamente el 45 %), seguidos por siete casos de ataques piratas y cinco casos de ataques de denegación de servicio distribuida (DDoS). Los objetivos principales de los ataques fueron las líneas aéreas con 16 incidentes (aproximadamente el 48%), seguidas por los aeropuertos, con siete; la cadena de suministro, con siete, y las administraciones de aviación civil (CAA), con tres.

1.3 Se prevé que casos como los anteriores sigan aumentando y, considerando el gran número de incidentes que no se reportan, se debe reconocer ahora mismo a las ciberamenazas como un peligro real y actual en el sector de la aviación.

2. ANÁLISIS

2.1 El Anexo 17– *Seguridad de la aviación*, en la sección 4.9, requiere la identificación de los sistemas de tecnologías de la información y la comunicación y datos críticos que se empleen para los fines de la aviación civil y, cuando resulte oportuno en función de la evaluación de riesgo, la elaboración y aplicación de medidas para protegerlos de actos de interferencia ilícita.

2.2 El año pasado, la República de Corea demostró su cumplimiento de las normas pertinentes en el marco del USAP-CMA (Enfoque de Observación Continua del Programa Universal de Auditoría de la Seguridad de la Aviación) mediante sus reglamentos nacionales de ciberseguridad, y se espera que varios Estados miembros puedan cumplir dichas normas en un grado suficiente.

2.3 Además, recientemente, el Grupo Experto en Ciberseguridad elaboró y publicó en parte una serie de documentos de orientación de los últimos cuatro años con el fin de fortalecer las capacidades en materia de ciberseguridad de la aviación, lo que ha ayudado a los Estados miembros a la aplicación de dichas capacidades en la aviación civil con más facilidad.

2.4 Desde esta perspectiva, se considera que es el momento adecuado para elaborar, en paralelo, un curso de instrucción de la OACI sobre esas orientaciones. Y también es necesario elaborar programas de educación e instrucción sobre las orientaciones de ciberseguridad que estén en proceso de elaboración o que ya se hayan publicado (existe actualmente un programa de ciberseguridad entre los cursos de la OACI).

3. CONCLUSIÓN

3.1 El análisis de las estadísticas de los últimos cinco años y los datos recientes muestran que debemos reconocer que este es el momento para enfocarse proactivamente en el fortalecimiento de la resiliencia de la ciberseguridad de la aviación civil, pues las ciberamenazas a la aviación civil se han vuelto una realidad.

3.2 El Grupo Experto en Ciberseguridad está dirigiendo la elaboración de orientaciones de ciberseguridad basadas en las recomendaciones de la sección 4.9 del Anexo 17— *Seguridad de la aviación* para su publicación. Resulta necesario que todos los Estados miembros tomen conocimiento de esas orientaciones y preparen medidas que se adapten a sus instituciones.

3.3 Para hacer frente a la situación actual, la necesidad más imperiosa es la elaboración de programas de instrucción y educación en ciberseguridad. Si bien el Grupo Experto en Ciberseguridad está elaborando orientaciones de instrucción, solo existe un curso de instrucción oficial de la OACI en esta materia. La OACI debería alentar a que muchos Estados miembros elaboren cursos de instrucción en ciberseguridad y, posteriormente, efectúen una labor de normalización.

— FIN —