Cuestión 5A del Orden del Día: **Efectividad en los planes**

ESTRATEGIA DE CIBERSEGURIDAD AERONÁUTICA

Nota presentada por Colombia, "*El País de la Belleza*"

RESUMEN

La aviación está experimentando una transformación digital sin precedentes. Tecnologías como las comunicaciones digitales, la integración de sistemas inteligentes, el análisis de datos, la vigilancia avanzada, los sistemas ATM predictivos y la computación en la nube; están redefiniendo el sector. Sin embargo, esta creciente interconexión aumenta la superficie de ataque y la vulnerabilidad a ciber amenazas. Los ataques, cada vez más sofisticados, ponen en riesgo la seguridad operacional, la privacidad de los datos y la confianza en el sistema.

Para contrarrestar este desafío, es crucial fortalecer la ciberseguridad del sector. Los Estados miembros deben implementar las recomendaciones de la OACI, como la Estrategia de Ciberseguridad y el Plan de acción de ciberseguridad, y adaptarlas a sus contextos nacionales, fortaleciendo su cultura organizacional, su infraestructura tecnológica y sus regulaciones en la materia para afrontar los retos específicos de la ciberseguridad en la aviación civil.

Ademas, la transaccionalidad del ciberespacio obliga tambien a generar mecanismos de diálogo y cooperación técnica y operativa en el área entre los estados miembros.

Referencias:
- Anexo 17 de OACI: Seguridad de la aviación AVSEC.
- Documento OACI: Estrategia de Ciberseguridad de la Aviación.
- Documento OACI: Orientación sobre la política de Ciberseguridad.
- Documento OACI: Resolución A41-19 Abordar la Ciberseguridad en la Aviación civil.
- Documento OACI: Plan de acción de Ciberseguridad

Objetivos Estratégicos de la OACI:	- *Seguridad operacional.* - *Capacidad y eficiencia de la navegación aérea.* - *Seguridad de la aviación y facilitación.* - *Cada vuelo es seguro (Safety and Security)* - *La aviación proporciona movilidad fluida, accesible y confiable para todos* - *Ningún País se queda atrás.*

1. Introducción

1.1 La aviación mundial en los últimos años viene experimentando una transformación digital global sin precedentes, enmarcada por el crecimiento del uso de tecnologías como la nube, grandes bases de datos, integración de sistemas y uso de información digital como parte de los procesos de tecnificación y optimización del uso del espacio aéreo. Sin embargo, este crecimiento de la frontera digital propone un gran desafío para la ciberseguridad del sector. La creciente interconexión de sistemas aumenta la vulnerabilidad a ciberataques que podrían interrumpir servicios esenciales, comprometer la seguridad operacional, vulnerar la privacidad de los datos y socavar la confianza en el sistema. Fortalecer la ciberseguridad es crucial para mitigar estos riesgos y garantizar la seguridad operacional, la protección de la información y la continuidad de las operaciones aéreas.

1.2 Los Estados reconocen la importancia de la ciberseguridad y ha venido implementado una estrategia integral que incluye primero la preparación del talento humano de la Autoridad Aeronáutica en estos temas, fortalecimiento de las tecnologías de seguridad digital, desarrollo de un marco regulatorio local, colaboración público-privada y cooperación internacional. Esta estrategia busca fortalecer la infraestructura tecnológica, la gestión de riesgos y la capacitación del personal.

1.3 La cooperación de los Estados miembros es fundamental para construir un espacio aéreo resiliente a las ciberamenazas como respuesta a la naturaleza transnacional del ciberespacio, que exige mecanismos de diálogo y cooperación técnica y operativa eficiente entre los Estados miembros. Compartir información, mejores prácticas y coordinar respuestas a incidentes cibernéticos son claves para la seguridad de la aviación civil global. Este esfuerzo conjunto permitirá construir un espacio aéreo más seguro y confiable para todo y responder coordinadamente a fallos o problemas de ciberseguridad como el presentado por Microsoft [1] el 19 de julio de 2024, donde sistemas administrativos de algunas aerolíneas se vieron afectados en todo el mundo. De esta manera se minimizaría el impacto, coordinando una respuesta oportuna y garantizando la seguridad operacional.

2. Discusión

2.1 La digitalización ha optimizado los procesos en todos los ámbitos de la aviación civil, desde el CNS-ATM hasta los sistemas de información de las diferentes organizaciones del sector. Las redes digitales, la automatización, el análisis de datos y el comercio electrónico han impulsado la competitividad y el crecimiento del sector, no obstante, esta transformación digital plantea desafíos significativos en términos de seguridad, confidencialidad, integridad, privacidad y calidad de la información. Sistemas que antes operaban de forma aislada ahora están interconectados, creando puntos de vulnerabilidad que pueden ser explotados por actores maliciosos. La aviación, es naturalmente una actividad colaborativa entre Estados, que exige una conexión permanente entre sistemas que optimizan el proceso del vuelo y es por eso por lo que estos Estados deben fortalecerse de manera individual y coordinada con el fin de minimizar amenazas, ya que los riesgos pueden ir desde el acceso no autorizado a datos sensibles hasta la manipulación de sistemas críticos, impactando la seguridad operacional, la continuidad del negocio y la confianza en el sector.

2.2 Desde esta perspectiva, la OACI reconoce la ciberseguridad como una responsabilidad compartida que exige cooperación internacional. Sin embargo, la rápida evolución de las ciberamenazas y su capacidad de traspasar fronteras hacen esencial una respuesta rápida de los Estados y un enfoque coordinado para intercambiar información, mejores prácticas y recursos técnicos.

[1] https://cnnespanol.cnn.com/2024/07/19/ultima-hora-falla-informatica-global-aerolineas-empresas-en-vivo/

2.3 La aviación civil se enfrenta al reto de mantener los beneficios de la digitalización y al mismo tiempo, garantizar la ciberseguridad. Esto implica la implementación de tecnologías de seguridad digital, la capacitación del personal, el intercambio de experiencias y el desarrollo de políticas y estrategias de seguridad de la información y seguridad digital para las empresas que hacen parte con el sector.

2.4 Es necesario iniciar un proceso para fortalecer sus capacidades de ciberseguridad en la aviación civil. Su estrategia se centra en cuatro ejes: (i) capacitación del personal; (ii) fortalecimiento de la infraestructura tecnológica interna; (iii) desarrollo de un marco regulatorio que promueva la ciberseguridad en todo el sector aeronáutico civil; y (iv) cooperación entre entidades.

2.5 Con esta estrategia, se busca como primera instancia, asegurar la integridad, disponibilidad, confidencialidad y continuidad de la información de los sistemas críticos y la información sensible de la entidad, protegiendo así la seguridad de la aviación civil y la continuidad del negocio contra amenazas cibernéticas, lo que permitirá de la mano de un talento mejor capacitado garantizar; la prestación de los servicios y la protección de la información. Hacia el sector se busca establecer un marco regulatorio que asegure la protección de las organizaciones que conforman el sector aeronáutico civil en el país, definiendo mecanismos de control, auditoria, gobernabilidad y respuesta a incidentes; promoviendo la implementación de prácticas robustas de ciberseguridad en todas las entidades involucradas en la aviación, desde aerolíneas, y aeropuertos hasta proveedores de servicios, empresas proveedoras, aerolíneas y fabricantes de equipos.

2.6 También es necesario establecer un dialogo constante con autoridades y empresas del sector con el fin de establecer un frente de respuesta frente a amenazas cibernéticas. Sin embargo, el ciberespacio no conoce fronteras y es por esto por lo que este dialogo debe extenderse a los Estados que deben generar mecanismos eficientes y robustos con el fin de intercambiar experiencias y recomendaciones frente a las estrategias nacionales de ciberseguridad.

2.7 En general el sector a nivel global debe proponer estrategias para proteger la información crítica, garantizar la seguridad de la aviación civil, y establecer un marco regulatorio si no común, coordinado; que promueva la implementación de prácticas robustas de ciberseguridad en todas las organizaciones del sector.

2.8 Es fundamental que las estrategias nacionales de ciberseguridad se basen en las legislaciones y regulaciones de cada Estado, pero que también sean interoperables para garantizar la seguridad operacional a nivel global. Es necesario fomentar la colaboración y el intercambio de información entre expertos para identificar y abordar vulnerabilidades y fortalecer la resiliencia del sector frente a ciberataques. Tambien es importante abrir un espacio continuo en el que los expertos de las entidades puedan retroalimentarse frente a las estrategias locales con el fin de trabajar conjuntamente en cerrar brechas que puedan ser aprovechadas por los ciberdelincuentes o ciber terroristas que afecten al sector.

2.9 En conclusión, la ciberseguridad en la aviación civil es un desafío que requiere una respuesta global y coordinada. La OACI, en colaboración con los Estados miembros, debe liderar el camino hacia un sector más resiliente y seguro frente a las ciber amenazas. La seguridad de millones de pasajeros y la estabilidad del sistema de aviación global dependen de ello.

3. **Acción sugerida**

3.1 Se invita a la Reunión a:

a) Definir dentro de la estrategia para la transformación de la región SAM acciones a partir del documento la Ciberseguridad para la aviación civil, ampliando su alcance a todos los vinculados en la operación aérea y los sistemas de distribución para asegurar un transporte aéreo eficiente dentro del conceto de ciberseguridad ampliada.

- FIN -