



ASAMBLEA — 42º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 24: Iniciativas prioritarias de seguridad operacional de la aviación y navegación aérea

CRITERIOS PARA LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA GESTIÓN DE DATOS DE SEGURIDAD OPERACIONAL EN AERONÁUTICA CIVIL

(Presentada por Perú y apoyada por Estados miembros de la CLAC²)

RESUMEN	
Con el crecimiento exponencial en la recopilación de datos de seguridad operacional en la aviación civil, surge la necesidad de utilizar tecnologías emergentes como la inteligencia artificial (IA) para apoyar la toma de decisiones basada en conocimiento derivado de los datos. Esta nota presenta un conjunto de criterios enunciativos, destinados a guiar a los Estados y organizaciones en la implementación de sistemas de IA dentro del marco de la gestión de la seguridad operacional. Dichos criterios inciden en la gobernanza ética, la transparencia y explicabilidad, la compatibilidad normativa, la mejora continua y validación de la toma de decisiones en pro de la seguridad operacional, la capacitación y desarrollo de competencias, y la integración con sistemas existentes (SSP/SMS).	
<i>Objetivos Estratégicos:</i>	Esta nota de estudio se relaciona con <i>Todos vuelos son seguros y protegidos</i> .
<i>Repercusiones financieras:</i>	No se requieren recursos adicionales.
<i>Referencias:</i>	• Anexo 19 - <i>Gestión de Seguridad Operacional</i> • Documento OACI 9859 (<i>Manual de Gestión de Seguridad Operacional - SMS</i>). • Marco ético de la OACI sobre inteligencia artificial (<i>en desarrollo</i>) • Normativas EASA sobre IA en aviación. • Principios éticos de IA de la UE.

¹ La versión en español fue proporcionada por Perú.

² Belice, Estado Plurinacional de Bolivia, Chile, Colombia, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, República Dominicana, Uruguay y la República Bolivariana de Venezuela.

1. INTRODUCCIÓN

1.1 La creciente automatización de los procesos de seguridad operacional y la disponibilidad masiva de datos (Big Data) plantean nuevas oportunidades para mejorar el análisis predictivo, la identificación de riesgos y la toma de decisiones informadas. En este contexto, la implementación de sistemas basados en inteligencia artificial puede fortalecer significativamente los programas de seguridad operacional de los Estados.

1.2 Las tecnologías de IA pueden detectar patrones complejos en grandes volúmenes de datos de vuelo, reportes de incidentes, registros de mantenimiento y otros elementos clave del Sistema de Gestión de la Seguridad Operacional (SSP/SMS). Esto puede contribuir a una mejora sustancial en la predicción de eventos, la mitigación de riesgos y el aprendizaje organizacional.

1.3 Sin embargo, el uso de la IA conlleva desafíos técnicos, éticos y regulatorios. A fin de orientar una implementación responsable, esta nota presenta un conjunto de criterios para considerar al introducir IA en los sistemas de gestión de datos de seguridad operacional.

1.4 La falta de lineamientos estandarizados sobre su implementación puede derivar en interpretaciones divergentes entre los Estados respecto de la información obtenida por una misma fuente de IA y posibles riesgos de sesgo algorítmico, pérdida de trazabilidad de decisiones o falta de alineación con los marcos legales actuales.

2. DISCUSIÓN

2.1 Con base en la experiencia técnica acumulada y las recomendaciones internacionales emergentes, se proponen los siguientes criterios:

2.1.1 **Gobernanza y ética:** Todo sistema de IA debe operar dentro de un marco ético claro que asegure la responsabilidad humana, el respeto por los derechos fundamentales y la protección de la información confidencial y sensible de seguridad operacional.

a) Se debe considerar en la gestión ética y responsable:

- 1) Evitar sesgos algorítmicos que puedan afectar la toma de decisiones en seguridad operacional.
- 2) Establecer un marco de gobernanza con supervisión humana en aplicaciones críticas.

b) La protección de la información debe considerar:

- 1) Cumplir con normativas internacionales (ej. GDPR, OACI Anexo 19) en el manejo de datos sensibles.
- 2) Asegurar el anonimato y encriptación de datos personales en informes de seguridad.

2.1.2 **Transparencia y explicabilidad:** Los algoritmos y modelos utilizados deben ser comprensibles para los operadores humanos, permitiendo rastrear el razonamiento detrás de las recomendaciones o decisiones automatizadas, es decir:

a) Los algoritmos de IA deben ser interpretables por los responsables de seguridad operacional.

b) Las decisiones basadas en IA deben poder ser auditadas y justificadas para mantener la confianza en el sistema.

2.1.3 Compatibilidad normativa: Los sistemas de IA deben ser compatibles con los marcos regulatorios existentes de la OACI, incluidos los requisitos del Anexo 19 sobre gestión de la seguridad operacional, así como con las políticas nacionales sobre protección de datos.

2.1.4 Mejora continua y validación: Se debe establecer un proceso continuo de validación, monitoreo de desempeño y actualización de los modelos de IA, garantizando su eficacia y adaptabilidad a nuevas condiciones operacionales.

2.1.4.1 Estos modelos se deben mantener en el tiempo seguros y fiables, es decir:

- a) Los sistemas de IA deben garantizar un alto nivel de confiabilidad y precisión en el procesamiento de datos de seguridad operacional; y
- b) Deben implementarse mecanismos de validación y verificación continua para minimizar errores y sesgos.

2.1.5 Capacitación y desarrollo de competencias: La implementación de IA debe ir acompañada de programas de formación para el personal involucrado, asegurando la comprensión de los sistemas y la capacidad de intervención humana ante resultados inesperados.

2.1.5.1 Se debe considerar la capacitación y concientización para:

- a) Formar a los profesionales de aviación civil en el uso y limitaciones de la IA; y
- b) Promover una cultura de seguridad que combine IA con criterio humano.

2.1.6 Integración con Sistemas Existentes (SSP/SMS): La implementación de IA debe considerar, que:

- a) La IA debe complementar, no reemplazar, los procesos tradicionales de gestión de seguridad operacional (SSP/SMS).
- b) Debe existir interoperabilidad con plataformas de reporte como ADREP, ECCAIRS, o sistemas nacionales.

3. CONCLUSIÓN

3.1 La inteligencia artificial representa una herramienta estratégica para fortalecer la seguridad operacional mediante una gestión de datos más eficaz y predictiva, ofreciendo oportunidades transformadoras para la gestión de seguridad operacional en aviación civil, pero su implementación debe ser segura, ética y alineada con los estándares OACI. Los criterios propuestos brindan un marco inicial para su implementación responsable y efectiva, buscando guiar a los Estados y organizaciones en la adopción responsable de estas tecnologías.