

Artículo Nº 02/2026 CIBERAMENAZAS EN LA AVIACIÓN MODERNA



*Por Victor Villalobos Collao. Director de Asuntos Aeronáuticos.
10 de febrero de 2026. 10 Min. Lectura.*



Introducción

La aviación civil y comercial constituye uno de los pilares fundamentales de la economía global y de la movilidad internacional. Cada día, millones de pasajeros confían en que los sistemas tecnológicos que sustentan vuelos, reservas, operaciones aeroportuarias y logística funcionen de manera segura y confiable. Sin embargo, la creciente digitalización del sector ha abierto la puerta a un nuevo tipo de riesgo: las ciberamenazas. Estas no solo comprometen la eficiencia operativa, sino que también ponen en entredicho la seguridad de los pasajeros, la estabilidad económica y la soberanía de los Estados. En este artículo se analizarán las principales ciberamenazas que enfrenta la aviación, sus impactos, ejemplos recientes y las estrategias de mitigación que se están implementando, con el objetivo de comprender la magnitud del desafío y la necesidad de una respuesta coordinada.

1. La digitalización de la aviación y su vulnerabilidad

La aviación moderna depende de sistemas digitales altamente interconectados: desde el software de planificación de vuelos y mantenimiento de aeronaves, hasta las plataformas de reservas en línea y los sistemas de control de tráfico aéreo.

Esta interconexión, aunque mejora la eficiencia, también amplifica la superficie de ataque. Un fallo en un sistema puede propagarse rápidamente y afectar operaciones críticas.

La dependencia tecnológica convierte a la aviación en un blanco atractivo para ciberdelincuentes, grupos organizados e incluso actores estatales.

2. Tipos de ciberamenazas más frecuentes



- a. Ransomware: Los ataques de secuestro de datos han paralizado aeropuertos y aerolíneas, generando pérdidas millonarias y retrasos masivos.
- b. Phishing y robo de credenciales: Representan más del 70% de los incidentes, ya que permiten acceso no autorizado a sistemas sensibles.
- c. Ataques a infraestructura crítica: Sistemas de navegación aérea, radares y torres de control son objetivos de alto valor.
- d. Ciberespionaje: Estados y organizaciones buscan información estratégica sobre rutas, logística y tecnología aeronáutica.
- e. Ataques a la cadena de suministro: Los proveedores de software y mantenimiento son vulnerables, lo que abre puertas indirectas a los atacantes.

3. Impacto económico y social

El impacto de un ataque cibernético en aviación trasciende lo técnico. Un solo incidente puede provocar:

- a. Pérdidas económicas millonarias: El mercado de ciberseguridad en aviación se estima en más de 5.320 millones de dólares para 2025.

- b. Retrasos y cancelaciones masivas: Afectan la confianza del pasajero y la reputación de las aerolíneas.
- c. Riesgos para la seguridad operacional: Un ataque a sistemas de navegación puede comprometer la vida de miles de personas.
- d. Implicaciones geopolíticas: La aviación es estratégica para la soberanía nacional, por lo que ataques pueden tener fines políticos o militares.

4. Ejemplos recientes



En el año recién pasado se registraron ataques significativos contra aerolíneas y aeropuertos, perpetrados por 22 grupos distintos. En un informe reciente sobre la amenaza cibernética en el sector aeronáutico, el grupo de defensa y tecnología Thales contabilizó 27 ciberataques de tipo ransomware entre enero de 2024 y abril de 2025 en la aviación, lo que representa un aumento del 600% en un año, apuntando a aerolíneas, aeropuertos, sistemas de navegación e incluso subcontratistas.

En agosto de 2024, el aeropuerto internacional de Seattle-Tacoma, en EE.UU., sufrió un ataque de ransomware vinculado al grupo Rhysida. El incidente afectó servicios de Wi-Fi, check-in, gestión de equipaje y cartelería digital. Durante varias horas, el aeropuerto debió operar manualmente, notificando a más de 90.000 empleados y usuarios.

En diciembre de 2024, Japan Airlines fue blanco de un ataque en plena temporada navideña. Las ventas de pasajes aéreos quedaron interrumpidas, más de 20 vuelos se retrasaron y la aerolínea tuvo que suspender temporalmente operaciones.

El caso más reciente ocurrió en junio de 2025, cuando la canadiense WestJet reportó un ciberataque que generó errores intermitentes en su página web y app. Aunque la compañía afirmó que los vuelos no se vieron afectados, la investigación sigue abierta para determinar si se filtraron datos personales de los clientes.

En Europa el mismo año 2025, un ataque de ransomware paralizó sistemas de check-in, generando caos en varios aeropuertos. En Asia, aerolíneas reportaron intentos de acceso a sistemas de planificación de vuelos mediante credenciales robadas. Estos casos reflejan la diversidad de actores y métodos empleados, así como la necesidad de respuestas rápidas y coordinadas.

Los aeropuertos europeos de Heathrow-Londres, Berlín, Bruselas y Dublín sufrieron retrasos y cancelaciones de vuelos debido a un ciberataque contra el sistema de registro de equipajes y pasajeros.

En los terminales de Londres y Bruselas se observaron largas filas de pasajeros que esperaban frente a los mostradores y consultaban las pantallas informativas donde se multiplicaban los avisos de retrasos.

Heathrow aconsejó a los pasajeros verificar el estado de su vuelo con su aerolínea y llegar con mucho tiempo de antelación para realizar los trámites de registro.

En su sitio en internet, el aeropuerto de Berlín también indicó que tenía un "problema técnico con un proveedor", y en los de Dublín y Cork, en Irlanda, se registraron "consecuencias menores" por el ciberataque.

"Hemos tomado conocimiento de una disrupción relacionada con ciberataques en nuestro software MUSE en ciertos aeropuertos", dijo la empresa Collins Aerospace en una escueta comunicación. Esta compañía provee servicios de registro en 170 aeropuertos en todo el mundo, según su sitio web.

5. Estrategias de mitigación en ciberataques en la aviación civil

a. Normativas y marcos regulatorios

- OACI (Organización de Aviación Civil Internacional): Estrategia global de ciberseguridad que promueve cooperación internacional, intercambio de información y estándares comunes.
- Reglamento UE 2022/1645: Obliga a aeropuertos y proveedores de servicios a integrar prácticas sólidas de ciberseguridad desde octubre de 2025.
- Normas de la industria (IATA, EASA, FAA): Establecen requisitos de seguridad digital para aeronaves y sistemas de control.

b. Medidas técnicas

- Segmentación de redes críticas: Separar sistemas de navegación, control de tráfico aéreo y operaciones de pasajeros para reducir el riesgo de propagación de ataques.

- Cifrado y autenticación fuerte: Proteger comunicaciones entre aeronaves, torres de control y sistemas de mantenimiento.
- Monitoreo en tiempo real: Uso de sistemas de detección de intrusiones (IDS) y análisis de tráfico para identificar anomalías.
- Actualizaciones y parches regulares: Evitar vulnerabilidades en software de aeronaves y sistemas aeroportuarios.
- Pruebas de penetración y simulacros: Evaluar la resiliencia de los sistemas frente a ataques simulados.

c. Gestión organizacional

- Planes de respuesta a incidentes: Protocolos claros para contener, investigar y recuperar operaciones tras un ataque.
- Capacitación del personal: Entrenamiento en ciberseguridad para pilotos, controladores y personal de tierra.
- Colaboración interinstitucional: Compartir inteligencia sobre amenazas entre aerolíneas, gobiernos y proveedores tecnológicos.
- Evaluaciones de riesgo periódicas: Identificar vulnerabilidades en sistemas críticos y priorizar inversiones.

6. La industria ha comenzado a implementar medidas de defensa más sofisticadas

- a. Autenticación multifactor y cifrado avanzado para proteger credenciales y datos sensibles.
- b. Segmentación de redes que impide que un ataque se propague a sistemas críticos.
- c. Capacitación constante del personal frente a técnicas de ingeniería social como el phishing.
- d. Planes de contingencia y recuperación rápida que permiten reanudar operaciones tras un ataque.
- e. Colaboración internacional mediante organismos como la Organización de Aviación Civil Internacional (OACI), que promueve estándares globales de ciberseguridad.

7. El papel de la cooperación internacional



La aviación es un sector global por naturaleza. Un ataque en un aeropuerto puede tener repercusiones en vuelos internacionales y afectar a múltiples países. Por ello, la cooperación internacional es esencial. Compartir inteligencia sobre amenazas, coordinar respuestas y establecer protocolos comunes son pasos fundamentales para enfrentar un problema que no reconoce fronteras. Además, la colaboración público-privada entre gobiernos, aerolíneas y proveedores tecnológicos fortalece la resiliencia del sector.

8. Perspectivas futuras

El avance de tecnologías como la inteligencia artificial, el Internet de las Cosas (IoT) y la automatización de procesos incrementará la eficiencia de la aviación, pero también abrirá nuevas vulnerabilidades. Los sistemas autónomos de control de tráfico aéreo, por ejemplo, podrían ser blanco de ataques sofisticados. Asimismo, la creciente interconexión con servicios externos, como aplicaciones móviles de pasajeros, amplía la superficie de ataque. La industria debe anticiparse a estas amenazas mediante inversión en innovación y resiliencia digital.



Conclusión

Las ciberamenazas en aviación representan uno de los mayores desafíos de la era digital. No se trata únicamente de proteger datos o sistemas, sino de garantizar la seguridad de millones de pasajeros y la estabilidad de un sector estratégico para la economía global.

Los ataques recientes demuestran que los ciberdelincuentes y actores estatales ven en la aviación un objetivo de alto valor. Frente a ello, la respuesta debe ser integral: inversión en tecnología, capacitación del personal, planes de contingencia y, sobre todo, cooperación internacional. La aviación del futuro será cada vez más digital, y su seguridad dependerá de la capacidad de anticipar, prevenir y responder a las ciberamenazas. Solo así se podrá mantener la confianza de los pasajeros y la continuidad de un sector que conecta al mundo.

Bibliografía:

1. International Civil Aviation Organization (ICAO). (2019). Aviation Cybersecurity Strategy. Montréal, Canada: ICAO. Recuperado de <https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx>
2. International Air Transport Association (IATA). (2022). Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation (4^a ed.). Montreal, Canada: IATA.
3. International Air Transport Association (IATA). (2024). Annual Security Report (IASeR). Montreal, Canada: IATA.
4. Cipher – Grupo Prosegur. (2025, febrero 17). Cinco principales amenazas que enfrenta la industria de la aviación en 2025. Santiago, Chile: Sala de Prensa Cipher.
5. Organización de Aviación Civil Internacional (OACI). (2019). Estrategia de ciberseguridad de la aviación. Montreal, Canadá: OACI.