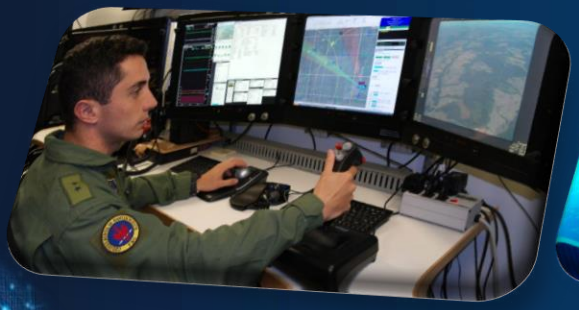
BOLETÍN INFORMATIVO **AAAES**

BI-001-2025

TRABAJAMOS POR LA SEGURIDAD DE AVIACIÓN DE ESTADO

# CIBERSEGURIDAD EN LA AVIACIÓN DE ESTADO

## Amenazas y Estrategias de Protección



La creciente amenaza cibernética en la aviación de Estado, crea la necesidad de implementar estrategias de mitigación para proteger las operaciones aéreas, infraestructura y datos estratégicos.

Los ataques dirigidos a infraestructuras críticas, sistemas de navegación y comunicaciones, así como el robo de información estratégica, representan un riesgo latente para la seguridad nacional.

FUERZA AEROESPACIAL COLOMBIANA

Oficina de Autoridad Aeronáutica de Aviación de Estado
Carrera 13 No. 66-47 oficina 203
601 3159800 Ext. 63000
aaaes@fac.mil.co

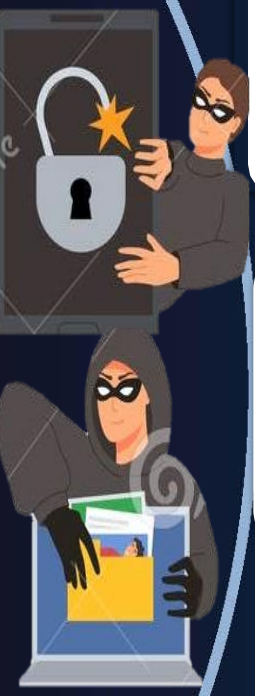
ÁREA DE SEGURIDAD AEROPORTUARIA

BOLETÍN INFORMATIVO **AAAES**

BI-001-2025

TRABAJAMOS POR LA SEGURIDAD DE AVIACIÓN DE ESTADO

# Principales Amenazas Cibernéticas en la Aviación de Estado



**1. ATAQUES A LA INFRAESTRUCTURA DE CONTROL AÉREO.**

Riesgo de interrupciones en sistemas de navegación y comunicaciones.

**4. INTERFERENCIA EN SISTEMAS DE AERONAVES:**

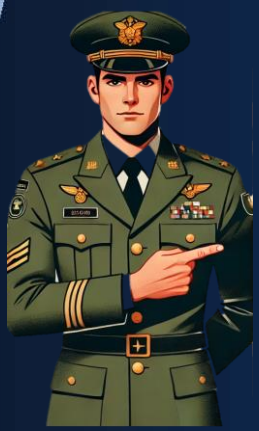
Posible manipulación de sistemas de vuelo a través de vulnerabilidades tecnológicas.

**2. ROBO DE INFORMACIÓN ESTRATÉGICA.**

Espionaje y fuga de datos sensibles de las fuerzas militares y cuerpos de seguridad.

**3. MANIPULACIÓN DE DATOS DE NAVEGACIÓN Y COMUNICACIÓN**

Alteración intencionada de la información transmitida entre aeronaves, torres de control y otros sistemas de gestión del tráfico aéreo.



## TENGA EN CUENTA QUE..

Este tipo de ataques pueden comprometer gravemente la seguridad de la aviación de Estado, razón por la cual se deben implementar medidas de ciberseguridad avanzadas para proteger los sistemas de navegación y comunicación contra accesos no autorizados.

FUERZA AEROESPACIAL COLOMBIANA

Oficina de Autoridad Aeronáutica de Aviación de Estado
Carrera 13 No. 66-47 oficina 203
601 3159800 Ext. 63000
aaaes@fac.mil.co

ÁREA DE SEGURIDAD AEROPORTUARIA

BOLETÍN INFORMATIVO **AAAES**

BI-001-2025

TRABAJAMOS POR LA SEGURIDAD DE AVIACIÓN DE ESTADO

# EL ELEMENTO HUMANO DE LA CIBERSEGURIDAD

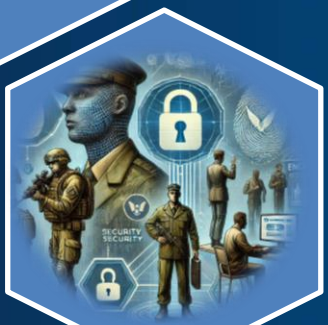

Un incidente cibernético puede ser causado por una entidad externa o interna.

Eventos internos pueden ser intencionales o debido a un error humano.



Elementos como una adecuada capacitación debe ser parte de una estrategia de ciberseguridad.

La seguridad de la información no es solo una cuestión de tecnología, también de las personas.



FUERZA AEROESPACIAL COLOMBIANA

Oficina de Autoridad Aeronáutica de Aviación de Estado
Carrera 13 No. 66-47 oficina 203
601 3159800 Ext. 63000
aaaes@fac.mil.co

ÁREA DE SEGURIDAD AEROPORTUARIA

BOLETÍN INFORMATIVO **AAAES**
BI-001-2025

TRABAJAMOS POR LA SEGURIDAD DE AVIACIÓN DE ESTADO

# ESTRATEGIAS DE PROTECCIÓN Y MITIGACIÓN

Implementación de sistemas de detección y prevención de intrusos en redes aeronáuticas militares.

Capacitación en ciberseguridad: Capacitación continua del personal en ciberseguridad y protocolos de respuesta a incidentes.

Cooperación entre organismos nacionales e internacionales para compartir información sobre amenazas cibernéticas.

Uso de inteligencia artificial en detección de amenazas: identificar patrones de ataque en tiempo real.

Fuente: OTAN (Estrategia de Ciberseguridad 2023), RACAE 160 Capítulo G (Medidas de Seguridad Física y Ciberseguridad).

FUERZA AEROESPACIAL COLOMBIANA

Oficina de Autoridad Aeronáutica de Aviación de Estado
Carrera 13 No. 66-47 oficina 203
601 3159800 Ext. 63000
aaaes@fac.mil.co

ÁREA DE SEGURIDAD AEROPORTUARIA

# REFERENCIAS

•OTAN: "Cyber Defence" (Defensa Cibernética), que detalla las estrategias y políticas de la OTAN en materia de ciberseguridad.
•OACI: "Anexo 17 - Seguridad", que aborda las normas y métodos recomendados para la seguridad de la aviación civil, incluyendo aspectos relacionados con la ciberseguridad.
•https://eu-lac-app.eu/public/uploads/Presentacion-OACI-CIBERSEGURIDAD-Dec-2020-EU_LAC-APP.pdf
- Enlace: Política de Ciberdefensa de la OTAN.

◈ OACI:
- Documento: "Manual de Gestión de la Ciberseguridad en la Aviación". https://www.icao.int/NACC/Documents/Meetings/2023/AIMTF6/AIMTF6-P04-SPA.pdf
- Contenido: Proporciona estrategias para la evaluación de riesgos cibernéticos en el sector aeronáutico.

◈ RACAE 160:
- Capítulo G: Medidas de Seguridad Física y Ciberseguridad.
- Capítulo H: Métodos para enfrentar interferencias ilícitas.
- Capítulo F: Medidas relativas al ciberterrorismo.

## IMÁGENES DE REFERENCIA

- ESCUELA DE Postgrados FAC – Briefing Seguridad Operacional pdf
- https://iworld.com.mx/ciberseguridad-en-la-aviacion-como-proteger-la-infraestructura-critica/
- https://www.emavi.edu.co/ - Escuela Militar de Aviación Marco Fidel Suarez
- https://tbsek.mx/blog/2024/02-febrero/183.IPS.html
- https://s3.amazonaws.com/files.todaysmilitary.com/s3fs-public/2022-12/Futures2020-AirNG-Logan_Balvik-00121_20200128.jpg
- Imágenes de IA