

Implementación de estrategias de ciberseguridad





Plan Nacional de Acción en ciberseguridad de la aviación civil

- Determinación de responsabilidades (Autoridad Aeronáutica).
- Marco regulatorio de ciberseguridad.
- Determinación de responsabilidades (Industria).
- Categorización de empresas (NMT).
- Capacitación y formación.
- Vigilancia y seguimiento.
- Lecciones aprendidas.





Determinación de responsabilidades (Autoridad Aeronáutica)

Perfil del Inspector Aeronáutico en Ciberseguridad.

Acreditación: Instituto Universitario de Aviación Civil (IUAC).

Nueva área de trabajo: vigilancia y supervisión.





Marco regulatorio en ciberseguridad

Normativas y circulares



CIRCULAR DE SEGURIDAD DE LA AVIACIÓN
DISPOSICIONES PARA LA PROTECCIÓN DE SISTEMAS DE
TECNOLOGÍA DE LA INFORMACIÓN, LAS COMUNICACIONES Y DATOS
CRÍTICOS EN LAS OPERACIONES AERONÁUTICAS

1. Propósito
Establecer los lineamientos para la protección de los sistemas de tecnología de la información, las comunicaciones y datos críticos utilizados en las operaciones aeronáuticas, considerando su naturaleza y la información crítica que contienen, para la seguridad operacional y la protección de la aviación civil, de acuerdo con lo establecido en el Plan Nacional de Seguridad de la Aviación Civil (PNSAC), las Reguleciones Aeronáuticas Venezolanas (RAV), Anexo 17 - Seguridad, del Convenio sobre Aviación Civil Internacional de la Organización de Aviación Civil Internacional (OACI).

2. Aplicabilidad
La presente Circular de Seguridad de la Aviación, será de aplicación y observancia obligatoria para los explotadores de aeródromos y aeropuertos, explotadores de aeronaves, operadores de sistemas de aeronaves pilotado a distancia (RPAS) y los prestadores de servicios de tránsito aéreo dentro del territorio de la República Bolivariana de Venezuela.

3. Objetivos
3.1 Documentar e implementar políticas básicas y procedimientos en concordancia con las necesidades de cada organización, contemplando aspectos de seguridad físicos y lógicos, restricción de acceso, separación de redes, entre otros controles, que permitan la disposición de un marco regulatorio interno para el desarrollo, implementación y mejoramiento continuo de políticas de seguridad de la información ante incidentes, amenazas o actos de interferencia ilícita, que puedan representar daños o pérdidas para la aviación civil.
3.2 Realizar continuamente evaluaciones de riesgo, donde se contemple vulnerabilidades e interdependencia entre los sistemas críticos de aviación, para la mitigación de posibles ciberataques, mediante el establecimiento de medidas para la observancia de las leyes y normativas existentes en materia de ciberseguridad.
3.3 Diseñar planes preventivos y correctivos que permitan minimizar y mitigar intentos de sabotaje, interferencia, violación de privacidad, entre otros riesgos e incidentes que representen un daño parcial o total sobre los activos y recursos tecnológicos asociados a las operaciones de aviación civil.
3.4 Fomentar la sensibilización y concientización del personal, terceros o proveedores involucrados en las operaciones aeronáuticas, sobre la importancia de la seguridad en los activos tecnológicos y de información asociados a las actividades de aviación civil.

CA-13-097
Bogotá, República de Colombia
Marzo de agosto 2021

1 de 20

Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para el Transporte | Instituto Nacional de Aeronáutica Civil | 200 BATALLA DE CARABOBO

CIRCULAR DE SEGURIDAD DE LA AVIACIÓN DISPOSICIONES PARA LA PROTECCIÓN DE SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN, LAS COMUNICACIONES Y DATOS CRÍTICOS EN LAS OPERACIONES AERONÁUTICAS

Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para el Transporte | Instituto Nacional de Aeronáutica Civil | 200 BATALLA DE CARABOBO

CIRCULAR DE SEGURIDAD DE LA AVIACIÓN DISPOSICIONES PARA EVALUACIONES DE RIESGO SOBRE CIBERSEGURIDAD EN LA AVIACIÓN CIVIL

Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para el Transporte | Instituto Nacional de Aeronáutica Civil | 200 BATALLA DE CARABOBO

CIRCULAR DE SEGURIDAD DE LA AVIACIÓN DISPOSICIONES PARA LA IMPLEMENTACIÓN DE UN PROGRAMA DE CIBERSEGURIDAD EN AVIACIÓN CIVIL





Determinación de responsabilidades (Industria)

Responsable: Ciberseguridad en Aviación Civil.

Nombramiento oficial ante la autoridad aeronáutica.

Título profesional / Experiencia.





Determinación de responsabilidades (Industria)

Funciones



Planificar las etapas para las evaluaciones de riesgo.

Desarrollar e implementar el marco de ciberseguridad.

Reportar a la AA las novedades e incidentes.





Categorización de empresas (nivel de madurez tecnológica)

Realidad o Infraestructura tecnológica

Adopción e incorporación TI/OT.

Fortalecer y mejorar procesos.

Reportar a la AA las novedades e incidentes.





Capacitación y formación

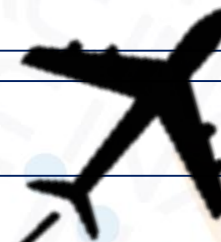
Dirigido a la industria

Fundamentos de ciberseguridad en aviación civil.

Metodología de evaluación de riesgos.

Desarrollo de programas y planes.

Fundamentos de la ISO 27001.





Vigilancia y seguimiento

Dirigido a la industria

Políticas y procedimientos de ciberseguridad.

Evaluación de riesgos.

Plan de tratamiento de riesgos.

Procedimientos de gestión de incidentes.

Plan de contingencia y continuidad.





Avances/Lecciones aprendidas SNA



Marco normativo en ciberseguridad

Evaluación de
riesgo

Programa
SGSI

Contingencia y
Continuidad



Avances/Lecciones aprendidas SNA

Responsable de ciberseguridad.

Grupo de trabajo: técnicos / operativos.

Política de seguridad.

Procedimientos de gestión activos.

Evaluación de riesgo y gestión de riesgos.





Avances/Lecciones aprendidas Orientación técnica y acompañamiento

- Gestión de tecnología de protección.
- Gestión de identidad y control de acceso.
- Seguridad física y del entorno.
- Seguridad de las operaciones/comunicaciones.
- Gestión de riesgos de la cadena de suministro.
- Gestión de incidentes de seguridad.
- Gestión de la continuidad de las operaciones.



Avances/Lecciones aprendidas Selección de un marco

Seleccionar un marco, estándar o una metodología.

Mantener un compromiso fuerte y continuo.

Proceso permanente, continuo y cíclico.

Revisión y actualización de forma regular.





Avances/Lecciones aprendidas Cómo comenzar o fortalecer

Modelos de orientación y lineamientos

Documento: 8973 - 9985

Estrategia de Ciberseguridad.

Plan de Acción de Ciberseguridad.

Cultura de Ciberseguridad en la Aviación Civil.

Orientación sobre Políticas de Ciberseguridad.





Avances/Lecciones aprendidas Cómo comenzar o fortalecer

Modelos de orientación y lineamientos

Esquema de Política de Ciberseguridad para
la Gestión de Tráfico Aéreo.

Guía de evaluación de riesgos cibernéticos.

Estándar de Excelencia en Ciberseguridad.

Serie ISO 27000: 27001/27002/27003.

CANSO

ISO





Avances/Lecciones aprendidas Uso y adopción de tecnologías

Diagnóstico de la situación actual del sector de la aviación en cuanto al uso y adopción de tecnologías.

Fase de diagnóstico y acercamiento.

Mesas de trabajo: consulta/análisis.

Realidad, fortalezas, y necesidades.



Avances/Lecciones aprendidas resultados o hallazgos

Adopción e implementación de prácticas.

Ausencia de procedimientos / documentación.

95% de las violaciones de ciberseguridad son
causadas por errores humanos.

Procedimientos incorrectos



Filtraciones de información

Contraseñas débiles



Actualizaciones de seguridad





Gracias por su atención

