In cooperation with

ICAO canso AIRBUS

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

# Reconocimientos

Este documento fue producido por la Organización Aviación Civil Internacional (OACI), la Organización Civil de Proveedores de Servicios de Navegación Aérea (CANSO) y Airbus.

Se reconoce a las siguientes personas por sus valiosas contribuciones:

- **Mayda Ávila**, Regional Officer, Communications, Navigation and Surveillance, ICAO NACC Office
- **Julien Touzeau**, Product Security Director, Americas, Safety, Security & Technical Affairs – AAG, Airbus
- **Yann Berger**, Product Security Expert, APSYS – Product Security, Airbus
- **Gaelle Hubert**, Governance specialist and security auditor, Airbus
- **Poulin Estelle**, Physical security specialist, Aviation Security specialist and ACC3 auditor, Airbus
- **Javier Vanegas**, Director, Latin America and Caribbean Affairs, CANSO
- **Shayne Campbell**, Safety Programme Manager, CANSO
- **Eduardo Garcia**, Manager European ATM Coordination and Safety, CANSO

**Traducción:**

- **Gabriel Gutiérrez Serrato**, Communications, Navigation and Surveillance Unit, ICAO NACC Office

# Contenidos

# Introducción

La primera década del siglo veintiuno ha mostrado un incremento un incremento en la actividad de terrorismo contra diversos objetivos utilizando una diversidad de métodos. Estos han ido desde el uso de explosivos en ataque contra aeronaves, trenes y edificios, hasta ciberataques contra sistemas de información y comunicaciones. Al mismo tiempo, los equipos y sistemas que apoyan a los servicios de navegación aérea han evolucionado hacia una digitalización y conectividad haciéndolos vulnerables a los ciberataques. Los sistemas de gestión de la información que apoyan en tiempo real la toma de decisiones son sensibles y merecen especial atención en cuanto a su protección.

Los ciberataques se han convertido en una amenaza crecimiento a nivel mundial como resultado del alza en la digitalización y en los sistemas de interconectividad. La aviación civil es particularmente sensible a esta amenaza emergente debido a sus amplios requisitos de interconectividad. Cualquier interrupción de los sistemas debido a los ciberataques pueden afectar seriamente la seguridad operacional y la seguridad de la aviación de los vuelos y también la reputación de la aviación civil a los ojos del público. Como tal, la OACI ha abordado esta amenaza emergente a la aviación civil a través de la resolución A39-19 "abordando la ciberseguridad en la aviación civil" durante la Asamblea 39 del consejo de la OACI.

Es vital que el sector de la aviación civil integre las políticas de ciberseguridad como parte de sus procedimientos normales, integrándolas en cada parte de su sistema de aviación.

En este contexto, la Gestión del tránsito aéreo (ATM), los sistemas de Comunicación, Navegación y Vigilancia (CNS), Gestión de la información (AIM) y otros sistemas importantes de aviación están expuestos a muchos tipos de riesgos potenciales, provenientes de:

- Acciones que pueden ser intencionales y hostiles,
- Accidentales o negligentes,
- Impacto de un desastre natural.

Los sistemas aeronáuticos son vulnerables a amenazas cibernéticas como el sabotaje a IT, corrupción y disponibilidad de datos (notablemente secuestro de datos), corrupción de software, disrupción o interrupción de las comunicaciones, interferencia de la comunicación satelital, ciberataques incluyendo sistemas de sabotaje, brechas de datos, destrucción y daño de hardware. Las amenazas cibernéticas también pueden ser parte de una trama más grande, como pueden ser el secuestro, la toma de rehenes, lesiones físicas o muerte.

Las Autoridades de Aviación Civil (AAC) y los Proveedores de Servicio de Navegación Aérea (ANSP) en la región de América Latina y el Caribe han mostrado su preocupación sobre el incremento de las amenazas de ciberataques derivado de la implementación de tecnología de punta, sin las protecciones necesarias y los procedimientos de resiliencia para asegurar su continuidad para cumplir con los niveles requeridos de seguridad. Se recomienda, por lo tanto, que los Estados amplíen su visión sobre ciberseguridad para abarcan los sistemas de Navegación Aérea, considerando los sistemas satelitales (por ejemplo, ADS-B), sistemas de información, sistemas de gestión de tránsito aéreo y otros que pudieran ser vulnerables a ciberataques. La digitalización y la conectividad a Internet significan que los equipos que antes no eran sospechosos ahora son vulnerables.

A fin de proteger sus Operaciones de amenazas internas y externas, deberían implementarse mecanismos sobre ciberseguridad a través de todo el sistema ATM.

También se recomienda que la ciberseguridad sea incluida en la cultura de la seguridad a través de entrenamiento del personal (Proveedores de Servicios de Navegación Aérea –ANSP-, aerolíneas y aeropuertos). La aplicación de buenas prácticas básicas introducidas en la capacitación puede reducir la probabilidad de ciberataques que, a pesar un mínimo riesgo a la seguridad, pueden afectar la confianza del público.

Mientras que las tecnologías Emergentes estarían mejor preparadas para resistir un ciberataque, el legado tecnológico que todavía se utiliza en los aeropuertos, aerolíneas y ANSP pueden no estar preparados. Como resultado, la ciberseguridad es considerada como un asunto interrelacionado por la OACI debido a sus funciones y tecnología interconectada. La razón de esto es la amenaza percibida de un ciberataque que afecte las operaciones de aeródromos, aeronavegabilidad y sistemas y servicios de navegación aérea.

# 1. Cómo utilizar el presente documento

Este documento no reemplaza ninguna regulación nacional.

Los Estados, de acuerdo con su infraestructura aeronáutica operacional/técnica, deberían:

- Identificar sus infraestructuras críticas relacionadas con las comunicaciones, navegación y vigilancia de los servicios de tránsito aéreo y protegerlas adecuadamente.
- Proteger los sistemas automatizados que apoyan las unidades de Servicio de Tránsito Aéreo (ATS), sus sistemas de información aeronáutica entre otros, para asegurar la confidencialidad, integridad y disponibilidad de la información, así como la resiliencia de las operaciones.
- Realizar un análisis de riesgo para evaluar las amenazas a la ciberseguridad y vulnerabilidades, relacionados con el impacto a los servicios de tránsito aéreo.
- Revisar y actualizar las especificaciones técnicas y operacionales de los sistemas considerando que nuevas tecnologías han sido implementadas en los servicios de tránsito aéreo proporcionando mayor eficiencia y simplificando la gestión de operaciones; sin embargo, pueden ser vulnerables a amenazas cibernéticas. Esta revisión puede ayudar a mitigar riesgos cibernéticos y asegurar resiliencia.
- Monitorear y analizar el intercambio de información y las conexiones para identificar posibles ciberataques y establecer medidas de protección adecuadas para los sistemas de tránsito aéreo.
- Colaborar y cooperar con la industria fin de que se adapten Requisitos técnicos para el ritmo de desarrollo de las nuevas tecnologías y asegurar que el hardware y el software que apoyan los sistemas de Tránsito Aéreo estén actualizados y preparados contra un ciberataque. También, todas las partes interesadas (Estados, ANSP e Industria) necesitan colaborar en un diseño de procedimientos operacionales normalizados (SOPs) para asegurar una adecuada protección de sus operaciones.
- Proporcionar capacitación y calificaciones al personal que gestiona áreas técnicas y operacionales ANS para una correcta provisión del servicio. El personal debería conocer y tener las habilidades para realizar planes de recuperación en el caso de un incidente cibernético.

# 2. Documentos aplicables

- Anexo de la OACI
- Documento OACI 8973 – Manual de seguridad de la aviación de la OACI
- Documento OACI 9985 – Manual de seguridad ATM de la OACI
- Estrategia sobre Ciberseguridad de la Aviación de la OACI
- Norma de proceso ED 205 para los aspectos de seguridad de la certificación/declaración de los sistemas terrestres de gestión del tráfico aéreo / servicios de navegación aérea (ATM/ANS)

# 3. Enfoque

Este documento cubre completamente la estructura funcional de la aviación y a todas las partes interesadas, como son las autoridades de aviación civil, los proveedores de servicios de navegación aérea, explotadores de aeropuertos, y cualquier otra organización que es parte del sistema estatal de la aviación para asegurar la implementación de los procedimientos y prácticas de ciberseguridad en todos los servicios bajo la vigilancia del Estado, tales como:

- Unidades de servicio de tránsito aéreo (TWR, APP y ACC)
- Datos e infraestructura de comunicación, navegación y vigilancia
- Sistemas de información digital (información aeronáutica, información meteorológica y otra información que apoye la toma de decisiones)
- Sistemas para la interoperabilidad de la aviación
- Otros de acuerdo con los servicios y Operaciones del Estado

Este documento es aplicable a todas las locaciones e instalaciones del Sistema de aviación que alberguen:

- Información requerida por servicios ATM.
- Infraestructura de tecnologías de la información (IT) de las que dependen los servicios ATM
- Tecnología operacional (OT) y Sistemas industriales interconectados y controlados automáticamente and Sistemas interconectados industriales y controlados automáticamente (IACS).
- Servicios extendidos y asociación, e interconexiones de sistemas de información relacionados
- Todo el personal de la aviación y organizaciones externas que tienen acceso a información e instalaciones de navegación aérea

# 4. Objetivos

Los objetivos generales de esta política de seguridad del sistema de la aviación son:

- Asegurar la resiliencia del Sistema de aviación de los Estados
- Asegurar la integridad, disponibilidad y confidencialidad de la información
- Proteger el hardware/software que apoya la infraestructura del Sistema de aviación para reducir riesgos en todos los servicios de aviación de los Estados
- Apoyar la implementación de los procedimientos y procesos de ciberseguridad en toda la infraestructura y servicios de la aviación
- Apoyar la seguridad de la aviación civil, la seguridad y defensa nacionales y el cumplimiento de la ley.

# 5. Objetivo de la arquitectura de seguridad

Además de la implementación de las mejores prácticas identificadas en los documentos referidos, este documento recomienda encarecidamente la identificación, definición e implementación de medidas de seguridad basados en su relevancia en cuanto a la seguridad operacional y operatividad [1].

1 En seguridad de la información se estima la criticidad con respecto a la CIA (confidencialidad, integridad, disponibilidad) que podría impactar la seguridad y operatividad..

# 6. Documentación de seguridad ATM

### Requisitos ATMSP-001-01:

Sobre la base de esta política de seguridad, se debe definir, implementar y mantener un sistema de gestión de seguridad de la información basado en un enfoque de gestión de riesgos.

NB: Las normas ISO27001 e ISO27002 proporcionan procesos aprobados y mejores prácticas para ISMS.

# 7.Gestión del riesgo

### Requisito ATMSP-002-01:

La seguridad ATM debería estar dirigida por inteligencia, basada en amenazas y gestionada por riesgos.

### Requisito ATMSP-003-01:

La gestión de riesgos de seguridad de la información se considerará parte integral del proceso general del ciclo de vida del sistema.

### Requisito ATMSP-004-01:

Todos los activos ATM (datos, sistemas, personal ...) deberán tener propiedad definida.

### Requisito ATMSP-005-01:

Los principios de defensa en profundidad, tal como se definen en 5 – Objetivo de la arquitectura de seguridad, serán parte de la gestión de la seguridad de la información.

### Requisito ATMSP-006-01:

El enfoque basado en riesgos de seguridad operacional, ATM, deberá implementar medidas técnicas de seguridad y medidas de seguridad operativa (políticas y procesos) para reducir el riesgo a un nivel aceptable con respecto a:

- Ciberataque exitoso (intencional)
- Error humano,
- Accidente o incidente,
- Impacto de desastres naturales.

### Requisito ATMSP-007-01:

La organización a cargo de la seguridad física o de la información ATM debe garantizar un tratamiento eficiente y coordinado de los riesgos de seguridad.

### Requisito ATMSP-008-01:

Los riesgos de seguridad de la información ATM se revisarán y controlarán periódicamente.

# 8. Gobernanza y organización de la seguridad

### Requisito ATMSP-009-01:

La Autoridad de Aviación Civil designará la autoridad apropiada (AA) responsable de la seguridad general ATM.

### Requisito ATMSP-010-01:

El responsable de seguridad ATM designado por la AAC deberá definir como mínimo:

- Funciones y responsabilidades para la gestión de riesgos de seguridad ATM;
- Procesos de gestión de riesgos;
- Procesos de gestión de incidentes y crisis.

### Requisito ATMSP-011-01:

Se mantendrán actualizadas las habilidades y competencias del personal designado para funciones y responsabilidades de seguridad ATM.

# 9. Recursos humanos

### Requisito ATMSP-012-01:

El personal será parte de la seguridad ATM durante todas las fases de empleo:

- Antes del empleo: a través de medidas tales como verificación de antecedentes de acuerdo con las regulaciones locales;
- Durante el empleo: desarrollando una cultura de seguridad mediante la formación periódica y la sensibilización; y
- Después del empleo: asegurando el respeto del proceso de desabastecimiento y recordando al personal los compromisos de no divulgación de la información.

### Requisito ATMSP-013-01:

El personal de seguridad debe asegurarse de que las personas con acceso a las instalaciones ATM, las áreas controladas y los datos confidenciales ATM no constituyan un riesgo inaceptable (según el Capítulo 7 Gestión de riesgos).

# 10. Gestión de activos

### Requisito ATMSP-014-01:

Se desarrollará y mantendrá actualizado un inventario de los activos ATM.

### Requisito ATMSP-015-01:

ATM clasificará sus activos de acuerdo con su criticidad para implementar los medios de protección apropiados.

### Requisito ATMSP-016-01:

Los datos ATM se clasificarán por defecto con un nivel adecuado de clasificación.
*Información adicional: consulte la normativa nacional aplicable*

### Requisito ATMSP-017-01:

Los datos ATM se protegerán durante el almacenamiento, el procesamiento y el intercambio, de acuerdo con su perfil de sensibilidad.

# 11. Control de acceso

### Requisito ATMSP-018-01:

El acceso a cualquier activo ATM debería ser permitido bajo:

- La verificación de la ausencia de riesgo inaceptable (según el Capítulo 7 Gestión de riesgos); y
- Una base de necesidad de conocimiento.

# 12. Seguridad física y del entorno de los componentes CNS/ATM

### Requisito ATMSP-019-01:

La seguridad física de los Sistema de Gestión de Tránsito Aéreo debe asegurarse de integrar las infraestructuras de TI, OT, IACS y CNS/ATM contra las interferencias ilegales y el acceso no autorizado.

### Requisito ATMSP-020-01:

Los responsables de la Seguridad Física del Sistema ATM identificará las zonas que albergan activos CNS/ATM en función de su criticidad en cuanto a seguridad y operatividad.

### Requisito ATMSP-021-01:

Las medidas de seguridad física del Sistema ATM deberá asegurarse de proteger todo el Sistema CNS/ATM de la interrupción ilegal o intencionada de los servicios y operaciones.

### Requisito ATMSP-022-01:

La seguridad física de la Sistema de Gestión Aéreo protegerá los flujos de entrada y salida de las zonas de almacenamiento y los centros de datos.

# 13. Seguridad de las operaciones

### Requisito ATMSP-023-01:

La unidad responsable de ciberseguridad del Sistema de Gestión de Tránsito Aéreo deberá garantizar la coordinación de las operaciones de seguridad, el seguimiento y la mejora continua del procesamiento de la información.

### Requisito ATMSP-024-01:

La unidad responsable de ciberseguridad del Sistema de Gestión de Tránsito Aéreo incluirá la infraestructura de TI, OT, IACS y CNS / ATM en el ámbito de las operaciones de seguridad.

### Requisito ATMSP-025-01:

La unidad responsable de ciberseguridad del Sistema de Gestión de Tránsito Aéreo deberá mantener la eficacia de las medidas de seguridad durante todo su ciclo de vida.

### Requisito ATMSP-026-01:

La unidad responsable de ciberseguridad del Sistema de Gestión de Tránsito Aéreo operará desde zonas dedicadas que tengan un perímetro de seguridad físico y lógico dedicado.

*Información adicional: las zonas deben definirse de acuerdo con los principios de "zonas y conductos" definidos en IEC 62443.*

**Requisito ATMSP-027-01:**

La unidad responsable de ciberseguridad evitará la explotación de vulnerabilidades técnicas en la infraestructura de TI, OT, IACS y CNS / ATM.

**Requisito ATMSP-028-01:**

La unidad responsable de ciberseguridad prohibirá el uso de dispositivos móviles personales para actividades CNS / ATM.

**Requisito ATMSP-029-01:**

La unidad responsable de ciberseguridad garantizará que los dispositivos móviles profesionales no constituyan un riesgo inaceptable para la seguridad (según el Capítulo 7 Gestión de riesgos).

## 14. Seguridad de las comunicaciones

**Requisito ATMSP-030-01:**

La unidad responsable de ciberseguridad mantendrá un mapeo actualizado de las redes y sus interconexiones.

**Requisito ATMSP-031-01:**

La unidad responsable de ciberseguridad deberá estar segregadas lógica o físicamente en función de su criticidad con respecto a la seguridad y la operatividad.

**Requisito ATMSP-032-01:**

La unidad responsable de ciberseguridad garantizará que las tecnologías inalámbricas y el acceso a Internet no constituyan un riesgo inaceptable para la seguridad y la protección (según el Capítulo 7 Gestión de riesgos).

## 15. Adquisición, desarrollo y mantenimiento de sistemas

**Requisito ATMSP-033-01:**

La unidad responsable de ciberseguridad garantizará que la seguridad de la información sea una parte integral de los sistemas de información CNS / ATM durante todo el ciclo de vida.

*Información adicional: Esto también incluye los requisitos para los sistemas de información que brindan servicios ATM a través de redes públicas.*

**Requisito ATMSP-034-01:**

La unidad responsable de ciberseguridad garantizará que los sistemas de información CNS/ATM se diseñen con base en los siguientes principios (lista no exhaustiva):

- Ningún punto de vulnerabilidad único ni común;
- Definición e implementación de reglas de codificación de seguridad;
- Gestión de vulnerabilidades en software y hardware COTS;
- Implementación de estándares y recomendaciones de la industria (NIST, OWASP,…).

## 16. Relaciones con proveedores y socios

**Requisito ATMSP-035-01:**

La unidad responsable de ciberseguridad proporcionará seguridad de extremo a extremo desde la cadena de suministro a los socios en el alcance del sistema de gestión de ciberseguridad CNS/ATM.

**Requisito ATMSP-036-01:**

La unidad responsable de ciberseguridad debe garantizar que las relaciones con entidades externas no constituyan un riesgo inaceptable (según el Capítulo 7 Gestión de riesgos).

## 17. Gestión de incidentes de seguridad

**Requisito ATMSP-037-01:**

La unidad responsable de ciberseguridad garantizará un enfoque coherente y eficaz para la gestión de incidentes de seguridad CNS/ATM, incluida la comunicación sobre eventos y debilidades de seguridad.

**Requisito ATMSP-038-01:**

La seguridad operacional y la continuidad de las operaciones serán las principales prioridades de la gestión de incidentes de seguridad ATM.

## 18. Aspectos de seguridad de la gestión de la continuidad de las operaciones

**Requisito ATMSP-039-01:**

La continuidad de las operaciones ATM se diseñará de acuerdo con los resultados de la gestión de riesgos.

**Requisito ATMSP-040-01:**

La unidad responsable de ciberseguridad deberá establecer una estrategia común, coherente y eficaz para gestionar la seguridad CNS/ATM mediante la integración de todas las partes interesadas con esfuerzos comunes, compartiendo información, para completar sus objetivos operativos.

## 19. Protección de datos personales

**Requisito ATMSP-041-01:**

La unidad responsable de ciberseguridad garantizará la privacidad y protección de la información de identificación personal de acuerdo con las regulaciones aplicables.

# 20. Compliance

### Requisito ATMSP-042-01:

Los sistemas de información CNS/ATM deberán recibir una calificación de validación de seguridad reconocida antes de la entrada en servicio de conformidad con el estándar de proceso ED 205 para los aspectos de seguridad de los sistemas terrestres de gestión del tránsito aéreo/servicios de navegación aérea (ATM/ ANS) de la certificación/declaración.

*Información adicional: el proceso de acreditación reconocido debe definirse a nivel nacional y aplicarse para infraestructuras críticas.*

### Requisito ATMSP-043-01:

La validación de la seguridad de los sistemas de información CNS/ATM se controlará periódicamente.

### Requisito ATMSP-044-01:

La unidad responsable de ciberseguridad debe garantizar que cualquier desviación, detectada a través del proceso de validación, no constituya un riesgo inaceptable (según el Capítulo 7 Gestión de riesgos).

# Referenced Documents

| Reference | Title | Issue | Date |
|---|---|---|---|
| **ISO27001-2013** | Gestión de la información de seguridad | 2013 | |
| **ISO27002-2013** | Tecnología de la información – Técnicas de seguridad | 2013 | |
| **NIST SP 800-53** | Controles de seguridad y privacidad para información federal Sistemas y Organizaciones | R4 | 2015 |
| **IEC-62443** | Seguridad de las redes y sistemas industriales | | |
| **Doc 9985** | Manual de seguridad de la gestión del tránsito aéreo | 1 | 2013 |
| | Estrategia de ciberseguridad de la aviación – OACI | | Oct 2019 |
| **ED-205** | Estándar de proceso para los aspectos de seguridad de la certificación / declaración de los sistemas terrestres de gestión del tránsito aéreo / servicios de navegación aérea (ATM / ANS) | | Mar 2019 |
| | Referencia: Manual para vigilancia de la seguridad nacional ATM (EUROCONTROL) | 2.0 | Oct 2013 |
| | Estrategia para la ciberseguridad en la aviación (Estrategia Europea) | 1.0 | Sep 2019 |
| **CANSO** | Ciberseguridad y riesgo de CANSO | | Jun 2014 |
| **CANSO** | Guía de evaluación | | Sep 2020 |
| | Guía de evaluación de riesgo cibernético de CANSO | | |

# Términos y definición

| Término | Definición |
|---|---|
| **Activo** | Un activo es todo aquello en lo que la organización pone valor. El término activo abarca, pero no se limita a, personal, valores digitales, recursos de tecnología de la información, legado tecnológico, instalaciones, sistemas industriales interconectados y controlados automatizados o tecnología operativa, productos, programas, seguridad de la información evaluaciones y marcas.<br>Los activos se pueden clasificar de la siguiente manera:<br>• Activo tangible: software, hardware, equipos, instalaciones, personas<br>• Activo intangible: procesos e información de negocio |
| **ATM** | Gestión de tránsito aéreo |
| **Seguridad ATM** | Organización, gestión y actividades de ciberseguridad de ATM involucradas en la protección de la infraestructura funcional de ATM contra interferencias electrónicas no autorizadas intencionales |
| **CNS/ATM** | Sistemas de comunicaciones, navegación y vigilancia, que emplean tecnologías digitales, incluidos sistemas satelitales junto con varios niveles de automatización, aplicados en apoyo de un sistema de gestión del tránsito aéreo global sin fisuras |
| **IACS** | Sistemas controlados automatizados e industriales interconectados [basado en: ISA / IEC 62443] |
| **IT** | Tecnología de la información |
| **IUEI** | Una circunstancia o evento con el potencial de afectar una aeronave debido a la acción humana que resulta del acceso, uso, divulgación, denegación, interrupción, modificación o destrucción no autorizados de información y / o interfaces del sistema de la aeronave. Esto incluye las consecuencias del malware y los datos falsificados y los efectos de los sistemas externos en los sistemas de las aeronaves, pero no incluye los ataques físicos o las perturbaciones electromagnéticas. [basado en: ED-202A / DO-326A] |
| **Operatividad** | La operatividad es la capacidad de mantener un equipo, un sistema o una instalación industrial completa en condiciones de funcionamiento seguras y fiables, de acuerdo con los requisitos operativos predefinidos. |
| **OT** | Tecnología operacional |
| **Riesgo** | Combinación de la probabilidad de un evento y su consecuencia. [basado en: ISO27000-2018 y NIST SP 800-53-r4]<br>Una medida de la medida en que una entidad está amenazada por una circunstancia o evento potencial, y típicamente una función de:<br>• los impactos adversos que surgirían si ocurriera la circunstancia o evento; y<br>• la probabilidad de que ocurra.<br>Nota: Los riesgos de seguridad relacionados con el sistema de información son aquellos riesgos que surgen de la pérdida de confidencialidad, integridad o disponibilidad de información o sistemas de información y reflejan los impactos adversos potenciales en las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), organizacionales. activos, individuos, otras organizaciones y la Nación. Los impactos adversos para la nación incluyen, por ejemplo, compromisos a los sistemas de información que respaldan las aplicaciones de infraestructura crítica o que son primordiales para la continuidad de las operaciones del gobierno según lo define el Departamento de Seguridad Nacional. [Basado en NIST SP 800-12 Rev. 1] |
| **Seguridad operacional** | Doc. 9859 de la OACI: Seguridad operacional es el estado en el que la posibilidad de daños a las personas o/a la propiedad se reduce y se mantiene en un nivel aceptable o por debajo de él mediante un proceso continuo de identificación de peligros y gestión de riesgos. |
| **Vulnerabilidad** | Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados o desencadenados por una fuente de amenaza. [CNSS Inst. 4009, adaptado] [Fuente: NIST SP800-53, Rev. 2]<br>Una falla o debilidad en los procedimientos de seguridad del sistema, el diseño, la implementación o los controles internos que podrían ejercerse (activarse accidentalmente o explotarse intencionalmente) y resultar en una brecha de seguridad o una violación de la política de seguridad del sistema. [Fuente: ED-202 / DO-326] |

Visit us:
**canso.org**