Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

OACI

NOTA DE ESTUDIO

NACC/WG/7 — NE/34
30/08/22

Séptima Reunión del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/7)
Oficina Regional NACC de la OACI, Ciudad de México, 29 de agosto al 1 de septiembre 2022

Cuestión 4 del Orden del Día: **Actualización del Programa de Trabajo del NACC/WG hasta 2024**
4.5 Tecnologías emergentes y retos regionales

CIBERSEGURIDAD EN LOS SERVICIOS DE NAVEGACIÓN AÉREA

(Presentada por la Secretaría)

RESUMEN EJECUTIVO	
La presente nota de estudio brinda un resumen acerca de la información disponible sobre ciberseguridad para los servicios de navegación aérea.	
Acción:	Acciones sugeridas se presentan en la Sección 3.
Objetivos Estratégicos:	• Seguridad Operacional
Referencias:	• Webinario sobre la implementación de ciberseguridad de la aviación OACI/CANSO/AIRBUS, diciembre 2020. https://www.icao.int/NACC/Pages/meetings-2020-aci.aspx • Segundo Webinario de la OACI/CANSO/AIRBUS sobre implementación de la ciberseguridad en la aviación - Manual de políticas de ciberseguridad https://www.icao.int/NACC/Pages/meetings-2021-canso02.aspx • Sexta Reunión del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/06), en línea, 25 – 27 de agosto de 2021. https://www.icao.int/NACC/Pages/meetings-2021-naccwg6.aspx.

1. Introducción

1.1 Los servicios de navegación aérea han evolucionado en las ultimas década, implementándose tecnologías altamente digital y automatizada que requiere la implementación de otros mecanismos de seguridad a los que hasta la fecha hemos conocido.

1.2 La tecnología y los sistemas cibernéticos se han convertido en algo esencial para la sociedad moderna, siendo un componente de muchas actividades que han pasado a depender de la tecnología de la información. Junto con el beneficio de las tecnologías cibernéticas, surgen inseguridades que afectan a todos los sistemas e infraestructuras.

1.3 La ciber-amenaza y el ciber-ataque tienen un componente y un efecto transnacional, ya que los sistemas mundiales están interconectados. Además, la complejidad de la acción tiene implicaciones para diversos actores a nivel nacional, regional e internacional.

1.4 Es en este entorno de ciber-inseguridad donde la aviación civil desarrolla su actividad. La aviación civil depende principalmente de la tecnología cibernética que se utiliza para aumentar la seguridad y la eficiencia del transporte aéreo. Sin embargo, la interconectividad de los sistemas y la dependencia de la tecnología han creado las premisas óptimas para que surjan nuevos riesgos.

1.5 El sector de la aviación utiliza una amplia gama de sistemas interconectados basado en la informática, que abarca desde los sistemas de navegación aérea, los sistemas de control y comunicación a bordo de las aeronaves, los sistemas de tierra de los aeropuertos, los sistemas de información de vuelo, los controles de seguridad y muchos otros que se utilizan a diario y para todas las operaciones relacionadas con la aviación. La tendencia del sector de la aviación es a digitalizarse cada vez más. La digitalización conlleva nuevos peligros, ya que las interacciones entre las personas y los sistemas hacen que el riesgo sea más difícil de predecir.

1.6 Reconociendo la urgencia y la importancia de proteger las infraestructuras críticas de la aviación civil, los sistemas de tecnología de la información y la comunicación y los datos contra las ciber-amenazas, la OACI se ha comprometido a desarrollar un marco sólido de ciberseguridad. El 40 Periodo ordinario de sesiones de la Asamblea de la OACI adoptó la Resolución *A40-10 - Abordar la ciberseguridad en la aviación civil*. La resolución aborda la ciberseguridad a través de un enfoque horizontal, transversal y funcional, reafirmando la importancia y la urgencia de proteger los sistemas de infraestructura crítica y los datos de la aviación civil contra las ciber-amenazas, y pide a los Estados que apliquen la Estrategia de Ciberseguridad de la OACI.

1.7 Estrategia de ciberseguridad de la aviación engloba descansa sobre siete pilares:

1. Cooperación internacional
2. Gobernanza
3. Leyes y reglamentos eficaces
4. Política de ciberseguridad
5. Intercambio de información
6. Gestión de incidentes y planificación ante emergencias
7. Creación de capacidad, instrucción y cultura de ciberseguridad

1.8 El documento completo está disponible en el siguiente enlace:

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf

1.9 Desde 2020, la Oficina Regional NACC de la OACI desde realizó una alianza con CANSO y AIRBUS y se concentró en el desarrollo de documentación guía que permita a los Estados evaluar los sistemas de navegación aérea y en base a ello desarrollar su propia política de ciberseguridad personalizada a sus operaciones. El documento es un manual llamado: *Plantilla de Política de Ciberseguridad para la Gestión de Tránsito Aéreo*

1.10 El manual esta realizado siguiendo las recomendaciones de la resolución *A40-10 - Abordar la ciberseguridad en la aviación civil*, y bajo la estrategia de Ciberseguridad de la OACI, basado en el pilar número 4 “Política de ciberseguridad”.

1.11 Se solicita al Grupo de Trabajo NACC/WG la adopción del documento para que sea utilizado por la región CAR.

2. Plantilla de Política de Ciberseguridad para la Gestión del Tránsito Aéreo.

2.1 Los objetivos de este documento son:

1. Contribuir a la resiliencia del sistema de aviación del Estado.
2. Proporcionar apoyo a la integridad, disponibilidad y confidencialidad de la información.
3. Proteger el hardware/software que soporta la infraestructura del sistema de aviación para reducir los riesgos para todos los servicios del Estado.
4. Apoyar la implementación de procedimientos y procesos de ciberseguridad a toda la infraestructura y servicios.
5. Apoyar la ciberseguridad y la resistencia de la aviación civil.

2.2 El documento enumera una serie de requisitos que los Estados deben evaluar acerca de su arquitectura y sus operaciones. Identifica la infraestructura y sistemas que son el núcleo de sus operaciones e implementa mecanismos que aseguren su protección y lo más importante la continuidad de sus operaciones.

2.3 El documento se encuentra en el **Apéndice** a esta nota de estudio. Esta segunda versión incorpora los comentarios de las Oficinas de Navegación Aérea y Transporte Aéreo de la OACI.

2.4 También se ha integrado a esta nueva versión una lista de verificación que sirve de guía al Estado para evaluar los requisitos que cumple o no de acuerdo con sus operaciones.

2.5 La Oficina Regional NACC de la OACI ha realizado una serie de eventos dirigidos al entendimiento de lo que significa ciberseguridad, y a identificar amenazas a las operaciones de aviación, pero es necesario que los Estados tomen de forma muy seria las actividades que deben ser realizadas en cuanto a esta área.

2.6 La ciberseguridad requiere un compromiso de los Estados para asignar recursos en todas las áreas, desde humanos y financieros. Sin embargo, es necesario que los Estados previo a desarrollo de proyectos dirigidos a esta área realicen un análisis de sus operaciones y la *Plantilla de Política de Ciberseguridad para la Gestión de Tránsito Aéreo* apoya esta actividad.

2.7 Los proyectos dirigidos a esta área requieren una inversión que debe ser respaldada en datos que apoyen la toma de decisiones y la evaluación de sus operaciones. La plantilla apoyará al Estado a definir las actividades que necesite desarrollar.

2.8 La Oficina Regional NACC de la OACI agradece a CANSO y AIRBUS por este trabajo en forma conjunta. Es importante enfatizar que los trabajos en conjunto entre las organizaciones permiten tomar ventaja de los expertos, experiencia y trabajar de forma más efectiva en las tareas de interés común y para beneficio de los Estados.

3 Acciones sugeridas

3.1 Se invita a la reunión a:

a) aprobar la adopción del documento como una Guía Regional para los Estados;

b) designar personal Punto de contacto (PoC) por parte de los Estados para trabajar directamente con ellos;

c) trabajar con la Oficina Regional de la OACI en las actividades programadas para tratar los temas de ciberseguridad dirigidos a los servicios de navegación aérea; y

d) otra acción que aplique.

— — — — — — — — — — —

In cooperation with

canso ICAO AIRBUS

Plantilla de Política de Ciberseguridad para la Gestión de Tránsito Aéreo

DESCARGO DE RESPONSABILIDAD

La información contenida en esta publicación está sujeta a revisión continua a la luz de los cambios en las normas y reglamentos de la OACI y otra información importante proporcionada por la OACI, CANSO y Airbus.

Esta publicación tiene como objetivo ayudar a los Estados Centroafricanos y de América Latina en la evaluación e iniciar su trabajo sobre ciberseguridad.

América Latina y la Región CAR han implementado tecnología de punta para apoyar la evolución de sus operaciones de navegación aérea, en ese sentido es muy importante apoyar esta evolución incorporando información para apoyar a los Estados en la implementación de seguridad cibernética.

Los ciberataques no se detienen, cada año aumenta el porcentaje de incidentes, incluido el sector de la aviación.

Esta publicación no sustituye a ninguna otra normativa nacional o autonómica.

Esta publicación renuncia expresamente a cualquier y toda responsabilidad hacia cualquier persona o entidad, ya sea un usuario de esta publicación o no, con respecto a cualquier cosa hecha u omitida, y las consecuencias de cualquier cosa hecha u omitida, por dicha persona o entidad en confianza en el contenido de esta publicación.

La mención de empresas y productos específicos en esta publicación no implica que sean respaldados o recomendados por ninguno de los anteriores con preferencia a otros de naturaleza similar, que no se mencionan.

Ninguna parte de esta publicación puede ser reproducida, reformulada, reformateada o transmitida de ninguna forma por ningún medio, electrónico o mecánico, incluyendo fotocopias, grabaciones o cualquier sistema de almacenamiento y recuperación de información, sin el permiso previo por escrito de los autores.

Reconocimientos

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

Se reconoce a las siguientes personas por sus valiosas contribuciones:

- **Shayne Campbell**, Gerente del programa de seguridad operacional, CANSO
- **Eduardo Garcia**, Gerente de Coordinación y seguridad operacional de ATM europeo, CANSO
- **Mayda Ávila**, Especialista Regional, Comunicaciones, Navegación y Vigilancia, Oficina Regional NACC de la OACI
- **Julien Touzeau**, Director de seguridad del producto para las Américas, Seguridad operacional, Seguridad de la aviación y asuntos técnicos – AAG, Airbus
- **Yann Berger**, Experto en seguridad del producto, APSYS – Seguridad del producto, Airbus
- **Gaelle Hubert**, Especialista en gobernanza y auditor en seguridad de la aviación, Airbus
- **Pouline Estelle**, Especialista en seguridad física y en Seguridad de la aviación y auditora ACC3, Airbus

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 A40-10: “Abordando la ciberseguridad en la aviación civil” durante la Asamblea A40 - 40° período de sesiones en Montreal, del 24 de septiembre al 4 de octubre de 2019.

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 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 Método o práctica recomendada de la OACI (SARPs), ningún procedimiento para los servicios de navegación aérea (PANS), ni alguna regulación nacional. Este documento apoya a los documentos citados.

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 apoyar la confidencialidad, integridad y disponibilidad de la información, así como la resiliencia de las operaciones.
- Realizar y mantener 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 tránsito 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:

- Contribuir a la resiliencia del Sistema de aviación de los Estados
- Proporcionar apoyo para 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 y otros documentos disponibles en las regulaciones nacionales, y organizaciones dentro de los Estados.

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 responsabilidad 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
- 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.

Nota: Este requisito dependerá de las regulaciones y acuerdos nacionales.

Requisito ATMSP-010-01:

El responsable de seguridad ATM designado 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 ciberseguridad 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.

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 organización del departamento de ciberseguridad de los ANSP deberá garantizar la coordinación de las operaciones de ciberseguridad, 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 ciberseguridad.

Requisito ATMSP-025-01:

La unidad responsable de ciberseguridad del Sistema de Gestión de Tránsito Aéreo deberá mantener la eficacia de las medidas de ciberseguridad 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 ciberseguridad de los ANSP CD-ATM debería proteger contra la explotación de vulnerabilidades técnicas en la infraestructura de TI, OT, IACS y CNS / ATM.

Requisito ATMSP-028-01:

La ciberseguridad ATM debería prohibir el uso de dispositivos móviles personales para actividades regulares CNS / ATM.

Requisito ATMSP-029-01:

La ciberseguridad ATM debería garantizar 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 ciberseguridad ATM debería garantizar que la seguridad de la información sea una parte integral de los sistemas 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 CNS/ATM se diseñen con base en los siguientes principios (lista no exhaustiva):

- Ningún punto de falla única 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 ciberseguridad ATM debería garantizar 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 ciberseguridad ATM 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 ciberseguridad ATMgarantizará la privacidad y protección de la información de identificación personal de acuerdo con las regulaciones aplicables.

20. Cumplimiento

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 debería ser periódica.

Requisito ATMSP-044-01:

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

21. Lista de verificación

El **Anexo** a este documento incorpora la lista de verificación a ser utilizada para evaluación de su sistema de aviación en cuanto a la implementación de Ciberseguridad.

Documentos de referencia

Referencia	Título	Volumen	Fecha
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	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	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. Los activos se pueden clasificar de la siguiente manera: • Activo tangible: software, hardware, equipos, instalaciones, personas
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 /
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] Una medida de la medida en que una entidad está amenazada por una circunstancia o evento potencial, y típicamente una función de: • los impactos adversos que surgirían si ocurriera la circunstancia o evento; y • la probabilidad de que ocurra. 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 800-13 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] 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]

In cooperation with

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

ANEXO

Introducción

El presente documento es una lista de verificación que tiene como objetivo una autoevaluación de todos los requisitos explicados en la Plantilla de la política de gestión de la ciberseguridad.

El documento no es un requisito obligatorio para la implementación, pero contiene información relevante que apoya el desarrolla de su propio Manuel de política de ciberseguridad.

Enfoque

Este documento cubre toda la estructura funcional para los Proveedores de Servicios de Navegación Aérea y toda parte involucrada y toda entidad u organización que es parte de un sistema estatal de aviación, para asegurar la implementación de procedimientos y prácticas de ciberseguridad en todos los servicios bajo la vigilancia del Estados, como son:

- ✓ Unidades de servicios 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 de apoyo a la información para la toma de decisiones.
- ✓ Sistemas para interoperabilidad de la aviación
- ✓ Otras de acuerdo con los servicios y operaciones del Estado

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

- ✓ Información requerida por los servicios ATM.
- ✓ Infraestructura de tecnologías de la información (TI) en la que confían los servicios ATM.
- ✓ Tecnología operacional (TO) y sistemas industriales interconectados y sistemas controlados automatizados (IACS).
- ✓ Servicios extendidos y asociación e interconexiones de sistemas de información relacionados.
- ✓ Todo el personal de la aviación y organizaciones externas que tengan acceso a la información de navegación aérea, servicios e instalaciones.

In cooperation with

ICAO canso AIRBUS

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

Estado:	
Punto de Contacto (s): Por favor integre nombre, posición en la Organización, correo electrónico y número telefónico.	

Lista de verificación

1. Documentación de seguridad ATM

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 6

		Sí	% en progreso	No
1.1	¿Ha establecido una política de seguridad de información para su organización?			
1.2	¿Ha establecido ISMS para su organización?			
1.3	Su documentación ATM está: • Implementada • Con mantenimiento • Basada con un enfoque de gestión del riesgo			
	¿Ha identificado y delimitado su infraestructura (como "TI", "TO" y "IACS") para que su seguridad pueda ser gestionada apropiada y proporcionalmente?			

Infraestructura TI	Infraestructura TO y IACS

Anexe otras hojas si es necesario, para listar toda la infraestructura TI, TO y IACS

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

2. Gestión del riesgo

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 7

		Sí	% en progreso	No
2.1	¿Se aborda la seguridad en todas las fases del ciclo de vida del sistema?			
2.2	¿Tiene implementado un procedimiento (metodología) de gestión del riesgo definido y repetible?			
2.3	Los riesgos de seguridad son: • Rastreados • Monitoreados • Periódicos y revisados			
2.4	¿Ha tomado pasos para procesar la gestión de vulnerabilidades en los sistemas?			
2.5	¿Ha identificado todos los activos ATM (datos, sistemas, personal) y establecido procedimientos de control para éstos?			
2.6	¿Ha empoderado al personal adecuado para tomar decisiones de tratamiento sobre riesgos de seguridad?			
2.7	¿Tiene procesos definidos sobre gestión de la información de seguridad? (abordando todas las actividades de seguridad)			
2.8	¿Ha establecido medidas técnicas y operacionales de seguridad ¿políticas y procedimientos? La intensión de esto es reducir el riesgo a un nivel aceptable a pesar del error humano, accidente o incidente, impacto de un desastre natural y otros.			
		Sí	% en progreso	No

2.9	¿Ha identificado interfaces (enlaces) para asegurar tratamiento del riesgo de seguridad sobre la seguridad ATM eficientes y coordinadas? Do you have identified interfaces to ensure efficient and coordinated treatment of security risk about ATM security?			
2.10	¿Ha establecido un proceso de gestión del riesgo cubriendo riesgos de seguridad de la información ATM con una revisión y monitoreo regular?			
3. Gobernanza de la seguridad y organización -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 8				
		Sí	**% en progreso**	**No**
3.1	¿Ha establecido una autoridad apropiada para la gestión de la seguridad ATM a nivel de Unidad?			
3.2	¿Ha establecido roles y responsabilidades dentro de la gestión del riesgo de seguridad ATM?			
3.3	¿Ha implementado procesos definidos para inteligencia y monitoreo de la amenaza?			
3.4	¿Ha implementado procesos definidos para la gestión de incidentes y crisis?			
4. Recursos humanos (Medidas de seguridad durante todas las fases de empleo) -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 9				
		Sí	**% en progreso**	**No**
4.1	Antes del empleo: ¿utiliza medidas tales como revisión de antecedentes de acuerdo con las regulaciones locales?			

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

4.2	Durante el empleo: ¿desarrolla una cultura de la seguridad a través de capacitación regulas y levantando conciencia?			
		Sí	**% en progreso**	**No**
4.3	¿Después de la contratación: ¿se protege asegurando el proceso de desprovisión de acceso y recordando al personal los compromisos de no divulgación (cuando lo permite la ley)?			
4.4	¿Tiene procedimientos para asignar y limitar el acceso del personal de acuerdo con sus responsabilidades?			
5. Gestión de activos -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 10				
		Sí	**% en progreso**	**No**
5.1	¿Tiene un inventario de activos ATM y los mantiene actualizados?			
5.2	¿El inventario incluye evaluación de la criticidad (sobre seguridad operacional y operatividad) de cada activo?			
5.3	¿Ha considerado acceso lógico y físico y se ha asegurado de que hay consistencia entre ellos?			
5.4	¿Se han considerado y clasificado todos los datos ATM y han sido protegidos a un nivel adecuado?			
5.5	¿Tiene procedimientos que asegurar que todos los datos ATM serán protegidos durante su almacenaje,			

	procesamiento e intercambio, en línea con perfil de sensibilidad?			
6. Control de acceso -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 11				
		Sí	**% en progreso**	**No**
6.1	¿El acceso a todos los activos ATM es a través de un proceso de verificación adecuado para evitar riesgos inaceptables?			
6.2	¿Tiene control para cubrir los accesos de los sistemas físicos y lógicos?			
7. Seguridad física y del entorno de los componentes CNS/ATM -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 12				
		Sí	**% en progreso**	**No**
7.1	¿Se ha asegurado que la seguridad física ATM salvaguarda TI, TO, IACS y la infraestructura CNS/ATM contra interferencia ilícita y acceso no autorizado?			
7.2	¿Se ha asegurado que la seguridad física ATM identifica zonas que alberguen activos CNS/ATM de acuerdo con su criticidad (desde la perspectiva de seguridad operacional y operatividad)?			
7.3	¿Ha implementado medidas de seguridad física ATM para proteger todos los servicios y operaciones CNS/ATM de interferencia intencional o ilícita?			

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

7.4	¿Ha implementado seguridad física ATM para proteger flujos de información entrante y saliente entre zonas de almacenaje y centros de datos?			
8. Seguridad de las operaciones -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 13				
		Sí	**% en progreso**	**No**
8.1	¿Ha establecido zonas confiables?			
8.2	¿Ha establecido procedimientos para asegurar la coordinación sobre ciberseguridad ATM de las operaciones de seguridad, monitoreo y mejora continua del procesamiento de información?			
8.3	¿Se ha asegurado que las Operaciones de ciberseguridad ATM incluyan TI, TO, IACS e infraestructura CNS/ATM en el enfoque de seguridad de las operaciones?			
8.4	¿Ha implementado Operaciones de ciberseguridad ATM para mantener la efectividad de las medidas de seguridad a través de su ciclo de vida?			
8.5	¿Ha establecido un perímetro de seguridad a través de zonas de ciberseguridad ATM para zonas físicas y lógicas?			
8.6	¿Tiene procedimientos para prevenir la explotación de vulnerabilidades técnicas sobre TI, TO, IACS e infraestructura CNS/ATM			
8.7	¿Tiene controles de seguridad sobre el uso de aparatos móviles del personal para actividades CNS/ATM (por ejemplo, su utilización es prohibida?			

8.8	¿Ha tomado pasos para asegurar que los aparatos móviles del personal no representen un riesgo a la seguridad de las actividades CNS/ATM actividades (por ejemplo, conectar un dispositivo personal al equipo operativo para cargarlo)?			
9. Comunicaciones de seguridad -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 14				
		Sí	**% en progreso**	**No**
9.1	¿Ha reunido y mantenido un mapeo actualizado de sus redes e interconexiones?			
9.2	¿Se asegura de que las redes ATM están segregadas lógica y físicamente basadas en su criticidad en cuanto a la seguridad operacional y operatividad?			
9.3	¿Ha tomado pasos para asegurar que las tecnologías inalámbricas y acceso a Internet no constituyen un riesgo inaceptable a la seguridad operacional y la seguridad de la aviación?			
10. Adquisición, desarrollo y mantenimiento de sistemas -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 15				
		Sí	**% en progreso**	**No**
10.1	¿La seguridad de la información es una parte integral de su gestión de sistemas de información CNS/ATM durante el ciclo de vida completo?			
10.2	¿Se asegura que los sistemas de información están diseñadas con base en los siguientes principios? • Ningún punto de vulnerabilidad único ni común • Uso de reglas de codificación de seguridad definidas y verificadas			

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

	• Gestión de la vulnerabilidad en software y hardware COTS • El uso de estándares y recomendaciones industriales apropiados (por ejemplo, NIST, OWASP, EUROCAE/RTCA, etc.)?			
11. Relaciones con proveedores y socios -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 16				
		Sí	**% en progreso**	**No**
11.1	¿Ha evaluado la madurez de la seguridad de los proveedores y socios antes de contratarlos?			
11.2	¿Su proceso de gestión del riesgo también abarca el riesgo de proveedores?			
12. Gestión de incidentes de seguridad -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 17				
		Sí	**% en progreso**	**No**
12.1	¿Tiene un procedimiento y listas de comunicación en caso de un incidente de seguridad o identificación de debilidades?			
13. Aspectos de seguridad de la Gestión de la continuidad del negocio -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 18				
		Sí	**% en progreso**	**No**
13.1	¿Ha identificado interfaces entre la continuidad de negocio AMT y los procesos de gestión de riesgo? Do you have defined interfaces between ATM Business continuity and Risk Management processes?			

13.2	¿Realiza ejercicios de gestión de crisis y pruebas basadas en casos de seguridad ATM?			
14. Protección de datos personales -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 19				
		Sí	**% en progreso**	**No**
14.1	¿Ha definido una interface entre DPO y el proceso de seguridad ATM? Do you have defined interface between DPO and ATM security process.			
15. Cumplimiento -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 20				
		Sí	**% en progreso**	**No**
15.1	¿Realiza auditorias se seguridad de terceras partes de sistemas de información ATM/CNS?			
15.3	¿Los resultados de seguridad disparan actualizaciones de la evaluación del riesgo?			

- FIN -