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

OACI

NOTA DE ESTUDIO

AIM/TF/7 — NE/02
23/07/24

Séptima Reunión del Grupo de Tarea para la Implementación de la Gestión de la Información Aeronáutica del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/AIM/TF/7)

(Willemstad, Curazao, 30 de julio – 2 de agosto de 2024)

Cuestión 2 del Orden del Día: **Datos AIM y ciberseguridad**

CONCEPTOS Y APLICACIONES DE CIBERSEGURIDAD EN AIM

(Presentada por la Secretaría)

RESUMEN EJECUTIVO

El propósito de esta Nota de Estudio es presentar el concepto de la OACI y el papel de la ciberseguridad en el sector de la aviación, identificar deficiencias en su provisión y regulación de datos e información aplicables a AIM, y formular propuestas destinadas a mejorar los estándares y garantizar el nivel adecuado de ciberseguridad de la aviación.

Acción:	La acción sugerida se presenta en la Sección 5.
Objetivos Estratégicos:	• Objetivo estratégico 1 – Seguridad Operacional • Objetivo estratégico 2 – Capacidad y eficiencia de la navegación aérea
Referencias:	• Resolución A41-19 sobre Abordaje de la Ciberseguridad en la Aviación Civil • “Estrategia de ciberseguridad de la aviación” de la OACI • “Orientación sobre políticas de ciberseguridad” de la OACI • Convenio para la supresión de actos ilícitos relacionados con la aviación civil internacional (Convenio de Beijing) • Protocolo Suplementario del Convenio para la supresión del apoderamiento ilícito de aeronaves (Protocolo de Beijing)

1. Introducción

1.1 La ciberseguridad en el sector aeronáutico ha adquirido relevancia en el creciente nivel de desarrollo de las tecnologías de la información en el sector aeronáutico, y en particular en el AIM para la gestión e intercambio de datos, por lo que es necesario un análisis detallado de los estándares y normas internacionales existentes para garantizar la ciberseguridad de la aviación y su implementación con diversas iniciativas y tecnologías en esta materia, comenzando por el estudio de los Documentos con las estrategias y planes de la OACI, para enfrentar la problemática de los ciberdelitos en esta área de la aviación que representan riesgos significativos para la seguridad de la aviación.

1.2 El concepto de ciberseguridad y sus implicaciones para el sector de la aviación y la digitalización en la industria del transporte aéreo ha permitido a las entidades relevantes brindar mejores servicios a sus clientes. Al mismo tiempo, también aumentó el nivel de exposición a amenazas, especialmente ciberataques. Con base en lo anterior, cabe señalar que los conceptos y categorías clave se consideran en el proceso de análisis y presentación del material. Para empezar, es importante determinar cómo se entiende el término seguridad de la información, ya que este concepto puede entenderse desde varios puntos de vista.

2. Discusión

2.1 El objeto del estudio son las relaciones que surgen en materia de seguridad de la aviación y ciberseguridad en el sector de la aviación.

2.2 En cuanto a la legislación interna de los Estados, la seguridad de la información es una alta prioridad de protección de los intereses vitales tanto de una persona como de la sociedad y del propio Estado. En tal situación, se evita de todas las formas posibles el daño causado por el suministro de datos e información incompletos, inexactos y fuera de plazo. Además de proporcionar la información "negativa" especificada a las acciones maliciosas correspondientes, este acto regulatorio también incluye el impacto negativo de la información y las consecuencias correspondientes del uso de tecnologías de la información, distribución no autorizada, uso y violación de la confidencialidad, accesibilidad, integridad de información.

2.3 Así, cabe señalar que no todas las cuestiones de seguridad de la información están relacionadas con la noción de "ciberseguridad". Al fin y al cabo, existen sistemas de la aviación, aislados de las redes, e incluidos en el circuito tecnológico del control del tránsito aéreo.

2.4 Es por eso, que, garantizar la seguridad de los datos en ellos debe armonizarse exitosamente con los fundamentos de seguridad de los datos/información de un sistema de nivel superior. El ciberespacio constantemente mencionado se puede definir como un área global en el entorno de datos/información, que incluye sistemas de información, redes interdependientes de sistemas de infraestructura de información, redes de telecomunicaciones y sistemas informáticos, y similares.

3. Soluciones a problemas de ciberseguridad en el sector aeronáutico

3.1 El problema de la ciberseguridad de la aviación obligó a las autoridades aeronáuticas de muchos Estados, así como a organismos internacionales como la OACI, a hacer todos los esfuerzos posibles para crear las condiciones adecuadas para garantizar la seguridad en esta Área de riesgo.

3.2 Durante la **41ª Asamblea de la OACI**, celebrada en la Sede (Montreal), se adoptó la **Resolución A41-19** sobre **Abordaje de la Ciberseguridad en la Aviación Civil** (**Apéndice A,** solamente en inglés), que declaró la necesidad de abordar conjuntamente este problema bajo el Convenio de Beijing, para instar a todos los Estados a implementar la “Estrategia de ciberseguridad de la aviación” de la OACI, octubre de 2019 (**Apéndice B**). El objetivo principal de la Resolución es organizar la cooperación no solo entre los Estados sino también entre las organizaciones internacionales y la industria para desarrollar políticas (ver la “Orientación sobre políticas de ciberseguridad” de la OACI, enero de 2022 – **Apéndice C**) para garantizar un enfoque holístico de la ciberseguridad de la aviación.

3.3 Además, y considerando que el Convenio para la supresión de actos ilícitos relacionados con la aviación civil internacional (Convenio de Beijing) y el Protocolo Suplementario del Convenio para la supresión del apoderamiento ilícito de aeronaves (Protocolo de Beijing) mejorarían el marco jurídico global para abordar los ataques cibernéticos a la aviación civil internacional como delitos y, por lo tanto, una amplia ratificación de esos

instrumentos por parte de los Estados garantizaría que tales ataques serían disuadidos y castigados en cualquier parte del mundo en que ocurran.

3.4 Además, en el Programa TRAINAIR PLUS de la OACI se propuso un curso de “Fundamentos de Ciberseguridad para la Aviación”. El curso tiene como objetivo capacitar a los profesionales de la aviación en la identificación de amenazas cibernéticas existentes y potenciales para que estos participantes puedan responder de manera más efectiva y rápida a dichos problemas. De este modo, la formación especificada contribuirá a garantizar la seguridad de los viajes aéreos para los pasajeros de todo el mundo. Los primeros destinatarios de los nuevos conocimientos serán los representantes de los organismos reguladores de la aviación civil, las aerolíneas civiles y los aeropuertos.

3.5 Para lograrlo, se aplicarán un grupo de principios y métodos de un mecanismo especial, que incluye siete componentes clave, a saber:

a)	cooperación entre Estados y organizaciones
b)	el intercambio de datos importantes entre estas entidades
c)	el desarrollo de una legislación eficaz
d)	la introducción de una política cibernética transparente
e)	planificación conjunta de acciones reaccionarias en caso de incidentes y emergencias
f)	la formación de una cultura de ciberseguridad
g)	en paralelo con la formación de profesionales en esta área

4. Conclusiones

4.1 Hoy en día, la ciberseguridad es una de las cuestiones clave en la industria de la aviación. Las aerolíneas y otras organizaciones internacionales que operan en esta área están interactuando activamente e implementando diversos métodos y tecnologías para garantizar un nivel suficiente de seguridad, tanto física como virtual (digital). Para la mayoría de los Estados del mundo, el sector del transporte aéreo forma parte de la infraestructura crítica de los Estados. Por lo tanto, muchas autoridades de aviación civil también están preocupadas por la implementación de nuevas normas y regulaciones para abordar los riesgos en el ciberespacio.

4.2 Pero al mismo tiempo, la industria y las organizaciones (OACI, IFAIMA, ACI, IATA, CANSO y otras) desarrollan iniciativas relevantes para enfrentar las ciber amenazas en el campo de la navegación y el transporte aéreo que son reales y generalmente reconocidas, tanto por las organizaciones individuales como por todos los Estados cooperan activamente con el objetivo de educación, información y protección mutuas en el área considerada.

4.3 La comunidad de la aviación mundial se enfrenta a la necesidad de desarrollar un sistema de medidas coordinadas y un procedimiento especial de toma de decisiones para garantizar la protección del sistema mundial de la industria de la aviación contra los ciberataques. Es importante no sólo implementar tales acciones, sino también aprender a combinarlas exitosamente con acciones periódicas para proteger los componentes del ciberespacio aeronáutico de influencias externas.

4.4 Finalmente, en opinión de la Secretaría, está la aplicación de las prácticas recomendadas por la OACI, así como la armonización del marco regulatorio nacional con los principios y estándares internacionales en materia de ciberseguridad. La resolución de los problemas de ciberseguridad en el sector de la aviación civil requiere un esfuerzo concertado de todos los actores de la industria aeroespacial (ver **Apéndice D**). Podemos decir con seguridad que el sector de la aviación de alta calidad depende cada vez más de la disponibilidad,

integridad y confidencialidad de la información, los datos y los sistemas. La protección contra ataques cibernéticos en la aviación debería convertirse en una prioridad estratégica tanto para la comunidad mundial de la aviación como para las autoridades nacionales de seguridad y seguridad para cada Estado individual.

5. Acciones sugeridas

5.1 Se invita a la Reunión a:

a) tomar nota de la información presentada en esta Nota de Estudio y en sus **Apéndices A, B, C y D**

b) proporcionar comentarios sobre el estado actual de las acciones de ciberseguridad de acuerdo con la **Resolución A41-19 de la OACI** sobre **Abordar la ciberseguridad en la aviación civil** como se solicita en el **Apéndice A**; y

c) sugerir acciones adicionales si corresponde.

— — — — — — — — — — —

APÉNDICE A
(únicamente en inglés)

Resolution A41-19: Addressing Cybersecurity in Civil Aviation

Whereas the global aviation system is a highly complex and integrated system that comprises systems that are critical for the safety and security of civil aviation operations;

Noting that the aviation sector is increasingly reliant on the availability, integrity and confidentiality of information, data, and systems;

Mindful that cyber threats to civil aviation are rapidly and continuously evolving, that aviation continues to be a target for perpetrators in the cyber domain as in the physical one, and that cyber threats can evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity events affecting the safety of civil aviation are unlawful and/or intentional;

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions and noting that cyber risks can simultaneously affect a wide range of aviation areas and spread rapidly;

Reaffirming the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation;

Considering that the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) would enhance the global legal framework for dealing with cyber-attacks on international civil aviation as crimes and therefore wide ratification by States of those instruments would ensure that such attacks would be deterred and punished wherever in the world they occur;

Reaffirming the importance and urgency of addressing the cybersecurity and cyber resilience of civil aviation's critical systems, data, and information against cyber threats and hazards, including common interfaces between civil and military aviation;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework to address aviation cybersecurity and to support the cybersecurity and cyber resilience of the global aviation system to cyber threats that may jeopardize the safety and/or security of civil aviation;

Recognizing ICAO's leadership and work in the fields of aviation cybersecurity and cyber resilience across the different aviation disciplines;

Recognizing that aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to ensure the consistency and full interoperability of protection measures and risk management systems;

Recognizing the importance of developing clear national governance and accountability for civil aviation cybersecurity, including the designation of a competent national authority responsible for aviation cybersecurity in coordination with concerned national authorities and agencies; and

Acknowledging the value of relevant initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and holistic manner.

The Assembly:

1. *Urges* Member States to adopt and ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) as a means for dealing with cyberattacks against civil aviation;

2. *Calls upon* States and industry stakeholders to take the following actions to address cyber threats to civil aviation:

a) implement the ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan as a tool to support the implementation of the Aviation Cybersecurity Strategy;

b) designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies;

c) define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;

d) develop and implement a robust cybersecurity risk management framework that draws on relevant safety and security risk management practices, and adopt a risk-based approach to protecting critical civil aviation systems, information, and data from cyber threats;

e) establish policies and instruments, and allocate resources to ensure that, for critical aviation systems: system architectures are secure by design; systems are protected and resilient; data is secured and available in storage and while in transfer; system monitoring, and incident detection and reporting, methods are implemented; incident recovery plans are developed and practiced; and forensic analysis of cyber incidents is carried out;

f) encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;

g) encourage civil/military cooperation with regard to identifying, protecting, and monitoring common vulnerabilities and data flows at interfaces between civil and military aviation systems, and collaborate in response to common cyber threats and recovery from cyber incidents;

h) develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

i) design and implement a robust cybersecurity culture across the civil aviation sector;

j) encourage States to continue contributing to ICAO in the development of international Standards, strategies, and best practices to support advancing aviation cybersecurity and cyber resilience; and

k) continue collaborating in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving aviation safety, aviation security,

facilitation, air navigation, communication, surveillance, air traffic management, aircraft operations, airworthiness, and other relevant disciplines.

3. *Instructs* ICAO to:

a) continue to promote the universal adoption and ratification of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol); and

b) continue to ensure that cybersecurity and cyber resilience matters are considered and coordinated in a cross-cutting manner through the new mechanism in ICAO to address aviation cybersecurity.

Orientación sobre la política de ciberseguridad

Publicado bajo la responsabilidad del Secretario General

Enero de 2022

Organización de Aviación Civil Internacional International

S22-2979

1. Introducción

Esta orientación es cónsona con la Estrategia de Ciberseguridad de la Aviación de la OACI[1] y el Plan de Acción de Ciberseguridad[2], en una de cuyas acciones (CyAP 0.1) se recomienda que la Organización de Aviación Civil (OACI) elabore un modelo de política de ciberseguridad que sirva de referencia a los Estados miembros y la industria a la hora de formular sus propias políticas nacionales/ internas.

El apéndice A de la presente orientación contiene dicho modelo de política de seguridad.

2. Alcance

En el modelo de política de ciberseguridad que figura en el apéndice A se aborda la protección y la resiliencia de la infraestructura crítica de la aviación civil internacional contra las ciberamenazas y el requisito de la colaboración multilateral tanto dentro del sector de la aviación civil como con autoridades externas del sector militar, de la ciberseguridad y la seguridad nacional.

3. Objetivos

El propósito de este modelo de política de ciberseguridad es servir de guía para ayudar a los Estados y la industria a concentrar sus recursos y acciones en la aplicación de un enfoque sistémico ante la ciberseguridad en la aviación civil, que incluya tanto los sistemas actuales como los sistemas anteriores. El objetivo último es que los Estados y las partes interesadas puedan crear un "sistema de sistemas" que permita proteger a la aviación civil de las ciberamenazas, responder a los ciberincidentes, recuperarse de ellos de una manera oportuna y, en consecuencia, hacer frente a las nuevas amenazas sin que se produzcan disrupciones mayores.

A continuación se señalan los principales resultados que se prevé alcanzar con la aplicación de una política de ciberseguridad.

3.1 Velar por la protección de la aviación civil contra las ciberamenazas

La protección de la aviación civil frente a las ciberamenazas se lleva a cabo mediante la aplicación de las normas y métodos recomendados, procedimientos y textos de orientación de la OACI sobre ciberseguridad. Dicha protección contempla la ejecución de prácticas sólidas de gestión de riesgos, la identificación de infraestructuras críticas y la implantación de un enfoque holístico a múltiples niveles para la ciberseguridad. Este enfoque debería servir para cuidar de que un ataque exitoso contra un determinado nivel no afecte otros niveles del sistema y/o conduzca a la pérdida de la seguridad operacional, la seguridad de la aviación o la continuidad de funciones críticas. El sistema también debería adoptar un enfoque de mejoramiento continuo para asegurar la coordinación, implantación y actualización de las mejoras necesarias a las evoluciones técnicas y de procedimientos previstas.

3.2 Velar por la ciberresiliencia de la aviación civil

Un sistema de aviación civil ciberresiliente es un sistema que, aun bajo ataque, puede mantener sus funciones críticas, es decir, que sostiene la continuación de unas operaciones de vuelo seguras y sin disrupción alguna, o con disrupciones mínimas. El sistema debería incluir además mecanismos apropiados

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.
[2] Comunicación de la OACI núm. 2020/114.

de cooperación e intercambio de información entre las partes interesadas de la aviación, como gobiernos, la industria y, de proceder, las autoridades civiles de observancia de la ley y las autoridades militares.

3.3 **Velar por el autofortalecimiento de la aviación civil mediante la adopción de un enfoque de "seguridad por diseño"**

La adopción de un enfoque de seguridad por diseño requiere, desde la etapa de concepción de un sistema, considerar los objetivos de seguridad que deben lograrse durante el proceso de diseño del sistema, junto con los objetivos operacionales y de seguridad operacional tradicionales. Garantizar la seguridad de los elementos y procesos críticos "por diseño" cambia el paradigma de seguridad de reactivo a proactivo y fomenta la creación de un sistema de aviación civil autoprotegido que, en consecuencia, le permite evolucionar y brinda una mayor seguridad y resiliencia.

3.4 **Velar por la coordinación de la ciberseguridad de la aviación tanto dentro de la aviación civil como con partes interesadas ajenas a dicho sector**

Con la finalidad de garantizar la aplicación de un enfoque congruente y complementario a la ciberseguridad de la aviación en todas las disciplinas del sector, el sistema de aviación civil debe asegurarse de gestionar de manera integral los ciberriesgos a la aviación civil mediante la coordinación de los aspectos de seguridad operacional y seguridad de la aviación en el ámbito de la ciberseguridad. Además, la coordinación de la ciberseguridad de la aviación debería extenderse más allá de la aviación civil hacia otras entidades interesadas, como las autoridades nacionales, regionales e internacionales de ciberseguridad, los organismos de observancia de la ley, el sector militar, etc.

4. **Elementos de la política de ciberseguridad**

En esta sección se proporciona orientación sobre los elementos incluidos en el modelo de política de ciberseguridad del apéndice A. Por ello, se recomienda leer esta sección conjuntamente con el referido modelo.

4.1 **Gobernanza y organización**

4.1.1 Los Estados deberían designar una "autoridad apropiada para la ciberseguridad de la aviación" (AA/Ciberseguridad), la cual asumiría el mandato y la responsabilidad general de la ciberseguridad y la ciberresiliencia de la aviación.

4.1.2 No existe un único enfoque en cuanto a la posición de la AA/Ciberseguridad dentro de las estructuras institucionales de la aviación civil de cada Estado. La decisión obedecería a varias consideraciones relacionadas con la aviación nacional y las distintas entidades y mandatos pertinentes ajenos a la aviación. Sin embargo, es importante que la AA/Ciberseguridad cuente con los recursos y las facultades que se requieren para poder cumplir su mandato, lo que incluye la negociación y coordinación con partes interesadas fuera del sector de la aviación.

4.1.3 En términos generales, la AA/Ciberseguridad designada debería:

- determinar, en coordinación con la autoridad nacional competente a cargo de la ciberseguridad, las funciones y responsabilidades que cada autoridad ha de asumir;
- conducir la elaboración de reglamentos sobre ciberseguridad de la aviación;
- definir claramente las funciones y responsabilidades de los diferentes ámbitos de la aviación civil dentro de la autoridad nacional competente en materia de aviación civil;

- coordinar la definición de las funciones y responsabilidades de las entidades de aviación civil supervisadas por la autoridad nacional competente en materia de aviación civil a través de los programas nacionales de seguridad operacional y seguridad de la aviación;
- definir los elementos de una cultura de ciberseguridad de la aviación civil y observar su implantación;
- definir reglamentos, procesos, requisitos y funciones para la gestión de crisis de ciberseguridad, incluidos los requisitos y las frecuencias de ensayos de verificación; y
- coordinar los aspectos transversales de la ciberseguridad de la aviación con las partes interesadas fuera del sector de la aviación que tienen que ver con la ciberseguridad de la aviación, como el intercambio de información y la investigación de incidentes.

4.2 **Gestión de riesgos**

4.2.1 La gestión de los riesgos de ciberseguridad debería valerse de los marcos de gestión de riesgos de la seguridad operacional y seguridad de la aviación a fin de realizar una evaluación integrada y precisa de las ciberamenazas y los ciberriesgos, y velar por la formulación y ejecución de medidas de mitigación eficaces que tengan en cuenta los requisitos de seguridad operacional y las implicaciones de dichas medidas de mitigación para la seguridad operacional y la continuidad de la aviación.

4.2.2 La propiedad y procedencia de todos los datos y sistemas deberían indicarse en todo momento. La identificación y el mantenimiento de la propiedad permiten fijar responsabilidades y facilita la gestión de los datos y sistemas desde la adopción hasta la eliminación. En consecuencia, los propietarios deberían definir reglas y procesos para incluir la ubicación física de los datos y sistemas, derechos de acceso, derechos de gestión y requisitos de seguridad con base en la clasificación de los datos y los sistemas. Esto contribuirá en última instancia al uso adecuado de los datos y los sistemas por parte de las personas correctas, la formulación y aplicación de normas de control de calidad y la resolución de problemas y conflictos.

4.3 **Seguridad de sistemas críticos**

4.3.1 Deberían aplicarse principios de defensa en profundidad para proteger los sistemas críticos. La defensa en profundidad integra a personas, tecnologías y capacidades operativas para establecer barreras variables a múltiples niveles y misiones de una organización[3]. Es un enfoque de ciberseguridad que estipula la superposición de una serie de mecanismos defensivos a fin de proteger sistemas, datos e información críticos. Este enfoque de múltiples niveles con redundancias intencionales aumenta la seguridad de un sistema en general y aborda numerosos y diferentes vectores de ataque[4].

4.3.2 La AA/Ciberseguridad debería asegurarse de que las entidades de aviación civil definan y protejan adecuadamente sus sistemas críticos y desarrollen la capacidad de detectar y responder a ciberincidentes, así como recuperarse de un ataque de este tipo.

4.4 **Seguridad de los datos**

4.4.1 Debería considerarse el hacer periódicamente copias de respaldo fuera de línea de datos críticos para facilitar la disponibilidad e integridad de la información. No obstante, es de suma importancia contar con una política de respaldo sólida, en consonancia con las evaluaciones de riesgo, dado que las copias de

[3] NIST, Publicación especial núm. 800-53 Rev.5: https://doi.org/10.6028/NIST.SP.800-53r5.
[4] La defensa en profundidad es comúnmente denominada el “enfoque de castillo”, porque sigue el patrón de niveles de protección de un castillo medieval, donde los atacantes que intentan penetrar enfrentan fosos, puentes levadizos, murallas, torres, etc.

respaldo fuera de línea realizadas durante un ciberataque quedarían comprometidas y, en consecuencia, no podrían utilizarse posteriormente para restaurar el acceso a información crítica.

4.4.2 Debería considerarse el cifrado de datos sensibles como herramienta para contribuir a la confidencialidad de la información. Sin embargo, es importante definir, conjuntamente con las evaluaciones de riesgos, procesos para utilizar el cifrado que proporcionen un equilibrio correcto entre el nivel de confidencialidad y los requisitos de performance operacional, especialmente en el caso de los datos "vivos" requeridos para la seguridad de vuelo, así como tomar en cuenta los recursos necesarios para gestionar los datos.

4.4.3 Deberían establecerse procesos que aseguren la continuidad de las funciones críticas en caso de pérdida de la disponibilidad y/o integridad de los datos.

4.5 **Seguridad de la cadena de suministro**

4.5.1 Las entidades deberían cuidar de que los programas y equipos informáticos utilizados en funciones críticas de aviación cumplan con los requisitos de ciberseguridad a lo largo del ciclo de vida de los sistemas de aviación, desde el diseño y desarrollo, durante la operación y el mantenimiento y hasta su eliminación segura.

4.5.2 Pueden fortalecerse los acuerdos de nivel de servicio mediante la inclusión de requisitos sobre ciberseguridad para los programas y equipos informáticos así como para la actualización, mejoramiento y reparación en caso de descubrirse vulnerabilidades.

4.6 **Seguridad física**

4.6.1 Como ejemplos de controles de la seguridad física podrían mencionarse la definición de políticas de gestión y control del acceso físico, verificación de los antecedentes del personal que goza de derechos administrativos relacionados con los sistemas/las bases de datos, o que tiene acceso a datos sensibles y/o críticos, recomendaciones relativas a la separación de derechos y/o la rotación del personal con acceso a sistemas críticos o con la capacidad de modificarlos, entre otros.

4.7 **Seguridad de la información, las comunicaciones y la tecnología (ICT)**

4.7.1 Como ejemplos de controles de seguridad de las ICT pertinentes para la ciberseguridad de la aviación podrían mencionarse las políticas de control del acceso y la aplicación de principios de privilegio mínimo, cortafuegos para equipos y programas informáticos y seguridad de la red, criptografía, políticas de contraseñas de la organización, protección de los puntos finales, vigilancia de la red y detección de anomalías, separación de redes, gestión de dispositivos, etc.

4.8 **Gestión de incidentes y continuidad de funciones críticas**

4.8.1 La AA/Ciberseguridad debería definir reglamentos, procesos, requisitos y funciones para la gestión de ciberincidentes, la recuperación y la continuidad de los sistemas críticos.

4.8.2 Los planes existentes de gestión de crisis y continuidad de las operaciones deberían fortalecerse para incluir las respuestas a los ciberincidentes y la recuperación tras un incidente de este tipo.

4.8.3 Deberían realizarse ensayos de los planes de respuesta y continuidad de las operaciones periódicamente a fin de mejorar dichos planes y las capacidades del personal de respuesta. Estas pruebas deberían incluir a todas las partes interesadas pertinentes y combinar ejercicios teóricos con ensayos reales.

4.9 **Cultura de ciberseguridad**

4.9.1 Debería implantarse una cultura de ciberseguridad en todas las entidades de la aviación.

4.9.2 La dirigencia de la organización debería suscribir la cultura de seguridad e incluir un programa que todo el personal ha de cumplir.

4.9.3 El programa debería incluir actividades regulares de formación en materia de ciberseguridad (incluidos los principios de las prácticas de ciberhigiene), concientización sobre las amenazas más recientes, instrucción y ensayos (tanto como parte de la instrucción como con simulacros de ataque) a fin de evaluar el nivel de conciencia/higiene sobre la ciberseguridad.

4.9.4 La cultura de ciberseguridad debería incluir elementos de las culturas de seguridad operacional y seguridad de la aviación, por ejemplo, la autonotificación, la denuncia de prácticas/comportamientos sospechosos, cultura justa, etc.

— — — — — — — —

Apéndice A

Modelo de política de ciberseguridad

1. Introducción

1.1 La presente política de ciberseguridad será el marco para profundizar la formulación e implantación de la ciberseguridad de la aviación. La política será publicada, difundida a las partes interesadas pertinentes y revisada periódicamente.

1.2 Se prepararán otros textos de orientación para facilitar la aplicación de esta política de ciberseguridad.

2. Alcance

2.1 La ciberseguridad de la aviación abordará la seguridad y la resiliencia del sistema de aviación civil, y facilitará la colaboración con entidades y autoridades ajenas a dicho sector, incluidas la autoridad nacional de ciberseguridad, la seguridad nacional, las entidades de observancia de la ley y las autoridades militares, según corresponda.

2.2 La ciberseguridad de la aviación se coordinará a nivel nacional con la seguridad operacional de la aviación, la seguridad de la aviación, la protección de infraestructura crítica, la ciberdefensa y el sector militar.

2.3 La ciberseguridad de la aviación se coordinará a nivel internacional con las debidas autoridades extranjeras designadas para esta labor.

3. Objetivos

3.1 Los objetivos generales de esta política de ciberseguridad de la aviación son velar por la seguridad operacional, la resiliencia y el autofortalecimiento del sistema de aviación civil frente a ciberamenazas y ciberriesgos, y cuidar de la coordinación de la ciberseguridad de la aviación con las autoridades y entidades nacionales pertinentes.

4. Gobernanza y organización

4.1 De conformidad con [título del reglamento/la legislación pertinente para la designación], [nombre de la entidad] será la autoridad apropiada de la ciberseguridad de la aviación (AA/Ciberseguridad) a cargo de hacer cumplir el mandato general sobre ciberseguridad y ciberresiliencia de la aviación.

4.2 La AA/Ciberseguridad deberá:

- interactuar con la autoridad nacional competente en materia de ciberseguridad para definir las funciones y responsabilidades de cada autoridad relativas a la ciberseguridad de la aviación;
- coordinar y contribuir a la formulación de reglamentos sobre ciberseguridad de la aviación;
- definir, coordinar y apoyar a las autoridades apropiadas de seguridad operacional y seguridad de la aviación a fin de incluir requisitos sobre ciberseguridad de la aviación, como elementos de vigilancia y control de calidad, en el Programa Estatal de Seguridad Operacional (SSP) y el Programa Nacional de Seguridad de la Aviación Civil (NCASP);
- definir, facilitar y observar la ejecución del programa de cultura de ciberseguridad por todas las partes interesadas de la aviación civil;

- definir reglamentos, procesos, requisitos y funciones para la gestión de crisis de ciberseguridad; y
- coordinar los aspectos transversales de ciberseguridad de la aviación con las debidas partes interesadas ajenas a la aviación pero vinculadas a la ciberseguridad en dicho sector.

5. Gestión de riesgos

5.1 La ciberseguridad obedecerá a información de inteligencia, se basará en amenazas y se gestionará con base en los riesgos.

5.2 La gestión de riesgos formará parte integral del ciclo de vida de todos los sistemas.

5.3 La propiedad de todos los datos y sistemas estará debidamente indicada en todo momento.

6. Seguridad de sistemas críticos

6.1 Las funciones, sistemas e infraestructura de índole crítica se identificarán mediante procesos de gestión de riesgos.

6.2 Se aplicarán el enfoque de seguridad por diseño y los principios de defensa en profundidad a fin de proteger los sistemas críticos.

6.3 La redundancia de los sistemas críticos se considerará una medida facilitadora de la seguridad de los sistemas.

7. Seguridad de los datos

7.1 Los datos y la información se protegerán durante su almacenamiento y transmisión, en consonancia con su perfil de sensibilidad.

8. Seguridad de la cadena de suministro

8.1 La gestión de extremo a extremo de la cadena de suministro de equipos y programas informáticos formará parte de la gestión de la ciberseguridad de la aviación.

8.2 Los programas y equipos informáticos utilizados en funciones críticas de aviación cumplirán con los requisitos sobre ciberseguridad a todo lo largo del ciclo de vida de los sistemas de aviación.

9. Seguridad física

9.1 La seguridad física (incluida la seguridad del personal) formará parte de la gestión de la ciberseguridad de la aviación.

9.2 La seguridad física resguardará a las personas, la infraestructura, las instalaciones, los equipos, materiales y documentos contra actos de interferencia ilícita y protegerá los sistemas críticos de aviación contra el acceso físico no autorizado.

9.3 La seguridad física contribuirá a la gestión de riesgos mediante la facilitación de la identificación de actores de amenazas y/o la posibilidad de ataques contra la infraestructura crítica de la aviación civil.

10. **Seguridad de la información, las comunicaciones y la tecnología (ICT)**

10.1 La seguridad de las ICT formará parte de la gestión de la ciberseguridad de la aviación.

10.2 La seguridad de las ICT definirá y aplicará medidas de seguridad lógicas y contribuirá con los procesos de gestión de ciberincidentes, recuperación de ciberincidentes y continuidad de las operaciones.

10.3 La seguridad de las ICT contribuirá con la gestión de riesgos mediante la detección de vulnerabilidades, la identificación de vectores de ataque y la vigilancia de la evolución del contexto de amenazas a la ciberseguridad de la aviación.

11. **Gestión de incidentes y continuidad de las funciones críticas**

11.1 La seguridad de las operaciones y la continuidad de las funciones críticas serán los principales impulsores de los procesos de gestión de incidentes.

11.2 El ensayo de los planes de gestión y recuperación de crisis formará parte integral de la gestión de incidentes.

12. **Cultura de ciberseguridad**

12.1 Un plan de formación, concientización, instrucción y ejercicios formará parte integral de la gestión de la ciberseguridad de la aviación.

12.2 La cultura de ciberseguridad se coordinará plenamente con las culturas existentes sobre seguridad operacional y seguridad de la aviación.

12.3 La cultura de ciberseguridad descansará sobre sólidas prácticas internas y, de ser posible, externas de intercambio de información.

— FIN —

OACI

Objetivo estratégico de Seguridad de la aviación y facilitación

Estrategia de ciberseguridad de la aviación

Octubre, 2019

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Objetivo estratégico de Seguridad de la aviación y facilitación

Estrategia de ciberseguridad de la aviación

Octubre, 2019

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

Publicado por separado en español, árabe, chino, francés, inglés y ruso,
por la ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

La información sobre pedidos y una lista completa de los agentes de ventas
y libreros pueden obtenerse en el sitio web de la OACI: www.icao.int

Estrategia de ciberseguridad de la aviación
https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

© OACI 2019

Reservados todos los derechos. No está permitida la reproducción de ninguna parte de esta publicación, ni su tratamiento informático, ni su transmisión, de ninguna forma ni por ningún medio, sin la autorización previa y por escrito de la Organización de Aviación Civil Internacional.

ESTRATEGIA DE CIBERSEGURIDAD DE LA AVIACIÓN

VISIÓN DE UNA ESTRATEGIA MUNDIAL DE CIBERSEGURIDAD DE LA AVIACIÓN CIVIL

El sector de la aviación civil depende cada vez en mayor medida de la disponibilidad de sistemas de tecnología de información y comunicaciones, así como de la integridad y confidencialidad de los datos. La amenaza de posibles incidentes cibernéticos para la aviación civil evoluciona de forma constante, con unos perpetradores que actúan maliciosamente para perturbar las operaciones y robar información por razones políticas, financieras y de otra índole.

Dada la naturaleza polifacética y multidisciplinaria de la ciberseguridad, y en vista de que los ciberataques pueden afectar de forma simultánea una amplia gama de áreas y propagarse con rapidez, es imperioso concebir una visión común y definir una estrategia de ciberseguridad.

La visión de la OACI sobre la ciberseguridad mundial es que el sector de la aviación civil sea resiliente a los ciberataques y siga siendo seguro y fiable en todo el mundo, al tiempo que continúa innovando y creciendo.

Esto puede lograrse mediante:

- el reconocimiento de parte de los Estados de sus obligaciones en virtud del *Convenio sobre Aviación Civil Internacional* (Convenio de Chicago) de velar por la seguridad operacional y la seguridad y continuidad de la aviación civil, incluida la ciberseguridad;
- la coordinación de la ciberseguridad de la aviación entre las autoridades estatales a fin de garantizar una gestión eficaz y eficiente de los riesgos de ciberseguridad a escala mundial; y
- el compromiso de todas las partes interesadas de la aviación de profundizar la resiliencia en este ámbito y protegerse contra los ciberataques que pudieran afectar la seguridad operacional, la seguridad de la aviación y la continuidad del sistema de transporte aéreo.

La estrategia se alinea con otras iniciativas de la OACI relativas a la ciberseguridad y se coordina con las disposiciones pertinentes sobre gestión de la seguridad operacional y la seguridad de la aviación. La finalidad de la estrategia se cumplirá mediante un conjunto de principios, medidas y actividades contenidos en un marco que 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. COOPERACIÓN INTERNACIONAL

1.1 Por naturaleza, la ciberseguridad y la aviación no conocen fronteras. Ambas requieren de la cooperación a nivel nacional e internacional y requieren del mutuo reconocimiento de los esfuerzos desplegados para mejorar la ciberseguridad a fin de proteger el sector de la aviación civil de todos los ciberataques a la seguridad operacional y la seguridad de la aviación.

1.2 La ciberseguridad de la aviación debe armonizarse a nivel mundial, regional y nacional con el objeto de promover la coherencia en todo el mundo y velar por la plena interoperabilidad de las medidas de protección y los sistemas de gestión de riesgos.

1.3 La OACI es el foro mundial idóneo para interactuar con los Estados y abordar la ciberseguridad en la aviación civil internacional. A tal efecto, la OACI organizará, facilitará y promoverá eventos internacionales que sirvan de plataforma para el intercambio de conocimientos entre Estados, organizaciones internacionales e industria. Se alienta a los Estados a participar en las deliberaciones sobre la ciberseguridad en la aviación civil.

2. GOBERNANZA

2.1 Se alienta a todos los Estados miembros de la OACI a apoyar y aprovechar la Estrategia OACI de ciberseguridad de la aviación para velar por la seguridad operacional y la seguridad y continuidad de la aviación civil un mundo cada vez más en peligro ante las amenazas de ciberseguridad.

2.2 Se alienta a los Estados a establecer un plan claro de gobernanza y rendición de cuentas a nivel nacional para la ciberseguridad de la aviación civil. Se invita a las administraciones de la aviación civil a asegurar la coordinación con su autoridad nacional competente en materia de ciberseguridad, dado que la autoridad general en materia de ciberseguridad para todos los sectores puede no ser responsabilidad de la administración de aviación civil. También es esencial establecer los canales apropiados de coordinación entre las diversas autoridades estatales y las partes interesadas de la industria.

2.3 Por último, se alienta a los Estados miembros a incluir la ciberseguridad en sus programas nacionales de seguridad operacional y seguridad de la aviación civil. A tales fines, la OACI debería incluir también la ciberseguridad en sus planes y actividades regionales y mundiales en pro de una base común para normas y métodos recomendados (SARPS) sobre ciberseguridad.

3. LEYES Y REGLAMENTOS EFICACES

3.1 El objetivo principal de las leyes y reglamentos internacionales, regionales y nacionales sobre ciberseguridad para la aviación civil es apoyar la implementación de una estrategia integral de ciberseguridad dirigida a proteger a la aviación civil y a los viajeros de los efectos de los ciberataques.

3.2 Los Estados miembros deben asegurarse de que se formulen y apliquen las leyes y reglamentos pertinentes de conformidad con las disposiciones de la OACI, antes de implantar una política nacional de ciberseguridad para la aviación civil. Es necesario formular nuevas orientaciones apropiadas para ayudar a los Estados y la industria a poner en práctica las disposiciones relacionadas con la ciberseguridad. En ese sentido, la OACI está comprometida a crear, examinar y, de ser el caso, enmendar los textos de orientación relativos a la inclusión de aspectos relacionados con la ciberseguridad en la seguridad operacional y la seguridad de la aviación.

3.3 Deberían analizarse los instrumentos jurídicos internacionales para determinar cuáles son las disposiciones jurídicas que existen o faltan en el derecho aéreo para la prevención, el enjuiciamiento y la reacción oportuna ante los ciberincidentes con el propósito de formar la base para una implementación uniforme y coherente de las leyes y reglamentos de ciberseguridad en el sector de la aviación. Mientras tanto, se alienta a los Estados a ratificar los instrumentos de la OACI, incluidos el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* (Convenio de Beijing) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves* (Protocolo de Beijing).

3.4 Se alienta a los Estados a considerar si sus respectivas legislaciones nacionales deben ser actualizadas y si debe adoptarse una nueva legislación nacional para permitir el enjuiciamiento de ciberataques relacionados con actos terroristas y aquellos que afectan adversamente a la aviación civil. También se alienta a los Estados a que, de forma paralela, establezcan mecanismos apropiados para cooperar en las investigaciones de seguridad de "buena fe", que es la actividad de investigación que se lleva a cabo en un entorno diseñado para evitar afectar la seguridad operacional y la seguridad y continuidad de la aviación civil.

4. POLÍTICA DE CIBERSEGURIDAD

4.1 La ciberseguridad ha de incluirse en los sistemas de seguridad de la aviación y seguridad operacional de un Estado como parte de un marco integral de gestión de riesgos.

4.2 Habida cuenta de las diferentes metodologías de evaluación de riesgos que existen, debe conferirse prioridad a la enmienda y la posible elaboración de textos de orientación relacionados con las evaluaciones de amenazas y riesgos de ciberseguridad, con el propósito de poder comparar los resultados de dichas evaluaciones.

4.3 En todo el sector de la aviación civil, las políticas de ciberseguridad pueden considerar el ciclo de vida completo del sistema de aviación e incluir elementos como: cultura de ciberseguridad, promoción de la seguridad por diseño, seguridad de la cadena de suministros de programas y equipos informáticos, integridad de los datos, control apropiado del acceso, gestión proactiva de las vulnerabilidades, mejoramiento de la rapidez de las actualizaciones de la seguridad de la aviación sin comprometer la seguridad operacional e incorporación de sistemas y procesos para vigilar los datos pertinentes de ciberseguridad.

5. INTERCAMBIO DE INFORMACIÓN

5.1 El sector de la aviación civil es un sistema global interdependiente con numerosos sistemas comunes, por lo que los ciberataques pueden propagarse fácilmente y tener repercusiones mundiales. El objetivo del intercambio de información es permitir la prevención, detección temprana y atenuación de sucesos relevantes de ciberseguridad antes de que sus efectos se extiendan hacia la seguridad operacional y la seguridad de la aviación. Una cultura de intercambio de información reducirá considerablemente los riesgos cibernéticos sistémicos en todo el sector de la aviación, y su valor ha quedado comprobado en el ámbito de la seguridad operacional y la seguridad de la aviación.

5.2 El intercambio de información sobre aspectos como las vulnerabilidades, amenazas, sucesos y mejores prácticas por medio de relaciones establecidas y fiables pueden reducir el impacto de los ataques en curso. Deben reconocerse los mecanismos apropiados de intercambio de información en consonancia con las disposiciones existentes de la OACI.

6. GESTIÓN DE INCIDENTES Y PLANIFICACIÓN ANTE EMERGENCIAS

6.1 Junto a los mecanismos existentes de gestión de incidentes, es menester contar con planes apropiados y ampliables que aseguren la continuidad del transporte aéreo durante un incidente cibernético. Se recomienda que los Estados y el sector de la aviación enmienden los planes de contingencia existentes para incluir disposiciones relativas a la ciberseguridad.

6.2 Los ejercicios de ciberseguridad son una herramienta útil para someter a prueba la resiliencia ante ciberataques y detectar las áreas que requerirían mejoras, por lo que se recomiendan altamente. Estos ejercicios pueden seguir formatos diferentes (p. ej., ejercicios teóricos, simulaciones o ejercicios en tiempo real) e igualmente variar en escala (internacional, nacional, institucional).

7. CREACIÓN DE CAPACIDAD, INSTRUCCIÓN Y CULTURA DE CIBERSEGURIDSAD

7.1 El elemento humano es el corazón de la ciberseguridad. Es de suma importancia que el sector de la aviación civil dé pasos tangibles para aumentar el número de funcionarios calificados y conocedores tanto de la aviación como de la ciberseguridad. Esto puede hacerse aumentando la conciencia sobre la ciberseguridad, así como con educación, contratación e instrucción. Deberían incluirse planes de estudio pertinentes a la ciberseguridad y – de ser viable – la ciberseguridad específicamente relacionada con la aviación, a todos los niveles del sistema educativo nacional y los programas internacionales de instrucción pertinentes. Deberían buscarse formas innovadoras de fusionar e interconectar las profesiones tradicionales de tecnología de información y cibernética con las profesiones pertinentes de la aviación.

7.2 El apoyo y la estimulación del desarrollo de aptitudes del personal existente y nuevo deberían conducir al fomento de la innovación en materia de ciberseguridad y las debidas investigaciones y diseño en el sector de la aviación. Debería ofrecerse instrucción apropiada y continua en el trabajo para apoyar al personal en sus actividades cotidianas.

7.3 La ciberseguridad podría incluirse en la estrategia para la próxima generación de profesionales de la aviación, ya que la OACI está bien posicionada para trabajar con los Estados y la industria en la formulación de los requisitos de competencias basadas en las funciones de los profesionales de la aviación.

7.4 El sector de la aviación civil tiene una historia envidiable de seguridad operacional con base en una cultura de seguridad operacional que se entiende como responsabilidad de todos. Los principios de esta cultura de seguridad operacional deben seguirse para crear y mantener una cultura de ciberseguridad en todo el sector de la aviación.

— FIN —

In cooperation with

ICAO CANSO AIRBUS

LATIN AMERICA & THE CARIBBEAN

ESQUEMA DE POLITICA DE CIBERSEGURIDAD PARA LA GESTION DE TRAFICO AEREO

SHAPING OUR FUTURE SKIES

canso.org

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

© Copyright CANSO, ICAO and Airbus March 2021

All rights reserved. No part of this publication may be reproduced, or transmitted in any form, without the prior permission of CANSO. This paper is for information purposes only. While every effort has been made to ensure the quality and accuracy of information in this publication, it is made available without any warranty of any kind.

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. Los activos se pueden clasificar de la siguiente manera: • Activo tangible: software, hardware, equipos, instalaciones, personas • 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] 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 800-12 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] 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]

CANSO

canso.org