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 —