Plan de acción de ciberseguridad

Publicado bajo la responsabilidad del Secretario General

Segunda edición, enero de 2022

Organización de Aviación Civil Internacional

S22-0544

Términos y definiciones[1]

caISMS: Sistema de Gestión de la Seguridad de la Información de aviación civil

Modelo para establecer, poner en práctica, controlar, supervisar, examinar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de la aviación civil sobre la base de una evaluación de riesgos y de los niveles de aceptación del riesgo de la organización concebidos para tratar y gestionar los riesgos. Fuente ISO 27000:2009.

Ciberseguridad

Conjunto de tecnologías, controles, medidas, procesos y prácticas diseñados para proteger la confidencialidad, integridad, disponibilidad y protección general de sistemas, redes, programas, dispositivos, información y datos contra ataques o daños y acceso, uso y/o explotación no autorizados.

Política de ciberseguridad

Una política de ciberseguridad documenta las intenciones y la orientación de una organización con respecto a la gestión de las amenazas a la ciberseguridad, y es responsabilidad de los niveles más altos de la dirección. Se trata de un documento escrito de una organización en el que se indica cómo protegerla de las amenazas de ciberseguridad, y cómo hacerles frente cuando se producen incidentes y sucesos de esta naturaleza.

Suceso

Caso detectado en un sistema, servicio o red que indica el posible incumplimiento de la política de seguridad de la información o fallas de control, o una situación previamente desconocida que pueda afectar a la seguridad [ISO/IEC 27035]. Cabe señalar que "caso" debe considerarse en un sentido amplio y no se entenderá como un caso (de seguridad operacional) que solo abarca los sucesos que han tenido o podrían tener, importancia en el contexto de la seguridad operacional de la aviación.

Incidente

Uno o varios sucesos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de poner en peligro las operaciones comerciales y amenazar la seguridad de la información [ISO/IEC 27035-1].

Seguridad de la información

Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, pueden tenerse en cuenta otras propiedades, tales como la autenticidad, la rendición de cuentas, el no repudio (irrenunciabilidad) y la fiabilidad [BS ISO/CEI 27000:2018].

Intercambio de información

Proceso mediante el cual una entidad proporciona información a una o más entidades a fin de facilitar la adopción de decisiones con base en los riesgos y promover las mejores prácticas.

Matriz de riesgo

Herramienta para clasificar y presentar los componentes de los riesgos (amenaza, probabilidad, repercusión/consecuencia y vulnerabilidad), medidas implantadas para mitigar los riesgos y, en último término, los riesgos residuales.

[1] Lista sujeta a revisión.

Entidad (o actor) de una amenaza

Entidad que es responsable, total o parcialmente, de un incidente que afecta o puede afectar a una organización o sistema.

Vulnerabilidad

Deficiencias de un sistema de información, de los procedimientos de seguridad del sistema o de los controles internos, o bien fallas de implementación que podrían ser aprovechadas o iniciadas por una entidad de amenaza. Puede tratarse de un sistema que facilita directa o indirectamente una función del sistema de aviación.

RESUMEN

La Asamblea de la Organización de Aviación Civil Internacional (OACI), en su 39° período de sesiones, reiteró la importancia y urgencia de proteger de los ciberataques los datos y los sistemas de infraestructuras que revisten una importancia crítica para la aviación civil, y que la OACI, sus Estados miembros y las partes interesadas de la industria se comprometan a escala mundial a tomar medidas al respecto, con la intención de ocuparse de manera colaborativa y sistémica de la ciberseguridad de la aviación civil y de mitigar las amenazas y los riesgos conexos. En la Resolución A39-19 – *Formas de abordar la ciberseguridad en la aviación civil* se señalaron las acciones que han de realizar los Estados y otras partes interesadas al respecto. En ese período de sesiones, la Asamblea también pidió a la OACI que elaborara un plan de trabajo integral en materia de ciberseguridad.

A fin de cumplir las expectativas de la Asamblea, el Grupo de Estudio de la Secretaría sobre Ciberseguridad (SSGC) elaboró una Estrategia de Ciberseguridad de la Aviación Civil.

En su 40º período de sesiones, la Asamblea de la OACI adoptó la Resolución enmendada A40-10 — *Formas de abordar la ciberseguridad en la aviación civil*, en la que se exhorta a los Estados a que implanten la Estrategia de Ciberseguridad y se subraya la importancia de elaborar un plan sostenible para ejecutarla, así como de seguir trabajando en la formulación de un marco de ciberseguridad firme.

El Plan de Acción de Ciberseguridad (CyAP) sirve de base para que los Estados, la industria, las partes interesadas y la OACI trabajen juntas con el objetivo de desarrollar la capacidad de determinar, prevenir y detectar los ciberataques a la aviación civil, y de darles respuesta y recuperarse de sus efectos, así como de crear un marco sólido de cooperación. El plan se ha creado con la finalidad de proponer una serie de principios, medidas y acciones para alcanzar los objetivos de los siete pilares de la estrategia.

Capítulo 1

INTRODUCCIÓN

1.1 ANTECEDENTES

1.1.1 En el contexto actual de la aviación civil, se prevé que el tráfico aéreo aumente a largo plazo, la tecnología siga una evolución acelerada, las operaciones sean cada vez más complejas y, consecuentemente, las condiciones operacionales se vuelvan más difíciles. Los rápidos cambios tecnológicos están alterando la forma en que funciona la aviación civil y haciendo que el sistema sea más vulnerable frente a las amenazas de ciberseguridad. Las ciberactividades malintencionadas pueden afectar a la aviación civil de diversas maneras, desde una breve disrupción de las operaciones hasta consecuencias catastróficas. Los riesgos se están incrementando velozmente, por lo que se necesita de forma apremiante un marco de ciberseguridad sostenible a nivel internacional, regional y nacional.

1.1.2 La creación de una infraestructura de ciberseguridad sólida, sustentada en una estrecha cooperación entre los Estados, la industria y la OACI, permite la creación de una conciencia común sobre la ciberseguridad que desemboque, a la postre, en un sistema de aviación civil más seguro y resiliente.

1.1.3 La OACI está adaptándose continuamente para hacer frente a un cuadro global de amenazas en constante evolución, de conformidad con las resoluciones del Consejo de Seguridad de las Naciones Unidas en las que se afirma que los Estados son responsables de garantizar la seguridad operacional de los servicios aéreos que operan dentro de su territorio y se exhorta a todos los Estados a que trabajen con la OACI para que sus normas internacionales de seguridad se revisen, actualicen y apliquen sobre la base de los riesgos actuales, en consonancia con el Convenio de Chicago. Dado que las ciberamenazas a la aviación civil están en plena evolución y que su prevalencia probablemente vaya en aumento, la OACI, en aplicación de lo dispuesto en la Resolución 2341 (2017) del Consejo de Seguridad de las Naciones Unidas, le dedica especial atención al establecimiento de mecanismos apropiados para mitigar y reducir los riesgos para infraestructuras importantes en la aviación de toda interferencia ilícita mediante vectores cibernéticos y de todo suceso que pueda afectar la seguridad de las operaciones.

1.1.4 En relación con lo anterior, se ha elaborado este plan de acción con el fin de cumplir debidamente los objetivos de los siete pilares de la Estrategia de Ciberseguridad de la Aviación y configurar un marco de ciberseguridad.

1.2 FINALIDAD

1.2.1 Este Plan de Acción de Ciberseguridad (CyAP) es un documento vivo, que irá evolucionando con los avances de la ciberseguridad y se actualizará regularmente a fin de reflejar los cambios requeridos, derivados entre otras cosas del análisis de las brechas y de las actividades que se describen en los capítulos 3 y 4. El CyAP recoge los objetivos y las acciones que han de realizarse para aplicar la Estrategia de Ciberseguridad de la Aviación Civil de la OACI. Los elementos presentados en este documento reflejan el trabajo efectuado o que se está efectuando actualmente en las distintas regiones/Estados o en la industria. El documento abarca los resultados del análisis de la situación actual del sistema de aviación desde la perspectiva de la ciberseguridad en comparación con la situación futura propuesta en la estrategia, y describe el plan de acción que puede impulsar la evolución hacia la visión estratégica.

1.2.2 Dada la ingente labor necesaria para concretar los objetivos y las acciones que se exponen en este documento, en el apéndice A se propone un enfoque por etapas en el que se determinan metas a corto, medio y largo plazo.

1.3 CONTEXTO DE RIESGO

1.3.1 La ciberseguridad no es un concepto nuevo en el ámbito de la aviación civil. No obstante, como las amenazas de ciberseguridad se han vuelto cada vez más frecuentes, se ha convertido en uno de los elementos centrales de los debates y análisis de riesgos y vulnerabilidades del sistema de aviación civil. El sector de la aviación civil está particularmente en situación de riesgo porque los ciberataques tienen más posibilidades de prosperar en un sector cuyos componentes aumentan de forma interdependiente desde el punto de vista funcional y digital, y también porque los mecanismos de ciberdefensa que usa actualmente el sector de la aviación civil aún no son adecuados para hacer frente a esta amenaza persistente y adaptable.

1.3.2 El Grupo Experto en Seguridad de la Aviación de la OACI recientemente evaluó y calificó de medio el nivel de riesgo planteado por la explotación de una vulnerabilidad en un contexto terrorista. Esta evaluación se basa en la vulnerabilidad residual en el ámbito de la ciberseguridad, dando por supuesto que los Estados hayan aplicado efectivamente las disposiciones del Anexo 17 – *Seguridad*. No obstante, los riesgos cibernéticos evolucionan rápidamente y deben evaluarse en función de todos los perfiles de ciberatacantes que podrían afectar en todo sentido a la seguridad de las operaciones de aviación civil. Además, a menudo resulta difícil encontrar el origen de los ciberataques, por lo que la atribución y el enjuiciamiento de ciberataques suelen ser complicados y difíciles de realizar, por lo que queda en manos de la víctima del ataque y sus aseguradoras el sufragar el costo de la recuperación. Por estas razones, es de extrema importancia que la OACI, los Estados y la industria trabajen en colaboración para aplicar la Estrategia de Ciberseguridad de una forma sistemática.

1.4 BENEFICIOS DEL PLAN DE ACCIÓN

1.4.1 El CyAP tiene por objeto garantizar el compromiso de la OACI, los Estados miembros y la industria de aplicar la Estrategia de Ciberseguridad de la Aviación y alcanzar los objetivos enunciados en sus siete pilares. Un marco de ciberseguridad sólido fortalecerá el sistema de aviación civil y será beneficioso para toda la comunidad de la aviación mundial.

Capítulo 2

OBJETIVO

2.1 OBJETIVO DEL PLAN DE ACCIÓN DE CIBERSEGURIDAD

2.1.1 El propósito del Plan de Acción de Ciberseguridad es lograr los objetivos que se indican en cada uno de los siete pilares de la Estrategia de Ciberseguridad, así como desarrollar un marco de ciberseguridad de la aviación civil sólido.

2.1.2 Los principios que constituyen los cimientos del presente plan de acción son los siguientes:

a) la comprensión por parte de los Estados miembros de sus obligaciones con respecto a la ciberseguridad dimanantes del *Convenio sobre Aviación Civil Internacional* (Convenio de Chicago) de velar por la seguridad y continuidad de las operaciones de aviación civil;

b) la coordinación de las medidas de ciberseguridad de la aviación entre las autoridades de los Estados miembros a fin de garantizar una gestión eficaz y eficiente de la ciberseguridad de la aviación a escala mundial; y

c) el compromiso de todas las partes interesadas de la aviación civil de profundizar la ciberresiliencia y de proteger a la aviación de todos los ciberataques, sea cual fuere el perfil del actor de la amenaza, que pudieran afectar la seguridad y la continuidad del sistema de transporte aéreo.

2.2 APLICACIÓN

2.2.1 Este documento, que está dirigido principalmente a los Estados miembros de la OACI y a la industria, es un instrumento para ayudarlos a gestionar los riesgos de ciberseguridad en la aviación civil mediante un enfoque global, coordinado y holístico.

2.2.2 Los Estados, la industria y las demás partes interesadas pertinentes deberían emprender las acciones derivadas de este plan de acción.

Capítulo 3

PLAN DE ACCIÓN ESTRATÉGICO

3.1 LOS SIETE PILARES DE LA ESTRATEGIA DE CIBERSEGURIDAD DE LA AVIACIÓN

3.1.1 Los elementos documentados en este capítulo se han elaborado con el objetivo de proponer un conjunto de principios, medidas y actividades para alcanzar los objetivos de los siete pilares de la Estrategia de Ciberseguridad de la Aviación, a saber:

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

PILAR 1 - COOPERACIÓN INTERNACIONAL
• Desarrollar la cooperación a nivel nacional e internacional entre todas las partes interesadas. • Hacer un reconocimiento mutuo de los esfuerzos desplegados (desarrollar, mantener y mejorar la ciberseguridad) para proteger la aviación civil. • Procurar la armonización de la reglamentación a nivel mundial, regional y nacional con el objeto de promover la coherencia en todo el mundo y mantener la interoperabilidad de las medidas de protección. • Lograr la participación de los Estados en el mantenimiento de la ciberseguridad en la aviación civil internacional. • Facilitar y promover eventos internacionales sobre ciberseguridad. • Reconocer que la ciberseguridad es una responsabilidad compartida entre todos los segmentos del sistema de aviación civil mundial.

PILAR 2 - GOBERNANZA
• Alentar, apoyar y aprovechar la Estrategia de Ciberseguridad de la OACI. • Establecer un plan nacional claro de gobernanza y rendición de cuentas para la ciberseguridad de la aviación civil. • Disponer la coordinación entre las autoridades de aviación civil y las autoridades nacionales competentes en materia de ciberseguridad. • Establecer los canales apropiados de coordinación entre las diversas autoridades estatales y la industria. • Incluir la ciberseguridad en los programas nacionales de seguridad operacional y seguridad de la aviación civil. • Incluir la ciberseguridad en los planes mundiales y regionales.

- Trabajar en pro de una base de referencia común para las normas y métodos recomendados de ciberseguridad.

PILAR 3 – LEYES Y REGLAMENTOS EFICACES
• Velar por que los instrumentos jurídicos internacionales proporcionen un marco apropiado para la disuasión de incidentes de ciberseguridad, así como para el enjuiciamiento de los responsables de estos incidentes. • Analizar la legislación nacional existente y, de ser necesario, actualizar o adoptar leyes nacionales que permitan la disuasión, la investigación y el enjuiciamiento de ciberataques que afecten la seguridad operacional y la seguridad, eficiencia o continuidad de la aviación civil. • Asegurarse de que existen leyes y reglamentos nacionales apropiados sobre a ciberseguridad de la aviación. • Formular directrices apropiadas para ayudar a los Estados y a la industria a poner en práctica las disposiciones relacionadas con la ciberseguridad.

PILAR 4 - POLÍTICA DE CIBERSEGURIDAD
• Asegurarse de que la ciberseguridad forme parte de los sistemas de seguridad operacional y de seguridad de la aviación civil y de marcos integrales de gestión de riesgos. • Velar por el mantenimiento de la comparabilidad entre las diferentes metodologías de evaluación de riesgos de la ciberseguridad de la aviación civil. • Elaborar políticas de ciberseguridad que tengan en cuenta el ciclo de vida completo de los sistemas de aviación.

PILAR 5 - INTERCAMBIO DE INFORMACIÓN
• Elaborar o fortalecer las plataformas y mecanismos existentes y reconocidos de intercambio de información, en consonancia con las disposiciones actuales de la OACI, para crear conciencia sobre la situación de la ciberseguridad y con ello facilitar la prevención, detección temprana y mitigación de sucesos relevantes de ciberseguridad. • Cuidar de que todo ciberincidente o vulnerabilidad en materia de ciberseguridad que pudiera representar un riesgo importante para la seguridad operacional o la seguridad de la aviación se notifique a la autoridad competente.

PILAR 6 – GESTIÓN DE INCIDENTES Y PLANIFICACIÓN ANTE EMERGENCIAS
• Asegurarse de contar con planes apropiados y adaptables que aseguren la continuidad de unas operaciones de aviación civil seguras en caso de incidentes cibernéticos. • Velar por que se refuercen los planes de contingencia existentes e incluir disposiciones que permitan responder a incidentes de ciberseguridad y recuperarse de estos, así como realizar ejercicios regularmente/periódicamente para comprobar las capacidades para detectar, responder y recuperarse de incidentes cibernéticos.

PILAR 7 - CREACIÓN DE CAPACIDAD, INSTRUCCIÓN Y CULTURA DE CIBERSEGURIDAD
• Garantizar las cualificaciones adecuadas del personal con base en las funciones que han de desempeñar, tanto en aviación como en ciberseguridad. • Aumentar la toma de conciencia sobre la ciberseguridad, lo cual incluye la realización de actividades para establecer una higiene apropiada en materia de ciberseguridad. • Asegurarse de que los planes de estudio del sistema educativo nacional incluyan contenidos de ciberseguridad para que se elabore un corpus transectorial de conocimientos sobre seguridad operacional y seguridad de la aviación en toda la organización, incluida su administración superior. • Fomentar la innovación y la debida investigación y desarrollo en ciberseguridad. • Incluir la ciberseguridad en la Estrategia para la próxima generación de profesionales de la aviación de la OACI.

Capítulo 4

PUESTA EN PRÁCTICA, OBSERVACIÓN, EXAMEN

4.1 PUESTA EN PRÁCTICA

El Plan de Acción de Ciberseguridad (CyAP) está dirigido a la OACI, sus Estados miembros, la industria y otras partes interesadas. Se insta a todos ellos a que adopten sus metas basándose en la hoja de ruta (véase el apéndice A), en la que se indican los resultados prioritarios, las acciones y las tareas relacionadas. Eso ayudará a la OACI, los Estados y otras partes interesadas a concentrarse en la labor destinada a ejecutar acciones y medidas efectivas con el fin de alcanzar el objetivo de elaborar un marco de ciberseguridad de la aviación mundial sólido.

4.2 OBSERVACIÓN Y EXAMEN

La OACI reexaminará el CyAP cuando y como corresponda. Además, proporcionará actualizaciones sobre los avances hacia las metas establecidas y los plazos previstos en el plan. Habrá aspectos en los que los Estados precisen asistencia para la aplicación del plan y la creación de capacidad, y/u otros esfuerzos pertinentes.

4.3 TRABAJO EN ASOCIACIÓN

Todos los interesados de la aviación deben colaborar en la mejora continua de la ciberseguridad de la aviación civil. El CyAP constituye un marco de referencia común para todos que establece las acciones que han de tomar la OACI, sus Estados miembros y la industria para crear un marco de ciberseguridad común.

4.4 FUNCIÓN DE LA OACI, LOS ESTADOS Y LAS PARTES INTERESADAS

4.4.1 La OACI desempeñará una importante función de liderazgo y supervisión a escala mundial en la aplicación y coordinación del CyAP, que incluye en particular las siguientes tareas:

- Actualizar el CyAP cuando sea necesario.
- Elaborar y mantener al día las normas y métodos recomendados (SARP) y los procedimientos para los servicios de navegación aérea (PANS), complementados con manuales y otros textos de orientación.
- Vigilar y examinar el panorama de amenazas y riesgos a la ciberseguridad.
- Proporcionar asistencia específica para resolver deficiencias en el ámbito de la ciberseguridad de la aviación civil.

4.4.2 Los Estados y la industria también tienen una importante función que desempeñar en la aplicación y la eficacia del CyAP. Se alienta a los Estados y a las partes interesadas a demostrar su progreso año tras año en la aplicación del Plan.

Capítulo 5

COOPERACIÓN INTERNACIONAL

5.1 ELABORACIÓN DE UN INVENTARIO DE INICIATIVAS DE CIBERSEGURIDAD DE LA AVIACIÓN

5.1.1 Se elaborará un inventario de iniciativas de ciberseguridad, que se mantendrá al día y se pondrá a disposición en el portal de la OACI para el público apropiado. En el inventario se compilarán las iniciativas de ciberseguridad de la aviación civil mundiales, regionales o nacionales. Para el inventario no solo se tendrán en cuenta las iniciativas de ciberseguridad de la aviación, sino también aquellas cuyos resultados sean relevantes para la aviación civil (p. ej., la ciberseguridad en otros ámbitos de transporte u otros sectores como la energía, las finanzas).

5.2 ESTABLECIMIENTO DE UNA BASE COMÚN PARA LA INTEROPERABILIDAD DE LAS MEDIDAS DE CIBERSEGURIDAD Y LOS SISTEMAS DE GESTIÓN[2]

5.2.1 Los Estados y la industria deberían implantar los principios y las herramientas/sistemas apropiados para garantizar la gestión uniforme, segura e interoperable de los sistemas de tecnología de la información/comunicaciones.

5.2.2 Como la confianza es la base de toda gestión eficaz, uniforme e interoperable de los intercambios de información, debería apoyarse la creación del Marco de Confianza para la Aviación Internacional para facilitar la gestión de la información y la interoperabilidad; además, y en la medida de lo posible, todas las partes interesadas deberían facilitar la adopción de políticas y procedimientos.

5.2.3 La interoperabilidad de las medidas de ciberseguridad y su gestión también pueden lograrse mediante la participación en diversas formas de acuerdos de cooperación internacional. Debería elaborarse un modelo para tales acuerdos a fin de posibilitar la cooperación, respetando a la vez las políticas de privacidad, seguridad de la información y seguridad nacional aplicables. A tal respecto, es necesario determinar los siguientes aspectos como base para los modelos de acuerdo:

- el tema y el objetivo del acuerdo;
- las entidades que podrían celebrar tales acuerdos;
- las funciones y responsabilidades de dichas entidades; y
- las medidas que podrían utilizarse para mejorar la ciberseguridad de la aviación civil y que deben ser coordinadas.

[2] En este contexto, los sistemas de gestión comprenden, sin carácter restrictivo, los sistemas de gestión de riesgos.

5.2.4 La finalidad de los acuerdos internacionales debería ser:

- establecer un diálogo entre las partes interesadas en busca de medios para reducir los riesgos colectivos y proteger las infraestructuras de aviación civil nacionales e internacionales;
- adoptar medidas de reducción y mitigación de riesgos para hacer frente a las amenazas de ciberseguridad de la aviación civil;
- intercambiar información sobre leyes nacionales de aviación civil, estrategias, políticas y mejores prácticas nacionales relativas a la ciberseguridad; y
- tomar medidas para contribuir a la creación de capacidad sobre ciberseguridad donde sea necesario.

5.2.5 En un contexto en el que los modelos y principios metodológicos de las partes interesadas de la aviación pueden ser múltiples, y el vocabulario diferente, es fundamental establecer un léxico y un marco de entendimiento comunes, específicamente en relación con la ciberseguridad de la aviación civil. En ese sentido, la OACI deberá seguir desarrollando un conjunto general de principios para la gestión apropiada, global y coordinada de los riesgos de ciberseguridad, en estrecha cooperación con los Estados miembros y la industria. Se llevará a cabo un análisis del marco existente con el fin de determinar cuál es la mejor forma de lograr una alineación sin fisuras y eficaz de estos principios y modelos.

5.3 ESTABLECIMIENTO DE UNA TERMINOLOGÍA COMÚN

5.3.1 Bajo los auspicios de la OACI se establecerá una terminología común sobre la ciberseguridad de la aviación civil, teniendo presente la terminología y los marcos existentes en materia de ciberseguridad y aviación para que todas las partes interesadas de la aviación, con independencia de su formación y actividades, puedan entenderse mutuamente.

5.3.2 El objetivo es facilitar las actividades relacionadas con la ciberseguridad. Eso no significa que se establecerá y/o acordará una sola definición para todos los términos. Es aceptable que existan varias definiciones para el mismo término (p. ej., probabilidad, gravedad, frecuencia etc.), siempre que sean específicas de un contexto dado y que esa repetición no genere una confusión que pueda interferir con la gestión eficaz de los riesgos de ciberseguridad de la aviación. Más concretamente, en una época en la que se hace mayor hincapié en la gestión integrada de los riesgos de seguridad operacional y seguridad de la aviación, la OACI debe prestar mucha atención a que la terminología esté alineada correctamente. Recordando la declaración del contexto mencionada anteriormente, y la aclaración para distinguir entre la seguridad de la aviación que se refiere a la gestión de los actos ilícitos e intencionales y la seguridad operacional que se refiere a los peligros intencionales, no intencionales y aleatorios, es preciso afinar más en cuanto a las cuestiones de gestión integrada de los riesgos, que pueden abarcar tanto preocupaciones de seguridad de la aviación como de seguridad operacional (pueden utilizarse las definiciones del Anexo 17 y del Anexo 19 como base de referencia). Concretamente, dados los objetivos diferentes de las disciplinas de seguridad operacional y de seguridad de la aviación (estando la seguridad operacional centrada en los peligros intencionales, no intencionales y aleatorios y la seguridad de la aviación en los actos ilícitos e intencionales), la introducción de la gestión integrada de los riesgos que se extienden a ambas disciplinas requiere una claridad de alcance y propósito de los términos utilizados.

5.4 ELABORACIÓN DE UN MAPA GENÉRICO DE INTERCAMBIO DE INFORMACIÓN/INTERACCIONES EN LA AVIACIÓN

5.4.1 Como requisito previo para entender el panorama de ciberriesgos, es necesario contar con un marco común para establecer mapas funcionales de alto nivel que describan los intercambios de información entre todos los actores de la aviación. Se necesita un marco común que permita establecer las correspondencias de alto nivel en los intercambios de información entre todas las partes interesadas de la aviación a fin de poder entender el panorama de los ciberriesgos.

5.4.2 Este mapa de alto nivel con los intercambios de información/interacciones debería ser lo suficientemente genérico para abarcar todo tipo de operaciones relacionadas con la aviación y, en la medida de lo posible, ser independiente de las estructuras físicas y/o técnicas en servicio (enfoque funcional/de servicios). Por ejemplo, el mapa de alto nivel debería abarcar los flujos de datos digitales para la gestión del tránsito aéreo vinculada a las actividades aeroportuarias y los flujos de datos digitales para las operaciones de las aeronaves en vuelo/mantenimiento. Este mapa debería aprovechar todas las iniciativas existentes que ya hayan puesto en marcha otros grupos. La finalidad es que cada una de las partes interesadas pueda completar/adaptar/personalizar su propio mapa de cómo interactúa con las demás. En última instancia, cada parte interesada debería ser capaz de desarrollar o adaptar este mapa a su propia situación particular. Así, los resultados de las evaluaciones de riesgos de seguridad realizadas por cada actor aplicando sus propios métodos y criterios (que pueden compararse gracias a un marco común de evaluación de riesgos – véase la sección 5.6) podrían, en la medida de lo posible, intercambiarse/compartirse con otras partes interesadas. Trabajando conjuntamente, usando marcos comparables de evaluación de riesgos de seguridad y el mapa de los intercambios de información/interacciones, las partes interesadas podrán entender cómo pueden propagarse los riesgos o ser gestionados por otros intervinientes que comparten ese mismo riesgo, o cómo este puede gestionarlo y así permitir el intercambio de información sobre los riesgos corridos o provocados por cada parte interesada.

5.5 INTERCAMBIO INTERINSTITUCIONAL DE INFORMACIÓN SOBRE EL RIESGO

5.5.1 Existen numerosas normas y documentos de orientación en los que se aborda la responsabilidad que cada organización tiene de gestionar su propia ciberseguridad cuando se trata de sus productos, datos, procesos y sistemas internos. No obstante, dado que los riesgos de ciberseguridad para la aviación civil se comparten entre múltiples partes interesadas, es necesario tener una visión que vaya más allá de cada organización en particular. Para lograr una gestión eficaz y eficiente de los riesgos compartidos, debe hacerse hincapié en el intercambio de información sobre el riesgo, que es una condición necesaria cuando se comparten sistemas, procesos, productos o datos, o se pasan de una organización a otra.

5.5.2 Debería estudiarse la posibilidad de concertar acuerdos externos con terceros proveedores a fin de permitir el intercambio de información sensible sobre ciberseguridad entre una organización y las autoridades/el ente normativo pertinente con la finalidad de facilitar la gestión de los riesgos y amenazas a la cadena de suministro.

5.6 ESTABLECIMIENTO DE CRITERIOS DE COMPARABILIDAD DE LAS POSTURAS DE EVALUACIÓN DE RIESGOS

5.6.1 En un contexto en el que los riesgos se extienden a múltiples organizaciones, es esencial que las partes interesadas puedan entender los riesgos de extremo a extremo y el interés de las demás partes interesadas en cuanto a la gestión de esos riesgos. Además, este tipo de contexto requiere que se establezcan criterios para facilitar la comprensión y la comparabilidad de las evaluaciones de riesgos de ciberseguridad.

5.7 ESTABLECIMIENTO DE UNA COORDINACIÓN CÍVICO-MILITAR APROPIADA

5.7.1 Cuando sea posible y compatible con las leyes nacionales, incluidos los requisitos de seguridad y defensa nacionales, las autoridades competentes de la aviación civil y militar deberían definir capacidades y procesos para cooperar en materia de asuntos relacionados con la ciberseguridad de la aviación.

5.7.2 El establecimiento de una coordinación e intercambio apropiados de información sobre ciberseguridad entre las partes interesadas de la aviación civil y militar desde una etapa temprana puede resultar sumamente útil para identificar posibles amenazas y riesgos cibernéticos, contribuyendo así a mitigar con éxito los ciberriesgos para el sistema de aviación.

5.7.3 El intercambio de información entre las partes interesadas de la aviación civil y militar también es importante para la gestión de las crisis relacionadas con la ciberseguridad. Los Estados pueden ofrecer apoyo a sus partes interesadas de la aviación civil y militar para organizar un arreglo que, en la medida de lo posible, facilite el intercambio de información por medio de los mecanismos apropiados.

5.8 PROMOCIÓN DE EVENTOS MUNDIALES Y REGIONALES RELACIONADOS CON LA CIBERSEGURIDAD DE LA AVIACIÓN CIVIL

5.8.1 La OACI apoyará y planificará la organización de eventos mundiales y regionales que promuevan la ciberseguridad de la aviación civil, según proceda.

Capítulo 6

GOBERNANZA

6.1 ESTABLECIMIENTO DE UNA ESTRUCTURA DE GOBERNANZA

6.1.1 La OACI debería establecer una estructura de gobernanza interna para la ciberseguridad de la aviación que garantice la adopción de un enfoque holístico, transversal y basado en los riesgos frente a la ciberseguridad y la ciberresiliencia en todos los ámbitos y áreas de especialidad de la aviación pertinentes.

6.1.2 Además, los Estados deberían definir y poner en práctica estructuras nacionales de gobernanza y rendición de cuentas para la ciberseguridad de la aviación civil, y velar por la formulación e implantación de requisitos nacionales e internacionales relativos a la ciberseguridad y la ciberresiliencia, así como definir las funciones y responsabilidades de cada parte interesada a nivel nacional. Estas acciones deberían tener en cuenta la necesidad de coordinar entre las autoridades nacionales competentes en materia de aviación civil y ciberseguridad.

6.2 ELABORACIÓN DE UNO O MÁS PLANES PLURIANUALES DE CIBERSEGURIDAD

6.2.1 Se recomienda que el Plan de Acción de Ciberseguridad (CyAP) esté debidamente alineado con el Plan Global para la Seguridad de la Aviación (GASeP), el Plan Mundial de Navegación Aérea (GANP) y el Plan Global para la Seguridad Operacional de la Aviación (GASP). En esos planes deberían incluirse y promoverse aspectos relacionados con la ciberseguridad, según proceda.

6.2.2 A fin de asegurar la debida ejecución y aplicación de los planes mundiales a nivel nacional, se insta a los Estados a incluir acciones de ciberseguridad coordinadas a nivel nacional en sus programas nacionales de seguridad operacional y seguridad de la aviación, así como en sus planes de navegación aérea.

6.3 DESARROLLO DE LA GOBERNANZA Y LA RENDICIÓN DE CUENTAS

6.3.1 La OACI debería elaborar unas orientaciones normativas de ciberseguridad para facilitar la armonización y la coherencia entre las políticas mundiales, regionales y nacionales sobre ciberseguridad.

6.3.2 La gobernanza de la ciberseguridad debería estar impulsada por las políticas y hacerse cumplir en función de estas, y debe determinarse la rendición de cuentas para garantizar su cumplimiento.

6.3.3 Los Estados deberían tomar medidas tangibles para mejorar constantemente la eficacia, calidad y coherencia de los procesos de gestión de la ciberseguridad a nivel nacional.

6.3.4 Si se justifica, los sistemas de gestión de la seguridad de la información (ISMS) pueden ser herramientas eficaces para gestionar la ciberseguridad, y pueden implantarse a nivel de Estado o de organización[3].

[3] Para definir la gobernanza de la ciberseguridad a nivel nacional, los Estados pueden inspirarse en la norma ISO 27001 para establecer los principios de liderazgo, como, por ejemplo: asegurarse de que los requisitos del sistema de gestión de la seguridad de la información se integren en los procesos de la organización; cuidar de que los recursos necesarios estén disponibles; y velar por que el sistema de gestión de la seguridad de la información alcance los resultados esperados.

Capítulo 7

LEGISLACIÓN Y MARCO REGLAMENTARIO EFICACES

7.1 EXAMEN DE LOS INSTRUMENTOS DE DERECHO AERONÁUTICO VIGENTES RELACIONADOS CON EL ÁMBITO DE LA CIBERSEGURIDAD

7.1.1 La OACI llevará a cabo un análisis de los instrumentos de derecho aeronáutico internacional con el fin de determinar cuáles son las carencias existentes y potenciales en relación con los riesgos cibernéticos y proponer posibles soluciones para colmar las carencias detectadas, de haberlas, con la finalidad de proteger aún más la aviación civil.

7.2 ALINEAMIENTO DE LAS DISPOSICIONES DE LA OACI CON LAS NECESIDADES DE CIBERSEGURIDAD

7.2.1 A medida que la ciberseguridad en la aviación vaya madurando, puede resultar necesario elaborar disposiciones para complementar o suplementar las SARPS y los PANS existentes. Esto debería hacerse caso por caso, teniendo en cuenta que, en la medida de lo posible, debería evitarse añadir nuevas disposiciones a los SARPS o los PANS y, cuando sea necesario, coordinarse entre todas las partes interesadas pertinentes.

7.3 RATIFICACIÓN DEL CONVENIO Y EL PROTOCOLO DE BEIJING

7.3.1 Se alienta a los Estados a ratificar el *Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional* (Convenio de Beijing, 2010) y el *Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves* (Protocolo de Beijing, 2010).

7.4 LOS ESTADOS DEBEN FORMULAR Y APLICAR LAS LEYES Y REGLAMENTOS NACIONALES PERTINENTES

7.4.1 Se alienta a los Estados a evaluar su marco jurídico nacional vigente en el ámbito de la ciberseguridad y de la aviación civil con el fin de detectar carencias y cerciorarse de que existan la legislación y los reglamentos apropiados sobre elementos específicos de la ciberseguridad de la aviación civil. Otro componente clave, que se alienta a los Estados a implantar si no existe ya en sus marcos jurídicos nacionales, es el mecanismo judicial para que los actos ilícitos cometidos contra la aviación civil por medios cibernéticos estén tipificados como delito y sean pasibles de enjuiciamiento.

Capítulo 8

POLÍTICA DE CIBERSEGURIDAD

8.1 ELABORACIÓN Y APLICACIÓN DE LAS POLÍTICAS DE CIBERSEGURIDAD

8.1.1 Una política de ciberseguridad tiene que formularse a nivel nacional y de cada organización. Los Estados deberían disponer de una política de ciberseguridad clara y concreta, que incluya:

- objetivos derivados de los resultados de las evaluaciones de los riesgos de ciberseguridad de la aviación civil;
- el compromiso de satisfacer los requisitos aplicables y la forma de evaluar el cumplimiento;
- consideraciones relativas a la gestión y a la coordinación con partes dependientes externas (véase el capítulo sobre cooperación internacional);
- el compromiso con la mejora continua del marco de ciberseguridad;
- disposiciones para que la política esté plenamente documentada y disponible en forma de información oficial; y
- disposiciones para que la política se divulgue adecuadamente.

8.2 IDENTIFICACIÓN Y EVALUACIÓN DE LOS CIBERRIESGOS PARA LA AVIACIÓN CIVIL

8.2.1 Una de las dificultades que plantean las actividades de identificación y evaluación de riesgos es la capacidad de anticipar los rápidos cambios de los orígenes y las características de las amenazas. La anticipación de las amenazas cambiantes es clave para ayudar a que el sistema de transporte aéreo adapte de forma proactiva su estrategia de protección, no solo en función de las amenazas actuales sino también en vista de las posibles amenazas futuras. Gracias a la anticipación, el sector de la aviación civil debería ser más proactivo en un contexto en el que existe una asimetría entre la habilidad de los atacantes, que son muy ágiles y con gran capacidad de adaptación, y quienes se defienden de los ataques, que tardan en reaccionar debido a la complejidad del sistema que deben proteger. En tal contexto, el enfoque proactivo cobra una importancia todavía más crítica. Así pues, para mitigar los riesgos es preciso elaborar un marco de identificación y evaluación de riesgos de ciberseguridad que satisfaga esta necesidad.

8.2.2 Se recomienda que los riesgos de ciberseguridad se identifiquen y evalúen teniendo en cuenta todas las consecuencias posibles de un ataque al sistema de aviación civil (protección, seguridad, eficiencia, resiliencia, continuidad del servicio, etc.), así como las posibles fuentes de las amenazas y las vulnerabilidades que existen frente a estas. Para ello, convendría aprovechar las matrices de ciberriesgos que se elaboraron bajo los auspicios del Grupo de Trabajo sobre Amenazas y Riesgos (WGTR) del Grupo Experto en Seguridad de la Aviación.

8.2.3 Dado que numerosas partes interesadas comparten una proporción significativa de los riesgos de ciberseguridad de la aviación civil, se recomienda que se considere hacer mapas de los intercambios de información/interacciones en la aviación (véase el capítulo 5.1). Estos mapas deberían utilizarse como medio para garantizar la exhaustividad de las hipótesis examinadas y para que las diferentes partes interesadas puedan entender cómo interactúan entre ellas y cuál es su dependencia del riesgo.

8.2.4 Puesto que el nivel de gravedad de los ciberriesgos variará con el tiempo (y, en comparación con riesgos de otro tipo, estos pueden evolucionar más rápidamente), se recomienda buscar un medio para adaptar cualquier respuesta de la aviación mundial a estos riesgos que pueda desplegarse de forma rápida y coherente (p. ej., estableciendo un equilibrio entre la necesidad de normas de aviación, textos de orientación, mejores prácticas provenientes de fuera de la aviación, y usando /recurriendo a respuestas de otros ámbitos).

8.2.5 Se recomienda que la identificación y evaluación de los riesgos de ciberseguridad las realice y coordine enteramente un grupo experto en ciberseguridad de la aviación civil o, en su defecto, un equipo experto en cibernética y en aviación civil, de preferencia con una amplia experiencia en ciberseguridad.

8.2.6 Este grupo experto debería encargarse de la elaboración de una Declaración sobre el contexto de riesgos para la ciberseguridad mundial.

Capítulo 9

INTERCAMBIO DE INFORMACIÓN

El intercambio de información sobre la ciberseguridad es esencial para la gestión de los riesgos de ciberseguridad que enfrentan los sistemas de aviación civil. Reconociendo que fomentar el intercambio de información es fundamental para crear una cultura de ciberseguridad, las partes interesadas en la aviación civil deberían elaborar programas o reforzar aquellos existentes que permitan compartir la información dentro de sus organizaciones y, en la medida de lo posible, con partes externas. Por medio de esos programas, deberían crear asociaciones y compartir información sustantiva con otras partes interesadas que poseen y gestionan infraestructura de la aviación civil, y elaborar planes y prácticas de intercambio de información dentro de sus organizaciones.

Estos programas de intercambio de información deberían permitir el desarrollo, el funcionamiento y el ajuste de ciberdefensas de la aviación civil frente a ciberamenazas conocidas y emergentes. Los programas deberían contribuir a:

- la conciencia de la situación tanto en las operaciones cotidianas normales como durante una crisis, incidente o suceso;
- la gestión operacional y táctica de los riesgos en previsión y respuesta a una amenaza;
- la planificación estratégica para crear capacidades que fortalezcan la ciberseguridad y la resiliencia para el futuro.

9.1 DESARROLLO DEL INTERCAMBIO DE INFORMACIÓN SOBRE RIESGOS

9.1.1 El intercambio de ciberinformación tiene dimensiones bilaterales y multilaterales, y en ese proceso de produce toda combinación entre las siguientes partes (a escala nacional, regional y mundial):

- las autoridades nacionales de cibernética;
- las autoridades nacionales de aviación civil;
- las autoridades nacionales de aviación militar;
- otras partes interesadas de la aviación (explotadores, proveedores de servicios y fabricantes); y
- las partes interesadas de otros sectores (cadena de suministro y proveedores de tecnologías de la información y de servicios de comunicaciones).

9.1.2 Se reconoce que hay muchos tipos de información sobre ciberseguridad, tales como los siguientes:

- *Ciberinteligencia* (como el cuadro de amenazas, información sobre la capacidad e intención de los actores causantes de las amenazas).
- *Indicadores de comprometimiento (IoC).*
- *Tácticas, técnicas y procedimientos (TTP)* – (como hipótesis de ataque y métodos preferidos de los intrusos cibernéticos).
- *Vulnerabilidades* (como equipo informático, programa informático, servicio, protocolo, norma, etc.), incluidas posibles hipótesis aprovechamiento de la vulnerabilidad.
- *Informes de incidentes.*

9.1.3 En función de la legislación nacional y de la naturaleza de la ciberinformación, podría haber diversos métodos y limitaciones para compartir la información con varios receptores (p. ej., la autoridad nacional en asuntos cibernéticos, la autoridad nacional de aviación civil, la autoridad nacional de aviación militar y otras partes interesadas de la aviación).

9.1.4 Las políticas y necesidades de intercambio de información y de colaboración (en particular, aunque no exclusivamente, en épocas de crisis) deberían determinarse a nivel mundial, regional y nacional.

9.1.5 Se recomienda usar el Protocolo del Semáforo (TLP) [4] para indicar el nivel de difusión/restricciones al distribuir y continuar intercambiando ciberinformación.

9.1.6 En la medida de lo posible, la ciberinformación que pueda contener cierta información sensible debería anonimizarse o expurgarse antes de compartirla en lugar de optar por no compartirla.

9.2 ELABORACIÓN DE PRINCIPIOS Y ORIENTACIÓN PARA LA DIVULGACIÓN RESPONSABLE DE INFORMACIÓN POR PARTE DE LOS INVESTIGADORES DE SEGURIDAD DE LA AVIACIÓN

9.2.1 Dado el creciente interés de la comunidad investigadora por la ciberseguridad de la aviación civil, y a fin de evitar la divulgación irresponsable de posibles conclusiones que podría resultar perjudicial para la seguridad, protección, eficiencia o continuidad de la aviación civil, es preciso establecer principios para la divulgación responsable de las vulnerabilidades que descubran las investigadoras e investigadores de seguridad de la aviación, o terceras partes, a fin de evitar que la divulgación resulte perjudicial para la ciberseguridad de la aviación civil. Para ello, debería tomarse en consideración la recomendación 4.4 de la Estrategia de ciberseguridad.

9.2.2 Debería establecerse una orientación para estos principios (que trate, entre otras cuestiones, del descubrimiento, la notificación del fabricante, la investigación, la notificación de la industria, la resolución y, por último, la divulgación) entre investigadoras/es y terceras partes por un lado y, por otro, las autoridades de aviación civil y las partes interesadas de la aviación para velar por que, en la medida de lo posible, esas actividades de investigación/descubrimiento y divulgación de vulnerabilidades no tengan repercusiones en la seguridad operacional y la prestación de servicios. Idealmente, en esa orientación no solo deberían abordarse los procesos de divulgación responsable, sino que habría que incluir además elementos educativos y de sensibilización.

9.3 ELABORACIÓN DE UNA RED MUNDIAL DE AUTORIDADES REGIONALES/ NACIONALES DE CIBERNÉTICA PARA LOS FINES DE LA AVIACIÓN CIVIL

9.3.1 En los Estados y la industria, la responsabilidad por la ciberseguridad no está asignada de manera uniforme, y los conocimientos especializados pertinentes están distribuidos entre un amplio abanico de partes interesadas vinculadas o no a la aviación, así como entre un conjunto de esferas funcionales. La dificultad inherente de esta diversidad es que crea dificultades para saber cuál es el punto de contacto sobre ciberseguridad dentro de una entidad, y para establecer y mantener unos canales de comunicación formalizados entre las partes interesadas. La orientación sobre cómo establecer y mantener un único punto de contacto para las cuestiones relacionadas con la ciberseguridad de la aviación civil en los Estados y las organizaciones puede facilitar el establecimiento de canales de comunicación mundiales, regionales y nacionales, la creación de las comunidades apropiadas de expertos en ciberseguridad e impulsar la cultura de la ciberseguridad.

[4] Véase el texto de orientación de la OACI en “Orientación sobre el protocolo del semáforo”.

9.4 CAPACIDADES MUNDIALES DE INTERCAMBIO DE INFORMACIÓN SOBRE CIBERSEGURIDAD PARA LA AVIACIÓN

9.4.1 Pueden desarrollarse capacidades de intercambio de información relacionada con la aviación civil de forma transversal a escala mundial, regional y/o nacional a fin de fomentar el intercambio de la información sobre ciberseguridad.

9.4.2 Los foros de intercambio de información pueden ser estructuras público-públicas, público-privadas y privado-privadas. Las partes interesadas deberían participar en comunidades fiables para facilitar el intercambio de mejores prácticas e inteligencia sobre amenazas.

Capítulo 10

GESTIÓN DE INCIDENTES Y PLANIFICACIÓN ANTE EMERGENCIAS

10.1 DESARROLLO DE CAPACIDADES DE RESPUESTA A INCIDENTES Y PLANIFICACIÓN DE LA RESPUESTA ANTE EMERGENCIAS

10.1.1 Se alienta enfáticamente a todas las partes interesadas a elaborar y ensayar planes de emergencia y de respuesta a incidentes de forma coordinada con sus asociados operacionales, lo que incluye:

- utilizar los planes de contingencia que ya existen y/o modificarlos incorporando disposiciones relativas a la ciberseguridad;
- las partes interesadas de la aviación civil deberían elaborar y mantener una variabilidad de escala apropiada que proporcione seguridad operacional, protección y continuidad de las operaciones del transporte aéreo durante posibles incidentes cibernéticos;
- elaborar disposiciones relativas a la respuesta a incidentes de ciberseguridad y a la capacidad de recuperación posterior, incluidos los planes de respuesta a contingencias y emergencias;
- lograr la participación de las partes interesadas de la aviación militar en el proceso de planificación para establecer líneas de comunicación de forma proactiva;
- alcanzar unos niveles aceptables de desempeño y satisfacer el requisito de mantener los niveles mínimos de servicios esenciales;
- formular una categorización armonizada para la notificación de ciberincidentes, y coordinar los esquemas de notificación de incidentes de ciberseguridad en la aviación civil a nivel nacional y regional y, cuando corresponda, a nivel internacional; y
- las partes interesadas de la aviación deberían realizar ejercicios periódicos reales para verificar la validez de los supuestos formulados durante la planificación y los ejercicios teóricos.

10.2 MEDIOS DE LAS PARTES INTERESADAS PARA LA DETECCIÓN, ANÁLISIS Y RESPUESTA ANTE INCIDENTES

10.2.1 En la medida de lo posible, deberían implementarse planes de respuesta a incidentes y las partes interesadas deberían desarrollar las capacidades necesarias para detectar y analizar incidentes de ciberseguridad, y darles respuesta, a todos los niveles. Es importante vigilar las condiciones de ciberseguridad de los sistemas/servicios que se consideran críticos para sostener la aviación civil con el fin de detectar posibles problemas y de hacer un seguimiento de la eficacia de las medidas de protección de la seguridad. Los incidentes de ciberseguridad, una vez detectados, deberían analizarse y activarse los planes de respuesta apropiados; esos planes deberían incluir medidas de mitigación para limitar los efectos del incidente de ciberseguridad.

10.3 CREACIÓN DE UNA CÉLULA DE COORDINACIÓN DE CRISIS PARA LA CIBERSEGURIDAD DE LA AVIACIÓN CIVIL

10.3.1 Cuando sea posible, debería instaurarse (sobre la base de los mecanismos ya existentes) una célula de coordinación de crisis de la aviación civil que cuente con expertos en ciberseguridad de la aviación civil y, cuando proceda, con partes interesadas en la aviación militar.

10.3.2 Deberían efectuarse ejercicios periódicamente, en particular ejercicios teóricos, con la participación de todas las partes interesadas relevantes de la industria, cuando se estime pertinente.

Capítulo 11

CREACIÓN DE CAPACIDAD, INSTRUCCIÓN Y CULTURA Y MATERIAL DIDÁCTICO SOBRE CIBERSEGURIDAD

11.1 DESARROLLO DE CAPACIDAD TÉCNICA, INSTRUCCIÓN Y CULTURA Y MATERIAL DIDÁCTICO SOBRE CIBERSEGURIDAD

11.1.1 Deberían definirse una educación, instrucción y sensibilización en ciberseguridad de la aviación civil y promoverse a nivel mundial, regional y nacional.

11.1.2 La cultura y las actividades educativas en materia de ciberseguridad deberían promoverse desde la administración superior en todas las organizaciones de aviación civil, y deberían destacarse las funciones principales de los diferentes intervinientes y sus expectativas. Esto debería llevar al desarrollo de un corpus de conocimientos cruzados sobre seguridad operacional y seguridad de la aviación en el ámbito de la ciberseguridad y debería incluir los siguientes elementos:

- nociones de principios seguros por diseño para mitigar las ciberamenazas en coordinación con la comunidad de la seguridad operacional de la aviación. Las nociones deberían ayudar a esa comunidad a tomar decisiones mejor fundamentadas a la hora de hacer frente a las ciberamenazas;
- un enfoque coordinado entre las partes interesadas en la seguridad operacional y la seguridad de la aviación, reconociéndose que los controles de seguridad no deben tener repercusiones negativas en la seguridad del vuelo, permitiendo la transferencia de conocimientos técnicos, y que se tomen decisiones con conocimiento de causa basadas en un panorama mutuamente entendido de los riesgos;
- nociones de prácticas de ciberhigiene para el personal operacional y de apoyo, que deberían ayudar a prevenir los posibles efectos adversos en el sistema de aviación civil causados por el creciente número de productos adquiridos en comercios y programas dañinos no específicos; y
- nociones de "cultura justa" procedentes de la comunidad de la seguridad operacional que favorezcan y estimulen la denuncia espontánea de sucesos resultantes de un comportamiento imprevisto del personal (p. ej., negligencia no intencionada en el manejo de una memoria USB).

11.1.3 Al realizar estas actividades, debería hacerse hincapié en las repercusiones o posibles repercusiones.

11.1.4 El desarrollo de esta cultura de la ciberseguridad y la promoción de la cultura y el material didáctico sobre ciberseguridad debería contribuir a que las comunidades de la seguridad operacional y de la seguridad de la aviación comprendan de la misma manera el panorama de riesgos de ciberseguridad y confíen mutuamente en las contramedidas que se estén poniendo en marcha.

11.1.5 La OACI debería propiciar los programas de intercambio transnacionales/transregionales de educación e instrucción en ciberseguridad[5].

[5] Por ejemplo, las iniciativas para la instauración de campus multinacionales o de redes y centros de competencia en ciberseguridad de la Unión Europea.

11.1.6 La cultura y las actividades educativas relativas a la ciberseguridad no deberían centrarse únicamente en el funcionamiento de los sistemas, sino más bien en su ciclo de vida completo, a saber:

- requisito (la ciberseguridad como parte ya integrada en la fase de requisitos);
- diseño (seguir una estrategia de seguridad por diseño, seguridad de los equipos, programas y datos informáticos, gestión del cambio, gestión de la vulnerabilidad);
- desarrollo (entorno seguro, ensayos de seguridad continuos e integrados);
- fabricación/adquisición (incluida la cadena de suministro de equipos y programas informáticos de las tecnologías operacionales y de información);
- funcionamiento (incluidos la gestión del acceso, la integridad de los datos y el funcionamiento seguro de los sistemas);
- mantenimiento (incluidos los parches y la estrategia de actualización); y
- eliminación (incluida la gestión de credenciales y los datos residuales en dispositivos de almacenamiento de datos).

Capítulo 12

CONCLUSIÓN

El Plan de Acción de Ciberseguridad reúne a la OACI, los Estados, la industria y otras partes interesadas para que hagan frente, de manera holística y coordinada, a los retos actuales y emergentes de la ciberseguridad. Además, pone de relieve el hecho de que la ciberseguridad es una cuestión transversal que abarca todos los ámbitos del sector de la aviación. El plan ayuda a aplicar la Estrategia de Ciberseguridad de la Aviación de la OACI y avanzar hacia la creación de un marco de ciberseguridad mundial sólido.

— — — — — — — —

APÉNDICE A

Hoja de ruta del Plan de acción de ciberseguridad

ACCIONES GENERALES DE LA ESTRATEGIA DE CIBERSEGURIDAD

Resultado prioritario		**ESTABLECER UNA VISIÓN GLOBAL Y CONSENSUADA**			
Acciones prioritarias		• Reconocer que es imperativo establecer una visión global y consensuada de la ciberseguridad como fundamento de una gestión sólida y coordinada de los riesgos de ciberseguridad en la aviación mundial; • Reconocer que el sector de la aviación civil será resiliente a los ciberataques y seguirá siendo seguro y fiable a escala mundial, al tiempo que continúa innovando y creciendo; • Reconocer que los riesgos de ciberseguridad de la aviación civil han de ser abordados dentro del ámbito del Convenio sobre Aviación Civil Internacional.			
Acciones					
Acción núm.	**A cargo de**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 0.1	OACI, Estados miembros e industria	La OACI redactará un modelo de política de ciberseguridad que ha de servir de referencia para los Estados miembros y la industria al momento de elaborar sus propias políticas nacionales/organizacionales.	Modelo disponible para los Estados miembros y la industria.	Alta	2021
CyAP 0.2	OACI y Estados miembros	Comenzar la labor de aplicación de la Estrategia de Ciberseguridad de la Aviación de la OACI a nivel nacional (tal como se indica en la Resolución A40-10) (Para poder comprobar cómo los Estados ejecutan la estrategia, es necesario establecer un conjunto de parámetros que permitan evaluar el grado de ejecución de determinadas acciones).	Pruebas del comienzo de la labor de aplicación a nivel nacional.	Alta	2023

CyAP 0.3	OACI	Realizar encuestas para establecer de qué manera han aplicado los Estados la Estrategia de Ciberseguridad de la Aviación de la OACI (encuesta para preguntar si los Estados han elaborado un plan de acción para aplicar la estrategia).	Encuesta/cuestionario de la OACI enviado a los Estados miembros.	Alta	2021-2022

PILARES DE LA ESTRATEGIA DE CIBERSEGURIDAD

Resultado prioritario	**1. LOGRAR LA COOPERACIÓN INTERNACIONAL**
Acciones prioritarias	• Desarrollar la cooperación a nivel nacional, regional e internacional entre todas las partes interesadas. • Reconocer mutuamente los esfuerzos desplegados (desarrollar, mantener y mejorar la ciberseguridad) para proteger la aviación civil. • Procurar la armonización de la reglamentación de la ciberseguridad a nivel internacional, regional y nacional con el objeto de promover la coherencia en todo el mundo y velar por la interoperabilidad de las medidas de protección. • Lograr la participación de los Estados en el mantenimiento de la ciberseguridad en la aviación civil internacional. • Facilitar y promover eventos internacionales en el ámbito de la ciberseguridad. • Reconocer que la ciberseguridad es una responsabilidad compartida entre todos los segmentos del sistema de aviación civil mundial.

Acciones

Acción núm.	**A cargo de**	**Trazabilidad a la Estrategia de Ciberseguridad de la Aviación**	**Trazabilidad en el capítulo 5**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 1.1	OACI y Estados miembros	1.1	5.2	Incluir la ciberseguridad en los programas de vigilancia de la seguridad operacional y la seguridad de la aviación de la OACI – incluir las normas pertinentes en los programas de auditoría de la OACI (tales como USOAP y USAP).	Los programas de auditoría de la OACI tanto desde la perspectiva de la seguridad operacional como de la seguridad de la aviación incluyen normas relativas a la ciberseguridad.	Alta	En curso

CyAP 1.2	OACI	1.1	5.1 Véase también el CyAP 4.6 (párrafo 8.2 del Plan de Acción)	Realizar encuestas sobre las iniciativas/prácticas de ciberseguridad a fin de determinar de qué manera están gestionando los Estados y la industria la ciberseguridad en la aviación civil.	Resultados de los cuestionarios, número de iniciativas y regiones.	Alta	En curso
CyAP 1.3	OACI	1.1	5.1	Elaborar un inventario de todas las iniciativas de ciberseguridad emprendidas en los diferentes grupos expertos de la OACI.	El Comité Ad Hoc de Coordinación de la Ciberseguridad elabora y mantiene un Programa de Trabajo sobre Ciberseguridad de la Aviación de la OACI.	Alta	2024
CyAP 1.4	OACI y Estados miembros	1.2	5.2.3 y 5.5 Véase también el CyAP 5.1 (párrafo 9.2 del Plan de Acción)	A) Elaborar modelos de memorando de acuerdo/ colaboración y acuerdos externos. B) Proporcionar directrices sobre cómo preparar esos acuerdos.	Disponibilidad de plantillas y directrices.	Baja	2023-2024
CyAP 1.5	OACI, Estados miembros e industria	1.2	5.3	Elaborar una terminología uniforme y concertada sobre la ciberseguridad de la aviación civil para que todas las partes interesadas de la aviación, con independencia de su formación y actividades, puedan entenderse mutuamente en materia de ciberseguridad.	Publicación de un glosario de ciberseguridad.	Media	2023
CyAP 1.6	OACI,	1.2	5.4	La OACI elaborará un marco común para establecer un mapa funcional de alto nivel con la descripción de los	Existencia de un marco común y establecimiento de un mapa genérico de intercambios de	Alta	2024

	Estados miembros e industria			intercambios de información entre los intervinientes de la aviación (p. ej., proveedores de servicios de navegación aérea, explotadores de aeronaves, gestión del tránsito aéreo, aeropuertos, servicios meteorológicos, organizaciones de reparación y mantenimiento, comunicaciones, navegación y vigilancia) como condición necesaria para facilitar la comprensión del cuadro de ciberriesgos. Los Estados miembros y la industria elaborarán esos marcos a nivel nacional e institucional.	información/interacciones en la aviación. Sensibilización y comprensión del mapa funcional.		
CyAP 1.7	OACI y Estados miembros	1.2	5.7 Véanse también el CyAp 6.2 y el párrafo 10.2 del Plan de Acción	La OACI establecerá modelos de cooperación entre la aviación civil y militar con el fin de elaborar, cuando proceda, modelos/orientaciones de interfaces interoperables entre aviación civil y militar. Determinar los criterios y el nivel de interacción apropiado.	Disponibilidad de esos modelos/orientaciones para la cooperación civil/militar e interoperabilidad cibernética. Publicación de la lista de criterios e interacciones mínimas requeridas.	Alta	2023
CyAP 1.8	OACI, Estados miembros e industria	1.3	5.8	Planificar, organizar y favorecer eventos internacionales y regionales que promuevan la ciberseguridad en la aviación civil.	Eventos, sensibilización, cooperación internacional.	N/A	En curso

CyAP 1.9	OACI Estados miembros e industria	1.3	5.4	Asegurarse de que todas las partes interesadas pertinentes tomen parte en actividades y debates sobre ciberseguridad en la aviación civil. Interacción y divulgación permanente con las partes interesadas pertinentes.	Publicar los resultados de las iniciativas comunes. Publicar pruebas de participación, como asociaciones, participación en grupos, etc.	Alta	En curso
CyAP 1.10	OACI, Estados miembros e industria	1.2	5.2.2	Elaborar un marco de confianza para la aviación internacional que permita a las distintas entidades interoperar con arreglo a la confianza que tengan en otras partes interesadas.	Establecimiento de un marco de confianza para uso de numerosas organizaciones.	Alta	2024-2025

Resultado prioritario	**2. DESARROLLAR LA GOBERNANZA Y LA RENDICIÓN DE CUENTAS**
Acciones prioritarias	• Alentar, apoyar y aprovechar la Estrategia de ciberseguridad de la OACI. • Establecer un plan nacional claro de gobernanza y rendición de cuentas para la ciberseguridad de la aviación civil. • Disponer la coordinación a nivel del Estado entre las autoridades de aviación civil y las autoridades nacionales competentes en materia de ciberseguridad. • Establecer los canales apropiados de coordinación entre las diversas autoridades estatales y la industria. • Incluir la ciberseguridad en los programas nacionales de seguridad operacional y seguridad de la aviación civil. • Incluir la ciberseguridad en los planes mundiales y regionales. • Trabajar en pro de una base de referencia común para las normas y métodos recomendados de ciberseguridad.

Acciones

Acción núm.	**A cargo de**	**Trazabilidad a la Estrategia de Ciberseguridad**	**Trazabilidad en el capítulo 6**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 2.1	OACI y Estados miembros		6.1	Establecer una estructura de gobernanza en el ámbito de la ciberseguridad de la aviación civil.	Determinación de estructuras de gobernanza adecuadas para la ciberseguridad de la aviación civil.	N/A	2021-2023
CyAP 2.2	OACI y Estados miembros	2.2	6.3	La OACI elaborará un conjunto general de principios sobre sistemas adecuados de gestión de la ciberseguridad de la aviación civil. Los Estados miembros los elaborarán a nivel nacional siguiendo el modelo de la OACI.	Publicación de principios generales.	Alta	2023-2024
CyAP 2.3	OACI Estados miembros e industria	2.2	6.3.2 Véase también el párrafo 8.1 del Plan	Elaborar textos de orientación para ayudar a las organizaciones a implantar marcos de gestión de la ciberseguridad para facilitar la aplicación de un enfoque	Publicación de directrices.	Alta	2023

			de Acción.	sistemático de gestión de los riesgos de ciberseguridad en la aviación y evaluar la madurez y eficacia de dichos marcos.			
CyAP 2.4	OACI y Estados miembros	2.2	6.3	Promover mecanismos de coordinación entre las autoridades de aviación civil y las de ciberseguridad.	Encuesta de la OACI - Número de mecanismos de coordinación existentes.	Media	2022
CyAP 2.5	OACI	2.3	6.2.1 Véase también el CyAP 1.9 (párrafo 5.2 del Plan de Acción)	La OACI incluirá la ciberseguridad en los planes regionales y mundiales para velar por la seguridad operacional y la seguridad y resiliencia de la aviación.	Publicación de planes actualizados.	N/A	2022-2023
CyAP 2.6	OACI		6.2	La OACI preparará un registro/directrices de buenas prácticas como sección del repositorio.	Repositorio OACI de mejores prácticas.	N/A	2020-2021
CyAP 2.7	OACI, Estados miembros e industria	3.2	6.3	La OACI elaborará modelos de procedimientos para notificar ciberincidentes, con orientaciones para la clasificación de incidentes. Los Estados miembros y la industria elaborarán procedimientos nacionales e institucionales para notificar ciberincidentes de manera oportuna y eficaz.	Procedimientos de notificación de ciberincidentes/número de incidentes notificados de acuerdo con los procedimientos.	Alta	2022-2023

CyAP 2.8	OACI y Estados miembros	2.2	6.2	La OACI evaluará el grado en que los Estados miembros incluyen la ciberseguridad en sus programas nacionales de seguridad operacional y seguridad de la aviación civil y sus planes de navegación aérea.	Encuesta OACI – Número de Estados que han incluido la ciberseguridad en sus programas nacionales de seguridad operacional y seguridad de la aviación civil.	Alta	Encuesta 2022 Otras acciones en curso

Resultado prioritario	**3. ELABORAR LEYES Y REGLAMENTOS EFICACES**
Acciones prioritarias	• Asegurarse de que los instrumentos jurídicos internacionales proporcionen un marco apropiado para la disuasión de ciberincidentes, así como para el enjuiciamiento de los responsables de tales actos. • Analizar la legislación nacional existente y actualizar o adoptar la legislación nacional de ser necesario para permitir la disuasión, investigación y el enjuiciamiento de los ciberataques que afecten la seguridad operacional y la seguridad, eficiencia y continuidad de la aviación civil. • Velar por la existencia de leyes y reglamentos nacionales apropiados para la ciberseguridad de la aviación civil. • Formular directrices apropiadas para ayudar a los Estados y a la industria a poner en práctica las disposiciones relacionadas con la ciberseguridad.

Acciones

Acción núm.	**A cargo de**	**Trazabilidad a la Estrategia de Ciberseguridad**	**Trazabilidad en el capítulo 7**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 3.1	Estados miembros	3.3	7.4	Los Estados deben ratificar los instrumentos de Beijing.	Número de Estados que han ratificado los instrumentos de Beijing.	Alta	En curso
CyAP 3.2	OACI	3.3	7.3	Análisis de los instrumentos de derecho aeronáutico internacional.	Examen y análisis de carencias de los instrumentos de derecho aeronáutico internacional pertinentes.	Alta	2022

CyAP 3.3	OACI y Estados miembros	3.3 y 3.4	7.2	Análisis de las leyes nacionales vigentes en el ámbito de la ciberseguridad de la aviación civil y detección de carencias, incluso en la legislación penal.	Encuesta sobre la situación de la legislación nacional en relación con el trato que acuerda a los actos ilícitos cometidos contra la aviación civil por medios cibernéticos.	Media	2023-2024
CyAP 3.4	OACI	3.3	7.1	Examinar las normas y métodos recomendados existentes de la OACI para determinar la necesidad de realizar posibles actualizaciones en materia de ciberseguridad.	Examen y análisis de las carencias de los SARPS de la OACI.	Alta	2022
CyAP 3.5	OACI	3.2		Crear, examinar y enmendar los textos de orientación relacionados con la aplicación de los requisitos de ciberseguridad de la aviación civil.	Publicación de textos de orientación sobre ciberseguridad de la aviación civil.	Alta	2021 y en curso

Resultado prioritario	**4. ELABORAR UNA POLÍTICA DE CIBERSEGURIDAD**
Acciones prioritarias	• Asegurarse de que la ciberseguridad forme parte de los sistemas de seguridad operacional y de seguridad de la aviación civil y de marcos integrales de gestión de riesgos. • Mantener la comparabilidad entre las diferentes metodologías de evaluación de riesgos para la ciberseguridad de la aviación civil. • Elaborar políticas de ciberseguridad que tengan en cuenta el ciclo de vida completo de los sistemas de aviación.

Acciones

Acción núm.	**A cargo de**	**Trazabilidad a la Estrategia de Ciberseguridad**	**Trazabilidad en el capítulo 8**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 4.1	Estados miembros e industria	4.1	8.1	Los Estados miembros y la industria han de garantizar el compromiso de su administración para abordar la ciberseguridad y la ciberresiliencia de la aviación civil.	Campaña de sensibilización / Prueba de compromiso, como una declaración de compromiso, responsabilidades definidas en el ámbito de la ciberseguridad en los manuales de gestión de autoridades y organizaciones.	Media	2022-2023
CyAP 4.2	OACI, Estados miembros e industria	4.3	8.2 (Véase también el párrafo 5.11 del Plan de Acción)	Alentar la realización de actividades de investigación y desarrollo en ciberseguridad de la aviación civil mediante la colaboración con universidades, institutos, comunidades de investigación, etc.	Número de interacciones y proyectos.	Alta	2022-2023
CyAP 4.3	Estados miembros e industria	4.2	5.6 y 8.2	La OACI definirá criterios para la evaluación de los riesgos compartidos por múltiples organizaciones, incluida la información que habrá de	Publicación de objetivos y criterios para la evaluación de riesgos compartidos por múltiples organizaciones.	Alta	2023

				compartirse y los criterios necesarios para la comparabilidad de riesgos. Los Estados miembros definirán esos criterios a nivel nacional y la industria a nivel organizacional.			
CyAP 4.4	OACI, Estados miembros e industria	4.3	8.1	Formular una política de seguridad de diseño como base de sistemas de aviación civil seguros en todo su ciclo de vida.	Formulación de una política de sistemas de aviación civil seguros en todo su ciclo de vida.	Media	2022-2023
CyAP 4.5	OACI, Estados miembros e industria	4.2	8.2	La OACI instaurará foros internacionales destinados a analizar las metas de ciberseguridad y de ciberresiliencia para múltiples organizaciones y funciones y el nivel mínimo de funciones esenciales para el sector de la aviación civil. Los Estados miembros crearán esos foros a nivel nacional y regional, y la industria creará foros específicos y participará activamente en los foros establecidos por la OACI y los Estados miembros.	Número de foros para analizar las metas.	Alta	2022-2023
CyAP 4.6	OACI, Estados miembros e industria	4.3	8.2	Establecer un inventario de iniciativas existentes de gestión de riesgos de ciberseguridad en la aviación civil (perfiles de riesgos, diferentes hipótesis, gestión de la vulnerabilidad y evaluaciones de riesgos).	Disponibilidad de un repositorio de iniciativas de gestión de riesgos de ciberseguridad.	Media	2023-2024

CyAP 4.7	OACI, Estados miembros e industria	4.3	8.3	La OACI elaborará una lista de hipótesis estratégicas de ciberriesgos a nivel internacional. Los Estados miembros y la industria elaborarán y proporcionarán listas similares a nivel nacional y organizacional.	Disponibilidad de 10 hipótesis de ciberriesgos.	Alta	2023-2024
CyAP 4.8	OACI, Estados miembros e industria		8.2	La OACI elaborará perfiles de riesgos para cada ámbito operacional. Los Estados miembros y la industria elaborarán y proporcionarán perfiles similares a nivel nacional y organizacional.	Disponibilidad de perfiles de riesgos.	Alta	2023
CyAP 4.9	OACI		8.2	Elaborar una Declaración sobre el contexto de riesgos para la ciberseguridad mundial.	Publicación de la Declaración sobre el contexto de riesgos para la ciberseguridad mundial.	Alta	2023

Resultado prioritario	**5. DESARROLLAR CAPACIDADES DE INTERCAMBIO DE INFORMACIÓN**
Acciones prioritarias	• Elaborar plataformas y mecanismos de intercambio de información o fortalecer los existentes, que sean reconocidos, en consonancia con las disposiciones existentes de la OACI, para crear conciencia sobre la situación de la ciberseguridad y con ello facilitar la prevención, detección temprana y mitigación de sucesos relevantes de ciberseguridad. • Velar por que todo ciberincidente o vulnerabilidad en materia de ciberseguridad que pudiera representar un riesgo importante para la seguridad operacional o la seguridad de la aviación se notifique a la autoridad competente.

Acciones

Acción núm.	**A cargo de**	**Trazabilidad a la Estrategia de Ciberseguridad**	**Trazabilidad en el capítulo 9**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 5.1	OACI	5.1	9.1 y 9.2	La OACI elaborará orientación para el intercambio de información.	Documento de orientación para el intercambio de información a disposición de la comunidad.	Alta	2022-2023
CyAP 5.2	OACI	5.1	9.1	La OACI definirá las necesidades de intercambio de información de ciberseguridad y de colaboración (en particular, aunque no exclusivamente, en momentos de crisis) y establecerá políticas al respecto con el apoyo de los Estados miembros y la industria.	Elaboración de una lista de posible información para compartir.	Media	2022-2024
CyAP 5.3	OACI	5.1	9.1	Preparar orientaciones sobre el TLP (Protocolo del Semáforo) para indicar el nivel de difusión/restricciones en la distribución y ulterior intercambio de ciberinformación.	Publicación de orientaciones de política para el uso del TLP en la distribución e intercambio de ciberinformación.	Alta	2021
CyAP 5.4	OACI, Estados miembros e industria	5.2	9.2	Considerar la viabilidad de definir criterios para la divulgación responsable de las vulnerabilidades en materia de ciberseguridad.	Disponibilidad y publicación de principios para la divulgación responsable de las vulnerabilidades si se estima viable.	Alta	2023

CyAP 5.5	OACI y Estados miembros	5.2	9.4	La OACI elaborará y mantendrá una red de puntos de contacto a nivel internacional para las cuestiones relacionadas con la ciberseguridad de la aviación civil para uso de los Estados y la industria. Los Estados miembros cooperarán con la OACI mediante formación de puntos de contacto de la red a nivel nacional.	Establecimiento de una red de puntos de contacto sobre ciberseguridad de la aviación civil. Publicación del punto de contacto de la red de cada Estado miembro.	Media	2024-2025

Resultado prioritario	**6. DESARROLLAR GESTIÓN DE INCIDENTES Y PLANIFICACIÓN ANTE EMERGENCIAS**
Acciones prioritarias	• Asegurarse de contar con planes apropiados y adaptables que proporcionen la continuidad de unas operaciones de aviación civil seguras en caso de un incidente cibernético. • Asegurarse de fortalecer los planes de contingencia existentes e incluir disposiciones para responder y recuperarse de incidentes de ciberseguridad y realizar ejercicios regulares/periódicos para comprobar la capacidad de detectar, responder y recuperarse de ciberincidentes.

Acciones

Acción núm.	**A cargo de**	**Trazabilidad a la Estrategia de Ciberseguridad**	**Trazabilidad en el capítulo 10**	**Medidas/Tareas específicas**	**Indicadores**	**Prioridad**	**Fecha de inicio de aplicación**
CyAP 6.1	Estados miembros e industria	6.1	10.1	Los Estados miembros establecerán metas y niveles mínimos de funciones esenciales para el sector de la aviación civil. La industria aplicará las metas establecidas.	Publicación de una lista de metas y niveles aceptables mínimos de las funciones para la continuidad de la aviación.	Alta	2022-2023
CyAP 6.2	OACI y Estados miembros	6.1	10.2	La OACI elaborará orientaciones y procesos para incluir a las partes interesadas militares en la planificación de respuesta a incidentes de ciberseguridad en la aviación civil. Los Estados miembros elaborarán procedimientos y acuerdos de cooperación entre las autoridades de aviación civil y militar.	Elaboración y publicación de orientaciones relativas a los procesos y procedimientos de cooperación cívico-militar en la repuesta a incidentes de ciberseguridad en la aviación civil.	Alta	2022-2023

CyAP 6.3	OACI, Estados miembros e industria	6.1	10.1	La OACI elaborará orientación sobre las capacidades de respuesta a ciberincidentes en la aviación civil y de recuperación posterior, incluidos planes de respuesta a contingencias y emergencias. Los Estados miembros y la industria elaborarán esa orientación a nivel nacional y organizacional ateniéndose a la orientación de la OACI.	Publicación de orientación sobre las capacidades de respuesta a ciberincidentes en la aviación civil y de recuperación posterior, incluidos los planes de respuesta a contingencia y emergencias.	Alta	2022-2023
CyAP 6.4	Estados miembros	6.1	10.2 y 10.3	Los Estados miembros desarrollarán y aplicarán capacidades y planes para la detección, análisis y respuesta a nivel operacional frente a ciberincidentes en la aviación civil.	Encuesta para dar seguimiento al nivel de aplicación.	Alta	2023-2024
CyAP 6.5	OACI y Estados miembros	6.1	10.1	Elaborar procesos para la coordinación de la aviación civil ante crisis de ciberseguridad, incluso a nivel nacional e internacional.	Definición de los procesos establecidos para la coordinación ante crisis de ciberseguridad. Publicación de textos de orientación.	Media	2024-2025
CyAP6.6	Estados miembros e industria	6.1	10.3	Realización periódica de ejercicios teóricos y reales.	Intercambio de lecciones extraídas, según corresponda.	Alta	2022-2023

Resultado prioritario	7. CREAR CAPACIDAD, INSTRUCCIÓN Y CULTURA DE CIBERSEGURIDAD
Acciones prioritarias	• Garantizar las cualificaciones apropiadas del personal con base en las funciones que se desempeñan tanto en aviación como en ciberseguridad. • Aumentar la toma de conciencia sobre la ciberseguridad, incluidas actividades para establecer la ciberhigiene apropiada. • Asegurarse de que los planes de estudio del sistema educativo nacional incluyan contenidos de ciberseguridad de la aviación para que se elabore un corpus transectorial de conocimientos sobre seguridad operacional y seguridad de la aviación en toda la organización, incluida su administración superior. • Fomentar la innovación, la investigación y el desarrollo en ciberseguridad. • Incluir la ciberseguridad en la Estrategia para la próxima generación de profesionales de la aviación de la OACI.

Acciones

Acción núm.	A cargo de	Trazabilidad a la Estrategia de Ciberseguridad	Trazabilidad en el capítulo 11	Medidas/Tareas específicas	Indicadores	Prioridad	Fecha de inicio de aplicación
CyAP 7.1	OACI, Estados miembros e industria	7.1	11.1	Definir una cultura y una educación en ciberseguridad de la aviación civil y promoverlas.	Disponibilidad de cursos y textos de orientación relacionados con la cultura de la ciberseguridad de la aviación civil.	Media	2022 - 2023
CyAP 7.2	Estados miembros e industria	7.2	11.1	Los Estados miembros y la industria prepararán requisitos de instrucción apropiada sobre ciberseguridad de la aviación con base en las funciones desempeñadas a todos los niveles de sus organizaciones.	Elaboración de instrucción apropiada sobre ciberseguridad de la aviación con base en las funciones desempeñadas.	Alta	2022-2023

CyAP 7.3	OACI y Estados miembros	7.3	11.1	La OACI incluirá la ciberseguridad en la Estrategia para la próxima generación de profesionales de la aviación (NGAP). Los Estados miembros incluirán la ciberseguridad en sus estrategias nacionales relativas a la NGAP.	Inclusión de la ciberseguridad en las estrategias NGAP.	Media	2022-2023
CyAP 7.4	OACI	7.3	11.1	La OACI analizará los medios y arbitrios para establecer requisitos de competencias según las funciones.	Inclusión de la instrucción sobre ciberseguridad según las funciones en los Doc 7192 y 9868 de la OACI, de estimarse viable.	Alta	2023-2025
CyAP 7.5	OACI, Estados miembros e industria	7.3	11.1	Preparación de actividades de creación de capacidad.	Disponibilidad de cursos de instrucción sobre ciberseguridad de la aviación.	Alta	En curso

— FIN —