OACI

Objetivo estratégico de Seguridad de la aviación y facilitación

Estrategia de ciberseguridad de la aviación

Octubre, 2019

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Objetivo estratégico de Seguridad de la aviación y facilitación

Estrategia de ciberseguridad de la aviación

Octubre, 2019

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

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

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

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

ESTRATEGIA DE CIBERSEGURIDAD DE LA AVIACIÓN

VISIÓN DE UNA ESTRATEGIA MUNDIAL DE CIBERSEGURIDAD DE LA AVIACIÓN CIVIL

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

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

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

Esto puede lograrse mediante:

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

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

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

1. COOPERACIÓN INTERNACIONAL

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

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

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

2. GOBERNANZA

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

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

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

3. LEYES Y REGLAMENTOS EFICACES

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

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

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

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

4. POLÍTICA DE CIBERSEGURIDAD

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

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

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

5. INTERCAMBIO DE INFORMACIÓN

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

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

6. GESTIÓN DE INCIDENTES Y PLANIFICACIÓN ANTE EMERGENCIAS

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

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

7. CREACIÓN DE CAPACIDAD, INSTRUCCIÓN Y CULTURA DE CIBERSEGURIDSAD

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

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

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

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

— FIN —