



**Tercera Reunión Virtual del Comité de Revisión de Programas y Proyectos (CRPP) del  
GREPECAS (eCRPP/03)**  
En línea, 22 - 23 de julio de 2021

**Cuestión 4 del  
Orden del Día: Otros asuntos**

**ANÁLISIS DE TECNOLOGÍAS EMERGENTES Y RETOS A LA AVIACIÓN**

(Presentada por la Secretaría)

**RESUMEN EJECUTIVO**

Esta nota de estudio presenta información dando seguimiento a la DECISIÓN eCRPP/02/04 en la cual se solicita los lineamientos para asistir a los Estados en los temas de sistemas de aeronaves no tripuladas (UAS) y ciberseguridad.

<b>Acción:</b>	Las acciones sugeridas se presentan en la Sección 4.
<i>Objetivos Estratégicos:</i>	<ul style="list-style-type: none"><li>• Capacidad y eficiencia de la navegación aérea</li><li>• Desarrollo económico del transporte aéreo</li></ul>
<i>Referencias:</i>	<ul style="list-style-type: none"><li>• Segunda reunión virtual del comité de revisión de programas y proyectos (CRPP) del GREPECAS (eCRPP/02), octubre de 2020.</li></ul>

**1. Introducción**

1.1 Durante la Segunda Reunión Virtual del Comité de Revisión de Programas y Proyectos (CRPP) del GREPECAS (eCRPP/02), en octubre del 2020, se discutió ampliamente las tecnologías emergentes como las operaciones de sistemas de aeronaves no tripuladas (UAS) y los nuevos retos en cuanto a ciberseguridad de la aviación que los Estados deben enfrentar en sus operaciones. Se identificó la necesidad de que los Estados estén preparados para afrontar ambos retos de forma oportuna.

1.2 En atención a la decisión eCRPP/02/04 “coordinación para la implementación y asistencia a los Estados en UAS/RPAS y ciberseguridad”, en el resultado del análisis a esta temática se consideró la necesidad de definir las actividades y responsabilidades para apoyar a los Estados en el desarrollo de estas actividades:

<b>DECISIÓN</b> eCRPP/02/04		<b>COORDINACIÓN PARA LA IMPLEMENTACIÓN Y ASISTENCIA A LOS ESTADOS EN UAS/RPAS Y CIBERSEGURIDAD</b>	
<b>Qué:</b> Que, considerando la temática de UAS/RPAS como la de ciberseguridad, como temas multidisciplinarios no exclusivos de tratarse en el GREPECAS, la Secretaría de GREPECAS coordine la definición de actividades y responsabilidades de apoyo a la implementación de estos temas con los grupos regionales de implementación en Seguridad de la Aviación, el Grupo Regional sobre Seguridad de la Aviación y Facilitación (AVSEC/FAL) CAR/SAM, así como con el Grupo Regional sobre Seguridad Operacional de la Aviación – Pan América (RASG-PA) <b>a más tardar en la eCRPP/03.</b>		<b>Impacto esperado:</b> <input type="checkbox"/> Político / Global <input checked="" type="checkbox"/> Inter-regional <input type="checkbox"/> Económico <input type="checkbox"/> Ambiental <input checked="" type="checkbox"/> Técnico/Operacional	
<b>Por qué:</b> Asegurar una implementación armonizada y coordinada entre los diferentes grupos regionales de la región para evitar duplicidad de tareas y optimizar los esfuerzos.			
<b>Cuándo:</b> eCRPP/03		<b>Estado:</b> <input checked="" type="checkbox"/> Válida / <input type="checkbox"/> Invalidada / <input type="checkbox"/> Finalizada	
<b>Quién:</b> <input type="checkbox"/> Coordinadores <input type="checkbox"/> Estados <input checked="" type="checkbox"/> Secretaría OACI <input type="checkbox"/> Sede de la OACI			

1.3 En ese sentido se ha realizado un análisis del impacto que las operaciones de aeronaves no tripuladas y los retos sobre las operaciones de control de tráfico aéreo en cuanto a ciberseguridad y la responsabilidad de los Grupos de Trabajo que apoyan las tareas de implementación regional.

## 2. Análisis

### SISTEMAS DE AERONAVES NO TRIPULADAS Y SISTEMAS DE AERONAVES PILOTADAS A DISTANCIA (UAS/RPAS)

2.1 Los UAS se utilizan cada vez más en todo el mundo para apoyar las misiones de emergencia y rescate, incendios urbanos, incendios forestales, inundaciones, terremotos, las operaciones con UAS ayudan a los bomberos, la policía, los paramédicos/médicos y durante la pandemia de COVID-19 se han visto sus aplicaciones en muchas otras actividades, desde socialización, sanitación, envío de provisiones y medicamentos, etc.

2.2 Las operaciones con aeronaves no tripuladas y los servicios que estos ofrecen están creciendo de forma exponencial y una de las preocupaciones fundamentales es que los Estados no estén preparados para estas operaciones y sus implicaciones. Uno de los más grandes retos que los Estados enfrentan es el establecimiento de un marco regulatorio para las operaciones de UAS que integren a su regulación estatal en aeronáutica civil, especialmente el establecimiento entre la regulación y requisitos de las operaciones de RPAS y UAS, así como la preparación y el desarrollo de la capacidad de inspectores nacionales.

2.3 La OACI ha desarrollado una serie de documentación para apoyar a los Estados en el proceso de desarrollo de sus regulaciones, procedimientos entre otras herramientas, para la integración de estas operaciones en su espacio aéreo. Esta documentación apoya a los Estados en el establecimiento de armonización en el desarrollo de su regulación, establecimiento de la seguridad para la integración de las operaciones de las aeronaves no tripuladas y sobre establecer la documentación de cómo los Estados deben tomar este tema y, de acuerdo a la documentación de OACI, integrar los requisitos y regulaciones para sus operaciones.

2.4 La OACI ha establecido la siguiente documentación para la operación de sistemas de aeronaves no tripuladas:

1. Categorización:

- a. Categoría abierta y categorías específicas: Modelo OACI para la regulación de UAS Parte-1 y parte-2, que es un ejemplo para que los Estados Miembros de OACI para el establecimiento de una regulación para las operaciones de aeronaves no tripuladas. Documento bajo el siguiente enlace:  
<https://www.icao.int/safety/UA/Documents/Final%20Model%20UAS%20Regulations3%20-%20Parts%20101%20and%20102.pdf>
- b. Categoría certificada: Aplican todos los anexos de OACI.
- c. Aprobación de organizaciones de aviación (AAO): Para operadores de aeronaves no tripuladas, ejemplo para el desarrollo de la regulación: Modelo OACI para la regulación de UAS Parte-149:  
<https://www.icao.int/safety/UA/Documents/Final%20Model%20UAS%20Regulations3%20-%20Part%20149.pdf>
- d. Además de información y guías que la OACI ha desarrollado para apoyar a los Estados a enfrentar la operación de las aeronaves no tripuladas debido a la diversidad de aplicaciones.

*Modelo regulatorio de OACI para las Aeronaves No Tripuladas*



2.5 En el caso de la categoría de aeronaves certificadas, se siguen los siguientes requisitos de acuerdo con los anexos de OACI.

2.6 El **Apéndice A** de esta nota de estudio presenta los requisitos que deben tenerse en cuenta en cuanto a las operaciones de aeronaves no tripuladas. Todos los Anexos de OACI se ven afectados por estas operaciones, por ello al momento del desarrollo de la regulación nacional, procedimientos y otros documentos, deben integrarse estos requisitos y analizarse su aplicabilidad acorde con el tipo de operación:

1. Servicios de Navegación Aérea: AIM, AGA, ATS, CNS y MET (*GREPECAS*)
2. Seguridad de la aviación y facilitación (*AVSEC/FAL*)
3. Seguridad Operacional (*RASG-PA*)

## CIBERSEGURIDAD

2.7 La tecnología y los ciberistemas se han convertido en algo esencial para la sociedad moderna, dependemos aún más de la tecnología, que proporciona mayor eficiencia a todas las actividades que se realizan día a día. Junto con el beneficio de las tecnologías cibernéticas, surgen inseguridades que afectan a todos los sistemas e infraestructuras. La ciber-amenaza y el ciber-ataque tienen un componente y un efecto transnacional, ya que los sistemas mundiales están interconectados. Además, la complejidad de la acción tiene implicaciones para diversos actores a nivel nacional, regional e internacional.

2.8 La Estrategia de Ciberseguridad de la Aviación desarrollada por OACI indica que 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.

2.9 La estrategia de ciberseguridad de la OACI establece siete pilares importantes para la implementación de ciberseguridad:

### Estrategia de ciberseguridad en la aviación



2.10 La Estrategia de Ciberseguridad de la OACI se encuentra bajo el siguiente enlace:  
<https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf>

2.11 La resolución A40-10: Formas de abordar la ciberseguridad en la aviación civil producto de la Asamblea 40 de la OACI insta a los Estados y la Industria a adoptar las medidas siguientes para contrarrestar las ciber-amenazas a la aviación civil:

- a) implantar la estrategia sobre ciberseguridad;
- b) identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y los sistemas críticos de la aviación civil y las graves consecuencias que pueden resultar de tales incidentes;
- c) definir las responsabilidades de los organismos nacionales y las partes interesadas de la industria con respecto a la ciberseguridad en la aviación civil;

- d) fomentar una interpretación común entre los Estados miembros de las ciberamenazas y riesgos y la formulación de criterios comunes para determinar qué bienes y sistemas son de carácter crítico y es preciso proteger;
- e) fomentar la coordinación entre gobierno e industria con respecto a las estrategias, políticas y planes de ciberseguridad de la aviación, así como el intercambio de información para ayudar a identificar las vulnerabilidades críticas que sea necesario resolver;
- f) formar y participar en asociaciones y mecanismos entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación;
- g) sobre la base de una interpretación común de las ciberamenazas y riesgos, adoptar un enfoque flexible y basado en el riesgo para proteger los sistemas de aviación críticos mediante la implantación de sistemas de gestión de la ciberseguridad;
- h) fomentar una sólida cultura de ciberseguridad en todos los aspectos dentro de los organismos nacionales y en todo el sector de la aviación;
- i) promover la elaboración y aplicación de normas internacionales, estrategias y mejores prácticas para proteger los sistemas críticos de tecnología de la información y las comunicaciones que se usan en la aviación civil de interferencias que puedan atentar contra la seguridad operacional de la aviación civil;
- j) establecer políticas y destinar recursos cuando sea necesario para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura; que sean resilientes; que tengan métodos seguros de transferencia de datos que garanticen su integridad y confidencialidad; que tengan métodos de vigilancia, detección y notificación de incidentes y que se lleven a cabo análisis forenses de los incidentes; y
- k) colaborar en el desarrollo del marco de ciberseguridad de la OACI adoptando un enfoque horizontal, intersectorial y funcional que integre la navegación aérea, las comunicaciones, la vigilancia, las operaciones de aeronaves, la aeronavegabilidad y demás disciplinas pertinentes.

2.12 Las operaciones de Navegación Aérea están soportadas por tecnología de punta, tanto a nivel de los equipos en tierra como de la aviónica a bordo de las aeronaves. Facilidades como intercambio de información aeronáutica, los protocolos automatizados entre los centros de control, ATFM, A-CDM, entre otros requieren que los datos cuenten con medidas de calidad, disponibilidad y certificación, esta información es base para la toma de decisiones en tiempo real.

2.13 Nuestro sector, incluye usuarios del espacio aéreo, proveedores de navegación aérea, explotadores de aeropuertos, autoridades de aviación civil y fabricantes de equipo, entre otros. En ese sentido se requiere realizar un análisis del sistema de aviación integrando todas las partes interesadas que forman parte del sistema.

2.14 La ciberseguridad requiere un enfoque holístico. Las interfaces entre los componentes de seguridad de la aviación merecen una atención especial, como por ejemplo la seguridad de la gestión de tránsito aéreo (ATM), la seguridad de los componentes y operaciones (ADS-B, GNSS, data Link) de Comunicación, Navegación y Vigilancia (CNS), y la seguridad del espacio aéreo y la seguridad de los aeropuertos. La seguridad de la gestión del tránsito aéreo debe ser parte integrante del sistema de seguridad de la aviación. El **Apéndice B** proporciona información de la aplicabilidad de la documentación disponible para comenzar los trabajos de análisis de riesgo y de ciberseguridad de las operaciones de control de tránsito aéreo. Todas las áreas de la aviación pueden ser afectadas por ciber-ataques.

### **3. Conclusiones**

3.1 Tanto para las operaciones de aeronaves no-tripuladas y los retos de ciberseguridad, requieren un trabajo en conjunto de todas las aéreas del sistema de Aviación Civil, integrando tanto las áreas internas y partes del sistema, como las partes interesadas externas a las operaciones de aviación civil.

3.2 Los retos que enfrentamos como Estados y como región, no pueden esperar:

- Cada día tenemos más aeronaves no tripuladas volando, nuevos servicios emergiendo, tecnología en desarrollo constante proporcionando nuevas aeronaves y operaciones que hay que regular para asegurar un espacio aéreo eficiente y seguro.
- Los ciber-ataques se han venido incrementando en los últimos años, la aviación no pensó que podía ser blanco de este tipo de amenazas, pero el uso de tecnología de punta, la interconectividad regional y mundial, además como otros intereses hacen a nuestro sector vulnerable a esta amenaza.

3.3 Ambos retos no pueden ser trabajados de forma aislada por los sectores de la aviación, ambos necesitan un trabajo que incluye todas las disciplinas de la aviación y requieren ver el sistema como un todo y no por partes.

### **4. Acciones sugeridas**

4.1 Se invita a los Estados a:

- a) tomar nota de la información presentada en esta nota de estudio;
- b) considerar la adopción de enfoques multidisciplinarios para trabajar en ambos retos;
- c) la adopción de tareas de acuerdo a los grupos de trabajo regional; y
- d) cualquier otra actividad que aplique.

-----

**APÉNDICE A**  
**Disposiciones de los Anexos de OACI para la operación de Aeronaves No Tripuladas**

<b>Anexo</b>	<b>Disposiciones</b>	<b>Área</b>
Anexo 1: Licencias al personal	Licencias piloto remotos	<i>Seguridad Operacional (SAF)</i>
Anexo 2: Reglamento del Aire	Reglas generales y documentación adicional bajo desarrollo.	<i>Navegación Aérea (ATM)</i>
Anexo 3: Servicios meteorológico para la navegación aérea internacional	Requerimientos para las operaciones	<i>Navegación Aérea (MET)</i>
Anexo 4: Cartas aeronáuticas	Requerimientos para las operaciones	<i>Navegación Aérea (AIM)</i>
Anexo 5: Unidades de medida que se emplearán en las operaciones aéreas y terrestres.	Por ser determinado	<i>Navegación Aérea (AIM)</i>
Anexo 6: Operaciones de aeronaves	Nuevo volumen en desarrollo	<i>Seguridad Operacional (SAF)</i>
Anexo 7: Marcas de nacionalidad y de matrícula de las aeronaves	Registro y marcas de aeronaves no tripuladas	<i>Navegación Aérea (AIM)</i>
Anexo 8: Aeronavegabilidad	Requerimientos de acuerdo al tipo de aeronave	<i>Seguridad Operacional (SAF)</i>
Anexo 9: Facilitación	Entrada y despegue de operaciones de aeronaves y transporte	<i>Seguridad de la aviación y facilitación (AVSEC/FAL)</i>
Anexo 10: Telecomunicaciones Aeronáuticas	Nuevo volumen en desarrollo para los enlaces requeridos para las operaciones de aeronaves no tripuladas	<i>Navegación Aérea (CNS)</i>
Anexo 11: Servicios de Tránsito Aéreo	Disposiciones para las operaciones de aeronaves no tripuladas	<i>Navegación Aérea (ATM)</i>
Anexo 12: Búsqueda y Salvamento	De acuerdo a las operaciones y tipo de aeronaves	<i>Navegación Aérea (ATM)</i>
Anexo 13: Investigación de accidentes e incidentes de la aviación	Requerimientos para las operaciones de aeronaves no tripuladas	<i>Seguridad Operacional (SAF)</i>
Anexo 14: Aeródromos	Requerimientos para las operaciones de aeronaves no tripuladas	<i>Navegación Aérea (AGA)</i>
Anexo 15: Servicios de Información aeronáutica	Requerimientos para las operaciones de aeronaves no tripuladas	<i>Navegación Aérea (AIM)</i>
Anexo 16: Protección al medio ambiente	Requerimientos para las operaciones de aeronaves no tripuladas	<i>Navegación Aérea (MET)</i>
Anexo 17: Seguridad	Requisitos de seguridad física y de ciberseguridad	<i>Seguridad de la aviación y facilitación (AVSEC/FAL)</i>
Anexo 18: Transporte sin riesgos de mercancías peligrosas por vía aérea	Transporte de mercancías peligrosas en aeronaves no tripuladas	<i>Seguridad Operacional (SAF)</i> <i>Seguridad de la aviación y facilitación (AVSEC/FAL)</i>
Anexo 19: Gestión de la seguridad operacional	Gestión y análisis del riesgo para operaciones de aeronaves no tripuladas	<i>Navegación Aérea (AIM, AGA, ATM, CNS, MET)</i> <i>Seguridad Operacional (SAF)</i>

Además, aplican a las Operaciones de UAS/RPAS:

1. Convenio de Chicago: artículo 2, 8, 29, 44.
2. Documento 9859: Manual de gestión de la Seguridad Operacional
3. Modelo OACI para la regulación de las operaciones de aeronaves no tripuladas (PART 101, 102, 149).
4. Otros acuerdos a la operación de las aeronaves no tripuladas.

-----

## APÉNDICE B

### Documentación de OACI disponible a los Estados sobre Ciberseguridad

La Ciberseguridad debe interactuar con otras disciplinas (seguridad, eficiencia) de forma similar a lo que ocurre actualmente con la seguridad "tradicional" de la aviación para garantizar la evaluación precisa de la exposición a las amenazas de Ciberseguridad y asegurar el desarrollo de estrategias de ciber-protección eficaces y eficientes basadas en el riesgo.

La Ciberseguridad debe tender puentes entre la seguridad y la protección de la aviación, ya que la naturaleza multidisciplinar de la Ciberseguridad debe beneficiarse de la seguridad y la protección

¿Por qué la Ciberseguridad en la Aviación Civil?

La interconexión e interoperabilidad de los sistemas digitales entre las partes interesadas de la aviación amplía el panorama de las ciber-amenazas.

Áreas de la navegación Aérea afectadas:

1. *Navegación Aérea*
2. *Seguridad y Facilitación*
3. *Seguridad Operacional*

Documentación disponible:

1. Resolución A40-10: Abordar la Ciberseguridad en la aviación civil
2. Plantilla de política de Ciberseguridad para la gestión del tráfico aéreo.
3. Manual de gestión de la seguridad (SMM) (Doc 9859).
4. Declaración del contexto de riesgo global de la seguridad de la aviación de la OACI (Doc 10108)
5. Manual de Seguridad de la Aviación (Doc 8973)
6. Anexo 17: Disposiciones de seguridad
7. Manual de seguridad para la gestión del tráfico aéreo (Doc 9985)
8. Anexo 19; Gestión de la seguridad.
9. Estrategia de Ciberseguridad de la aviación de la OACI
10. Norma de Excelencia en Ciberseguridad de CANSO
11. La serie ISO/IEC 27000 comprende normas de seguridad de la información
12. Plan de Acción de Ciberseguridad de la OACI