



INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)
ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL (OACI)

COMISIÓN LATINOAMERICANA DE AVIACIÓN CIVIL (CLAC)
LATIN AMERICAN CIVIL AVIATION COMMISSION (LACAC)



**SEGUNDA REUNIÓN DEL GRUPO REGIONAL SOBRE SEGURIDAD DE LA AVIACIÓN Y FACILITACIÓN
(AVSEC/FAL/RG/2)**

Antigua y Barbuda, 16 al 18 de mayo de 2012

AVSEC/FAL/RG/2 — NE/08
02/05/12

**Cuestión 4 del
Orden del día**

Seguridad de la Aviación (AVSEC)

**4.2 Informe sobre el Proyecto de Comunicaciones/Intercambio de
Información**

**INFORME SOBRE EL PROYECTO INTERCAMBIO Y PROTECCIÓN DE INFORMACIÓN
DE SEGURIDAD DE LA AVIACIÓN**

(Presentada por el Proyecto de Comunicaciones/Intercambio de Información –
Coordinado por Venezuela)

RESUMEN

Esta Nota de Estudio, presenta el informe sobre los avances del Programa de trabajo sobre Comunicaciones - Intercambio de Información, y del proyecto de Intercambio y Protección de Información de la Seguridad de la Aviación, asignado como parte del trabajo de la reunión del Grupo Regional de Seguridad de la Aviación y Facilitación (AVSEC/FAL/RG) celebrada en Asunción, Paraguay en el 2011.

Referencias:

- Programa y proyectos de trabajo, del Informe de la primera reunión del Grupo Regional sobre Seguridad de la Aviación y Facilitación (NAM/CAR/SAM OACI/CLAC)
- Anexo 17

Objetivos Estratégicos | *Esta nota de estudio se relaciona con el Objetivo estratégico B de la OACI.*

1. Introducción

1.1 En la pasada reunión del Grupo Regional de Seguridad de la Aviación y Facilitación (AVSEC/FAL/RG), para Norteamérica y el Caribe y Suramérica (NAM/CAR/SAM) de la Organización de Aviación Civil Internacional (OACI) y la Comisión Latinoamericana de Aviación Civil (CLAC), celebrada en la ciudad de Asunción, Paraguay del 25 al 27 de mayo del 2011, se conformó el grupo ad-hoc integrado por los representantes de Estados Unidos, Panamá y Venezuela, a fin de trabajar en el programa sobre Comunicaciones / Intercambio de Información, específicamente en el proyecto sobre Intercambio y Protección de Información de Seguridad de la Aviación. Todo esto en acuerdo con los Términos de Referencia aprobados en la referida reunión y los programas de trabajo y proyectos del AVSEC/FAL/RG.

1.2 Como objetivos del proyecto de Intercambio y protección de información de seguridad de la aviación, se establecieron:

- a) Mantener una base de datos actualizada de los responsables regionales en materia AVSEC.
- b) Desarrollo de un proceso efectivo y eficiente para garantizar el intercambio seguro de información sensitiva de seguridad de la aviación entre los Estados, y
- c) Revisar la guía modelo de orientación para el manejo de información sensitiva de seguridad (COCESNA/ACSA).

2. Avances en la actualización de la base de datos de puntos de contactos AVSEC

2.1 Bajo la premisa de mantener solo una base datos actualizada del personal de contacto en los Estados para tratar los asuntos relacionados con temas de seguridad de la aviación, a fin de facilitar el intercambio de información, y con especial interés en aquellos casos donde incidentes puedan poner en peligro la vida de personas y la continuidad seguir del sistema aeronáutico, se inicio consulta con los Estados a fin de actualizar el listado de los puntos de contacto AVSEC de las regiones NAM, CAR y SAM.

2.2 La Secretaria del AVSEC/FAL/RG, remitió por intermedio del oficio LS 8/21.1 – SA018, del 11 de enero del 2012, la consulta a los Estados de las regiones NAM/CAR/SAM, a fin de notificar sobre cambios o ratificar los datos de sus puntos de contacto con la intención de unificar las listas existentes de los funcionarios designados en la Red de Puntos de Contacto (PoC) de OACI y aquellos designados para el AVSEC/FAL/RG.

2.3 A la referida solicitud de la Secretaria del AVSEC/FAL/RG, se recibieron las respuestas de algunos Estados, dando como resultado los ajustes presentados en el **Apéndice A** a esta Nota de Estudio.

3. Revisión de la guía modelo de orientación para el manejo de información sensitiva de seguridad (COCESNA/ACSA).

3.1 Con base a la importante contribución del Grupo de Expertos AVSEC de Centroamérica en cooperación con los Oficiales regionales de la TSA y de OACI, dando como resultado la “Guía de Orientación para la Administración de Información Sensitiva de Seguridad de la Aviación”, presentada por COCESNA(ACSA) en la Nota de Estudio NE/17, en la pasada reunión del AVSEC/FAL/RG, en Paraguay, se procedió a realizar una revisión de la misma, dando como resultado las recomendaciones de ajustes presentadas en el **Apéndice B** a esta Nota de Estudio.

4. Avances en el diseño del proceso para el intercambio de información AVSEC

4.1 Con el sentido de facilitar el intercambio entre los Estados de información sensitiva relacionada con la seguridad de la aviación civil, se realizaron investigaciones que permitieran diseñar un modelo de protocolo para el intercambio de información de seguridad de la aviación. A raíz de esta investigación se encuentra que a nivel internacional se presentar diferentes iniciativas encaminadas al intercambio de información sensitiva en aspectos de seguridad (con o sin relación a la materia de seguridad de la aviación), y que dicho intercambio no ponga en peligro la seguridad de los Estados que intervienen en el acuerdo.

- 4.2 Como ejemplo de lo antes mencionado se encuentra iniciativas como;
- a) El Sistema de Intercambio de Información de Seguridad del MERCOSUR (SISME), el cual fue concebido como una herramienta de cooperación en materia de seguridad regional, donde se ofrece la posibilidad de intercambiar información, gracias a una plataforma de comunicaciones desarrollada en conjunto por los países parte del bloque y los Estados Asociados;
 - b) El Memorando de Cooperación entre la Administración de la Seguridad en el Transporte del Departamento de Seguridad Nacional (TSA/DHS), de los Estados Unidos y la Comisión Latinoamericana de Aviación Civil (CLAC);
 - c) La promulgación de un Modelo de Acuerdo Bilateral o regional sobre Seguridad de la Aviación, presentado por la OACI en el Doc. 8973 (Manual de Seguridad para la Protección de la Aviación Civil Contra los Actos de Interferencia Ilícita), entre otros.

4.3 Como aspectos fundamentales en los diferentes ejemplos mencionados, se encuentra una estructura legal que establezca los parámetros y condiciones para el manejo de información entre los Estado que acuerden dicho intercambio. Es por ello que el marco ideal para soportar este intercambio de información sensitiva de seguridad de la aviación, se encuentra en los acuerdos Bilaterales o Multilaterales, sobre los cuales podría existir la posibilidad de ampliar o anexas a su contenido consideraciones relacionadas con protocolos o modalidades de trabajo que garanticen un adecuado intercambio de información sensitiva de la seguridad de la aviación. A este respecto el **Apéndice C** a esta Nota de Estudio, presenta un modelo de acuerdo que considera las condiciones bajo las cuales se realizaría dicho intercambio de información.

5. Acción sugerida

- 5.1 Se invita a la Reunión a:
- a) instar a los Estados a notificar de manera permanente a la Secretaria del AVSEC/FAL/RG los cambios que puedan presentarse en la designación de los puntos de contacto en materia de seguridad de la aviación civil y facilitación;
 - b) instar a los Estados a utilizar la “Guía de Orientación para la Administración de Información Sensitiva de Seguridad de la Aviación”, presentada por COCESNA-ACSA, así como las sugerencias propuestas por este Proyecto, con el fin de que se consideren como material de referencia para la unificación de criterios al momento de brindar la adecuada protección a la información sobre la seguridad de la aviación; y
 - c) someter a la consideración de los Estados el modelo de acuerdo sobre protocolo funcional de un sistema de intercambio de información de seguridad de la aviación (Apéndice C), y tomar las acciones que consideren necesarias.

APÉNDICE B

**COMENTARIOS DE REVISIÓN A LA
GUÍA DE ORIENTACIÓN PARA LA ADMINISTRACIÓN
DE INFORMACIÓN SENSITIVA DE SEGURIDAD DE LA AVIACIÓN**

Comentarios del grupo Ad-Hoc del AVSEC/FAL/RG, sobre la guía de orientación para la administración de información sensitiva de seguridad de la aviación, a fin de complementar el excelente trabajo desarrollado por el Grupo de Expertos AVSEC de Centroamérica en cooperación con los Oficiales regionales de la TSA y de OACI.

Pág.	Sección	Version original	Comentarios
5	Aplicabilidad	a. Estos procedimientos se aplicaran, a todos los operadores de aeropuertos, explotadores de líneas aéreas, empresas prestadoras de servicios, instituciones y organismos del Estado a quienes se les entregue información AVSEC clasificada como Secreta, Confidencial y Sensitiva.	Cada Estado puede establecer diferentes niveles y definición es sobre la clasificación de la información sensitiva, por lo que se recomienda mencionar al final del párrafo: <i>“... Confidencial y sensitiva, o bajo la clasificación ya definida por el Estado”</i>
5	Documentos a ser divulgados	Documentos a ser divulgados	Recomendamos utilizar la expresión: <i>“Documentos a ser protegidos”</i>
5	Documentos a ser divulgados a 2	2. Partes pertinentes de los Programas Nacionales, Reglamentos y Regulaciones, resultados de pruebas de seguridad, investigaciones, Circulares de Seguridad.	Recomendamos redactar: <i>“Programas Nacionales, Reglamentos y Regulaciones, resultados de pruebas de seguridad, investigaciones, Circulares de Seguridad o las partes pertinentes de los mismos”</i>
5	Documentos a ser divulgados c. 1)	1. Programas de seguridad, partes pertinentes de los explotadores de líneas aéreas, empresas prestadoras de servicio, instituciones u organismos del Estado.	Recomendamos que la expresión <i>“Instituciones u organismos del Estado”</i> , deban ser incluida en el literal (a), en consideración a que su nivel de dependencia es con el Estado y no con la líneas aéreas.
6	Clasificación de la documentación	La clasificación de la información se hará de acuerdo a la importancia o al tipo de información contenida, y el responsable de la clasificación será la autoridad competente de cada Estado.	Cada Estado puede establecer diferentes definiciones sobre la clasificación de la información sensitiva, por lo que se recomienda mencionar una nota que indique: <i>“Nota: De existir diferencias, mencionar las definiciones sobre los niveles de clasificación de la información del Estado”</i> .

Pág.	Sección	Version original	Comentarios
6	Protección y Marcación el Documento a)	a. Los documentos impresos, fotocopias o información electrónica (CD, Diskette, DVD y USB) se marcaran con el título de su clasificación, Secreta, Confidencial y Sensitiva.	Se recomienda añadir una frase que indique que las marcas de clasificación de la sensibilidad de una información promulgada por un Estado, puede ser aceptado y utilizado por otro Estado para satisfacer este requisito, tomando en consideración la metodología utilizada por cada Estado para dicha clasificación.
6	Protección y Marcación el Documento c)	c. Cada párrafo se marcará de acuerdo a los niveles apropiados de la clasificación de la información. El documento o página será marcado basado en la clasificación más alta de los párrafos incluidos.	El marca porciones de párrafos bajo diferentes clasificaciones es una buena práctica, pero requiere de orientación detallada y una amplia formación de quien clasifica el documento.
8	Sanciones para personas responsables de la información a) y b)	a. A las personas responsables de salvaguardar la información y cometan una violación / infracción serán objetos de sanciones administrativas y hasta judiciales de acuerdo a lo establecido en la Ley del Estado, si la información que fue confiada bajo su responsabilidad, se ha utilizado para cometer o permitir que se cometan actos de interferencia ilícita en contra de la aviación civil. b. Las penas y las sanciones se determinaran de acuerdo a los resultados de las investigaciones y a la Legislación Nacional del Estado y/o Convenios Internacionales.	Toda violación debería ser reportada a las autoridades competentes aun cuando los incidentes no ocurran
8	Responsabilidad de la persona que maneja la información b)	b. Se debe dar a conocer la responsabilidad de salvaguardar la información que está bajo su custodia y que no puede divulgarse a menos que se sigan los procedimientos establecidos y bajo órdenes superiores.	Se recomienda que cada Estado defina en sus procedimientos internos, el “Nivel Superior” que pudiese tener la facultad de ordenar la divulgación de la información sensitiva de seguridad, a fin de identificar y delimitar los niveles de responsabilidad ante estas actuaciones.

Pág.	Sección	Version original	Comentarios
8	Responsabilidad de la persona que maneja la información e)	e. Información que no se debe dar a conocer al público que presenta vulnerabilidad del sistema de seguridad, entre otros: 1. Programa de seguridad 2. Planes de contingencia 3. Directivas de trabajo 4. Inspecciones de seguridad y sus resultados 5. Información de investigaciones 6. Información de amenaza investigación 7. Capacitación de seguridad 8. Pruebas del sistema 9. Procedimientos de seguridad	Se recomienda añadir a los términos: <i>“10. Las vulnerabilidades detectadas. 11. Las especificaciones de rendimiento de los equipos de seguridad, y 12. Otra información que indique las medidas específicas, amenazas y el nivel de riesgo de la operación”.</i>
8	Responsabilidad de la persona que maneja la información f)	f. Sí descubre una anomalía o incidente relacionado a la información, el responsable de esta área notificará al superior	Se recomienda añadir que el Estado, también comunicará al Estado que proporcionó la información sensible (de ser el caso), sobre la anomalía o incidente relacionada con la información.
9	Control de Calidad b)	b. La lista de verificación deberá incluir como mínimo lo siguiente: 2. Inspeccionar que la información clasificada no haya sido dejada en escritorios, copiadoras, impresoras, maquinas de fax y basureros.	Recomendamos incluir la expresión <i>“Escáner”</i> , en el numeral 2, del literal b).

CENTRAL AMERICAN AVSEC GROUP OF EXPERTS

GUIDELINES FOR MANAGEMENT OF SENSITIVE AVIATION SECURITY INFORMATION

**FIRST ISSUE
04 JUNE 2010**

Table of Contents

Issue and Amendment Record..... 2

List of Effective Pages 3

Table of Contents 4

Objective 5

Applicability 5

Documents to Be Disclosed 5

Classification Levels..... 6

Information Classification..... 6

Document Protection and Marking..... 6

Control of Information within an Organization 6

Copy Control..... 7

Document Destruction 7

Sanctioning of Custodians 7

Custodial Responsibilities 8

Information to Other States 8

Quality control..... 9

Annex 1..... 10

Annex 2..... 11

CENTRAL AMERICAN AVSEC GROUP OF EXPERTS

OBJECTIVE

To adopt security measures for protecting aviation security documentation and to prevent it from being delivered to the wrong hands which may violate the AVSEC system.

APPLICABILITY

- a. These procedures will be applied to all airport operators, air operators, service providers, and State institutions which are provided with AVSEC information classified as secret, confidential and sensitive.
- b. States requesting information.

DOCUMENTS TO BE DISCLOSED

- a. State
 1. Annexes, manuals, relevant sections of these manuals, circulars and other documents.
 2. Relevant sections of National Programs, Rules and Regulations, Security Test Results, investigations and Security Circulars.
- b. Airport Operator
 1. Programs or relevant sections of the air operators' security programs, contingency plans, security circulars, meeting minutes.
 2. Rules and regulations.
- c. Air Operators
 1. Security programs or relevant sections of these security programs of air operators, service providers, and State institutions.
 2. Rules and regulations.
- d. Regional States
 1. Information provided by other States, programs, security circulars, intelligence reports of possible terrorist activities or criminal organisations that may affect civil aviation of each State.
 2. Third party information that may contribute to the aviation security system, maintaining the confidentiality of the persons that provided such information.
 3. Information provided during training to security personnel. A control system shall be used for the aforementioned statements.

CLASSIFICATION LEVELS

- a. Secret
- b. Confidential
- c. Sensitive

INFORMATION CLASSIFICATION

Information will be classified based on importance or type. The entity responsible for this classification will be the Competent Authority of each State.

- a. **Secret** All highly sensitive information considered a priority and that can only be known by a reduced number of persons.
- b. **Confidential** All medium level information related to aviation security and which may cause damage to the security system.
- c. **Sensitive.** All low level information that shall be disseminated to persons who require it for the performance of their tasks.

DOCUMENT PROTECTION AND MARKING

- a. Printed documents, photocopies or electronic information (CD-ROMs, Diskettes, DVDs and USBs) must have an outer label with "Secret, Confidential or Sensitive Information" markings.
- b. Information will be in headers, footers, and in a watermark, stating the classification level.
- c. Each paragraph will be marked according to the appropriate information classification level. The document or page will be marked based upon the highest classification of the paragraphs contained in it.
- d. Secret, confidential and sensitive information will be stored in a safe place determined by the competent authority.
Note: The competent authority should include, in an appendix to these guidelines, relevant detailed information about the custody of classified information.
- e. Photocopies, printouts and copies will implement the security measures established by the competent authority.
- f. Each user of an electronic device containing classified information shall have a unique access code.

CONTROL OF INFORMATION WITHIN AN ORGANIZATION

- a. All information will be property of the competent authority

b. A record of information received and provided will be maintained; this record shall satisfy, at least, the following requirements:

1. Name, signature and position of the person providing the information
2. Name, signature and position of the person receiving the information
3. Date and time
4. Amount of pages
5. Document classification

Note: Programs, regulations, security circulars, minutes, and training material will include a security code on each page as established in national documentation. A record of security codes shall be maintained.

COPY CONTROL

- a. In case, photocopies, printouts or electronic copies of any classified documents are required, a record of the amount of pages copied or printed, the date, time, name of the person who copied or printed the document, and the name person who requested them, will be maintained.
- b. The equipment used for copying and disseminating information will be for exclusive use and it will not be connected to any network.

DOCUMENT DESTRUCTION

- a. Documents classified as secret, confidential and sensitive will be destroyed when determined by the competent authority or according to national laws.
- b. Documents will be destroyed as determined by the competent authority (paper shredder, burning, etc) in order to prevent reading them.
- c. Destruction will be performed by at least two persons authorized by the competent authority.
- d. A document stating the type of material destroyed and the persons present during that activity shall be prepared.

SANCTIONING OF CUSTODIANS

- a. Persons responsible for safeguarding information who commit a violation/ infraction will be subject to administrative and judicial sanctions according to the State Law; this, if the information assigned under his/her responsibility has been used to commit or to allow acts of unlawful interference against civil aviation.
- b. Sanctions will be determined based on the results of investigations and the State's National Legislation and/or International Conventions.

CUSTODIAL RESPONSIBILITIES

- a. Persons responsible for handling information related to programs, rules, regulations, circulars, minutes or other shall be aware of the importance of this information in order to prevent claiming ignorance.
- b. The responsibility of safeguarding information under custody shall be made clear and no information can be disclosed unless the established procedures have been followed and on the command of upper management.
- c. No information that may put at risk the life of passengers, crew, ground personnel shall be disclosed.
- d. No civil aviation information that may put at risk the integrity of the States shall be disseminated to the general public.
- e. Information, which shall not be disseminated to the general public due to the vulnerability to the security system it represents, includes:
 1. Security program
 2. Contingency plans
 3. Security directives
 4. Security inspections and its results
 5. Investigation information
 6. Threat information
 7. Security training
 8. Security tests
 9. Security procedures
- f. In case of discovering any finding or incident related to this information, the person responsible for handling SSI shall notify upper management.

INFORMATION TO OTHER STATES

- a. Information can be shared with other States provided that they request it through a formal letter to the civil aviation competent authority.
- b. The information that can be share includes: programs, rules, regulations and data on threats to civil aviation.
- c. Information will be handled through the Department of Foreign Affairs unless, imminent danger exists; in that case and due to the lack of time, information will be provided by the civil aviation competent authority.
- d. The requesting State shall sign a confidentiality of information Memorandum of Understanding and notify the security measures to be applied to the information requested. In addition, the requesting State shall allow the State from which it is requesting information to verify it when necessary. (See Annex 1)

QUALITY CONTROL

- a. The person responsible for the custody and handling of classified information will conduct verification when beginning and finishing his/her tasks in order to corroborate information status. (include sample checklist, Annex 2)
- b. Checklist shall include, at least, the following:
 1. Check classified information pouches or containers are locked
 2. Check classified information has not been left on desks, photocopiers, printers, fax machines or garbage collectors.
 3. Check electronic devices used to copy and disseminate classified information are turned off.
 4. Check the office door is locked.
 5. Check other areas required by the competent authority.

CENTRAL AMERICAN AVSEC GROUP OF EXPERTS

ANNEX 1

MEMORANDUM OF UNDERSTANDING FOR THE PROTECTION OF SENSITIVE SECURITY INFORMATION BETWEEN (State or other providing entity) and (State or receiving entity)

This Memorandum of Understanding (MOU) details the procedures under which the (State or receiving entity) handles sensitive security information (SSI) in the material authorised by (State or providing entity) (herein after referred to as CAA).

The (State or receiving entity) understands that the SSI is to be protected from disclosure according to the legislation of (State or providing entity) based on the CAA's criteria that disclosing such information will be harmful to aviation security.

The (State or receiving entity) acknowledges it has received the SSI material and that the following procedures will rule the handling of such SSI material. The SSI material labelled as sensitive by the (State or providing entity) shall be:

- a. Protected from disclosure, unless a written authorization from the (State or providing entity) exists;
- b. Kept in the official facilities, unless an authorization from the (State or receiving entity) exists;
- c. Provided only to the organizations or persons considered suitable by the Director of the Civil Aviation Authority to access information and who have a "need to know" in order to perform or assist in an official authorized function;
- d. Accessible only to the authorized persons or organizations that have read and understood the SSI material handling procedures. These procedures shall not be disclose to a third party. Authorized persons or organizations shall comply with the terms of this memorandum of understanding;
- e. Handled only by authorized persons taking all precautionary measures to safeguard material and prevent unauthorized access by securing the SSI material in a container or in a locked door office when not being actively used. In addition, a list of persons provided access to the documents will be maintained;
- f. Copying is not allowed, unless it is necessary for operating purposes of the (State or receiving entity) and authorized by the Director of the Civil Aviation Authority of the (State or receiving entity), and

The (State or providing entity) approves the provision of the following SSI material to an authorized representative of the CAA of the (State or receiving entity):

- 1. National Aviation Security Programs
- 2. Contingency Plans
- 3. National Aviation Security Training Programme
- 3. Any other document related to the aforementioned material

By signing, the representative duly authorized by the Civil Aviation Authority (of the State or receiving entity) acknowledges receipt of the SSI material and the handling procedures of such material as stated above.

 Name: _____ Date _____
 Position:
 State

**ANNEX 2
Checklist**

CAA
representative: _____

Date: _____

Task	YES	NO	Remarks
Check classified information pouches or containers are locked.	<input type="checkbox"/>	<input type="checkbox"/>	
Check classified information has not been left on desks, photocopiers, printers, fax machines or garbage collectors.	<input type="checkbox"/>	<input type="checkbox"/>	
Check electronic devices used to copy and disseminate classified information are turned off.	<input type="checkbox"/>	<input type="checkbox"/>	
Check the office door is locked.	<input type="checkbox"/>	<input type="checkbox"/>	
Check other areas required by the competent authority.	<input type="checkbox"/>	<input type="checkbox"/>	

Remarks:

APPENDIX C / APÉNDICE C

ACUERDO SOBRE PROTOCOLO FUNCIONAL DEL SISTEMA DE INTERCAMBIO DE INFORMACIÓN DE SEGURIDAD DE LA AVIACIÓN (SISA) ENTRE (NOMBRE DEL ESTADO) Y (NOMBRE DEL ESTADO)

El (Nombre de la institución del Estado) de (Nombre del Estado) y (Nombre de la institución del Estado) de (Nombre del Estado).

CONSIDERANDO el acuerdo (nombre del acuerdo bilateral / multilateral) suscrito entre (Nombre del Estado) y (Nombre del Estado) de fecha (fecha del acuerdo).

TENIENDO EN CUENTA la necesidad que impone la lucha para enfrentar los atentados contra la seguridad de la aviación civil, y de seguir avanzando permanentemente en el diseño de mecanismos contribuyentes para la cooperación y asistencia recíproca mutua entre los Estados comprometidos en la Seguridad de la región,

CONSIDERANDO el compromiso de los Estados en fortalecer el intercambio de información en materia de seguridad de la aviación, de acuerdo a lo contemplado en el Anexo 17 – Seguridad / Protección de la aviación civil contra los actos de interferencia ilícita.

RESULTANDO NECESARIO en la oportunidad dotar al referido Sistema de Intercambio de Información de Seguridad de la Aviación y Funcional que permita el acceso eficiente y responsable a la información,

ACUERDAN

Artículo 1

La suscripción entre (nombre del estado) y (nombre del estado) al denominado “Acuerdo sobre Protocolo Funcional del Sistema de Intercambio de Información de Seguridad de la Aviación (SISA)”, que como anexo forma parte integrante del presente acuerdo.

Artículo 2

Se comprometen a la adopción de todas las medidas, conforme a la legislación de cada país y a las capacidades materiales y humanas de las que se dispongan, a fin de cumplir con los propósitos que animan el presente Acuerdo

Artículo 3

El presente Acuerdo no restringirá la aplicación total o parcial de otros instrumentos que sobre la misma materia fueron suscritos o puedan ser suscritos entre las Partes, en tanto sus cláusulas resultaren más favorables para fortalecer la cooperación mutua en asuntos vinculados con la seguridad de la aviación civil. Dichas Partes podrán informar a las demás cuando la naturaleza de los mismos sea de su interés.

Artículo 4

El presente protocolo permanecerá en vigor durante un periodo indefinido. No obstante, cada parte tendrá el derecho a rescindirlo mediante aviso por escrito a la otra parte con (Colocar cantidad) meses de antelación. En caso de que una de las partes rescinda el presente protocolo, ambas partes adoptaran las medidas necesarias para asegurarse de que dicha rescisión no ponga en riesgo la ejecución de las operaciones de seguridad de la aviación de las partes.

Artículo 5

Las controversias que surjan sobre la interpretación, la aplicación, o el incumplimiento de las disposiciones contenidas en el presente protocolo entre los Estados Partes, se resolverán por medio de consultas entre las partes.

El presente protocolo entrara en vigor a la firma del mismo por parte de (Nombre del representante del Estado) y por (Nombre del representante del Estado)

Firmado en dos ejemplares en (lugar de la firma) a los (fecha), siendo ambos textos igualmente auténticos.

Por (Nombre del Estado)

Por (Nombre del Estado)

— C3 —

ANEXO**PROTOCOLO FUNCIONAL
DEL SISTEMA DE INTERCAMBIO DE INFORMACIÓN DE
SEGURIDAD DE LA AVIACIÓN ENTRE
(Nombre del Estado) y *(Nombre del Estado)*****CONSIDERACIONES GENERALES****Artículo 1**

Los Gobiernos de *(nombre del Estado)* y *(nombre del Estado)*, en adelante las Partes, crearán y mantendrán un sistema informático común denominado “Sistema de Intercambio de Información de Seguridad de la Aviación (SISA), que permita facilitar a las autoridades asignadas, con arreglo a sus funciones, el acceso eficiente y oportuno a informaciones relacionadas con la seguridad de la aviación civil, en procura de la protección de la aviación civil contra los actos de interferencia ilícita.

OBJETIVO**Artículo 2**

El objetivo del presente protocolo es optimizar los niveles de seguridad en los procesos de intercambio de información sensitiva en seguridad de la aviación entre los Estados que convengan dicho intercambio.

FORMAS DE COOPERACIÓN**Artículo 3**

A los efectos del presente protocolo, la cooperación comprenderá el intercambio de información sensitiva de seguridad, de análisis y de apreciaciones; la realización de actividades operativas coordinadas, simultáneas y/o complementarias y la generación de mecanismos e instancias para materializar esfuerzos comunes en el campo de la seguridad de la aviación.

La cooperación podrá comprender otras formas que las Partes acuerden según las necesidades.

RECURSOS**Artículo 4**

Los recursos necesarios para la ejecución del presente protocolo y para alcanzar su objetivo, serán responsabilidad de cada una de las Partes; no obstante, las mismas podrán acordar, cuando así lo consideren, otras formas de asumir los gastos.

ESTRUCTURA**Artículo 5**

El SISA implementará un Sistema de Consulta de Información constituido por un Nodo Nacional, que será aquella persona o grupo de personas quienes centralizaran dentro de cada Estado, las comunicaciones y serán responsables de todo tipo de interfaz entre los Estados y el Sistema de Intercambio de Información de Seguridad de la Aviación.

Artículo 6

El Nodo Nacional será administrado por la autoridad competente en materia de seguridad de la aviación de cada Estado. Dicho Organismo será responsable del correcto funcionamiento del citado Nodo Nacional y adoptará las medidas adecuadas para garantizar el cumplimiento del presente protocolo.

Artículo 7

Las Partes del presente protocolo, mediante las respectivas Representaciones Nacionales, prestarán cooperación para prevenir y/o tomar acción efectiva ante hechos relacionados contra la seguridad de la aviación civil, siempre que tales actividades no sean reservadas a otras autoridades por leyes de la Parte requerida y que lo solicitado no viole su legislación procesal o de fondo.

Artículo 8

Lo establecido en el párrafo anterior, no se opondrá a la cooperación directa entre las autoridades competentes en materia de seguridad de la aviación en el marco de sus respectivas jurisdicciones y competencias, en caso de que mediaren razones de urgencia operativa, con la obligación de dar, posteriormente, conocimiento inmediato a las respectivas Autoridades Nacionales.

USO DE LA INFORMACIÓN

Artículo 9

Las informaciones contenidas en el SISA no son de uso o conocimiento público.

Artículo 10

El intercambio de información se hará de acuerdo a la legislación vigente de cada país y sobre la base de los principios de reciprocidad y celeridad.

Artículo 11

Las Partes deberán contemplar medidas que garanticen que el tratamiento y destino de la información no deriven a fines distintos del interés de la seguridad o afecten las garantías y derechos de las personas.

Artículo 12

Las Partes se comprometen a contemplar resguardos especiales que impidan el conocimiento y uso de la información por parte de personas que no sean los destinatarios, o de terceros no autorizados expresamente para acceder a dicha información.

Estas medidas de seguridad deben entenderse referidas a la protección y el procedimiento para su envío y recepción.

Artículo 13

Cada Parte deberá establecer medidas para sancionar al que, intencional o negligentemente, permita que terceros no autorizados conozcan datos contenidos en el SISA.

INTERCAMBIO DE INFORMACIÓN

Artículo 14

Las solicitudes de cooperación e intercambio de información que se contemplan en el presente protocolo, salvo la situación descrita en el artículo 16, deberán cursarse en forma directa entre las respectivas Autoridades Nacionales competentes en materia de seguridad de la aviación, a través del Sistema de Intercambio de Información de Seguridad de la Aviación (SISA).

La Sección Nacional de la Parte requerida tramitará la solicitud imprimiéndole el trámite de urgente despacho, a partir de la instrumentación de un mecanismo que haga ello posible.

Artículo 15

Las Partes deberán contemplar procedimientos de validación de las consultas y respuestas a que dé lugar el SISA a fin de garantizar tanto la autenticidad del Nodo Nacional, como de la información.

Artículo 16

Las Partes establecerán mecanismos que garanticen el flujo expedito de la información estructurada. En caso de que esas informaciones no estén disponibles o no corresponden integralmente a las necesidades del solicitante, las partes deberán por medio de la mensajería o correo electrónico, salvo impedimento legal, intercambiar informaciones en el menor tiempo posible.

En caso de información solicitada por mensajería o correo electrónico, cada vez que se necesitare otorgar especial calificación de “Confidencial” a una información determinada, las Partes deberán señalarlo expresamente al requerirla o remitirla.

Artículo 17

La información solicitada en los términos del presente protocolo será suministrada por la Parte requerida, conforme a las respectivas legislaciones, en las mismas condiciones en que se proporciona para sus propias autoridades.

Artículo 18

Sin perjuicio de lo expresado precedentemente, la Parte requerida podrá aplazar el cumplimiento de la solicitud, o sujetarla a condiciones, en caso de que interfiera una investigación en curso en el ámbito de su jurisdicción.

Artículo 19

Las Partes deberán:

- a. A pedido de la Parte requirente, mantener el carácter confidencial de la solicitud y de su tramitación. Si la misma no pudiese tramitarse sin violar la confidencialidad, la Parte requerida informará tal situación a la requirente, la cual decidirá si mantiene vigente la solicitud.
- b. De la misma manera, la Parte requerida podrá solicitar que la información obtenida tenga carácter confidencial. En ese caso, la Parte requirente respetará las condiciones establecidas por la Parte requerida. Si la requirente no pudiese aceptarlas, lo comunicará a la Parte requerida, la que decidirá sobre la prestación de la colaboración.

Artículo 20

La Parte requerida informará a la requirente, lo más rápido posible, sobre el estado de cumplimiento de la solicitud tramitada.

Artículo 21

La solicitud deberá ser redactada en el idioma de la Parte requirente y estará acompañada de una traducción en el idioma de la Parte requerida, cuando fuere necesario. Los informes resultantes serán redactados solamente en el idioma de la Parte requerida.