| | | | |
|---|---|---|---|
| DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL GUATEMALA, C.A. | | | DE USO INTERNO |
| VIGENCIA: 24/01/2018 | CÓDIGO: GNA-MP-001-2018 | ÚLTIMA ACTUALIZACIÓN: 23/01/2018 | PÁGINA: 1 de 135 |

**ALCANCE:**

**DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL**
**SUBDIRECCIÓN TÉCNICO OPERATIVA**
**GERENCIA DE NAVEGACIÓN AÉREA**
**DEPARTAMENTO DE TRÁNSITO AÉREO (ATM)**
**GERENCIA DE COMUNICACIONES, NAVEGACIÓN Y VIGILANCIA DE RADAR**
**BIBLIOTECA TÉCNICA**

**TITULO:**

# MANUAL DE SEGURIDAD DE LA GESTIÓN DEL TRÁNSITO AÉREO

## DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

**GUATEMALA, ENERO DEL 2018.**

## INDICE

**1 LISTA DE DISTRIBUCIÓN DEL MANUAL** ..... ¡Error! Marcador no definido.
**2 RESOLUCIÓN** ..... **5**
**3 REGISTRO DE REVISIONES** ..... **7**
**4 INTRODUCCIÓN** ..... **8**
**5 INFORMACIÓN GENERAL** ..... **9**
*5.1 Definiciones* ..... 9
**6 ACRÓNIMOS** ..... **12**
**7 BASE LEGAL** ..... **14**
*7.1 Nacional* ..... **¡Error! Marcador no definido.**
*7.2 Internacional* ..... 14
**8 OBJETIVOS** ..... **15**
*8.1 Objetivo General* ..... 15
*8.2 Objetivos Especificos* ..... 15
**9 GENERALIDADES DEL MANUAL DE NORMAS Y PROCEDIMIENTOS PARA LA SEGURIDAD ATM.** ..... **16**
**10 ACTUALIZACION DEL MANUAL** ..... **16**
**11 ALCANCE** ..... **17**
**12 ANTECEDENTES** ..... **17**
**13 RESPONSABILIDADES DEL ESTADO EN MATERIA DE SEGURIDAD DE LA AVIACIÓN.** **17**
**14 DISTINCION ENTRE SEGURIDAD DE LA AVIACIÓN Y SEGURIDAD DE ATM** ..... **19**
**15 PROTECCIÓN DE LA INFRAESTRUCTURA DEL ATM** ..... **22**
*15.1 Antecedentes* ..... 22
*15.2 Principios De Protección De La Infraestructura Del Sistema Atm* ..... 23
**16 GOBERNANZA Y ORGANIZACION** ..... **24**
*16.1 Objetivos Del Programa* ..... 24
*16.2 Autoridad Aeronautica* ..... 24
*16.2.1 Vigilancia Estatal* ..... *24*
*16.3 Marco De Reglamentación* ..... 25
*16.4 Política De Seguridad:* ..... 25
*16.5 Estructura, Autoridad Y Responsabilidad* ..... 27
**17 SEGURIDAD FÍSICA DE LAS INSTALACIONES** ..... **28**
**18 SEGURIDAD FÍSICA DE LAS INSTALACIONES Y CONTROL DE ACCESO** ..... **28**
*18.1 Consideraciones Relativas Al Diseño De Las Intalaciones Atm* ..... 29
*18.2 Ayudas A La Navegación (Navaid)* ..... 30
*18.3 Componentes Del Sistema Atm* ..... 30
*18.4 Control De Equipos Y Audas A La Navegacion Aerea* ..... 30
**19 CAPAS DE DEFENSA PARA LAS INSTALACIONES Y OPCIONES DE ATENUACIÓN** ..... **31**
*19.1 Componentes De Las Instalaciones* ..... 31
*19.2 Capas De Defensa* ..... 31
*19.3 Opciones De Atenuación* ..... 32
**20 SEGURIDAD RELACIONADA CON EL PERSONAL** ..... **34**
**21 REQUISITOS DE SEGURIDAD DE LA AVIACIÓN** ..... **34**
*21.1 Personal De Seguridad* ..... 34
*21.2 Personal Que No Sea De Seguridad* ..... 35
**22 PROGRAMA DE SEGURIDAD RELACIONADA CON EL PERSONAL** ..... **35**
*22.1 Consideraciones Generales* ..... 35
*22.2 Categorias De Riesgos Relacionados Con El Puesto De Trabajo* ..... 35
*22.3 Inspección E Investigación Del Personal* ..... 35
*22.4 Cese De Empleo Del Personal* ..... 36
*22.5 Transferencia De Personal* ..... 36
*22.6 Acuerdos Relativos Al Acceso* ..... 36
*22.7 Personal De Seguridad Externo* ..... 37

*22.8 Sanciones Aplicables Al Personal* ..... 37
*22.9 Apoyo Para El Personal* ..... 37
*22.10 Control De Visitantes* ..... 37
**23 SEGURIDAD DE LOS SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES (ICT), (INCLUIDA LA CIBERSEGURIDAD)** ..... **38**
**24 ANTECEDENTES** ..... **38**
**25 CONTROLES DE SEGURIDAD DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES (ICT)** ..... **39**
*25.1 Categorías De Controles* ..... 39
*25.2 Controles Del Nivel De Riesgo* ..... 42
*25.3 Consideraciones Relativas Al Sistema Atm De Nueva Generación* ..... 43
**26 PLANIFICACIÓN DE CONTINGENCIA PARA LA SEGURIDAD DE ATM** ..... **44**
**27 FUNCIONES Y RESPONSABILIDADES ENTRE ESTADOS Y ATSP** ..... **44**
**28 PLANES DE RESERVA DE SERVICIOS DE TRÁNSITO AÉREO PARA LA SEGURIDAD DE ATM** ..... **44**
**29 MARCO DE PLANIFICACIÓN DE CONTINGENCIA PARA LA SEGURIDAD DE ATM** ..... **46**
*29.1 Elaborar Un Concepto Operacional Para Contingencias* ..... 47
*29.2 Consultar A Las Autoridades Estatales Y Los Usuarios* ..... 48
*29.3 Considerar Los Aspectos Jurídicos* ..... 48
*29.4 Establecer Coordinación Con Estados Vecinos Para Oficializar Operaciones Entre Varios Estados* ..... 48
*29.5 Considerar Los Aspectos Económicos* ..... 49
*29.6 Capacitar Al Personal De Contingencia* ..... 49
*29.7 Realizar Ejercicios Con El Plan De Contingencia* ..... 49
*29.8 Requisitos Genéricos Para Opciones De Contingencia* ..... 49
**30 OPERACIONES DE SEGURIDAD DE ATM** ..... **52**
*30.1 Antecedentes* ..... 52
*30.2 Colaboración Entre Organismos* ..... 52
**31 CONSIDERACIONES ESPECIALES RELATIVAS A LA PLANIFICACIÓN** ..... **53**
*31.1 Pérdida De Comunicación* ..... 53
*31.2 Objeto Sospechoso (Toi)* ..... 54
**32 CONTRIBUCIÓN DE ATM A LA PROTECCIÓN CONTRA INTERFERENCIA ILÍCITA** ..... **56**
*32.1 Función De Seguridad De Atsp Respecto A Otras Organizaciones* ..... 56
*32.2 Funciones De Seguridad De Atm Para La Seguridad De La Aviación* ..... 57
*32.3 Funciones Tácticas De Seguridad De Las Operaciones* ..... 58
*32.3.1 Vigilancia Y Detección De Posibles Casos De Interferencia Ilícita* ..... *59*
*32.3.2 Respuesta A Casos De Interferencia Ilícita* ..... *60*
*32.3.3 Amenazas De Bomba* ..... *63*
*32.3.4 Amenazas De Bomba Y Gestión De Amenazas Comunicadas Por Teléfono* ..... *63*
*32.3.5 Respuesta A Amenazas De Bomba* ..... *63*
**33 ANTECEDENTES** ..... **65**
**34 AMENAZAS DE LÁSER** ..... **65**
**35 AMENAZAS CON SISTEMAS PORTÁTILES DE DEFENSA ANTIAÉREA (MANPADS)** ..... **67**
**36 APOYO DE ATM A LA RESPUESTA Y RECUPERACIÓN EN CASO DE CATÁSTROFE** ..... **68**
**37 ENFERMEDADES TRANSMISIBLES Y OTROS RIESGOS PARA LA SALUD PÚBLICA A BORDO DE LAS AERONAVES** ..... **69**
**38 VIGILANCIA Y NOTIFICACIÓN DEL SOBREVUELO DE ZONAS DE IDENTIFICACIÓN PARA FINES DE SEGURIDAD** ..... **71**
**39 CONTROL DE SEGURIDAD DE EMERGENCIA DEL TRÁNSITO AÉREO** ..... **72**
**40 CREACIÓN, PROMULGACIÓN Y VIGILANCIA DE RESTRICCIONES TEMPORALES EN EL ESPACIO AÉREO Y LOS VUELOS** ..... **74**
**41 ANTECEDENTES** ..... **75**
**42 PLANIFICACIÓN Y OPERACIONES ESTRATÉGICAS DE SEGURIDAD** ..... **75**
*42.1 Operaciones Tácticas De Seguridad* ..... 78

*42.2 Seguridad Especial De La Interoperabilidad Para Operaciones Civiles Y Militares..... 80*
*42.3 Administración De Las Operaciones De Seguridad De Atm ..... 81*
**43 INTRODUCCIÓN..... 82**
**44 MECANISMO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD..... 82**
**45 GESTIÓN DE RIESGOS PARA LA SEGURIDAD, COLABORACIÓN DE LA ORGANIZACIÓN88**
**46 INTRODUCCIÓN..... 89**
**47 CONCEPTOS Y DEFINICIONES ..... 90**
**48 REQUISITOS DE SEGURIDAD PARA CIBERSISTEMAS ICT..... 91**
**49 MEDIDAS DE SEGURIDAD PARA LA INFRAESTRUCTURA DE CIBERSISTEMAS ICT CRÍTICOS..... 93**
**50 INTRODUCCIÓN..... 96**
**51 CATEGORÍAS DE CONTROLES ..... 96**
**52 NIVELES DE CONTROL..... 98**
**53 MARCO EUROPEO DE GESTIÓN DE INCIDENTES EN VUELO RELACIONADOS CON LA SEGURIDAD..... 117**
*53.1 Procedimientos Para Sucesos En Vuelo Relacionados Con La Seguridad En El Reino Unido..... 122*
*53.2 Procedimientos De La Red De Sucesos En El Territorio Nacional De Los Estados Unidos ..... 130*
*53.3 Centro De Gestión De La Respuesta A Incidentes De Organización Del Tránsito Aéreo (Ato) (Airmac) De La Sede De La Faa ..... 133*
**54 APROBACIÓN Del MANUAL DEL DEPARTAMENTO DE INVENTARIOS ..... 134**
**55 PERSONAL QUE PARTICIPÓ EN LA COORDINACIÓN Y ELABORACIÓN del manual ... 134**

# 1 RESOLUCIÓN

GOBIERNO DE LA REPÚBLICA DE GUATEMALA

DGAC DIRECCION GENERAL DE AERONAUTICA CIVIL

**RES-DS-078-2018**

**EL DIRECTOR GENERAL DE LA**
**DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL**

**CONSIDERANDO**

Que la Dirección General de Aeronáutica Civil es el órgano encargado de normar, supervisar, vigilar y regular, con base en lo prescrito en la Ley de Aviación Civil, Decreto Número 93-2000 del Congreso de la República de Guatemala, reglamentos, regulaciones y disposiciones complementarias, los servicios aeroportuarios, los servicios de apoyo a la Navegación Aérea, los servicios de Transporte Aéreo, de Telecomunicaciones y en general todas las actividades de Aviación Civil en el territorio y espacio aéreo de Guatemala, velando en todo momento por la defensa de los intereses nacionales; asimismo, está facultada para elaborar, emitir, revisar, aprobar y modificar las regulaciones y disposiciones complementarias de aviación que sean necesarias, para el complimiento de la Ley y sus Reglamentos.

**CONSIDERANDO**

Que con la necesidad de velar por el cumplimiento de las operaciones, requisitos y disposiciones relativas con relación a la seguridad de la gestión de los servicios de transito aéreo. Por parte de esta Dirección General se reedita el **"MANUAL DE SEGURIDAD DE LA GESTIÓN DEL TRÁNSITO AÉREO"**, el cual se elaboró en el mes de enero del 2018.

**POR TANTO**

La Dirección General de Aeronáutica Civil; con fundamento en los Considerandos, Ley de Aviación Civil, Decreto Número 93-2000 del Congreso de la República de Guatemala, Reglamento de la Ley de Aviación Civil, Acuerdo Gubernativo Numero 384-2001 del Presidente de la República.

**RESUELVE:**

I) **APROBAR** la reedición del Manual de Seguridad de la Gestión del Tránsito Aéreo.
II) La presente resolución tiene efectos inmediatos.
III) Notifíquese.

Guatemala 24 de enero del 2018.

DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL GUATEMALA, C.A. DGAC DESPACHO SUPERIOR

**Capitán P.A. Carlos Fernando Velásquez Monge**
**Director General**
**Dirección General de Aeronáutica Civil**

1

## 2 LISTA DE DISTRIBUCIÓN DEL MANUAL

| DEPENDENCIA | PUESTO | FECHA |
|---|---|---|
| Dirección General DGAC | Director General. | |
| Subdirección Técnica-Operativa DGAC | Subdirector Técnico-Operativo. | |
| Subdirección Administrativa DGAC | Subdirector Administrativo. | |
| Gerencia de Navegación Aérea | Gerente de Navegación Aérea | |
| Unidad de Planificación | Coordinador de la Unidad de Planificación | |
| Biblioteca Técnica DGAC | Encargado de Biblioteca. | |

Este ejemplar del manual de Normas y Procedimientos es propiedad de la DGAC de la República de Guatemala, y ha sido consignado para las personas que ocupan las posiciones antes indicadas.

El manual debe mantenerse en lugar accesible para rápida consulta y debe promoverse su divulgación verbal y escrita entre el personal subordinado.

## 3 REGISTRO DE REVISIONES

1. Todas las revisiones, modificaciones y publicación de este manual son responsabilidad de la DGAC a través de la Gerencia de Navegación Aérea.

2. Se deberá mantener al día las revisiones colocando número de revisión, número de página revisada, descripción del tema revisado, fecha cuando se efectuó la revisión y el nombre de la persona que efectuó la revisión.

3. El presente manual no es un instrumento rígido, por lo que debe registrar en el toda modificación en su estructura, por lo cual se solicita que todo error que se detecte o corrección que ayude a mejorar el mismo sea informado a la Unidad de Planificación de la DGAC en forma escrita para su estudio y actualización.

| No. | Página revisada | Descripción | Fecha | Persona |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 4 INTRODUCCIÓN

Las normas y métodos recomendados (SARPS) relativos al mantenimiento de la seguridad de las operaciones de la aviación civil fueron adoptados por primera vez el 22 de marzo de 1974 por el Consejo de la Organización de Aviación Civil Internacional (OACI) y publicados como Anexo 17 — Seguridad — Protección de la aviación civil internacional contra los actos de interferencia ilícita al Convenio sobre Aviación Civil Internacional. En las disposiciones de dicho Anexo se exige, entre otras cosas, que los Estados establezcan y apliquen un programa nacional de seguridad de la aviación civil (NCASP).

La aplicación del NCASP se limitaba inicialmente a los explotadores de aeronaves y los aeropuertos, concentrándose en apoderamiento ilícito y amenazas de bomba. Sin embargo, después de haberse utilizado las propias aeronaves como armas para destruir el World Trade Center en Nueva York el 11 de septiembre de 2001, aumentó la conciencia acerca de la posibilidad de otros tipos de sucesos relacionados con la seguridad, incluida la posibilidad de ataques semejantes o ataques contra instalaciones de servicios de tránsito aéreo y la infraestructura de navegación y vigilancia.

Por consiguiente, en respuesta a las inquietudes relativas a la seguridad de la aviación, el 17 de noviembre de 2010, el Consejo de la OACI adoptó la Enmienda 12 del Anexo 17 en la que se exige que los Estados incluyan a los proveedores de servicios de tránsito aéreo (ATSP) en el NCASP y se aseguren de que apliquen disposiciones de seguridad apropiadas para satisfacer las disposiciones del NCASP.

También ha aumentado la frecuencia con la que se ha pedido a los ATSP que apoyaran diversas categorías de operaciones de seguridad nacional e imposición de la ley. Dicho apoyo a menudo exige el establecimiento de restricciones temporales en el espacio aéreo y los vuelos por motivos de seguridad tales como: protección de los desplazamientos de jefes de Estado; operaciones de supervisión y vigilancia en el aire, a menudo con aeronaves pilotadas a distancia (RPA); restricción del acceso de aeronaves no verificadas al espacio aéreo en la zona de grandes eventos deportivos u otras reuniones públicas de gran escala; o suministro de información en apoyo a la gestión del espacio aéreo para fines relacionados con la seguridad. Los ATSP necesitan orientación relativa al suministro de servicios relacionados con operaciones de seguridad, así como sobre la protección de la infraestructura del sistema de gestión del tránsito aéreo (ATM) al servicio de la aviación internacional.

---

# 5 INFORMACIÓN GENERAL

## 5.1 DEFINICIONES

1. Cuando los términos indicados a continuación figuren en el contenido del presente manual, tendrán el significado siguiente:

***Actos de interferencia ilícita.*** Actos, o tentativas, destinados a comprometer la seguridad de la aviación civil y el transporte aéreo:

1. Apoderamiento ilícito de aeronaves;
2. Destrucción de una aeronave en servicio;
3. Toma de rehenes a bordo de aeronaves o en los aeródromos;
4. Intrusión por la fuerza a bordo de una aeronave, en un aeropuerto o en el recinto de una instalación aeronáutica;
5. Introducción a bordo de una aeronave o en un aeropuerto de armas o de artefactos o sustancias peligrosos con fines criminales;
6. Uso de una aeronave en servicio con el propósito de causar la muerte, lesiones corporales graves o daños graves a los bienes o al medio ambiente; y
7. Comunicación de información falsa que comprometa la seguridad de una aeronave en vuelo, o en tierra, o la seguridad de los pasajeros, tripulación, personal de tierra y público en un aeropuerto o en el recinto de una instalación de aviación civil.

***Amenaza.*** En materia de seguridad de la aviación, las amenazas son actos deliberados e intencionales llevados a cabo por personas u organizaciones, generalmente con fines hostiles. Sin embargo, la seguridad nacional y la imposición de la ley pueden resultar afectadas por amenazas intencionales o involuntarias. Las catástrofes naturales y la propagación involuntaria de enfermedades pandémicas podrían clasificarse como amenazas involuntarias. La posibilidad o probabilidad de amenazas intencionales depende de los medios o la capacidad de actuar, los motivos y la intención para hacerlo. La posibilidad o probabilidad de amenazas involuntarias depende de factores humanos o meteorológicos y el emplazamiento de la infraestructura del sistema ATM. Los factores humanos pueden dar lugar a errores humanos y la pérdida de servicios ATM críticos. El emplazamiento y las condiciones meteorológicas determinan la posibilidad de repercusiones en la infraestructura del sistema ATM ocasionadas por inundaciones, incendios, terremotos, huracanes, tornados, temperaturas extremas, efectos solares y accidentes en sistemas de transporte cercanos o instalaciones de producción y almacenamiento de material químico, biológico, radiológico y nuclear (CBRN) que podrían dar lugar a la evacuación de las instalaciones, etc.

***Dominio aéreo.*** El espacio aéreo mundial; todas las aeronaves pilotadas o no pilotadas que efectúen operaciones en el espacio aéreo; todas las personas y la carga presentes en el espacio aéreo mundial; y toda infraestructura relacionada con la aviación.

***Evaluación de riesgos.*** Ejercicio continuo y permanente para actualizar la gama completa, magnitud y categoría de amenazas creíbles y su probabilidad, basándose en información fiable de los servicios de inteligencia, la vulnerabilidad a las mismas y las posibles consecuencias o repercusiones de la pérdida o degradación causada por ataques efectivos.

Gestión del espacio aéreo para seguridad de ATM. Gestión del espacio aéreo para:

1. Disuadir, prevenir, detectar y resolver, cuando sea posible, amenazas a bordo, incluidas las relacionadas con interferencia ilícita

2. Prever un control de seguridad de emergencia para el tránsito aéreo; y

3. Iniciar restricciones temporales en el espacio aéreo y los vuelos y vigilarlas para apoyar actividades de seguridad nacional e imposición de la ley.

***Gestión del tránsito aéreo (ATM).*** Gestión dinámica e integrada del tránsito aéreo y del ***espacio*** aéreo, incluidos los servicios de tránsito aéreo, la gestión del espacio aéreo y de la afluencia de tránsito aéreo — en condiciones de seguridad, economía y eficiencia mediante el suministro de instalaciones y servicios sin límites perceptibles en colaboración con todas las partes y utilizando las instalaciones de a bordo y en tierra.

***Infraestructura del sistema ATM.*** La infraestructura del sistema ATM incluye personas, procedimientos, información, recursos, instalaciones, incluidos los centros de control, aeropuertos y equipo, lo que abarca los sistemas de comunicaciones, navegación y vigilancia (CNS) y de información.

***Objeto sospechoso (TOI).*** Objeto en el aire, representado en la pantalla, que plantea una amenaza o posible amenaza a la seguridad. Entre los indicadores de un posible TOI cabe señalar los siguientes:

1. Incumplimiento de instrucciones de ATC o reglamentos aeronáuticos;

2. Pérdida de comunicaciones prolongada;

3. Transmisiones o conducta de vuelo inhabituales;

4. Entrada no autorizada en espacio aéreo controlado o zona de identificación para fines de seguridad;

5. Incumplimiento de restricciones temporales en el espacio aéreo y los vuelos dictadas u otras restricciones de vuelo o procedimientos de seguridad emitidos; y

6. Interferencia ilícita con tripulaciones de vuelo en el aire, incluido el secuestro.

En ciertas circunstancias, un objeto en el aire puede convertirse en TOI basándose en información específica y creíble relativa a dicha aeronave u objeto, sus pasajeros o su carga.

***Protección de la infraestructura del sistema ATM.*** Protección de la infraestructura del sistema ATM mediante seguridad de la tecnología de la información y las comunicaciones (ICT), seguridad física y seguridad relacionada con el personal.

***Proveedor de servicios de tránsito aéreo (ATSP).*** En la Enmienda 12 del Anexo 17 se utiliza el término ATSP en la norma relativa a la seguridad de la aviación. Por consiguiente, se utiliza también en el presente manual para fines de coherencia con la norma de la OACI. Sin embargo, los Estados que, por ley, deben utilizar la expresión “proveedor de servicios de navegación aérea” (ANSP) deberían reemplazar ATSP por ANSP. ANSP debería considerarse como sinónimo de ATSP, utilizado en el presente manual.

***Restricciones temporales en el espacio aéreo y los vuelos.*** Procedimientos ATM establecidos mediante avisos a los aviadores (NOTAM) en que se disponen restricciones

geográficamente limitadas y a corto plazo a actividades de vuelo específicas por motivos de seguridad nacional, imposición de la ley o seguridad operacional. En dichas restricciones se especifican los procedimientos ATM relacionados con zonas temporales de identificación para fines de seguridad que refuerzan la seguridad de la aviación, la seguridad operacional y el uso flexible del espacio aéreo que se necesita para actividades como eventos nacionales, grandes eventos deportivos, espectáculos aéreos, gestión de crisis en caso de catástrofes naturales, lanzamientos espaciales y desplazamientos de líderes nacionales. Estas restricciones son diferentes a las zonas restringidas de la OACI y constituyen condiciones de vuelo impuestas a raíz de la aplicación del reglamento del aire o prácticas o procedimientos de los servicios de tránsito aéreo y no pueden designarse como zonas restringidas.

***Riesgo.*** Posibilidad de un resultado no deseado causado por un incidente, evento o suceso. El riesgo puede estimarse considerando la probabilidad de amenazas, vulnerabilidades y consecuencias o repercusiones.

***Seguridad de ICT.*** Aplicación de medidas de seguridad para proteger la información y los datos procesados, almacenados y transmitidos en sistemas ICT (análogos y digitales) contra pérdida accidental o intencional de integridad, confidencialidad y disponibilidad, y evitar la pérdida de integridad o disponibilidad de los propios sistemas. Dichas medidas abarcan las relativas a protección de computadoras y redes (cibersistemas), transmisión de información y datos, emisión y seguridad criptográfica, así como detección, documentación y neutralización de amenazas a la información y las comunicaciones y a los sistemas ICT.

*Integridad* significa proteger contra la modificación o destrucción indebida de información y asegurar el no repudio y la autenticación de la información.

*Confidencialidad* significa preservar las restricciones autorizadas al acceso y la divulgación, incluidos los medios de protección de la privacidad personal y la información de propiedad exclusiva.

*Disponibilidad* significa asegurar un acceso oportuno y fiable a la información y su uso.

***Seguridad de la aviación.*** Protección de la aviación civil contra los actos de interferencia ilícita. Este objetivo se logra mediante una combinación de medidas y recursos humanos y materiales.

***Seguridad de la gestión del tránsito aéreo.*** Protección del sistema ATM contra amenazas y vulnerabilidades relacionadas con la seguridad y contribución del sistema ATM a la seguridad de la aviación civil, la seguridad y defensa nacionales y la imposición de la ley.

***Seguridad física.*** Parte de la seguridad relacionada con medidas físicas elaboradas para proteger a las personas, impedir el acceso no autorizado a equipo, instalaciones, material y documentos y protegerlos contra un incidente relacionado con la seguridad.

***Seguridad relacionada con el personal.*** Parte de la seguridad relacionada con procedimientos elaborados para determinar si puede otorgarse acceso inicial y continuo a información confidencial y zonas controladas a una persona, teniendo en cuenta su lealtad, honradez y fiabilidad, sin que constituya un riesgo inaceptable para la seguridad.

***Sistema de gestión del tránsito aéreo.*** Sistema que proporciona ATM mediante la

integración, en colaboración, de seres humanos, información, tecnología, instalaciones y servicios, con el apoyo de comunicaciones, navegación y vigilancia basadas a bordo, en tierra o en el espacio.

***Solución relativa a un objeto sospechoso (TOI).*** Un caso de TOI se considerará normalmente resuelto cuando:

1. La aeronave o el objeto ya no esté en vuelo;
2. La aeronave cumpla las instrucciones de ATC, los reglamentos de la aviación o las restricciones de vuelo o los procedimientos de seguridad emitidos, incluidas las restricciones temporales en el espacio aéreo y los vuelos;
3. Se restablezca el contacto por radio y se verifique el control autorizado de la aeronave;
4. Se intercepte la aeronave y se confirme que no tenía intención amenazadora u hostil;
5. Se haya identificado el TOI basándose en información específica y creíble que luego se determinó como inválida o poco fiable; y
6. Se determinen y clasifiquen como válidos los datos presentados.

***Tecnología de la información y las comunicaciones (ICT).*** Expresión amplia que incluye todo dispositivo (análogo o digital) de información o comunicación o aplicación y abarca: radio, televisión, teléfonos, teléfonos inteligentes, equipo SmartPad, soportes físicos y lógicos de computadoras y redes, sistemas y dispositivos de almacenamiento de datos, sistemas de satélite, sistemas de vigilancia, sistemas de navegación, así como los diversos sistemas y aplicaciones asociados con los mismos.

***Vulnerabilidad.*** Característica física o atributo operacional debido a los cuales una entidad, activo, sistema, red o zona geográfica se exponen a explotación o ataque o son susceptibles a determinado peligro. La vulnerabilidad aumenta el riesgo de repercusiones negativas a raíz de un incidente, evento o suceso.

## 6 ACRÓNIMOS

1. Los acrónimos empleados en este manual o en otros manuales de la DGAC relacionados con la seguridad de aviación tienen el significado siguiente:

- ADS-B Vigilancia dependiente automática — radiodifusión ADS-C Vigilancia dependiente automática — contrato ATC Control de tránsito aéreo
- ATIS Servicio automático de información terminal
- ATM Gestión del tránsito aéreo
- ATS Servicios de tránsito aéreo
- ATSP Proveedor de servicios de tránsito aéreo
- CAA Administración de aviación civil
- CBRN Químico, biológico, radiológico y nuclear CNS Comunicaciones, navegación y vigilancia COMLOSS Pérdida de radiocomunicaciones
- CPDLC Comunicaciones por enlace de datos controlador-piloto ETA Hora prevista de llegada
- FIR Región de información de vuelo

- FL Nivel de vuelo
- HVAC Calefacción, ventilación y aire acondicionado
- ICT Tecnología de la información y las comunicaciones
- IDENT Elemento de identificación en el sistema de identificación amigo/enemigo (IFF) IED Artefacto explosivo improvisado
- IFF Identificación amigo/enemigo
- IFSO Oficial de seguridad de a bordo
- IT Tecnología de la información
- LEA Autoridad de imposición de la ley
- LOA Carta de acuerdo
- MANPADS Sistemas portátiles de defensa antiaérea MOA Memorando de acuerdo
- MOU Memorando de acuerdo
- NAVAID Ayuda para la navegación
- NCASP Programa nacional de seguridad de la aviación civil NEXTGEN Sistema de transporte aéreo de la próxima generación NGA Autoridad gubernamental nacional
- NOTAM Aviso a los aviadores
- NSA Autoridad nacional de supervisión
- OACI Organización de Aviación Civil Internacional
- OMS Organización Mundial de la Salud
- PANS Procedimientos para los servicios de navegación aérea QRA Alerta de reacción rápida
- RPA Aeronave pilotada a distancia
- RPG Granada propulsada por cohete
- RTF Instalación de transmisión radioeléctrica SARPS Normas y métodos recomendados
- SESAR Investigación ATM en el marco del cielo único europeo SOP Procedimiento operacional normalizado
- SRM Gestión de riesgos para la seguridad operacional
- SSR Radar secundario de vigilancia
- SWIM Gestión de la información de todo el sistema TOI Objeto sospechoso
- UAS Sistema de aeronave no pilotada
- UE Unión Europea
- VFR Reglas de vuelo visual
- VHF Muy alta frecuencia
- VIP Personalidad destacada
- VOR Radiofaro omnidireccional VHF

# 7 BASE LEGAL

## 7.1 NACIONAL

| ENTIDAD | DOCUMENTO |
|---|---|
| **Congreso de la República de Guatemala** | • Ley de Aviación Civil. Decreto 93-2000 |
| **Presidencia de la República** | • Reglamento de la Ley de Aviación Civil. Acuerdo Gubernativo 384-2001 |

## 7.2 INTERNACIONAL

Debido al carácter internacional de la aviación, una seguridad eficaz exige la participación de todos los Estados. Con objeto de lograr una aplicación uniforme de las disposiciones relativas a la seguridad, se han elaborado varios instrumentos jurídicos internacionales (convenios) que constituyen una base para la aplicación uniforme de las disposiciones relativas a la seguridad en el mundo entero.

Los convenios siguientes se relacionan específicamente con la interferencia ilícita en las aeronaves:

1. Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves (Convenio de Tokio), firmado en Tokio el 14 de septiembre de 1963.
2. Convenio para la represión del apoderamiento ilícito de aeronaves (Convenio de La Haya), firmado en La Haya el 16 de diciembre de 1970.
3. Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil (Convenio de Montreal), firmada en Montreal el 23 de septiembre de 1971.
4. Protocolo para la represión de actos ilícitos de violencia en los aeropuertos que presten servicio a la aviación civil internacional, complementario del Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, hecha en Montreal, firmada en Montreal el 24 de febrero de 1988.
5. Convenio sobre la marcación de explosivos plásticos para los fines de detección, hecho en Montreal el 1 de marzo de 1991.
6. Convenio para la represión de actos ilícitos relacionados con la aviación civil internacional (Convenio de Beijing), hecha en Beijing el 10 de septiembre de 2010.
7. Protocolo complementario del Convenio para la represión del apoderamiento ilícito de aeronaves (Protocolo de Beijing), hecho en Beijing el 10 de septiembre de 2010.

Dichos convenios cubren una amplia gama de categorías de interferencia ilícita en aeronaves, instalaciones y servicios de navegación aérea y aeropuertos.

En el presente contexto, el aspecto más importante de las disposiciones contenidas en dichos convenios consiste en que se obliga a los Estados parte en los mismos a promulgar legislación para que los actos definidos en los convenios se consideren como delitos punibles mediante sanciones rigurosas en virtud de sus leyes.

# 8 OBJETIVOS

## 8.1 OBJETIVO GENERAL

1. El objetivo del presente Manual es apoyar en el cumplimiento de las operaciones, desarrollo, requisitos y disposiciones relativas con relación a la Seguridad de la Gestión de los Servicios de Tránsito Aéreo.

## 8.2 OBJETIVOS ESPECIFICOS

1. Proveer al personal de la Gerencia de Navegación Aérea los procedimientos a utilizar en la realización de las funciones y actividades asignadas por parte de la Dirección General de Aeronáutica Civil mediante:

   a) Mejorar los procedimientos de control con los que cuenta esta Dirección General;

   b) Mejorar la eficiencia de las operaciones en lo relativo a la seguridad de la gestión del de los servicios de tránsito aéreo con los que cuenta esta Dirección General, dentro del marco legal correspondiente;

   c) Mejorar la eficacia de las operaciones por parte de la entidad.

   d) Tener una guía adicional, para procedimientos de aeronaves que estén siendo objeto de interferencia ilícita.

   e) La generación de información útil, oportuna, confiable y razonable sobre el control con los que cuenta la Dirección General de Aeronáutica Civil;

   f) La utilización eficiente de los recursos de la institución;

   g) La aplicación de las leyes, reglamentos, políticas y procedimientos diseñados para el buen funcionamiento del Estado y sus entidades;

   h) La motivación del personal a tener la capacidad administrativa para reaccionar frente a los estímulos negativos de su entorno, para que esté en condiciones de identificar, comprobar e impedir, posibles malos manejos de los recursos disponibles, así como identificar los riesgos existentes.

2. Establecer claramente la responsabilidad y autoridad que tiene cada persona para desempeñar las funciones en el proceso. Asimismo, es importante que quede evidencia escrita de lo que hace cada persona que participa en los diferentes procesos que lleva la Gerencia de Navegación Aérea.

3. No caer en un manejo excesivo de papelería o en trámites que en lugar de facilitar la operación de control.

## 9 GENERALIDADES DEL MANUAL DE NORMAS Y PROCEDIMIENTOS PARA LA SEGURIDAD ATM.

1. El manual está dirigido a dar normas y procedimientos de Seguridad de la Gestión de Tránsito Aéreo.

2. El presente Manual, brinda una descripción detallada de los procedimientos que se llevan a cabo en la Gerencia de Navegación Aérea de la DGAC, para su debido funcionamiento. En relación a la seguridad de la gestión de tránsito aéreo.

3. El Manual pretende que se realicen los procesos de la seguridad de la gestión de los servicios de tránsito aéreo, así como el registro y control de los bienes, para asegurar que los recursos de la DGAC produzcan los resultados esperados. Y se lleven a cabo las funciones de los servicios de tránsito aéreo en forma segura, para el personal y los equipos utilizados para proporcionar los servicios.

4. Para el cumplimiento del objetivo del manual, es necesario que este instrumento sea socializado al interior de la Institución, incluyendo capacitación formal. Esto permitirá al personal enterarse y empoderarse de sus responsabilidades como parte activa del proceso.

5. El manual es un instrumento que regula los procedimientos internos y el flujo de los procedimientos de la Gerencia de Navegación Aérea. Es un objetivo el que sea un documento clarificador de cómo se lleva el control de los bienes dentro de la institución, quienes participan de este proceso y las responsabilidades.

## 10 ACTUALIZACION DEL MANUAL

1. Este documento constituye un proyecto que debe ser discutido, aceptado y/o modificado por las diversas unidades y en coordinación con la GRRHH de la DGAC que de una forma u otra, van a verse obligados a someterse a lo que en él se dispone. Con la aprobación posterior del Despacho Superior de la DGAC el manual entrará en vigor.

2. El manual se actualizará cuando se presenten circunstancias que así lo aconsejen o justifiquen.

3. En principio, y salvo acuerdo en contrario, se deberá efectuar una primera revisión al cumplirse tres (3) meses de su implantación. Posteriormente será revisado y actualizado al menos una (1) vez al año.

4. Para facilitar su actualización las páginas del manual serán intercambiables.

5. Se distinguirán dos opciones modificación y nueva edición. La modificación afectará a algunos de los puntos tratados en el manual (de una a tres páginas); cuando haya muchas modificaciones se procederá a una nueva edición.

6. Las modificaciones podrán ser por iniciativa del personal de la Gerencia de Navegación Aérea o solicitadas por cualquier persona de la institución, razonando sus causas.

## 11 ALCANCE

1. Los procedimientos abarcan principalmente a todas las áreas de la DGAC donde se desarrollen los procesos a nivel administrativo, operativo, financiero y demás actividades relacionadas con el uso y salvaguarda de los recursos de la institución.

2. El contenido del presente documento es aplicable a todos los funcionarios de la Gerencia de Navegación Aérea de la DGAC que desarrollan actividades dentro y fuera de las instalaciones de la DGAC y en los Aeropuertos Internacionales y Nacionales en territorio guatemalteco.

3. También es aplicable a todos aquellos que desarrollan actividades relacionadas con la seguridad de la Gestión de Tránsito Aéreo en los aeropuertos y aeródromos en el territorio guatemalteco.

4. Al ejercer los Recursos del Estado, las Unidades Administrativas y Técnico-operativas de la DGAC deberán contar con el soporte documental de los procedimientos de la Gerencia de Navegación Aérea, elegidos conforme a la normativa vigente.

## 12 ANTECEDENTES

El primer decenio del siglo XXI presenció un aumento en actividades terroristas contra una gama de objetivos utilizando diversos métodos que van del uso de artefactos explosivos para atacar aeronaves, trenes y edificios a ciberataques contra sistemas de información y comunicaciones. Como resultado de ello, algunos Estados han expresado su inquietud respecto a la posibilidad de que se atacara el sistema de gestión del tránsito aéreo (ATM); así, la protección del sistema ATM contra amenazas relativas a la seguridad se ha convertido en un tema de creciente inquietud.

Al mismo tiempo, los proveedores de servicios de tránsito aéreo (ATSP) han estado participando con mayor frecuencia en funciones de apoyo en situaciones de seguridad nacional e imposición de la ley, incluidas operaciones de prevención y recuperación en caso de catástrofes, no dirigidas intencionalmente contra el sistema de aviación, pero cuyas repercusiones serían profundas y negativas si no se aplicara una gestión eficaz. En dichas situaciones a menudo se exige la aplicación de procedimientos ATM, tales como restricciones temporales en el espacio aéreo y los vuelos, que constituyen medidas necesarias de seguridad operacional y protección y minimizan las repercusiones de los sucesos relacionados con la seguridad en las operaciones de vuelo en el sistema ATM.

## 13 RESPONSABILIDADES DEL ESTADO EN MATERIA DE SEGURIDAD DE LA AVIACIÓN

Legislación

La primera etapa para un Estado que establezca la seguridad de la aviación consiste en promulgar la legislación necesaria para dar efecto a los mencionados convenios. Dado que las normas y métodos recomendados (SARPS) relativos a la seguridad de la aviación pasaron a ser aplicables a partir de 1975, normalmente debería haberse adoptado ya la legislación del caso. Sin embargo, al implantar la seguridad de ATM por primera vez, los Estados deberían verificar si su legislación cubre debidamente los actos de interferencia ilícita en las instalaciones de servicios de tránsito aéreo, así como el suministro de servicios de seguridad de ATM exigidos por el programa nacional

de seguridad de la aviación civil (NCASP).

Aunque la definición de los delitos y la imposición de sanciones para actos de interferencia ilícita en la aviación son importantes, es también importante adoptar medidas para asegurar, en la medida de lo posible, la protección de la totalidad del sistema de aviación contra amenazas a su seguridad. Ningún sistema de seguridad puede garantizar que las medidas de protección permitirán evitar todos los ataques; por ello, la elaboración y aplicación de procedimientos para responder a los casos de interferencia ilícita deben incluirse en la planificación de la seguridad.

Programa nacional de seguridad de la aviación civil (NCASP)

En el Anexo 17 se exige que los Estados elaboren y apliquen un NCASP, en que se especifiquen las funciones y responsabilidades de todas las organizaciones y entidades, incluidos los ATSP, que puedan participar en operaciones relativas a la seguridad. El NCASP cubre la gama completa de actividades de seguridad incluidas, entre otras cosas, la evaluación de amenazas y riesgos, la selección y capacitación del personal (respecto a la seguridad), el control del acceso y otras medidas preventivas, la gestión de los actos de interferencia ilícita y el control de la calidad.

No todas las disposiciones del NCASP se aplicarán a ATSP. En el NCASP se determinan las responsabilidades específicas de cada una de las partes que desempeñan una función en las operaciones relacionadas con la seguridad.

A fin de asegurar la eficacia del NCASP, cada Estado debería promulgar legislación para crear una autoridad competente en materia de seguridad de la aviación a la que incumbirá la elaboración del NCASP y su enmienda, de ser necesario. También debería promulgar legislación en que se exija que las partes que tengan responsabilidades en virtud del NCASP apliquen disposiciones apropiadas en materia de seguridad para satisfacer las disposiciones del NCASP.

Comité nacional de seguridad de la aviación civil

Dado que el mantenimiento de la seguridad en la totalidad del sistema de aviación abarca numerosos organismos y organizaciones diferentes, en el Anexo 17 se exige que los Estados establezcan un Comité nacional de seguridad de la aviación civil. Su función consiste en facilitar la coordinación de las actividades relativas a la seguridad entre dichos organismos y organizaciones. Integran dicho comité representantes de todas las partes que desempeñan una función en virtud del NCASP. Según la estructura de los servicios en cada Estado, esto puede incluir (además de la autoridad competente en materia de seguridad de la aviación) Representantes de las siguientes instituciones:

1. ATSP;
2. Explotadores de aeronaves;
3. Explotadores de aeropuertos;
4. Autoridades de aduana;
5. Autoridades de inmigración;
6. Servicios de inteligencia;
7. Autoridad de imposición de la ley (lea);
8. Sector militar; y

9. Proveedores de servicios de seguridad contratados.

Comité de seguridad del aeropuerto

Además del Comité nacional de seguridad de la aviación civil, en el Anexo 17 se exige la creación de un comité de seguridad del aeropuerto para cada aeropuerto civil, en que debería estar representada la dependencia local de servicios de tránsito aéreo (ATS).

**Coordinación internacional**

Aunque la seguridad de la aviación sigue siendo una responsabilidad nacional, la creciente posibilidad de amenazas internacionales exige el mantenimiento de un alto nivel de cooperación entre los Estados. La autoridad competente en materia de seguridad de la aviación civil debería establecer procedimientos de coordinación con las autoridades correspondientes en los Estados adyacentes; además, deberían concertarse acuerdos relativos al intercambio de información sobre seguridad. Las dependencias ATS deberían haber elaborado ya cartas de acuerdo (LOA) con las dependencias ATS adyacentes dentro de uno o varios Estados, describiéndose en detalle los procedimientos de comunicaciones y coordinación. Si en dichas LOA no figuran procedimientos relativos a la seguridad, estas deberían actualizarse como parte de la planificación para aplicar procedimientos de seguridad de ATM.

Esta colaboración y cooperación es necesaria para que las políticas y disposiciones de gestión de la seguridad de ATM permitan afrontar eficazmente toda la gama de actos de interferencia ilícita, terrorismo u otros sucesos que amenacen a personas o instalaciones y servicios o puedan perturbar la capacidad del sistema ATM para proporcionar servicios.

## 14 DISTINCION ENTRE SEGURIDAD DE LA AVIACIÓN Y SEGURIDAD DE ATM

Dentro de las de las funciones de la seguridad a la gestión de los servicios de tránsito aéreo se incluye:

1) Aplicar los SARPS relativos a la seguridad de la aviación
2) Proteger la infraestructura del sistema ATM
3) Desempeñar otras funciones relacionadas con la seguridad.

**Definición de seguridad de la aviación**

El objetivo principal de la seguridad de la aviación consiste en “garantizar la seguridad y protección de los pasajeros, las tripulaciones, el personal de tierra, el público en general, las aeronaves y las instalaciones y servicios de los aeropuertos

Normas y métodos recomendados (SARPS) relativos a la seguridad de la aviación

En la novena edición (2011) del Anexo 17 — *Seguridad,* de la OACI, la importancia de la función de los ATSP en materia de seguridad de la aviación se reconoce mediante la introducción de los dos SARPS siguientes en la Enmienda 12:

“3.5 Proveedores de servicios de tránsito aéreo. Cada Estado contratante exigirá que los proveedores de servicios de tránsito aéreo que operan en su Estado establezcan y apliquen disposiciones de seguridad apropiadas para satisfacer los requisitos del programa nacional de seguridad de la aviación civil de ese Estado.”

“4.9 Medidas relativas al ciberterrorismo. Cada Estado contratante deberá elaborar medidas para proteger los sistemas de tecnología de la información y las comunicaciones empleados para los fines

de la aviación civil, contra interferencias que pudieran poner en peligro la seguridad operacional de la aviación civil."

Los ATSP contribuyen a la seguridad de la aviación en la prevención de los actos de interferencia ilícita y la respuesta a los mismos, lo que generalmente abarca la gestión del espacio aéreo por ATSP para fines de seguridad de ATM.

El Proveedor de servicios de tránsito aéreo, ha establecido cartas de acuerdo operacional y de cooperación en materia de seguridad del espacio aéreo Nacional.

La seguridad de ATM contribuye a la seguridad de la aviación dado su objetivo de proteger a la aviación civil contra actos de interferencia ilícita. Estos actos o tentativas comprometen, por su carácter, la seguridad de la aviación civil y pueden incluir otros aspectos como:

1. Apoderamiento ilícito de aeronaves en vuelo o en tierra;

2. Destrucción de una aeronave en servicio;

3. Toma de rehenes a bordo de aeronaves o en aeródromos;

4. Intrusión por la fuerza a bordo de una aeronave, en un aeropuerto o el recinto de una instalación aeronáutica;

5. Introducción a bordo de una aeronave o en un aeropuerto de armas, artefactos peligrosos o sustancias con fines criminales;

6. Uso de una aeronave en servicio con el propósito de causar la muerte, lesiones corporales graves o daños graves a los bienes o al medio ambiente; y

7. Comunicación de información falsa que comprometa la seguridad de una aeronave en vuelo o en tierra o la seguridad de pasajeros, tripulación, personal de tierra y público en un aeropuerto o en el recinto de una instalación de aviación civil.

**Definición de seguridad de ATM**

La seguridad de ATM abarca una amplia gama de aspectos que no se limitan a la seguridad de la aviación. La seguridad de ATM se define en la Circular 330 – *Cooperación cívico-militar para la gestión del tránsito aéreo*, de la OACI, como:

"La contribución del sistema ATM en la protección de la aviación civil, la seguridad y la defensa nacional, la aplicación de la ley y la protección del sistema de ATM contra las amenazas a la seguridad y las vulnerabilidades."

**El doble requisito de la seguridad de ATM**

La seguridad de ATM difiere de la seguridad de la aviación porque tiene el doble objetivo de proteger al sistema ATM contra amenazas y vulnerabilidades y suministrar servicios de seguridad de ATM para apoyar las organizaciones y autoridades que se ocupan de seguridad de la aviación, seguridad nacional, defensa e imposición de la ley. Así, la función de seguridad de ATM posee un elemento interno tradicional de protección del propio sistema ATM y un elemento operacional de apoyo a ciertos aspectos de la seguridad de la aviación, la seguridad nacional y la imposición de la ley.

**Protección contra amenazas y servicios de seguridad**

"La seguridad de la aviación se refiere a la protección frente a amenazas provenientes de actos intencionales (p. ej., terrorismo) o no intencionales (p. ej., errores humanos, desastres naturales) que afecten a aeronaves, personas o instalaciones en tierra. La seguridad adecuada de la aviación es una expectativa principal de la comunidad ATM... Por consiguiente, el sistema ATM debería contribuir a la seguridad de la aviación, y el sistema ATM, así como la información relacionada con ATM, deberían estar protegidos frente a amenazas a la seguridad de la aviación."

**Continuidad del servicio ATM**

"La realización del concepto [continuidad de servicio] requiere medidas de contingencia para proporcionar la máxima continuidad del servicio frente a interrupciones importantes, desastres naturales, perturbaciones civiles, amenazas a la seguridad y otras circunstancias inusuales."

Otros servicios de seguridad:

Las entidades esenciales a las que el sistema ATM proporcionará información o que podrán recibir información del mismo. Estas incluyen, en el dominio de seguridad de la aviación, las siguientes entidades:

1. Los sistemas de defensa aérea y los sistemas de vigilancia militar necesitarán información oportuna y precisa sobre los vuelos y las intenciones del sistema ATM. Participarán en las reservas de espacio aéreo y la notificación de actividades aéreas, así como en la aplicación de medidas relacionadas con la seguridad de la aviación;

2. Las organizaciones de búsqueda y salvamento SAR, necesitarán información oportuna y precisa relativa a la búsqueda y salvamento de aeronaves en peligro y accidentes puesto que tal información desempeña una función importante en la calidad de la función de búsqueda;

3. Las autoridades de investigación de accidentes e incidentes de aviación necesitarán utilizar los registros de datos de trayectoria de vuelo y acciones de ATM;

4. Las autoridades de imposición de la ley (incluidas las autoridades de aduanas y de policía) necesitarán identificación y datos de trayectoria de los vuelos, así como información acerca del tránsito en los aeródromos; y

5. Las autoridades de reglamentación necesitarán aplicar el marco normativo, dentro de los límites de las facultades jurídicas que se les han conferido, y supervisar el estado de la seguridad operacional del sistema ATM.

## ALCANCE

Alcance de la seguridad de ATM —

La seguridad de ATM abarca los servicios de seguridad que figuran en los SARPS relativos a la seguridad de la aviación e incluye lo siguiente:

**1.** Protección del sistema ATM contra amenazas y vulnerabilidades en materia de seguridad (protección de ATM); y

**2.** Suministro de servicios de seguridad que contribuyen a la seguridad de la aviación civil, la

seguridad nacional, la defensa y la imposición de la ley (operaciones de seguridad de ATM).

**3.** La protección de ATM se refiere a servicios internos de seguridad proporcionados por ATSP y destinados al mismo, como los siguientes:

a. Servicios de ciberseguridad para proteger los cibersistemas; y

b. Protección física de las instalaciones y servicios.

**4.** Las operaciones de seguridad de ATM se relacionan con servicios de seguridad externos proporcionados por ATSP, pero utilizados por entidades estatales, organismos y partes interesadas. Se indican a continuación algunos ejemplos de servicios de seguridad externos:

Apoyo a una interdicción aérea de defensa;

1. Medidas de búsqueda y salvamento;
2. Asistencia para una respuesta de imposición de la ley (p. Ej., protección fronteriza);
3. Control de tránsito aéreo (ATC) durante una interferencia ilícita en una aeronave en vuelo;
4. Desplazamientos de personalidades; y
5. Apoyo a respuestas de emergencia a catástrofes naturales.

## PARTE I

# 15 PROTECCIÓN DE LA INFRAESTRUCTURA DEL ATM

## 15.1 ANTECEDENTES

La definición de seguridad de ATM incluye la protección del sistema ATM contra amenazas y el apoyo que dicho sistema aporta a las organizaciones y autoridades que desempeñan funciones de seguridad de la aviación, seguridad nacional, defensa e imposición de la ley.

En la Parte I del manual se examina la protección de la infraestructura del sistema ATM y en la Parte II el suministro de servicios de seguridad de ATM para satisfacer diversos requisitos de seguridad de la organización.

La infraestructura del sistema ATM incluye personas, procedimientos, información, recursos, instalaciones y equipo. Las instalaciones abarcan centros de control y aeropuertos. El equipo incluye sistemas de comunicaciones, navegación y vigilancia (CNS) y de información.

La protección de la infraestructura del sistema ATM se refiere a su protección mediante seguridad de la tecnología de la información y las comunicaciones, seguridad física y seguridad relacionada con el personal. También abarca las disposiciones relativas a la continuidad del servicio durante una emergencia o catástrofes.

El programa de seguridad de ATM para la protección de la infraestructura posee los componentes siguientes:

1. Seguridad física;

2. Seguridad relacionada con el personal;

3. Seguridad de la tecnología de la información y las comunicaciones (ict); y

4. Planificación de contingencia en materia de seguridad para resolver problemas de seguridad relacionados con la recuperación en caso de catástrofes y la continuidad de las operaciones.

## 15.2 PRINCIPIOS DE PROTECCIÓN DE LA INFRAESTRUCTURA DEL SISTEMA ATM

**Programa de seguridad para apoyar las misiones de ATSP**

El programa de seguridad permite a la organización del proveedor de servicios de tránsito aéreo (ATSP) llevar a cabo sus misiones operacionales y se ha convertido en una necesidad para neutralizar las amenazas y reducir las vulnerabilidades. Al reforzar las medidas de seguridad, es importante recordar que esta no constituye un fin en sí. Un programa de seguridad permite que ATSP realice sus misiones de manera coherente respecto a las expectativas de las partes interesadas. El programa de seguridad protege a ATSP contra degradaciones del servicio y asegura la integridad, confidencialidad y disponibilidad de las funciones operacionales de la organización. Sin embargo, la práctica en materia de seguridad no debería impedir la ejecución de las misiones de ATSP o la de sus organismos operacionales. Al evaluar diversas fórmulas de control de la seguridad, ATSP debería comparar los beneficios en materia de seguridad con las repercusiones en la eficiencia y eficacia de las funciones operacionales.

**Gestión de la seguridad basada en el riesgo**

La gestión del riesgo constituye un elemento fundamental de los programas de seguridad de la organización ATSP. Mientras que el concepto de riesgo cero podría ser atrayente, es imposible diseñar un programa de seguridad libre de riesgos. Las organizaciones ATSP pueden maximizar el valor de la inversión en un programa de seguridad estableciendo una estrategia y objetivos que logren un equilibrio óptimo entre las metas operacionales y los riesgos correspondientes y utilizando los recursos eficiente y efectivamente. Basándose en niveles aceptables de riesgo, ATSP debería evaluar y seleccionar posibles métodos de atenuación de riesgos para la gestión de estos últimos.

**Gestión integrada de la seguridad**

La gestión, por ATSP, de los riesgos para la seguridad constituye una tarea compleja y multifacética que exige un enfoque integral, plenamente integrado en cada aspecto de la organización. La seguridad de ATM deberá analizarse considerando elementos clave del sistema ATM, incluidas las personas, los procedimientos, los sistemas ICT y otras categorías de equipo técnico e instalaciones con sus infraestructuras de apoyo. Mientras que las medidas de seguridad para dichos componentes exigen diversos especialistas, las decisiones globales en materia de gestión de la seguridad deberían considerarse primero a nivel de la organización. Estos elementos no son independientes, pero se relacionan entre sí en su aporte a la entrega de servicios.

ATSP es tan seguro como su eslabón más débil. Por ejemplo, los controladores de tránsito aéreo que hayan recibido capacitación deficiente pueden comprometer la protección de un sistema ICT debidamente diseñado. Además, las medidas de seguridad para un

componente de ATSP pueden aprovechar el aporte de otros elementos (p. ej., el control físico del acceso constituye una capa de seguridad para activos críticos de información dentro de la instalación). El enfoque integral permite entender las diversas relaciones, promoviendo así un enfoque completo, coherente y eficiente. Por lo que la Gerencia de seguridad aeroportuaria tendrá la responsabilidad de reforzar aquellas áreas de acceso que sean vulnerables, a los servicios de tránsito aéreo.

Las primeras medidas en materia de seguridad se han centrado en medios de protección para reducir la probabilidad de ataques efectivos. Con las amenazas cada vez mayores y la vulnerabilidad de los sistemas abiertos, es necesario que las medidas de seguridad atenúen las consecuencias de acontecimientos adversos y posiblemente catastróficos. El programa de seguridad de la gestión de tránsito aéreo cubre los siguientes elementos:

1. Capacidad más eficaz de detección de ataques;
2. Reducción de la vulnerabilidad a los ataques;
3. Elaboración de medidas de contingencia para reducir las repercusiones de la pérdida de cualquier elemento del servicio ATM; y
4. Reducción del plazo de recuperación a fin de atenuar las repercusiones de un ataque.

# 16 GOBERNANZA Y ORGANIZACION

## 16.1 OBJETIVOS DEL PROGRAMA

Los objetivos del programa de seguridad de ATSP para la protección de la infraestructura del sistema ATM Son los siguientes

1. La seguridad de la aviación y el objetivo principal de garantizar la protección y seguridad de pasajeros, tripulaciones, personal de tierra, público en general, aeronaves e instalaciones de un aeropuerto que presta servicios a la aviación civil en todo lo relacionado con la protección contra actos de interferencia ilícita perpetrados en tierra o en vuelo; y

2. La ejecución de las misiones de ATSP y reducción al mínimo de la perturbación del servicio atm causada por amenazas intencionales o involuntarias.

## 16.2 AUTORIDAD AERONAUTICA

De acuerdo a la Ley de Aviación Civil, En el artículo 6 establece que La Dirección General de Aeronáutica Civil, es el órgano encargado de normar, supervisar, vigilar y regular, con base en lo prescrito en la Ley citada, reglamentos, regulaciones y disposiciones complementarias, los servicios aeroportuarios, los servicios de apoyo a la navegación aérea, los servicios de transporte aéreo, de telecomunicaciones y en general todas las actividades de aviación Civil en el territorio y espacio aéreo de Guatemala, velando en todo momento por la defensa de los intereses nacionales.

### 16.2.1 VIGILANCIA ESTATAL

El Estado a través de la Dirección General de Aeronáutica Civil tiene la responsabilidad de vigilancia respecto a la seguridad de ATM. Si bien la vigilancia de la seguridad de la aviación se define como una función que permite a los Estados asegurarse de la aplicación efectiva de las normas y métodos recomendados (SARPS) y procedimientos conexos relacionados con la seguridad, contenidos en los Anexos al Convenio de Chicago (principalmente en el Anexo 17, pero también en las disposiciones relativas a la seguridad en el Anexo 9) y documentos conexos

de la Organización de Aviación Civil Internacional (OACI).

## 16.3 MARCO DE REGLAMENTACIÓN

El programa de seguridad de ATSP para la protección de la infraestructura se rige en diversos reglamentos nacionales relativos a la seguridad de la aviación, la seguridad de ICT y la protección de infraestructura crítica En este contexto para velar por la seguridad ATSP, Se establecen los comités siguientes:

1. El comité nacional de seguridad de la aviación civil;

2. El comité de seguridad aeroportuaria; y

3. La planificación, capacitación y prácticas para responder a interferencia ilícita o apoderamiento de aeronaves.

En cada comité habrá un representante titular y un suplente de los Servicios de Tránsito Aéreo.

## 16.4 POLÍTICA DE SEGURIDAD:

La política de seguridad constituye la primera etapa del compromiso de ATSP para mejorar su eficacia en materia de seguridad. Las políticas de seguridad de ATSP dan la pauta y el contexto para sus disposiciones relativas a la seguridad. Captan la percepción de la seguridad por la administración superior y la intención y orientación globales de la organización. Una política de seguridad es funcional e informativa. Desde el punto de vista funcional, orienta a la organización ATSP en sus acciones actuales y futuras. Desde el punto de vista de la información de la política, comunica a las partes interesadas y al público el compromiso de ATSP respecto a la seguridad.

La organización ATSP que apoya la seguridad de la aviación debería también influir en las entidades o personas responsables de la seguridad de las operaciones y del programa de seguridad para la protección de la infraestructura del sistema ATM. Esto se logra a través de los comités de seguridad de los aeropuertos.

El programa de seguridad para la gestión ATM, se define principalmente en las áreas siguientes:

1. Objetivos estratégicos de la seguridad para la organización ATM;

2. Tolerancia al riesgo (niveles aceptables o tolerables de riesgo); y

3. Motivos para evaluar riesgos.

Objetivos estratégicos de la seguridad. Los objetivos estratégicos de la seguridad definen los objetivos, requisitos jurídicos y reglamentarios y obligaciones respecto a terceros en materia de servicios y orientan la actividad siguiente del marco de gestión de la seguridad. Garantizan que el alcance y la evaluación de las repercusiones de la amenaza en los activos críticos de la infraestructura son pertinentes y corresponden a los objetivos estratégicos. Por consiguiente, los objetivos deben ser lo suficientemente específicos como para relacionarse a grupos de activos de la infraestructura y categorías de incidentes relacionados con la seguridad. En este contexto los objetivos estratégicos de la seguridad atm son los siguientes:

a. Los servicios de tránsito aéreo utilizan información referente a la prestación de los mismos, esta tiene que ser resguardar, de acuerdo a lo estipulado en el RAC ATS.

b. En la prestación de los servicios de transito aéreo las áreas sensibles deben ser resguardadas de acuerdo a las políticas de seguridad de los aeropuertos, estas áreas principalmente incluyen las torres de control, las salas radar y los equipos esenciales para la prestación de los servicios.

Tolerancia al riesgo. Una responsabilidad importante de la administración de ATSP consiste en determinar el nivel tolerable de riesgo. La tolerancia al riesgo puede consistir en una política fija o un marco para las decisiones de gestión. La adopción de un marco ofrece la ventaja de tener en cuenta el posible carácter dinámico de la tolerancia al riesgo. La política sobre aceptación del riesgo debe incluir el nivel aceptable de riesgos y repercusiones. La política basada en repercusiones permite tener en cuenta riesgos poco probables, pero que tienen repercusiones importantes y, a menudo, se establece elaborando el plan de continuidad de las operaciones. En este contexto los servicios de tránsito aéreo a través de la unidad de gestión de la seguridad operacional SMS, efectuara de manera conjunta con las unidades SMS de la gerencia aeroportuaria y seguridad de los aeropuertos, para la elaboración de los respectivos análisis de riesgo, determinar la tolerancia y las respectivas recomendaciones para su mitigación. Enfocados principalmente para:

a. No permitir la interrupción de la prestación de los servicios de tránsito aéreo debido a factores de seguridad

b. Que el personal que preste los servicios de tránsito aéreo, no se vean amenazados por factores externos.

**c.** Evaluar periódicamente las instalaciones físicas susceptibles para la prestación de los servicios.

Motivos para evaluar los riesgos. En este aspecto se deben especificarse las circunstancias en que se exige la evaluación de riesgos. Esta se lleva a cabo periódicamente para garantizar que las disposiciones relativas a la seguridad se adapten continuamente al entorno en mutación de las amenazas. Además, es prudente y conveniente reevaluar el riesgo en respuesta a:

a. Incidentes relativos a la seguridad en que se tienen en cuenta nuevos conocimientos relativos a vulnerabilidades o amenazas;
b. Políticas de seguridad que pueden modificar las prioridades en materia de riesgos o la aceptación de estos últimos;
c. Entornos de amenaza que presentan una nueva categoría o estrategia de ataque;
d. Cambios en el sistema que se deben a procedimientos de control de la configuración o al elaborar un nuevo sistema.

**Descripción garantizar la seguridad en la prestación de los servicios de tránsito aéreo:**

En la política de seguridad de ATSP debería describirse la estructura de gobernanza, lo que incluye la descripción de la persona responsable de establecer la política y supervisar su ejecución y la persona responsable de proteger activos específicos. Podrían también exigirse políticas de apoyo adicionales. Por último, la política de seguridad debería abarcar un enunciado de compromiso de todos los niveles de la organización. La administración superior y el personal deberían comprometerse respecto a las metas siguientes:

a. Lograr un rendimiento de trabajo seguro;

b. Proteger los activos y servicios de la organización;

c. Mejorar continuamente el mecanismo de gestión de la seguridad; y

d. Cumplir todas las disposiciones actuales aplicables.

Aunque la seguridad es responsabilidad colectiva de cada miembro de la organización, la responsabilidad final incumbe a la administración superior, de la Dirección General de Aeronáutica Civil, y en los organismos de Seguridad del Estado.

**Coherencia interna**

La política de seguridad debería ser coherente respecto a otras políticas ATM (p. ej., seguridad operacional, calidad, entorno, recursos humanos). La política debería ser apropiada para las amenazas que afronta la organización y para el alcance de sus operaciones.

**Coherencia externa**

En la política de seguridad debería definirse el alcance de la gestión de la seguridad de la organización y su relación con partes externas, tales como otras organizaciones ATM, sector militar, aeropuertos, etc. Los contactos con dichas partes externas deben convenirse con la autoridad nacional de supervisión (NSA), asegurando la coherencia global a nivel nacional y en el sector de aviación.

**Difusión amplia y oportuna**

La política de seguridad debería documentarse, implantarse y mantenerse. Además, debería comunicarse a todos los empleados y terceros pertinentes, incluidos contratistas y visitantes. Cuando corresponda, la política de seguridad debería estar al alcance de todas las partes interesadas. Cuando se modifique esto debería anunciarse y ponerse al alcance de todas las partes de manera oportuna.

## 16.5 ESTRUCTURA, AUTORIDAD Y RESPONSABILIDAD

La organización ATM está integrada a la seguridad en el mecanismo de gestión y establece una estructura oficial en que se definen claramente las funciones, responsabilidades y jerarquía para lograr los fines de las políticas, objetivos, metas y programas de gestión de la seguridad.

Así mismo los aspectos citados en el párrafo anterior deben de documentarse, comunicarse e implantarse efectivamente. Deben determinarse las relaciones entre la jerarquía de gestión y las funciones de gestión de la seguridad. También debe de evaluarse al personal periódicamente para vigilar su eficacia en la aplicación de políticas.

La gestión de los riesgos para la seguridad en ATSP exige la participación de toda la organización. La administración superior debe de comprometer a proporcionar una visión estratégica, metas de alto nivel y objetivos; que los dirigentes de nivel medio planifican y administran los proyectos; y que el personal de primera línea elabora, implanta y explota los sistemas que apoyan las misiones principales de la organización y sus procedimientos

operacionales.

La administración superior debe de asegurarse de que ATSP mantiene un programa de seguridad para proteger la infraestructura del sistema ATM y demostrar su compromiso respecto a la elaboración y aplicación de las disposiciones en materia de seguridad de la manera siguiente:

1. Nombrando a un administrador superior con responsabilidades en materia de seguridad (administrador superior de seguridad);

2. Asegurando la disponibilidad de recursos adecuados; y

3. Atendiendo a las expectativas de las partes interesadas.

El administrador superior de seguridad debe ser el ejecutivo superior en materia de seguridad en la organización ATSP. El será el responsable de proporcionar vigilancia y coordinación de las medidas de seguridad en toda la organización ATSP, asegurándose de que se disponga de los recursos necesarios y que estos se utilicen efectivamente. El programa de seguridad de ATSP incluirá planes para la seguridad física de las instalaciones, la seguridad relacionada con el personal y la seguridad de los sistemas de información, comunicación y tecnología. Con la dependencia creciente respecto a la tecnología de la información (IT) y su complejidad siempre creciente, convendría que ATSP nombre a otro administrador superior de seguridad que se concentraría en la ciberseguridad de ICT. Esta persona sería responsable de la ciberseguridad relativa a la tecnología de la información y las comunicaciones y la introducción de soluciones de ciber-tecnología apropiadas para otros programas de seguridad.

## CAPÍTULO 3

## 17 SEGURIDAD FÍSICA DE LAS INSTALACIONES

El programa de seguridad física de las instalaciones proporciona un entorno seguro a los empleados, bienes, contratistas y visitantes de ATSP. Dado que este desempeña una función crítica en la aviación civil, la seguridad física impide también que los bienes queden comprometidos y se utilicen para comprometer la seguridad y protección de pasajeros, tripulaciones y público.

La seguridad física abarca medidas asignadas para impedir el acceso directo de personal no autorizado a un edificio, recursos o información almacenada. Puede tratarse simplemente de una puerta cerrada o un método complejo por capas basado en medidas de disuasión, detección y defensa. Las medidas de seguridad deberían aplicarse de manera que se garantice el uso efectivo de los recursos disponibles. En otras palabras, las medidas de seguridad deben ser económicas respecto a las amenazas previstas y apropiadas respecto al nivel crítico de los activos. Véase más amplia información en el Apéndice A.

## 18 SEGURIDAD FÍSICA DE LAS INSTALACIONES Y CONTROL DE ACCESO

### Instalaciones aeroportuarias y de ATSP

La presente sección se describe los conexos, relativos a los requisitos de protección de las instalaciones de ATSP, considerándose que forman parte de una instalación aeroportuaria o constituyen una vulnerabilidad de la misma. Las medidas de seguridad física deberían estar apoyadas por personal debidamente capacitado y una planificación de contingencia apropiada y completa.

En el Manual de seguridad de la aviación se recomienda que los Estados promulguen legislación o reglamentos apropiados en que se dispongan sanciones para toda persona que deliberadamente viole o trate de violar una zona de seguridad restringida designada del aeropuerto, incluidas las instalaciones ATSP. Dicha legislación o reglamentos deberían también aplicarse a la violación o tentativa de violación de emplazamientos de comunicaciones y ayudas para la navegación (NAVAID) situados fuera del aeropuerto.

Se necesitan medidas de seguridad para proteger instalaciones ATM esenciales contra actos intencionales o involuntarios. Su pérdida podría tener repercusiones graves en la seguridad y protección de las operaciones de aviación civil. Antes de elaborar protección y medidas de seguridad apropiadas para instalaciones ATM, ATSP debería realizar una amplia evaluación de riesgos para cada una de ellas.

Esta evaluación de riesgos exigiría que se evalúe la vulnerabilidad de cada instalación y se analice la gravedad del efecto de una perturbación del servicio ligera, media o grave. Así, el alcance de los posibles efectos de ataques o catástrofes debería establecerse para cada instalación ATM, así como las repercusiones posibles de tales ataques en la seguridad y protección del público, los pasajeros y el personal en las operaciones del aeropuerto y en la totalidad de la región de información de vuelo (FIR) donde esté situada la instalación. Los ataques o catástrofes que afecten a instalaciones ATM mediante perturbación de las principales NAVAID, suministro de agua o electricidad, etc., podrían perturbar considerablemente el servicio, dificultando el uso de un aeropuerto o una FIR entera hasta que se efectúen las reparaciones necesarias (p. ej., restablecer las principales NAVAID, el suministro de agua y electricidad) y la instalación restablezca los servicios ATM críticos.

ATSP debería elaborar un enfoque de capas múltiples para proteger las instalaciones ATM basándose en una evaluación de riesgos para la seguridad y un análisis de rentabilidad. Dichas medidas podrían asegurar que un ataque contra la primera capa no interrumpa automáticamente las operaciones. Además, proporcionaría tiempo para tomar medidas adicionales de protección para las demás capas hasta que se atenúen las repercusiones en la primera. (Las capas de defensa se describen más detalladamente en la sección siguiente). Si un enfoque de capas múltiples es imposible o muy costoso, ATSP debería no obstante mantener medidas de protección que satisfagan los objetivos en materia de protección, seguridad y operaciones.

## 18.1 CONSIDERACIONES RELATIVAS AL DISEÑO DE LAS INTALACIONES ATM

Las instalaciones ATM podrían ser atacadas desde el exterior con armas convencionales como granadas propulsadas por cohetes (RPG) o armas de fuego pequeñas, así como mediante acceso no autorizado. La interrupción de la alimentación eléctrica podría también tener consecuencias negativas para las operaciones de la instalación. Debería considerarse la posibilidad de afrontar estas tres amenazas importantes en la etapa de diseño para asegurarse de que los perpetradores posibles no puedan lanzar una RPG o disparar armas pequeñas de gran calibre o larga distancia desde un emplazamiento disimulado cerca de la instalación o que posibles autores puedan tener acceso a la instalación fácilmente desde áreas públicas sin una rápida reacción de las fuerzas de seguridad (personal de seguridad de ATSP, fuerzas de imposición de la ley o fuerzas militares) basadas en el aeropuerto. Idealmente, las instalaciones ATM deberían estar rodeadas por áreas abiertas, tales como un estacionamiento o vías de acceso con vigilancia vídeo adecuada. Además, deberían instalarse generadores auxiliares para proteger la alimentación eléctrica en todas las zonas. Las consideraciones específicas relativas a forma, configuración, materiales y normas técnicas deberían seguirse para reforzar las estructuras, reducir las repercusiones a un mínimo y mantener la resistencia.

## 18.2 AYUDAS A LA NAVEGACIÓN (NAVAID)

Las NAVAID pueden situarse dentro del perímetro del aeropuerto, cerca de este último o en emplazamientos lejanos. Cuando estén situadas dentro del perímetro, todo el equipo y las medidas de protección instalados para proteger el perímetro constituyen la primera línea de defensa. Es importante asegurarse de que todas las NAVAID reunidas en la misma zona dentro del perímetro del aeropuerto cuenten con dispositivos y medidas de protección adicionales, tales como sistemas de detección de intrusos y vigilancia vídeo.

En el caso de las NAVAID situadas cerca del aeropuerto, pero fuera del perímetro, se necesitan dispositivos y medidas de protección adicionales a fin de detectar inmediatamente ataques posibles. Podría ajustarse el perímetro del aeropuerto para abarcar todas las NAVAID situadas cerca del mismo, de ser posible; de otro modo, se recomienda la instalación de un sistema de detección de intrusos.

En el caso de NAVAID remotas, se recomienda vigilancia vídeo con registro automático de las últimas 12 horas del exterior de la instalación. Deberían instalarse medios de alerta de modo que pueda iniciarse una reacción apropiada en caso de pérdida de un sitio remoto. Si las NAVAID no pueden protegerse adecuadamente con medidas de seguridad física y sistemas de detección de intrusos, el personal de seguridad o los técnicos de mantenimiento deberían visitarlas con frecuencia. Instalaciones con personal deberían contar con medidas estrictas de control del acceso y la admisión a las mismas debería exigir la presentación de un permiso de identidad válido.

## 18.3 COMPONENTES DEL SISTEMA ATM

Idealmente, debería asegurarse de que los sistemas de seguridad de las instalaciones que cuenten con componentes del sistema ATM estén estrechamente coordinados con las autoridades locales y nacionales competentes en materia de seguridad de la aviación, basándose en una evaluación de riesgos para la seguridad. Las amenazas y vulnerabilidades deberían evaluarse de modo que se determinen los riesgos y se elaboren y apliquen contramedidas apropiadas para reducirlos. En numerosos Estados, los componentes del sistema ATM son privatizados o están situados lejos de los aeropuertos; por consiguiente, debería prestarse atención especial a las medidas de protección para tales instalaciones.

## 18.4 CONTROL DE EQUIPOS Y AUDAS A LA NAVEGACION AEREA

La Gerencia de CNS, tendrá la responsabilidad de llevar un control del personal técnico que tenga acceso a los equipos utilizados para la prestación de los servicios de tránsito aéreo dentro de los aeropuertos y aeródromos del país. Así como del personal técnico y de seguridad que tienen acceso a los equipos o ayudas a la navegación aérea que se encuentran fuera de las instalaciones de los aeropuertos o aeródromos.

# 19 CAPAS DE DEFENSA PARA LAS INSTALACIONES Y OPCIONES DE ATENUACIÓN

En esta sección se ofrece a ATSP una amplia gama de medidas de atenuación, así como una lista de tales medidas y una descripción de las capas de defensa para la protección de las instalaciones.

## 19.1 COMPONENTES DE LAS INSTALACIONES

Una instalación abarca múltiples componentes. Se debe tomar en cuenta todos los factores que pueden afectar la prestación de los servicios; para determinar las vulnerabilidades posibles, es necesario evaluar las consecuencias de los daños o las pérdidas y determinar opciones de atenuación. Generalmente, los componentes son los siguientes:

1. Emplazamiento;
2. Diseño arquitectónico;
3. Sistemas estructurales
4. Sistemas de servicios públicos;
5. Sistemas mecánicos;
6. Sistemas de fontanería y gas;
7. Sistemas eléctricos;
8. Sistemas de alarma contra incendios; e
9. Sistemas ICT.

## 19.2 CAPAS DE DEFENSA

Las capas de defensa van de los activos críticos, hacia el exterior, identificando las capas del perímetro y determinando las estrategias de seguridad.

Primera capa de defensa. La primera capa de defensa exige un buen conocimiento del área circundante. Se concentra en edificios, instalaciones e infraestructura situados fuera del perímetro del emplazamiento. Esto abarca un estudio cuidadoso de las calles circundantes, los puntos de acceso a los servicios públicos (p. ej., electricidad, agua, desagüe, gas, otros combustibles), puntos de acceso a ICT y cualquier otra infraestructura cercana que pueda tener repercusiones en las operaciones de la instalación, tales como fábricas de productos químicos y líneas ferroviarias, carreteras y vías navegables por las que se transporten materiales peligrosos. La liberación de gases tóxicos durante la fabricación o el transporte podría exigir la evacuación de la instalación.

Segunda capa de defensa. La segunda capa de defensa se refiere al espacio que existe entre el perímetro del emplazamiento y los activos que deben protegerse. Esto supone el diseño de puntos de acceso, estacionamiento, carreteras, vías peatonales, barreras naturales, iluminación de seguridad y señalización. En el caso de zonas urbanas, se refiere específicamente al conjunto de edificios.

Tercera capa de defensa. La tercera capa de defensa se refiere a la protección del emplazamiento, el control del acceso y la reducción al mínimo de las repercusiones de un ataque. Suele comprender el reforzamiento de las estructuras y sistemas para incorporar sistemas eficaces de calefacción, ventilación y aire acondicionado (HVAC) y equipo de vigilancia, así como un diseño y una ubicación cuidadosos de los servicios públicos y los sistemas mecánicos.

## 19.3 OPCIONES DE ATENUACIÓN

En las Figuras I-3-1 y I-3-2 se presenta una gama de medidas de atenuación para un emplazamiento, correspondientes a la segunda y tercera capas de defensa. Las medidas se enumeran en orden ascendente según el nivel del esfuerzo de protección, costo y mantenimiento. Mientras existen numerosos factores que afectan a su viabilidad, costo y eficacia, la correspondiente lista constituye un punto inicial para el ATSP que prevea elaborar la seguridad de sus instalaciones.

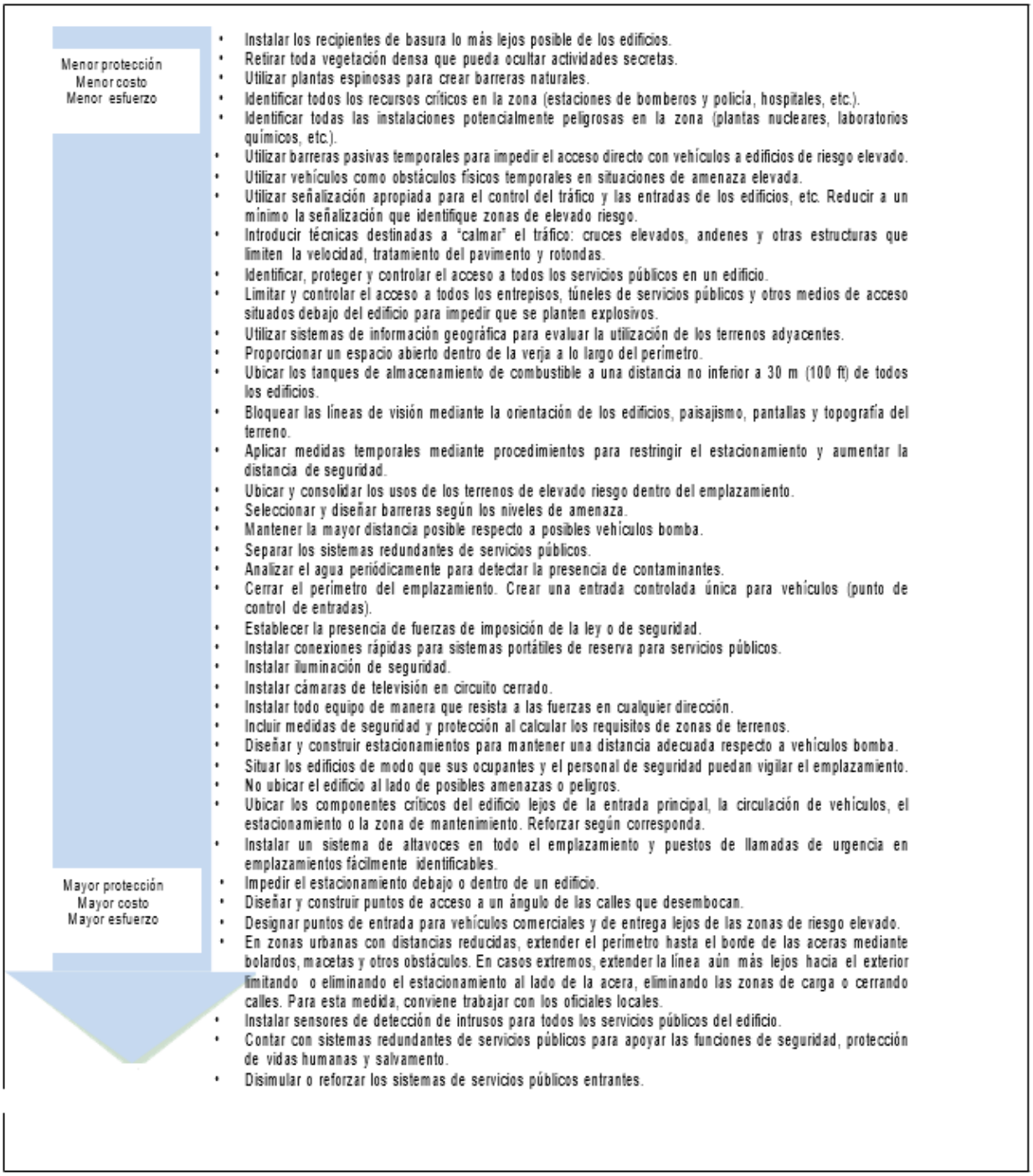

**Figura I-3-1. Opciones de control para la segunda capa de defensa**


**Figura I-3-2. Opciones de control para la tercera capa de defensa**

## CAPITULO 4

# 20 SEGURIDAD RELACIONADA CON EL PERSONAL

La seguridad relacionada con el personal se refiere a medidas que permiten evaluar la lealtad, honradez y fiabilidad del personal y otorgarle acceso a infraestructura confidencial o clasificada del sistema ATM, incluida la correspondiente información. El programa de seguridad relacionada con el personal de ATSP garantiza la integridad de los servicios de este último, incluida su capacidad de apoyar la seguridad de la aviación, la seguridad nacional y la imposición de la ley. También protege a la organización ATSP contra amenazas internas causadas por infiltración o por empleados decididos a causar daño. Sera responsabilidad de la Gerencia de Recursos Humanos aplicar las políticas y procedimientos de selección y contratación del personal técnico y operativo, para la prestación de los servicios de tránsito aéreo.

# 21 REQUISITOS DE SEGURIDAD DE LA AVIACIÓN

Los requisitos respecto al personal de seguridad y el que no sea de seguridad. Aunque en la definición de personal de seguridad en el Manual de seguridad de la aviación no figura el personal de seguridad de ATSP, se presume que los requisitos son aplicables al personal de seguridad de ATSP que desempeña funciones semejantes. Los requisitos de seguridad relacionada con el personal y de capacitación en materia de seguridad de ATSP deberían satisfacer las normas, criterios y procedimientos del Estado, teniendo en cuenta todos los requisitos nacionales.

## 21.1 PERSONAL DE SEGURIDAD

El personal de seguridad de ATSP son las personas encargadas de aplicar medidas de seguridad como las siguientes:

1. control del acceso;
2. Vigilancia y patrulla;
3. Inspección de vehículos;
4. Capacitación en materia de seguridad ATM;
5. Aplicación de medidas de control de la calidad;
6. Programa de seguridad relacionada con el personal; y
7. Programa de seguridad de ICT.

Todo el personal de seguridad o todos los empleados posibles de ATSP deberían ser objeto de verificaciones de antecedentes y verificaciones periódicas, según corresponda. Las verificaciones de antecedentes deberían abarcar la investigación de la participación en grupos que se sospechen de actividades o simpatías terroristas o criminales y la verificación de la identidad y experiencia previa de los candidatos y sus antecedentes penales, si así lo permite la ley. La verificación periódica de antecedentes debería tener lugar cuando deban renovarse las tarjetas de identificación de los empleados.
Sera responsabilidad de la Gerencia de Recursos Humanos de establecer el procedimiento y frecuencia de la presentación de antecedentes y documentación relacionada a personal técnico y operativo que presta los servicios de tránsito aéreo, así como del personal de

apoyo: administrativo y de mantenimiento.

### 21.2 PERSONAL QUE NO SEA DE SEGURIDAD

El personal que no sea de seguridad puede definirse como todo proveedor, técnico o miembro del personal de control de tránsito aéreo (ATC) que desempeña funciones relacionadas con las operaciones de la aviación civil y podría participar en la aplicación de medidas de seguridad.

Dicho personal que no sea de seguridad, especialmente las personas que necesiten acceder a zonas de seguridad restringidas, deberían ser objeto de verificaciones de seguridad durante el procedimiento inicial de selección y nuevamente a intervalos regulares, de conformidad con las disposiciones de los reglamentos nacionales.

## 22 PROGRAMA DE SEGURIDAD RELACIONADA CON EL PERSONAL

En la presente sección figura orientación general sobre el programa de seguridad relacionada con el personal de ATSP, que este podría seguir al elaborar su propio programa, pero ajustándolo a su situación concreta.

### 22.1 CONSIDERACIONES GENERALES

ATSP debería establecer y mantener un programa de seguridad relacionada con el personal, conforme a las leyes, reglamentos y disposiciones aplicables, y alcanzar un equilibrio entre el logro de un elevado nivel de seguridad y la protección de los derechos civiles y libertades personales. ATSP debería cumplir los reglamentos y procedimientos del Estado relativos a la privacidad al reunir, mantener, utilizar y divulgar información personal.

ATSP debería elaborar procedimientos oficiales y documentados para facilitar la implantación de la política de seguridad relacionada con el personal y los controles correspondientes. Estos deberían incluir al personal de ATSP y sus contratistas. El personal asignado a cargos sensibles o críticos deberá satisfacer una expectativa más elevada de honradez acorde con sus responsabilidades. Deberían también elaborarse procedimientos de seguridad relacionada con el personal para determinados sistemas ICT. Además, en el correspondiente programa deberían figurar disposiciones sobre la duración total del empleo (selección y revisión durante el empleo, transferencia y cese del empleo), teniéndose en cuenta los requisitos de terceros.

### 22.2 CATEGORIAS DE RIESGOS RELACIONADOS CON EL PUESTO DE TRABAJO

ATSP debería asignar una designación de riesgo a todos los puestos de trabajo (sensible o crítico) y establecer criterios de inspección para las personas que los ocupan. Dichas designaciones deben examinarse y revisarse, si corresponde, periódicamente y ajustarse a las políticas y orientaciones del Estado. Los criterios de inspección deberían incluir información clara sobre los requisitos de nombramiento para funciones de seguridad (p. ej., capacitación, habilitación de seguridad).

### 22.3 INSPECCIÓN E INVESTIGACIÓN DEL PERSONAL

ATSP debería asegurarse de que las autoridades competentes realicen un examen de antecedentes antes de seleccionar a una persona para un cargo o autorizar el acceso personal al sistema ICT. ATSP podría aceptar la admisibilidad de una persona

procedente de otra organización que haya realizado un examen de antecedentes comparable, si así lo permiten las leyes o reglamentos nacionales. ATSP debería también establecer las condiciones y frecuencia de nuevos exámenes o seguir lo prescrito. Pueden necesitarse condiciones y frecuencias diferentes para un nuevo examen para el personal que tenga acceso al sistema ICT, basándose en la sensibilidad del cargo y la información procesada, almacenada o transmitida por el sistema. Además, ATSP debería asegurarse de que todas las personas, así como los artículos que lleguen, se sometan a inspección y controles de seguridad antes de su entrada en las zonas de seguridad restringidas de la instalación que preste servicio a las operaciones de aviación civil.

## 22.4 CESE DE EMPLEO DEL PERSONAL

**Cuando cese el empleo de una persona, ATSP deberá:**

a) Poner término al acceso a instalaciones y sistemas ICT restringidos.
   Realizar entrevistas de salida.
b) Recuperar toda propiedad de la organización relacionada con la seguridad, incluidos sistemas ICT
c) Retener el acceso a información y sistemas ICT de la organización previamente bajo control de la persona cuyo empleo ha cesado.

Las entrevistas de salida garantizan que las personas entienden las limitaciones impuestas en materia de seguridad por haber sido empleados y que se logre una rendición de cuentas apropiada. Constituyen ejemplos de propiedad relacionada con la seguridad las claves de autenticación, manuales técnicos de administración del sistema, llaves, tarjetas de identidad y pases. Estas entrevistas se realizaran en coordinación con la Gerencia de Navegación Aérea y la Gerencia de Recursos Humanos.

## 22.5 TRANSFERENCIA DE PERSONAL

ATSP debería examinar las autorizaciones de acceso físico y lógico a instalaciones, información y sistemas ICT cuando se reasigne o transfiera personal a otros puestos de trabajo dentro de la organización, a título temporal o permanente. ATSP debería iniciar dichas medidas de seguridad de transferencia o reasignación definidas por la organización dentro de determinado plazo, aplicando los procedimientos oficiales de transferencia.

**Entre los ejemplos de medidas que pueden exigirse figuran los siguientes:**

1) Devolver viejas llaves y emitir nuevas llaves, tarjetas de identidad y pases
2) Cerrar cuentas anteriores relacionadas con el sistema ICT y establecer otras nuevas
3) Cambiar las autorizaciones y el acceso al sistema ICT.
4) Permitir el acceso a los registros oficiales a los que el empleado tenía acceso en su cargo anterior y en las cuentas precedentes relacionadas con el sistema ICT.

## 22.6 ACUERDOS RELATIVOS AL ACCESO

ATSP debería determinar las situaciones que exijan un acuerdo relativo al acceso, antes de otorgar acceso a información y sistemas ICT. La información que exige medidas especiales de protección incluye la información personal y la información de la organización. Constituyen ejemplos de acuerdos relativos al acceso los acuerdos sobre no divulgación, uso aceptable y conflictos de interés. Los acuerdos relativos al acceso

incluyen un reconocimiento de que los signatarios han leído, entendido y convenido en acatar las limitaciones relacionadas con el sistema ICT al que se autoriza el acceso.

## 22.7 PERSONAL DE SEGURIDAD EXTERNO

La Gerencia de Seguridad Aeroportuaria en coordinación con la Gerencia de Recursos Humanos y Gerencias relacionadas deberán establecer normas relativas a la seguridad relacionada con el personal, incluidas las correspondientes funciones y responsabilidades para proveedores externos (p. ej., contratistas, proveedores). Dichas normas deberían formar parte de los criterios de selección y ser aplicadas por los proveedores externos. ATSP debería también asegurarse de que los proveedores cumplan sus obligaciones.

Constituyen ejemplos de proveedores externos las oficinas de servicios, los contratistas (incluidos los de mantenimiento) y otras organizaciones que proporcionan desarrollo de sistemas ICT, servicios de tecnología de la información, aplicaciones en contratación externa y gestión de redes y seguridad.

## 22.8 SANCIONES APLICABLES AL PERSONAL

La Gerencia de recursos humanos en coordinación con las gerencias relacionadas establecerá un mecanismo oficial de sanciones en el caso del personal que no cumpla las políticas y procedimientos establecidos en materia de seguridad. Dicho mecanismo debería ajustarse a las leyes, políticas y orientaciones aplicables del Estado. Además, constituye parte de las políticas y procedimientos generales de ATSP relativos al personal y debería describirse en los acuerdos relativos al acceso.

## 22.9 APOYO PARA EL PERSONAL

La Gerencia de recursos humanos en coordinación con las Gerencias respectivas establecerá programas para proteger y apoyar a los empleados y otras personas que posean conocimientos críticos o desempeñen funciones críticas. Constituyen ejemplos de ello la instrucción relativa a la conciencia en materia de seguridad, la identificación y atenuación de las prácticas de miedo utilizadas por terroristas y agentes criminales y personal interno desleal, así como el suministro de protección y otros recursos a los empleados cuando sean objeto de amenaza.

La Gerencia de capacitación coordinara la capacitación necesaria para capacitar a los empleados y facilitar la detección y neutralización de amenazas internas señalando a la administración toda conducta sospechosa o anormal y las prácticas laborales de otros empleados.

## 22.10 CONTROL DE VISITANTES

La Gerencia de Navegación Aérea en coordinación con la Gerencia de Seguridad Aeroportuaria llevara un procedimiento y control de visitantes, para las visitas por personas o grupos grandes a cada categoría de instalación ATC. Deben de especificarse los requisitos de registro para visitas, las verificaciones de identidad exigidas para la entrada, los procedimientos de escolta durante las visitas y restricciones sobre la introducción en la instalación de dispositivos digitales y otras categorías de aparatos fotográficos o de registro.

## CAPITULO 5

## 23 SEGURIDAD DE LOS SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES (ICT), (INCLUIDA LA CIBERSEGURIDAD)

La información constituye un activo de la organización ATSP y debe protegerse. La organización ATSP podría poseer un volumen importante de información sobre empleados, pasajeros, tripulaciones de vuelo, operaciones de vuelo, registros históricos y situación financiera. Si dicha información confidencial cayera entre las manos de una entidad no autorizada, esta violación de la seguridad podría dar lugar al cierre total del sistema ATM, interferencia ilícita en las operaciones de aeronaves en vuelo, demandas judiciales o pérdida de vidas humanas. La protección de la información confidencial constituye, por consiguiente, una exigencia fundamental de la seguridad de ATM y, en muchos casos, un requisito ético y legal.

La seguridad de ICT se refiere a la aplicación de controles de seguridad para proteger a los sistemas ICT de ATM contra la degradación, intencional o accidental, de la integridad, confidencialidad y disponibilidad. La seguridad de dichos sistemas se aplica a personas, procedimientos y datos, así como a los soportes lógicos y físicos utilizados para reunir y analizar información digital y análoga utilizada en ATM.

ATSP debería aplicar un método de gestión del riesgo al elaborar el programa de seguridad de ICT, semejante a la elaboración de otros programas de seguridad (véase el Apéndice A, Mecanismo de gestión de riesgos para la seguridad).

## 24 ANTECEDENTES

Los controles de seguridad son salvaguardias, de carácter administrativo, operacional o técnico, implantadas para proteger la integridad, confidencialidad y disponibilidad de los sistemas ICT de ATM. Los controles se utilizan como sinónimo de contramedidas o atenuación de vulnerabilidades. A continuación se definen, en forma resumida, la integridad, confidencialidad y disponibilidad:

1. La integridad constituye un objetivo de la seguridad que garantiza que la información y los sistemas no se modifiquen indebida o accidentalmente. Cuando resulte comprometida la integridad, la información puede modificarse o destruirse;

2. La confidencialidad es un objetivo de la seguridad que garantiza que la información no se divulgue a entidades no autorizadas. Cuando resulte comprometida la confidencialidad, puede ocurrir una divulgación no autorizada de información. A menudo la confidencialidad se logra cifrando los datos en tránsito o almacenados; y

3. La disponibilidad es un objetivo de la seguridad que garantiza la continuidad, fiabilidad y accesibilidad de datos, recursos y servicios para entidades autorizadas, de manera oportuna.

4. Cuando resulte comprometida la disponibilidad, el sistema puede experimentar una perturbación temporal del servicio o una pérdida completa de su continuidad.

Para proteger al sistema ICT de ATM, es también necesario atender a la seguridad del entorno en que funciona. Por consiguiente, la seguridad de la información se relaciona también con la seguridad física, los proveedores, los servicios de infraestructura y terceros con los que ATSP se relaciona, tales como las autoridades de imposición de la ley, seguridad y reglamentación.

# 25 CONTROLES DE SEGURIDAD DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES (ICT)

Consideraciones relativas al desarrollo.

La orientación siguiente se elaboró teniendo en cuenta los dos aspectos siguientes:

1. La necesidad de asistir a las organizaciones en la selección de controles apropiados a partir del gran número especificado en las normas internacionales; y

2. La amplia gama de organizaciones atsp y categorías de sistemas ict.

Para tratar dichos aspectos, la presente orientación abarca una lista de controles de seguridad ICT (véase el Apéndice B, Ciberseguridad de los sistemas ICT) basada en la recopilación y consolidación de las normas internacionales siguientes:

1. Todas las normas pertinentes sobre seguridad de la información en las telecomunicaciones en ISO/IEC 27001:2005; y

2. Otras normas pertinentes, particularmente las de los Objetivos de control de la tecnología de la información (COBIT) y el grupo de normas ISO/IEC 13335-4.

La lista abarca también los mejores métodos para una aplicación práctica y actualizada de dichas normas. Al seguir la orientación, la organización ATSP cumpliría las normas internacionales vigentes.

Además, los controles de seguridad de ICT pueden organizarse por niveles según la clasificación de riesgos para los sistemas ICT establecida por la organización. El nivel más bajo de riesgo exige el nivel más bajo de controles básicos; y el riesgo más elevado exige el nivel más elevado.

## 25.1 CATEGORÍAS DE CONTROLES

**Los controles de seguridad de ICT pueden clasificarse en nueve categorías:**

### A. Controles de la orientación y políticas de la organización

Los controles de la orientación y políticas de la organización se relacionan con el conjunto de personas, entidades externas y organizaciones que se adhieren a las políticas y procedimientos de seguridad de determinada organización.

Las políticas de seguridad constituyen un documento aprobado por la administración, distribuido a todos los empleados y entidades externas, que cubre todos los sistemas y describe las responsabilidades de cada una de las partes respecto al uso de los sistemas previstos en las políticas. Constituye un documento en evolución sometido a ciclos de revisiones programadas y actualizaciones no programadas, según corresponda, para garantizar la actualidad y eficacia de las políticas que contiene. La política de seguridad forma también parte del enfoque de gestión de riesgos para la evaluación y gestión de la seguridad de ICT.

### B. Controles de la organización, cultura y gestión

El éxito de la elaboración e implantación de un sistema de seguridad de ICT basado en políticas depende en gran medida de la participación y apoyo de la administración a los esfuerzos, con un compromiso claro y permanente respecto al mecanismo.

Los controles armonizan los objetivos de las operaciones de la organización con sus objetivos de seguridad, basándose en funciones de gestión bien definidas y objetivos claros en materia de seguridad.

**C. Controles relativos a recursos humanos**

Los controles relativos a recursos humanos para la seguridad de ICT se relacionan con los empleados y contratistas, así como sus funciones, responsabilidades e idoneidad. Se examinan y reducen los riesgos asegurándose de que se sometan a la debida investigación y reciban capacitación para sus funciones. Los riesgos inherentes de hurto y uso indebido de recursos constituyen ámbitos de preocupación.

**D. Controles de la seguridad física y la seguridad relativa al entorno**

Los controles de la seguridad física y la seguridad relativa al entorno de ICT se relacionan con sus vulnerabilidades respecto al emplazamiento de la instalación, el perímetro de seguridad, las técnicas de control del acceso y el equipo de seguridad diverso que protege la organización y sus activos ICT.

**E. Controles del funcionamiento del sistema ICT**

Los controles del funcionamiento del sistema ICT garantizan que se aplique debidamente la seguridad operacional definida en los procedimientos y políticas. La capacitación de los usuarios del sistema permite asegurarse de que entiendan las políticas y cumplan sus obligaciones.

**F. Controles de los mecanismos e infraestructura técnicos**

Los controles de los mecanismos e infraestructura técnicos garantizan que los controles apropiados de la configuración de la red proporcionan suficiente protección a esta última y que los controles técnicos seleccionados impiden que entidades no autorizadas tengan acceso a los datos del sistema.

Suele aplicarse el principio de “menor privilegio” para asegurarse de que una persona o sistema no reciba más acceso de lo necesario para desempeñar su tarea.

Constituyen ejemplos de estos controles los cortafuegos, los sistemas de detección de intrusos, las listas de control del acceso, el cifrado de datos, las contraseñas, la separación de redes y los controles de rutas.

**G. Controles de la adquisición y el desarrollo**

Los controles de la adquisición y el desarrollo para la seguridad de ICT se establecen utilizando metodologías comprobadas de ingeniería de sistemas para garantizar que la seguridad está plenamente integrada en todas las fases del ciclo de adquisición y desarrollo.

**H. Controles de la vigilancia y las auditorías**

Los controles de la vigilancia y las auditorías para la seguridad de ICT se relacionan con el registro de sucesos, auditorías y fallas para fines de seguridad. Se utilizan medios de vigilancia de las alertas y alarmas del sistema para detectar condiciones de alerta y uso no autorizado del sistema.

## I. Controles del cumplimiento

Los controles del cumplimiento para la seguridad de ICT aseguran que el sistema satisfaga los acuerdos y requisitos legales, reglamentarios y contractuales. Los controles suelen ejercerse mediante auditorías del sistema.

En la Tabla I-5-1 se establece la relación entre los objetivos de integridad, confidencialidad y disponibilidad en materia de seguridad y los controles de seguridad de ICT que se acaban de describir.

La ciberseguridad es un aspecto integrante de la seguridad de ICT. Para más amplia información sobre la ciberseguridad, véase el Manual de seguridad de la aviación, Capítulo 18, sobre las amenazas de ciberataques contra sistemas críticos de tecnología de la información y las comunicaciones de la aviación. Véase también el Apéndice B, Ciberseguridad de los sistemas ICT.

En el NCASP deberían destacarse tres ámbitos de preocupación para los programas de seguridad de ICT:

1. Protección de los sistemas contra acceso no autorizado;

2. Prevención de interferencia en los sistemas; y

3. Detección de ataques contra los sistemas. Se indican a continuación categorías de controles para alcanzar los mencionados objetivos:

Proteger a los sistemas contra acceso y usos no autorizados:

1. Reforzar el perímetro físico de la instalación;

2. Defender la arquitectura de seguridad de la red a fondo; y

3. Determinar instrumentos de control de la gestión y el acceso;

Impedir interferencia en los sistemas:

1. Instrumentos para la integridad de los archivos; y

2. Separación de tareas y “menor privilegio” respecto al sistema;

Detectar ataques dirigidos contra los sistemas:

1. Utilización de sistemas de prevención de intrusiones;

2. Utilización de sistemas de detección de intrusos;

3. Vigilancia de las operaciones de seguridad para determinar alertas y alarmas; y

4. Recopilación de información de los registros del sistema.

El establecimiento de categorías de controles según las funciones de la organización permite relacionar partes funcionales diferentes de una organización con un grupo más pequeño de controles. No obstante, esto no significa que la gestión de los riesgos de

la organización puedan centrarse en una sola función para proteger determinado activo; suelen necesitarse controles para diversas funciones

## 25.2 CONTROLES DEL NIVEL DE RIESGO

Las organizaciones ATSP varían según su importancia y categoría. Por ejemplo, puede tratarse de una organización con poco personal que proporciona una gama limitada de servicios (p. ej., NAVAID) o una organización que dirige centros ATC complejos. En algunos Estados, el organismo gubernamental que proporciona servicios de tránsito aéreo, mediante una amplia gama de sistemas o instalaciones ATM, desempeña también la función de ATSP.

Para tener en cuenta la gama de organizaciones ATSP y sus sistemas ICT, los controles de seguridad apropiados podrían reunirse en seis niveles de creciente rigor, como se ilustra en el Apéndice C. La diferencia principal reside en el nivel de riesgo del sistema ICT de ATM que varía según el carácter crítico del servicio proporcionado por la organización ATSP, la vulnerabilidad del sistema ICT y el carácter de las amenazas.

Los niveles de control deberían ser cumulativos y corresponder a los requisitos básicos de control de ICT para organizaciones ATM. Cada nivel de control debería tener un grado creciente de complejidad ICT o activos ICT con riesgo creciente. Por ejemplo, el nivel 1 debería ser el más bajo y es apropiado para una organización con un sistema ICT limitado y aislado. El nivel más alto exigiría una implantación competente de todos los requisitos de control y sería apropiado para organizaciones ATSP más complejas. La diferencia principal reside en el nivel de riesgo del sistema ICT de ATM, que varía según el carácter crítico del servicio proporcionado por la organización ATSP, la vulnerabilidad del sistema ICT y el carácter de las amenazas al sistema ATM. En el Apéndice C se indican las características generales de los niveles de control propuestos como ejemplo, así como una descripción detallada de cada nivel respecto a cada una de las nueve funciones de la organización.

---

**TABLA I-5-1. CATEGORÍAS DE CONTROL E INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD**

| Categoría de control de ICT | Integridad | Confidencialidad | Disponibilidad |
|---|---|---|---|
| Orientación y políticas de la organización | Políticas para asegurar que los controles protegen la integridad de los datos | La política de la organización puede dictar la protección de la información | Política que asegura el tamaño apropiado del sistema para garantizar la disponibilidad |
| Organización, cultura y gestión | Procedimientos y políticas de utilización de datos | Procedimientos y políticas de la administración sobre protección de datos | Identificación de activos y mantenimiento de recursos |
| Recursos humanos | Capacitación del personal | Capacitación del personal sobre utilización de datos confidenciales | Capacitación del personal |
| Seguridad física y seguridad relativa al entorno | Seguridad y controles del acceso a los datos | Perímetros seguros y protecciones físicas | Equipo y emplazamientos redundantes y de reserva |
| Funcionamiento del sistema ICT | Control de la gestión del cambio | Procedimientos para proteger los soportes extraíbles; políticas de interconexión | Acuerdos sobre servicios para operaciones de sistemas |
| Mecanismos e infraestructura técnicos | Instrumentos de integridad de archivos | Mecanismos de cifrado | Soluciones fácilmente accesibles |
| Adquisición y desarrollo | Procedimientos oficiales de gestión del cambio | Requisitos de las operaciones para la protección de datos | Requisitos operacionales para garantizar la disponibilidad |
| Vigilancia y auditorías | Cambios en el registro de auditorías | Vigilancia y resultados de auditorías de la protección de la información, incluso respecto a ataques y tentativas de ataques | Vigilancia del buen funcionamiento y utilización de sistemas críticos |
| Cumplimiento | Cumplimiento de las políticas relativas a pérdida, destrucción o falsificación de datos | Controles criptográficos utilizados de conformidad con acuerdos y leyes | Cumplimiento de los planes de continuidad de operaciones |

## 25.3 CONSIDERACIONES RELATIVAS AL SISTEMA ATM DE NUEVA GENERACIÓN

La seguridad de ICT desempeñará un papel más importante en los sistemas ATM de nueva generación, tales como el sistema de transporte aéreo de nueva generación (NextGen) en los Estados Unidos y la Investigación ATM en el marco del cielo único europeo (SESAR) en Europa. Dado que los enlaces de comunicación de datos reemplazan los canales de comunicación vocales actuales, es más importante asegurarse de que los enlaces de datos que utilizan controles de seguridad sean oportunos y fiables dado que serán vitales para el éxito de los programas.

La gestión de la información de todo el sistema (SWIM) ofrece la oportunidad de compartir datos ATM como los relativos a meteorología, afluencia del tránsito aéreo, trayectorias de vuelo y vigilancia. La entrega oportuna, segura y fiable de datos reviste suma importancia para el éxito de los sistemas ATM de nueva generación.

## CAPITULO 6

## 26 PLANIFICACIÓN DE CONTINGENCIA PARA LA SEGURIDAD DE ATM

La planificación de contingencia debería incluir aspectos relativos a la seguridad de ATM y cubrir la degradación de un servicio en una situación de contingencia y su regreso ordenado a la situación de funcionamiento con capacidad normal. La continuidad de funcionamiento permite que la organización ATSP desempeñe sus funciones fundamentales de forma segura durante el plazo especificado.

Primero, pese a la implantación de controles de prevención y protección, los incidentes relacionados con la seguridad siguen siendo posibles y ATSP debe prepararse para tales situaciones. Segundo, los controles de contingencia podrían considerarse como parte de la estrategia de control integrada y ofrecen soluciones más económicas para controles de protección y prevención. Las medidas de contingencia permiten el funcionamiento continuo de funciones fundamentales para la misión, aun cuando falle la protección. El paso de protección del sistema a resistencia del sistema representa un cambio importante de paradigmas en el programa de seguridad.

## 27 FUNCIONES Y RESPONSABILIDADES ENTRE ESTADOS Y ATSP

Las funciones de los Estados derivan del Anexo 11 al Convenio de Chicago, particularmente de la sección 2.30, Arreglos para casos de contingencia, según lo interpreta la orientación en el Adjunto C del mismo Anexo. Incumbe a los Estados proporcionar los servicios de tránsito aéreo y los correspondientes servicios de apoyo en su espacio aéreo. Esta responsabilidad abarca las situaciones de contingencia para instituir medidas destinadas a garantizar la seguridad de las operaciones de la aviación civil y, en lo posible, disponer lo necesario a fin de proporcionar instalaciones y servicios de alternativa. Dichas medidas deben abarcar disposiciones relativas a la seguridad, de lo contrario no puede garantizarse la seguridad operacional.

Así, los Estados deben asegurarse de que el ATSP designado, en que se hayan delegado los servicios, elabore planes de contingencia. Los Estados pueden asumir la vigilancia o delegar esta tarea en otra entidad mediante instrumentos apropiados. Les incumbe también la coordinación con otros Estados afectados por los planes de contingencia y, de ser necesario, la concertación de acuerdos a nivel estatal.

La primera responsabilidad de ATSP consiste en elaborar planes de contingencia de conformidad con las disposiciones del Estado. La fase de preparación incluye la definición de los controles y la coordinación con otras partes interesadas, tales como el Estado (incluida la seguridad de la aviación civil, el sector militar y las autoridades de imposición de la ley), posiblemente otros ATSP y compañías de seguro. Incumbe a ATSP preparar la lista de contacto para fines de notificación en caso de un incidente que cause la interrupción del servicio. ATSP debería también determinar el conjunto mínimo de información y el plazo para su entrega a las dependencias de servicios de tránsito aéreo (ATS) en las FIR o los Estados vecinos, en coordinación con la autoridad de reglamentación. Incumbe también a ATSP implantar el plan en determinados casos.

## 28 PLANES DE RESERVA DE SERVICIOS DE TRÁNSITO AÉREO PARA LA SEGURIDAD DE ATM

Afectar considerablemente a la capacidad de una dependencia ATS para seguir proporcionando el nivel normal de servicio. Si el daño ocasionado impide que una instalación funcione, serán necesarios arreglos de reemplazo. Si la torre de control está dañada, puede proporcionarse servicio limitado utilizando equipo portátil de comunicaciones; sin embargo, un daño considerable a un centro en ruta exigiría que se transfiera a otra dependencia la responsabilidad respecto al espacio

aéreo.

En la sección 2.30 del Anexo 11 se exige que ATSP establezca planes de contingencia para estas categorías de sucesos, así como otros que podrían perturbar los servicios, como en caso de incendio en un centro ATC.

Los planes para delegar los servicios de tránsito aéreo en otro ATSP pueden consistir en planes de reserva locales o de FIR regionales. La gestión de dichos planes se lleva a cabo a menudo mediante una carta de acuerdo (LOA) entre instalaciones adyacentes, en cuyo caso las circunstancias y capacidades para atender a las emergencias no ordinarias se determinan, desarrollan y practican mediante ejercicios de contingencia:

**1.** Cobertura de vigilancia;

**2.** Intercambio de datos;

**3.** Comunicaciones;

**4.** Espacio aéreo y servicios atsp;

**5.** Dotación de personal;

**6.** Capacitación;

**7.** Duración; y

**8.** Compartición de costos.

La superposición de cobertura de vigilancia en determinado emplazamiento depende de la disponibilidad o capacidad del equipo. Si no se cuenta con tal superposición, se aplicaría la separación basada en procedimientos ATC en una situación no ordinaria, lo que exigirá mayor separación entre aeronaves. Esto también dependerá de la capacidad de las instalaciones de reserva para atender a mayor demanda.

Los daños ocasionados a las instalaciones y los daños generalizados a infraestructura esencial pueden en determinado espacio aéreo.

En la Figura I-6-1 se ilustran dos opciones para una cobertura de reserva en una situación de contingencia.

En una opción, cuando ATSP B se degrada y carece de otras opciones de reserva, tales como modificar la utilización de una instalación de simulación o capacitación para cubrir la degradación, ATSP A amplía su cobertura para incluir a toda la zona de ATSP B. En la otra opción, ATSP A y ATSP C amplían su cobertura con lo que cada uno de ellos cubre la mitad del área de ATSP B.

Durante operaciones degradadas, las instalaciones ATSP adyacentes podrían aceptar los datos de reserva intercambiados entre la instalación degradada y la instalación que la reemplaza. En muchas partes del mundo es práctica común intercambiar una imagen del aire y datos con la instalación adyacente. Podría también considerarse la posibilidad de un seguimiento continuo de los datos entre instalaciones adyacentes.

Los enlaces de comunicación con las aeronaves en una región podrían también intercambiarse; de no ser así, la ATSP de cobertura puede utilizar la frecuencia de emergencia de 121,5 MHz y dirigir a las aeronaves hacia una frecuencia que permita a la aeronave establecer contacto con el ATSP

que asume las responsabilidades respecto al espacio aéreo.

El ATSP de cobertura debe asegurarse de que dispone de personal suficiente. Para que su personal pueda ocuparse de la carga de trabajo adicional, es importante que obtenga información relativa al espacio aéreo de los sectores vecinos y sus dimensiones y frecuencias, todo preparado de antemano. Podría también considerarse la posibilidad de enviar al personal de la instalación que ha fallado a la instalación ATSP de reemplazo.

Debería organizarse capacitación relativa a situaciones degradadas de manera periódica (p. ej., anualmente). Esto permitiría al personal de ATSP adquirir la aptitud necesaria para atender fácilmente a situaciones de contingencia no ordinarias y proporcionar servicios de seguridad de ATM en el espacio aéreo afectado.

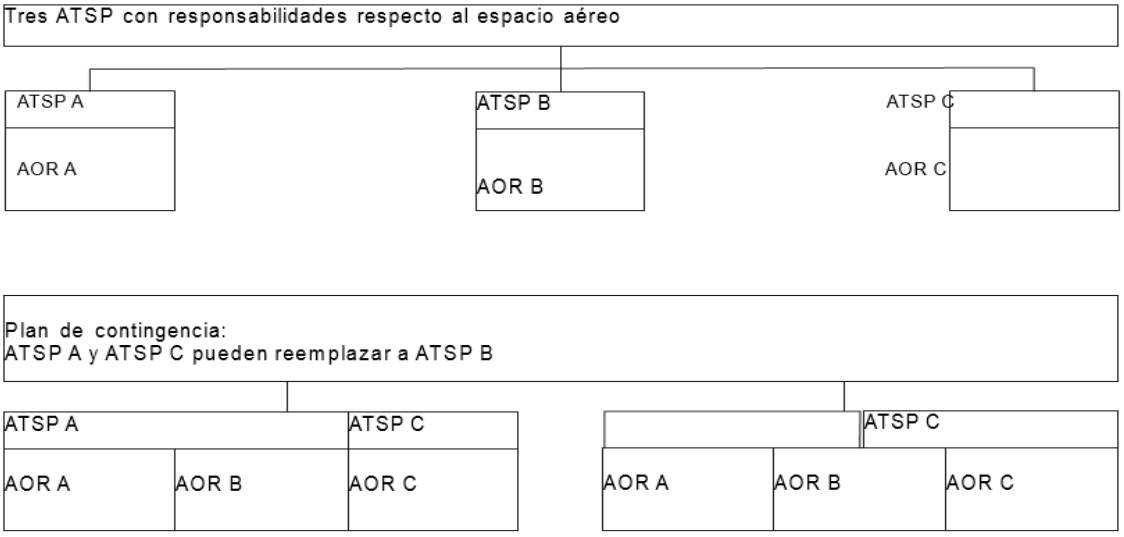


**Figura I-6-1. Ejemplos de delegación de servicios de tránsito aéreo**

Debería considerarse plenamente la duración de una operación degradada. Si el ATSP degradado tiene capacidad de reserva móvil o puede tener acceso a tal medio mediante asistencia de la OACI, tal vez necesite un plazo más largo para la coordinación; no obstante, puede también asegurarse de que el personal de la instalación degradada pueda continuar funcionando plena o parcialmente.

Por último, en la LOA debería describirse el arreglo de compartición de costos. Si se incurre en costos, estos deberían incluirse en un presupuesto o planificarse.

## 29 MARCO DE PLANIFICACIÓN DE CONTINGENCIA PARA LA SEGURIDAD DE ATM

En la presente sección se describe un marco de planificación de contingencia que establece un enfoque completo, sistemático y racional para las actividades de contingencia de ATSP, como se ilustra en la Figura I-6

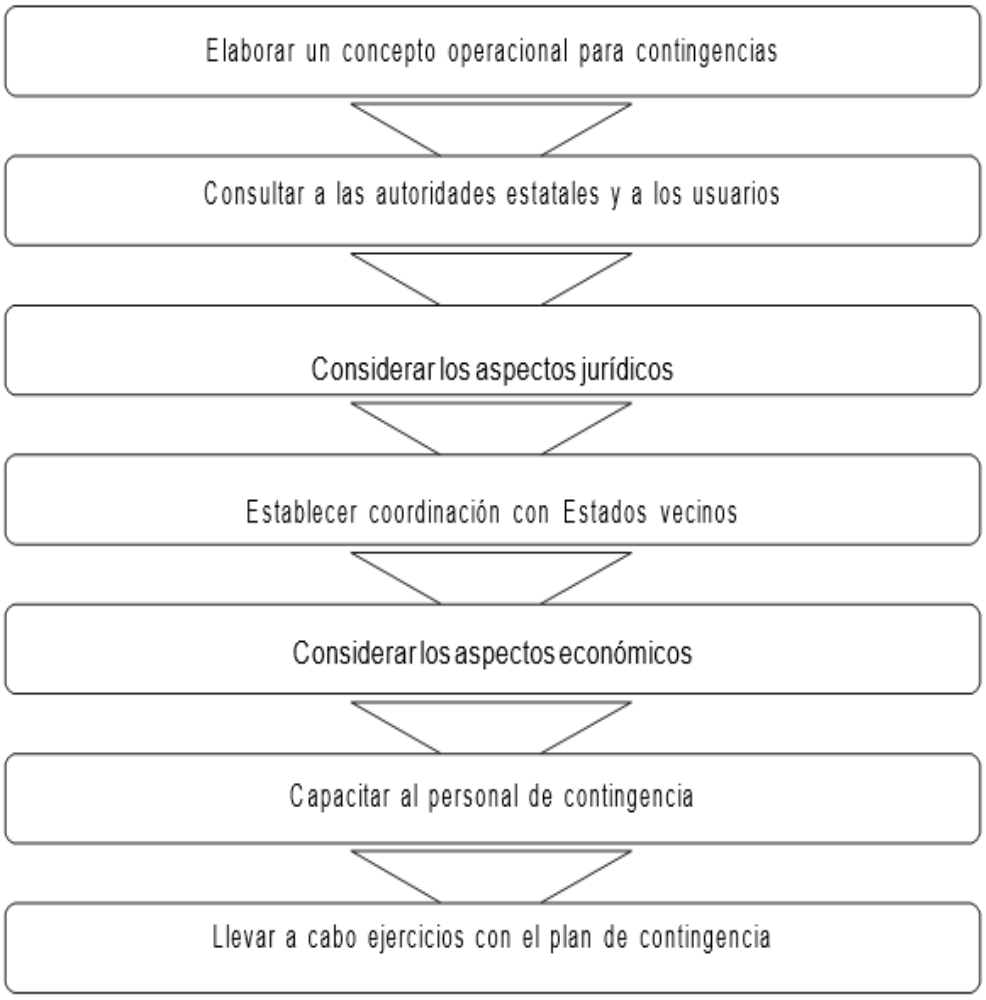


Figura I-6-2. Marco de planificación de contingencia

### 29.1 ELABORAR UN CONCEPTO OPERACIONAL PARA CONTINGENCIAS

En el concepto operacional para contingencias se consideran y documentan los elementos siguientes:

1. política de contingencia de ATSP: es indispensable que la administración superior defina claramente los objetivos y alcance globales de la organización en materia de contingencia y establecer su propio marco y responsabilidad para la planificación de contingencia;

2. principales sucesos de contingencia y riesgos correspondientes: preparar una lista de los principales sucesos de contingencia, peligros y áreas de riesgo conexas que la organización haya determinado y contra las cuales desee protegerse;

3. estrategias de contingencia posibles: enunciar el alcance, contexto y criterios de medidas de contingencia para indicar las estrategias que deben describirse más ampliamente en los planes de contingencia. Por ejemplo, cuando se dañe la

instalación, las opciones de medidas de contingencia pueden abarcar lo siguiente:

a) Instalaciones en emplazamiento común;

b) Instalaciones polivalentes;

c) Instalaciones centralizadas; y

d) Soluciones de sistemas comunes internacionales compartidas con otros países.

### 29.2 CONSULTAR A LAS AUTORIDADES ESTATALES Y LOS USUARIOS

Las autoridades estatales (incluidas la seguridad de la aviación civil, el sector militar y las autoridades de imposición de la ley), los ATSP y los usuarios (del espacio aéreo y de los aeropuertos) deberían establecer un mecanismo para elaborar los requisitos de las medidas de contingencia. En dicho mecanismo, las autoridades estatales tienen primacía en la definición de requisitos. Los ATSP, de común acuerdo con los usuarios del espacio aéreo y de aeropuertos, deberían elaborar medidas apropiadas para satisfacer dichos requisitos y objetivos adicionales para operaciones locales, según lo indicado en su política de planificación de contingencia.

### 29.3 CONSIDERAR LOS ASPECTOS JURÍDICOS

ATSP debe considerar los aspectos jurídicos, incluidos la responsabilidad civil y el seguro, especialmente en el contexto del suministro transfronterizo de servicios durante una contingencia. Respecto al suministro transfronterizo de servicios debe asegurarse lo siguiente:

1. Una clara definición de las normas y reglamentos aplicables;

2. Aprobación de los acuerdos por todos los Estados participantes;

3. Función aprobada de ATSP como dependencia que presta asistencia;

4. Función aprobada de ATSP como dependencia que ha fallado; y

5. Elaboración de un marco jurídico para proporcionar servicios ATC en una zona respecto a la cual el controlador pueda carecer de conocimientos o de capacitación apropiada.

### 29.4 ESTABLECER COORDINACIÓN CON ESTADOS VECINOS PARA OFICIALIZAR OPERACIONES ENTRE VARIOS ESTADOS

En el párrafo 5.4 del Adjunto C del Anexo 11 al Convenio de Chicago, se recomienda que, en caso de arreglos entre varios Estados, se establezca con cada uno de ellos una coordinación detallada para acordar oficialmente el plan de contingencia. Todo suceso que limite la capacidad de una instalación ATC para atender a los niveles normales de tránsito tendrá repercusiones en instalaciones ATC adyacentes, independientemente de que la situación exija la transferencia del control de parte o la totalidad del espacio aéreo a otras dependencias. Por consiguiente, los planes de contingencia deberían coordinarse con todas las instalaciones ATC adyacentes. Debería establecerse coordinación semejante con los Estados cuyos servicios resultarán afectados significativamente y con las organizaciones internacionales interesadas.

## 29.5 CONSIDERAR LOS ASPECTOS ECONÓMICOS

Un objetivo fundamental al definir planes de contingencia consiste en lograr una capacidad de contingencia adecuada a un costo razonable. Al realizar inversiones a corto o largo plazo para contingencias, ATSP debería considerar factores como los siguientes:

1. Existencia de otros emplazamientos y sistemas de contingencia posibles;

2. Inversiones y costo de funcionamiento para lograr determinada capacidad;

3. Probabilidad de un accidente, falla o violación de la seguridad y pérdidas o costos en que se incurra como resultado de perturbación o interrupción del servicio; y beneficios posibles de la implantación de medidas de contingencia (p. ej., primas de seguro inferiores).

Al tomar decisiones respecto a inversiones para contingencias, debería también considerarse un análisis económico, pero este constituye únicamente parte del procedimiento de toma de decisiones relativas a la continuidad del servicio. Entre los demás factores figuran el carácter obligatorio del marco jurídico (p. ej., OACI) y consideraciones y decisiones políticas.

## 29.6 CAPACITAR AL PERSONAL DE CONTINGENCIA

ATSP debe capacitar al personal para asegurarse de su capacidad de realizar sus tareas durante un suceso real. Debería capacitarse al personal de contingencia en materia de coordinación y comunicación entre equipos, notificación de procedimientos, requisitos de seguridad, procedimientos específicos para equipos y responsabilidades individuales. ATSP debería también asegurarse de que el personal de contingencia sea titular de licencias, competencias y habilitaciones apropiadas.

## 29.7 REALIZAR EJERCICIOS CON EL PLAN DE CONTINGENCIA

ATSP debería realizar ejercicios con el plan de contingencia para simular situaciones de emergencia y someter a prueba y validar la viabilidad de uno o varios aspectos del plan. Los aspectos que no se hayan considerado o las lecciones adquiridas durante los ejercicios deberían revisarse, investigarse y utilizarse para ajustar el plan de contingencia.

## 29.8 REQUISITOS GENÉRICOS PARA OPCIONES DE CONTINGENCIA

En la Tabla I-6-1 se introducen consideraciones genéricas respecto a diversas estrategias de contingencia posibles. Se trata de una secuencia de etapas que cubren la planificación relativa a la degradación de un sistema hasta el logro de una situación segura y protegida, la continuidad del servicio y la recuperación de los modos de funcionamiento. Se cubre también el mantenimiento de los planes de contingencia.

**Tabla I-6-1. Requisitos genéricos para estrategias de contingencia**

| |
|---|
| **Planificación** |
| • Establecer requisitos para contingencia:<br>— determinar los recursos principales, incluida la gestión de instalaciones;<br>— asegurarse de que el personal principal en los ATSP (o sea, las posibles dependencias que hayan fallado o puedan asistir) cuente con medios de comunicación a corto plazo.<br>• Establecer enlace con subcontratistas y proveedores de infraestructura.<br>• Crear un grupo de planificación de contingencia.<br>• Asegurarse de un rápido contacto con la autoridad de reglamentación o NSA, según corresponda; por ejemplo:<br>— obtener aprobación de las autoridades de reglamentación y la autoridad estatal respecto a procedimientos y prácticas que afectan al espacio aéreo de la dependencia que haya fallado;<br>— aclarar las cuestiones de otorgamiento de licencias y capacitación cuando el personal pueda proporcionar servicios relacionados con la seguridad operacional y la protección del espacio aéreo de un país vecino.<br>• Asegurarse de la capacitación del personal (ATCO y ATSP) en materia de medidas de contingencia.<br>• Documentar los planes de contingencia.<br>• El organismo de supervisión debería verificar la existencia y el contenido de los planes de contingencia.<br>— en caso de suministro transfronterizo de servicios durante una contingencia, las NSA de la dependencia que haya fallado y de la dependencia que preste asistencia deberían verificar los planes de contingencia. |
| **Paso de un sistema degradado a una situación segura y protegida** |
| **Fase 1 — Acciones inmediatas** |
| Se ha determinado la existencia de una situación peligrosa. Concentrarse en la gestión segura y protegida de la aeronave en el espacio aéreo de la dependencia que haya fallado, aplicando todos los medios técnicos que aún funcionen:<br>• Asegurar la situación del tránsito.<br>• Considerar la evacuación del espacio aéreo — “despejar el cielo”.<br>Si el tiempo lo permite, consultar con equipos de ingeniería de sistemas y subcontratistas para determinar si pueden resolver una falla antes de que se tome una decisión crítica.<br>• Determinar la magnitud del problema y la duración de la interrupción del servicio.<br>• Preparar instrucciones de reserva para asegurar operaciones en condiciones de seguridad y protección y permitir una transición sin obstáculos hacia las Fases 2 a 5 inclusive.<br>• Determinar la gravedad de la situación e iniciar medidas de contingencia apropiadas; esto corre a cargo de las autoridades competentes.<br>• Iniciar la notificación de todas las partes interesadas. |

| |
|---|
| **Fase 2 — Acciones inmediatas** |
| Centrarse en estabilizar la situación y, de ser necesario, prepararse para arreglos de contingencia a más largo plazo:<br>• iniciar medidas de contingencia;<br>• finalizar la notificación de todas las partes interesadas;<br>• determinar y coordinar medidas de control de la afluencia; |
| Continuidad del servicio |
| **Fase 3 — Iniciación de la opción** |
| • El contenido depende de la estrategia que se haya considerado. |
| **Fase 4 — Optimización** |
| Optimizar gradualmente la capacidad hasta un máximo posible (dentro de las estructuras de rutas y sectorización publicadas o reducidas de la OACI, de conformidad con las expectativas convenidas de los usuarios y la autoridad de reglamentación):<br>• perfeccionar, en la medida de lo posible, los medios de comunicación;<br>• aplicar, en la medida de lo posible, procedimientos de coordinación “normales”;<br>• considerar las consecuencias o el “efecto dominó” en otros ATSP o Estados que resultarán afectados por el aumento de la carga de trabajo para las dependencias que prestan asistencia. |
| Recuperación |
| **Fase 5 — Respuesta y recuperación a largo plazo** |
| Regresar a la dependencia y al puesto de trabajo originales de manera protegida, segura y ordenada:<br>• iniciar el plan de transición, teniendo en cuenta las condiciones técnicas y operacionales;<br>• informar a todas las partes interesadas de la intención de regresar a operaciones “normales”;<br>• asignar al personal entre la dependencia que ha fallado y la instalación de contingencia para operaciones “en la sombra” o paralelas durante el período de transición;<br>• coordinar el momento en que puedan reanudarse las operaciones normales;<br>• implantar actualizaciones a los sistemas de procesamiento de planes de vuelo y datos radar;<br>• autorizar la reanudación de operaciones “normales”. |
| Mantenimiento de los planes |
| • Organizar una sesión de evaluación inmediata.<br>• Realizar un ejercicio relativo a conocimientos adquiridos a raíz de una demostración real o práctica de planes de contingencia.<br>• Revisar los arreglos de planificación de contingencia y promulgar los cambios necesarios.<br>• Asegurarse de que la planificación de contingencia forme parte de los procedimientos de gestión del cambio de la organización. |

**PARTE II**

# 30 OPERACIONES DE SEGURIDAD DE ATM

## 30.1 ANTECEDENTES

En la Parte II se proporciona orientación sobre el suministro de servicios de seguridad de ATM para apoyar la seguridad nacional, la seguridad de la aviación y la imposición de la ley. Se presentan regularmente a los controladores de tránsito aéreo casos de aeronaves que pierden sus comunicaciones, actúan sin cumplir las reglas y procedimientos de vuelo establecidos o de manera sospechosa, notifican actos de interferencia ilícita en vuelo o entran en espacio aéreo controlado o zonas de seguridad sin autorización. Por estos y numerosos otros motivos, una aeronave puede convertirse en objeto sospechoso (TOI) que exige vigilancia y solución de problemas relacionados con la seguridad. Además, los controladores deben conocer las medidas que han de adoptar si los organismos militares o de imposición de la ley responden a actos de interferencia ilícita, posibles actos de agresión o actividades criminales que afectan a aeronaves en el espacio aéreo bajo control de ATSP.

Así, la orientación presentada aquí permitirá a ATSP considerar la amplia gama de servicios de seguridad que se le pueden solicitar y le permitirá elaborar orientación pertinente para sus responsabilidades particulares. ATSP también hallará aquí orientación para facilitar la ejecución de numerosas responsabilidades respecto a las operaciones de seguridad de ATM necesarias para la seguridad de operaciones estratégicas y tácticas y la colaboración entre agencias o la seguridad de las operaciones compartidas.

Los requisitos y métodos para suministrar servicios de seguridad de ATM variarán de un ATSP a otro según numerosos factores, tales como relaciones con el sector militar y los organismos de imposición de la ley y disposiciones sobre seguridad de ATM en el programa nacional de seguridad de la aviación civil (NCASP). Reconociendo esto, en el Apéndice D figuran ejemplos nacionales y regionales concretos de suministro de servicios de seguridad de ATM en Europa, el Reino Unido y los Estados Unidos. Por último, el presente texto de orientación sirve de marco destinado a asistir a los ATSP en el suministro efectivo de servicios de seguridad de ATM y la estructuración de sus organizaciones para operaciones de seguridad de ATM eficientes.

## 30.2 COLABORACIÓN ENTRE ORGANISMOS

ATSP colabora con numerosas organizaciones públicas y privadas, así como con diversos usuarios en materia de seguridad, al proporcionar servicios de seguridad de ATM. Además de los organismos en materia de seguridad de la aviación indicados en el NCASP del Estado, participan también organizaciones de respuesta de emergencia, salud pública, servicios de salvamento y lucha contra incendios, aduana y seguridad fronteriza y organismos de imposición de la ley. En la Figura II-1-1 se ilustra el alcance de los servicios de seguridad de ATM, así como las diversas funciones de ATSP respecto al apoyo, salvaguardia y protección en materia de seguridad de la aviación, seguridad nacional e imposición de la ley.

ATSP debería establecer comunicaciones oficiales y estructuras de coordinación con todos los organismos del Estado en materia de seguridad de ATM. Los pormenores del reparto de responsabilidades entre ellos variarán de un Estado a otro y dependerán de las diferentes leyes, costumbres y jerarquías de los departamentos y organismos gubernamentales. ATSP debería también participar en la capacitación y en ejercicios

conjuntos para lograr una respuesta integrada y efectiva de todos los organismos. En la Figura II-2-1 se ilustra el hecho de que las operaciones de seguridad de ATM podrían prestar servicio a una, dos o tres categorías de organismos en materia de seguridad en cualquier momento mediante responsabilidades comunes de los organismos.

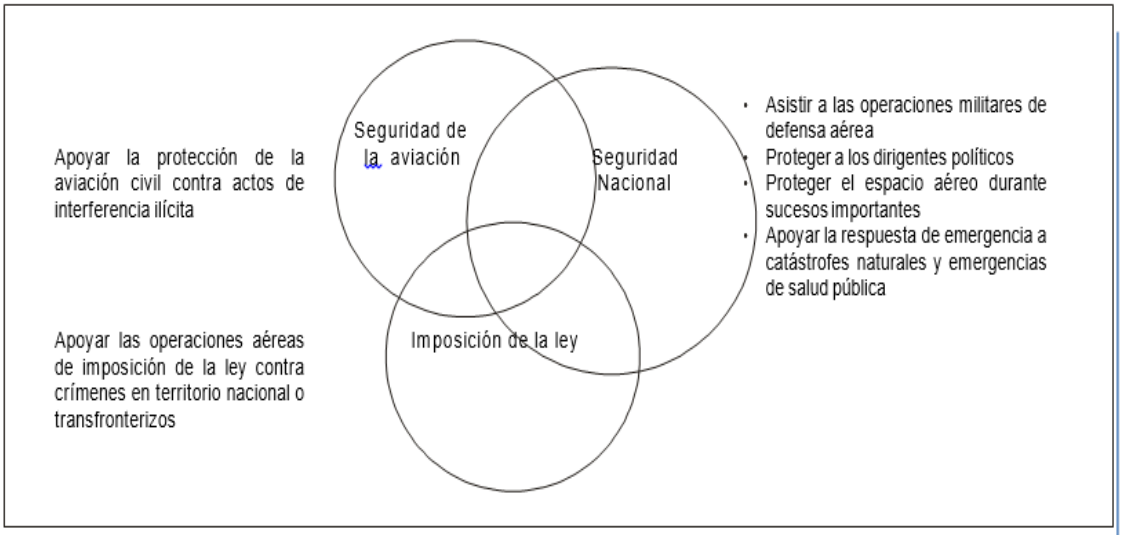


Figura II-1-1. Alcance del apoyo de ATSP a los socios en materia de seguridad

## 31 CONSIDERACIONES ESPECIALES RELATIVAS A LA PLANIFICACIÓN

En la presente sección se destacan dos temas que ATSP debería coordinar con las dependencias respectivas en materia de seguridad para lograr un consenso durante la planificación de operaciones de seguridad de ATM:

**1)** Pérdida de comunicación,

**2)** Objetos sospechosos. Ambos son importantes para que ATSP vigile y notifique todo vuelo que pueda constituir un motivo de inquietud en materia de seguridad para las organizaciones asociadas.

### 31.1 PÉRDIDA DE COMUNICACIÓN

En los últimos años, ciertos casos de pérdida de radiocomunicación (COMLOSS) con ATC se relacionaban con una amenaza a la seguridad. COMLOSS puede suceder por diversos motivos: fallas de equipo, errores humanos (p. ej., selección de un canal erróneo, volumen de la radio demasiado bajo) y actos de malicia intencionales. En un entorno de seguridad intensificada, una COMLOSS prolongada puede activar una alerta de seguridad y dar lugar a una respuesta militar o de imposición de la ley.

En el Manual de procedimientos de los servicios de tránsito aéreo, se consideran las pérdidas de comunicación. Refiérase al inciso No.

Sin embargo se deben de considerar otras situaciones. La intervención inicial de ATC podría consistir en lo siguiente, según los procedimientos convenidos:

1. Localizar y presentar la aeronave en pantalla;

2. Seguir vigilando la actuación sospechosa (p. Ej., incumplimiento de procedimientos establecidos);

3. Seguir tratando de establecer radiocomunicaciones bidireccionales vocales con la aeronave; y

4. Solicitar mayor asistencia para entrar en comunicación con la aeronave del modo siguiente:

5. Utilizar frecuencias de emergencia o voz basadas en radiofaros omnidireccionales VHF/VOR;

6. Si corresponde y es posible, solicitar que la oficina de despacho y operaciones de la aeronave utilice los canales vocales de la empresa o comunicaciones por enlace de datos de aeronave;

7. Solicitar que otras aeronaves en la última frecuencia asignada o frecuencia de la empresa traten de establecer contacto con la aeronave en situación comloss; y

8. Retransmitir la frecuencia apropiada por medio de un teléfono a bordo (p. Ej., teléfono por satélite), si existe.

Si no se restablece la radiocomunicación después de determinado plazo o no se reúnen condiciones o activaciones especificadas, EL ATC podría tomar otras medidas apropiadas basadas en protocolos o cartas de acuerdo operacionales en materia de seguridad y:

1. Continuar la vigilancia;

2. Alertar a las dependencias en materia de seguridad;

3. Preparar, a intervalos regulares, informes de seguimiento sobre la situación;

4. Asegurarse, mucho antes de que la aeronave atraviese el límite de la instalación ATC, de que la instalación siguiente esté al tanto de la situación y siga aplicando medidas apropiadas; y

5. Apoyar la operación el organismo respectivo del Estado considera que una interceptación es necesaria.

Debe analizarse y evaluarse una pérdida de comunicación para investigar sus causas y reducir al mínimo la posibilidad de que surjan en el futuro causas no relacionadas con la seguridad.

## 31.2 OBJETO SOSPECHOSO (TOI)

Se utiliza el mecanismo TOI para identificar un objeto en vuelo que pueda constituir un problema de seguridad. Es particularmente útil para facilitar la comunicación entre los organismos afines en materia de seguridad cuando se ignora la identidad del objeto en vuelo que activó la atención en materia de seguridad. Normalmente, ATC será la primera entidad que identifique un posible TOI.

Se indican a continuación situaciones que pueden activar el mecanismo TOI:

1. Incumplimiento de instrucciones de ATC, reglamentos de la aviación, restricciones temporales en el espacio aéreo y los vuelos u otros procedimientos de seguridad aplicables;

2. Pérdida de comunicaciones prolongada;

3. Transmisiones inhabituales, vagas o inapropiadas;

4. Actuación de vuelo inhabitual o sospechosa;

5. Entrada no autorizada en espacio aéreo controlado o zona de identificación para fines de seguridad;

6. Interferencia ilícita que afecte a las tripulaciones de vuelo en el aire, incluido el apoderamiento ilícito; y

7. Notificación de conducta sospechosa por dependencias o Estados adyacentes o por terceros.

Entre los ejemplos de incumplimiento de instrucciones de ATC por aeronaves pilotadas o pilotadas a distancia figuran los siguientes: la aeronave no activa el código de transpondedor asignado o el código cambia sin que la aeronave haya recibido instrucciones en ese sentido; o también, la aeronave se desvía de su vuelo o altitud asignados y no vuelve a los mismos cuando se le dan instrucciones al respecto. La conducta de vuelo inhabitual se refiere a una actividad incoherente o anormal de una aeronave tripulada o pilotada a distancia como: sobrevuelo o vuelo cerca de emplazamientos sensibles; incumplimiento de restricciones temporales en el espacio aéreo y los vuelos; vuelo en espacio aéreo protegido o restringido; velocidad o velocidad de ascenso/descenso inapropiada; omisión respecto a restricciones de cruce o puntos de notificación; notificación de dificultades de vuelo por los pilotos sin ninguna explicación o únicamente explicación vaga en respuesta a ATC; toda aeronave que solicite desviarse de su punto de destino o ruta originales por motivos desconocidos, salvo si se trata de: condiciones meteorológicas, solicitud de la empresa, solicitud de pasajeros, dificultades mecánicas, etc.; cualquier otro indicador de una situación sospechosa (p. ej., ruido de fondo, cambio en las inflexiones de la voz del piloto, etc.).

En ciertas circunstancias, un objeto en vuelo puede convertirse en TOI basándose en información específica y creíble relativa a dicha aeronave u objeto, sus pasajeros o su carga.

Normalmente se considera resuelta una situación TOI en las circunstancias siguientes, según el caso:

1. La aeronave o el objeto ya no está en el aire;

2. La aeronave acata las instrucciones de atc, los reglamentos de aviación aplicables, las restricciones en el espacio aéreo y los vuelos dictadas o los procedimientos de seguridad;

3. Se restablece el contacto por radio y se verifica el control autorizado de la aeronave;

4. La aeronave se intercepta y se verifica que su intención no es amenazante ni hostil;

5. Se identifica el TOI basándose en información específica y creíble que luego se determinó como inválida o poco fiable;

6. Se identifican los datos que aparecen en el radar y se caracterizan como inválidos (p. Ej., fondo, manada de aves); y

Cualquier información adicional que se obtenga indicando que no existe ningún motivo de inquietud respecto a la seguridad.

## CAPITULO 2

## 32 CONTRIBUCIÓN DE ATM A LA PROTECCIÓN CONTRA INTERFERENCIA ILÍCITA

A toda aeronave que se sospeche o se tenga información, que está siendo objeto de interferencia ilícita se le dará prioridad y se seguirán los procedimientos descritos en el Manual Operacional de los servicios de tránsito aéreo. Refiérase al inciso 24.

### 32.1 FUNCIÓN DE SEGURIDAD DE ATSP RESPECTO A OTRAS ORGANIZACIONES

El sistema de transporte aéreo es un sistema de redes abiertas e interconectadas que transporta personas y mercancías. La reducción del riesgo de interferencia ilícita en las aeronaves al mínimo exige un enfoque por capas como se ilustra en la Figura II-2-1. Dicho enfoque debería abarcar lo siguiente:

**Proteger el aeropuerto y demás infraestructura del sistema de aviación:** se incluyen medidas para impedir ataques contra aeronaves e instalaciones terrestres dentro del perímetro del aeropuerto o contra zonas de operaciones de aeronaves, zonas públicas, zonas estériles, instalaciones remotas y cualquier otra infraestructura relacionada con la aviación.

**Proteger a las personas:** se trata de medidas adoptadas para inspección de pasajeros y personal, verificaciones de antecedentes del personal, vigilancia y otros procedimientos de control del acceso encaminados a asegurarse de que solo estén a bordo de un vuelo o tengan acceso a la aeronave personas autorizadas y de que estas no lleven consigo artículos prohibidos.

**Proteger el equipaje:** se trata de la detección y prevención de amenazas debidas a objetos en el equipaje de mano o de bodega, incluidos explosivos, materiales químicos, biológicos, radiológicos y nucleares (CBRN) y otros materiales peligrosos.

**Proteger la carga y el correo:** se trata de medidas para reducir los riesgos planteados por artefactos peligrosos en la carga o el correo. En dichas medidas debería tenerse en cuenta la expedición desde la fuente hasta la salida. La cadena de expedición abarca la fuente de la carga, la preparación de contenedores, la reunión y expedición de la carga, los emplazamientos de inspección de carga y correo, en transporte aéreo hasta el punto de destino y todas las etapas intermedias de almacenamiento y transporte.

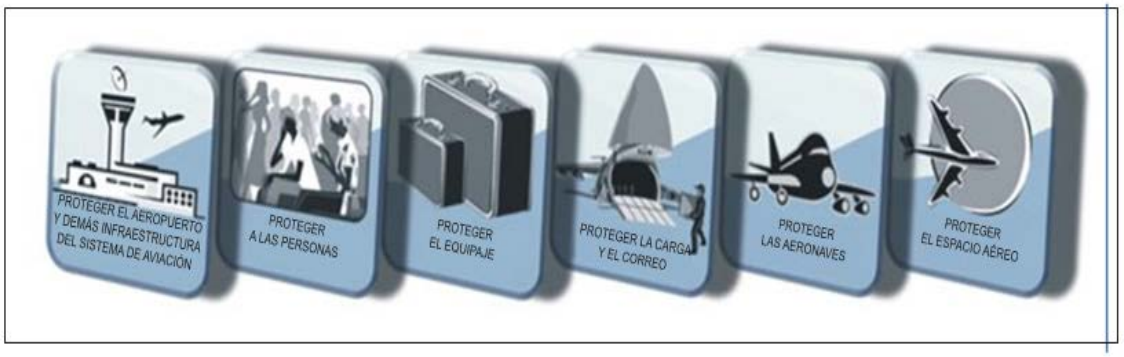


Figura II-2-1. Seguridad de la aviación por capas

**Proteger las aeronaves:** se trata de medidas para reducir el riesgo para las aeronaves y la probabilidad de que se utilicen como instrumento de terrorismo aeronaves pilotadas o no. En el primer caso, estas medidas podrían abarcar la presencia de oficiales de seguridad de a bordo (IFSO), cabina de pilotaje y célula reforzados y una comunicación aire-aire o aire-tierra más eficiente o mejorado. En el caso de aeronaves no pilotadas, deberían aplicarse las medidas de seguridad que se describen en la circular *Sistemas de aeronaves no tripuladas (UAS)* (Cir 328). En la clasificación de las aeronaves no tripuladas se incluyen los globos libres no tripulados y las aeronaves pilotadas a distancia.

Proteger el espacio aéreo: se trata de:

A. Impedir que un vuelo despegue cuando se reciba un aviso de inquietudes relativas a la seguridad del mismo.
B. Aplicar medidas de gestión de sucesos en vuelo relacionados con la seguridad.

Incumben en primer lugar a los explotadores de aeropuertos, proveedores de servicios de seguridad, explotadores de aeronaves, agentes de despacho de carga y autoridades postales las medidas de seguridad correspondientes a las primeras cinco capas de seguridad: protección de aeropuertos e infraestructura, personas, equipaje, carga y correo y aeronaves, mientas que ATSP, de común acuerdo con otros organismos en materia de seguridad de la aviación, contribuye a la capa que protege a las aeronaves en el aeropuerto y en el aire, así como la infraestructura del sistema ATM sea cual fuere su emplazamiento.

## 32.2 FUNCIONES DE SEGURIDAD DE ATM PARA LA SEGURIDAD DE LA AVIACIÓN

En la gestión de los actos de interferencia ilícita en las aeronaves. Debe reconocerse que pese a las medidas cada vez más estrictas de protección de las aeronaves en tierra y en el aire, es probable que surjan ocasionalmente amenazas y actos de interferencia ilícita. Es imposible predecir el momento, la naturaleza y los resultados posibles de tales sucesos. Por consiguiente, los planes de respuesta deberían ser flexibles y la administración debería asegurarse de que en los mismos se tenga en cuenta el carácter crítico e imprevisible de tales emergencias.

Los controladores deberían conocer los principios generales de la gestión de incidentes relacionados con la seguridad y las responsabilidades asignadas a ATSP en virtud del NCASP. Aunque no se impongan medidas específicas que ATSP debe tomar en determinada situación, en el NCASP se establece el marco de las responsabilidades y acciones de ATC en caso de interferencia ilícita en aeronaves en vuelo. Teniendo presentes

estos principios generales, deberían elaborarse procedimientos ATC específicos para apoyar la seguridad de la aviación.

Aunque ATSP no tiene una responsabilidad global para la gestión de incidentes relacionados con la seguridad de la aviación, el apoyo a otras organizaciones y entidades durante la respuesta a amenazas con interferencia ilícita en las aeronaves exige operaciones estratégicas y tácticas relacionadas con la seguridad. Las operaciones estratégicas de seguridad deben percibirse y elaborarse en el contexto de las responsabilidades y actividades convenidas de otras entidades; las operaciones tácticas de seguridad son las que se llevan a cabo al responder a incidentes concretos.

Todo el personal que participe en la gestión de emergencias relacionadas con la seguridad debería conocer los planes de contingencia y todos los demás documentos relacionados con la interferencia ilícita, incluidas las verificaciones operacionales y las LOA con instalaciones ATC adyacentes y debería estar capacitado para afrontar tales emergencias.

El Estado en que una aeronave objeto de un acto de interferencia ilícita haya aterrizado notificará el hecho y transmitirá, por el medio más rápido, toda información adicional pertinente al Estado de matrícula de la aeronave y al Estado del explotador, de conformidad con la norma 5.2.5 del Anexo 17. Dichas notificaciones normalmente incumbirán a la autoridad competente en materia de seguridad de la aviación. ATSP necesitará procedimientos para asegurarse de que la información sobre tránsito aéreo relativa a tales incidentes se comunique a las autoridades competentes.

Además de las notificaciones que se acaban de indicar, se exige que los Estados examinen y analicen todos los casos de interferencia ilícita. Al concluir el informe, debería presentarse a la OACI un informe sobre el incidente en cuestión.

Aunque normalmente la preparación del informe incumbirá a la autoridad competente en materia de seguridad de la aviación del Estado, se necesitará el registro de las acciones de ATC y la información recibida por el mismo para examinar el incidente y preparar el informe subsiguiente. Por ello, ATSP debería asegurarse de que las instrucciones locales (o documentos semejantes) para las dependencias ATS contengan disposiciones apropiadas relativas al mantenimiento de registros para garantizar la disponibilidad de la información necesaria. En los casos en que se registren las frecuencias y los canales de comunicaciones de ATC, los registros correspondientes al período del incidente deberían protegerse para ser utilizados en el informe.

## 32.3 FUNCIONES TÁCTICAS DE SEGURIDAD DE LAS OPERACIONES

Un incidente de interferencia ilícita a bordo podría ocurrir si fallan las medidas preventivas previas al despegue, lo que exigirá que ATC funcione en modo táctico para la gestión del incidente. Los actos de interferencia ilícita definidos en el Anexo 17 pueden reunirse en dos amplias categorías:

1. Actos cometidos por personas a bordo de la aeronave que comprometen la seguridad de la aeronave o las personas que se encuentran a bordo; y

2. Tentativa de introducción o introducción real o presumida de un arma o artefacto peligroso a bordo de una aeronave o en un aeropuerto o uso de armas basadas en tierra contra una aeronave o instalaciones aeroportuarias.

### 32.3.1 VIGILANCIA Y DETECCIÓN DE POSIBLES CASOS DE INTERFERENCIA ILÍCITA

A menudo ATC será el primero en enterarse de un caso de interferencia ilícita cometido por personas a bordo de una aeronave. De ser posible, una aeronave debidamente equipada debería notificar un acto de interferencia ilícita transmitiendo el código 7500 de transpondedor. Para cerciorarse de que no se trata de una transmisión accidental, el controlador debería solicitar a la tripulación de vuelo que confirme la selección de dicho código de conformidad con los procedimientos ATC publicados.

1. Existen también otros medios de notificación para:

2. aeronaves equipadas con vigilancia dependiente automática – radiodifusión (ADS-B), selección de modo de emergencia ADS-B;

3. aeronaves equipadas con vigilancia dependiente automática – contrato (ADS-C), selección del modo de emergencia ADS-C; y

4. aeronaves equipadas con comunicaciones por enlace de datos controlador-piloto (CPDLC), transmisión de un mensaje MAYDAY.

Cuando no sea posible seleccionar un código de transpondedor, un modo ADS o un mensaje CPDLC apropiados, las tripulaciones de vuelo pueden añadir la expresión “Squawking 7500” a las transmisiones locales inmediatamente después de haber transmitido el distintivo de llamada de la aeronave.

Las circunstancias de la interferencia ilícita podrían, en algunos casos, impedir a la tripulación transmitir cualquier información acerca de la situación a bordo. Por consiguiente, los controladores deberían conocer las categorías de conducta sospechosa que podría indicar que ha tenido lugar alguna forma de interferencia ilícita. Se indican a continuación ejemplos de esta conducta para aeronaves tripuladas o pilotadas a distancia:

1. Desviación del perfil de vuelo autorizado sin previa notificación o autorización;

2. Negativa o incapacidad de acatar instrucciones de atc (incluida guía vertical);

3. Desviación inhabitual del perfil de vuelo característico del tipo de aeronave;

4. Pérdida de contacto por radio relacionada con la desviación del perfil de vuelo;

5. Cambios no autorizados de código del radar secundario de vigilancia (ssr) o uso prolongado de la característica de identificación [p. Ej., ident en el sistema de identificación amigo o enemigo (iff)];

6. Uso por la tripulación de vuelo de fraseología no normalizada u otras tentativas disimuladas para destacar la situación (p. Ej., cambio marcado en las inflexiones de la voz o voz diferente);

7. Transmisión de radio no relacionada con atc (p. Ej., una declaración política); y

8. Transmisor abierto.

Aunque los controladores deben reconocer los diversos indicios de posibles actos de interferencia ilícita, también deberían darse cuenta de la posibilidad de falsas alertas y ejercer suma cautela y discreción al determinar la respuesta apropiada. Cuando los aspectos como los que se acaban de enumerar despiertan sospechas de que podría tratarse de interferencia ilícita, debería notificarse a las autoridades competentes.
Una aeronave tripulada o pilotada a distancia se desvía en dirección de emplazamientos sensibles dentro de zonas restringidas o prohibidas o no acata restricciones temporales en el espacio aéreo y los vuelos;

El equipo más antiguo ADS-B y ADS-C de aeronave puede transmitir un solo código de emergencia. La categoría de emergencia deberá establecerse mediante la voz o un mensaje CPDLC de texto libre. El equipo moderno puede transmitir uno de los cinco modos de emergencia para indicar la categoría de esta última. Véanse las secciones 8.5.4 y 13.4.3.4.5 de los PANS-ATM (Doc 4444).

Una aeronave tripulada o pilotada a distancia en espacio aéreo terminal se desvía en dirección de edificios o instalaciones terrestres importantes aun cuando no existan un espacio restringido ni restricciones relativas al espacio aéreo y los vuelos; y la presencia a bordo de personalidades políticas u otras celebridades que podrían constituir el objetivo de una tentativa de apoderamiento ilícito.

Una dependencia ATC podría también recibir información acerca de posibles actos de interferencia ilícita de las siguientes fuentes externas:

1. Dependencias ATS o Estados;

2. Fuentes no oficiales (p. Ej., agencias de prensa);

3. Explotadores de aeronaves respecto a perturbación a bordo; y

4. Terceros que notifican una amenaza no específica.

### 32.3.2 RESPUESTA A CASOS DE INTERFERENCIA ILÍCITA

Cuando una aeronave es objeto de un acto de interferencia ilícita, el posible carácter urgente del acto exige que se transmita inmediatamente información pertinente a la autoridad competente para permitir una respuesta oportuna a fin de proteger a la aeronave afectada y todas las demás aeronaves que podrían resultar afectadas por dicha operación. Por consiguiente, tan pronto como las circunstancias indiquen que deben tomarse precauciones relativas a la seguridad, la dependencia ATS debería transmitir un mensaje de alerta inicial que contenga toda la información pertinente a las autoridades competentes
En numerosos casos, la mayor parte de dicha información se obtendrá más fácilmente del explotador de la aeronave que solicitándola a la tripulación de vuelo en frecuencias de ATC. Sin embargo, para asegurarse de reunir toda la información disponible, en las instrucciones locales de la dependencia ATS (o documento similar) debería destacarse la necesidad de establecer un claro entendimiento con las demás partes respecto a la información que incumbe a cada organización o entidad recopilar.

La información fundamental siguiente que debería reunirse y transmitirse progresivamente a las partes interesadas es la siguiente:

1. Ruta de vuelo conocida o prevista;

2. Punto de destino conocido o sospechado y hora de llegada prevista;

3. Datos complementarios del plan de vuelo, tales como autonomía de combustible (expresada en horas y minutos, de ser posible) y el número de tripulantes y pasajeros a bordo;

4. Composición de la tripulación de vuelo y su conocimiento y experiencia de la ruta prevista;

5. Disponibilidad de cartas de navegación y documentación afín; y

6. Limitaciones en cuanto al tiempo de vuelo de la tripulación de vuelo, teniendo en cuenta el número de horas que sus miembros hayan realizado.

Pueden conocerse otros elementos de información, en cuyo caso deberían notificarse:

1. Distintivo de llamada, tipo de aeronave, matrícula y explotador;
2. Hora
3. Posición de la aeronave (latitud y longitud, si se conocen)
4. Ultimo código ssr asignado, ruta según el plan de vuelo observado o no, altitud.
5. Fase de vuelo (ascenso/descenso/crucero), rumbo, velocidad, velocidad vertical e indicación de inicio o fin del viraje;
6. Información sobre el plan de vuelo, incluidos los puntos de salida y llegada;
7. Intención del piloto, p. Ej., cambio de punto de destino, ruta prevista, asistencia necesaria para la aeronave y la tripulación de vuelo: ejecución de un descenso rápido, aterrizaje inmediato en un aeropuerto apropiado o en cualquier aeropuerto;

8. Frecuencia actual de la instalación de transmisión radioeléctrica (RTF) y entidad de control;

9. Otras aeronaves que no respondan a ATC;

10. Otras aeronaves que no sigan la última ruta ATC o nivel de vuelo (FL) autorizados;

11. Elementos que indican el apoderamiento ilícito de la aeronave, p. Ej., selección de código 7500 en modo a, declaración en RTF, suceso inhabitual, carácter de la actividad o conducta sospechosos de conformidad con criterios de notificación convenidos; e

12. Presencia de IFSO a bordo.

Además, según las circunstancias del suceso, debería comunicarse la información siguiente en la medida en que pueda obtenerse:

1. Número, nombres y apellidos y nacionalidad de los pasajeros y, de ser posible, de los infractores;

2. Número y estado de personas heridas a bordo;

3. Número y tipo o cualquier otra información sobre armas, explosivos, material incendiario u otras sustancias que se sabe o se cree que poseen los infractores;

4. Identidad, intenciones y exigencias de los secuestradores;

5. Posible lugar de aterrizaje a todo riesgo al alcance de la aeronave (con amenaza a qué objetos y en qué momento);

6. Aeropuertos para aterrizaje desviado o forzoso: capacidad en materia de seguridad, gestión de pasajeros, características operacionales (o sea, aproximación, plataforma, acuerdos de servicios mutuos); y

7. Estado físico de la tripulación de vuelo y, de ser el caso, los IFSO.

Para la gestión de los casos de interferencia ilícita, los controladores deberían realizar lo siguiente:

1. Ser discretos en sus comunicaciones con la tripulación de vuelo y evitar referencias evidentes a interferencia ilícita a menos que se sepa que los infractores no pueden escuchar las transmisiones;

2. Vigilar la aeronave y aplicar procedimientos normales de transferencia de control sin que se exijan transmisiones o respuestas del piloto a menos que el piloto haya establecido comunicaciones normales;

3. Si se envían aeronaves para interceptar y escoltar la aeronave objeto de apoderamiento ilícito, proporcionar toda asistencia posible a la aeronave de interceptación para ayudarla a situarse, inicialmente, en una posición detrás y por debajo de la aeronave objeto de apoderamiento; y

4. Notificar y coordinar la información pertinente con las autoridades de seguridad y defensa participantes.

Los controladores deberían seguir proporcionando a la aeronave en cuestión servicio de alerta normal y, en caso de COMLOSS, aplicar los procedimientos normalizados para fallas de las comunicaciones por radio. No obstante, también deberían darse cuenta de que es posible que la aeronave no siga dichos procedimientos.

Los controladores deben también seguir proporcionando servicios de separación normales a todas las aeronaves. Debe prestarse atención particular a la aeronave objeto de interferencia ilícita dado que su conducta podría ser imprevisible.

En todo momento, la seguridad de la aeronave y de las personas a bordo debería ser el aspecto más importante. Todas las solicitudes de la tripulación de vuelo relativas a desviaciones y paso a un nivel de amenaza más elevado deberían atenderse con prioridad, aunque esto exija que se enmienden las autorizaciones de otras aeronaves.

Si la tripulación de vuelo informa que desviará la aeronave hacia un aeropuerto que no es el punto de aterrizaje previsto, o si esto parece ser una posibilidad basándose en la conducta de la aeronave, debería informarse, lo antes posible, a la dependencia de control de aeródromo de dicho aeropuerto a fin de que pueda aplicar las medidas apropiadas especificadas en el plan de emergencia del aeropuerto.

### 32.3.3 AMENAZAS DE BOMBA

Para simplificar, en la presente sección se utilizará la expresión "**amenaza de bomba**" en sentido genérico para abarcar la amenaza que constituyen artefactos, armas o sustancias. Además, podría también tratarse de una amenaza de atacar una aeronave o una instalación ATC más bien que colocar un artefacto peligroso a bordo de la aeronave. Se aplican procedimientos semejantes a todas estas categorías de amenazas.

### 32.3.4 AMENAZAS DE BOMBA Y GESTIÓN DE AMENAZAS COMUNICADAS POR TELÉFONO

Varía considerablemente la manera en que las amenazas relativas a bombas u otros peligros pueden recibirse, así como la información que puedan contener: llamadas telefónicas, correo-e u otros tipos de mensajes por Internet o una nota escrita colocada en un lugar visible. La información inicial puede recibirse de una o varias fuentes: explotador de la aeronave, dependencia ATC, medios de comunicación, LEA, etc. y puede ser específica respecto a una aeronave o instalación ATC o referirse a una amenaza más general o también simplemente a "una bomba" o proporcionar información concreta sobre el tipo de bomba u otro artefacto peligroso.

Si el mensaje se recibe por teléfono, podría ser posible obtener más amplia información mediante una interrogación juiciosa, mientras pueda mantenerse al autor de la llamada en línea.

Numerosos sistemas telefónicos permiten determinar la fuente de las llamadas, aun después de que el autor de la llamada haya colgado, a condición de no cortar la línea en el punto de recepción. ATSP debería asegurarse de que, cuando exista, se implante dicha capacidad en todos los teléfonos de las instalaciones ATS.

ATSP debería asegurarse de que todo el personal que pueda responder a llamadas a números de teléfono al alcance del público conozca los procedimientos para la gestión de llamadas amenazantes y que esto se incluya en la capacitación de repaso.

### 32.3.5 RESPUESTA A AMENAZAS DE BOMBA

Las acciones iniciales de respuesta a una amenaza dependen de la manera en que se recibe la información. Si no la recibe una dependencia ATS, es importante obtener y registrar el nombre y apellido y la información de contacto de la persona que comunica el aviso y determinar las personas o entidades ya informadas.

La amenaza debe evaluarse y clasificarse como verdadera o falsa y se debe informar a los organismos correspondientes de seguridad.

En todos los casos de amenaza creíble a una aeronave en particular, debería declararse inmediatamente una fase de alerta y notificarse el centro de coordinación de salvamento apropiado.

Si la aeronave está en tierra, antes de la salida, el controlador de tránsito aéreo debería inicialmente denegar toda solicitud de autorización de despegue (o cancelarla si ya se ha otorgado) y notificar inmediatamente al personal de supervisión. Este debería entonces seguir los procedimientos establecidos para notificar a la empresa explotadora, a la autoridad aeroportuaria y a la autoridad competente en materia de seguridad de la aviación, como se indica en los planes de contingencia (salvo cuando se sepa que una o varias de dichas entidades ya estén al tanto de la situación). De ser necesario, la aeronave debería ser dirigida hacia el puesto de estacionamiento aislado designado o, si no lo hubiere, a otro apropiado, de conformidad con los procedimientos especificados en el plan de emergencia del aeropuerto local.

La autorización de salida debería otorgarse únicamente si la amenaza se ha declarado como falsa o se ha sometido la aeronave a registro y la autoridad competente ha determinado que no existe amenaza alguna.

Si la aeronave está en vuelo, por lo general el piloto al mando, de común acuerdo con el explotador de la aeronave, exigirá tratamiento prioritario para aterrizar lo antes posible. Los controladores deberían prestar toda asistencia posible para despachar el vuelo y satisfacer las solicitudes formuladas por el piloto.

Si corresponde, debería considerarse la posibilidad de mantener la aeronave lejos de zonas densamente pobladas. Sin embargo, la seguridad de la aeronave y sus ocupantes siempre debería constituir el aspecto predominante.

La situación debería notificarse lo antes posible a la torre de control del aeródromo de aterrizaje previsto. El controlador de la torre debería alertar al servicio de salvamento y extinción contra incendios, aplicar los procedimientos pertinentes del plan de emergencia del aeropuerto local y otorgar prioridad a la aeronave en cuestión para aterrizaje y rodaje hasta el puesto de estacionamiento aislado.

---

## CAPÍTULO 3 APOYO DE ATM A ORGANISMOS AFINES

### 33 ANTECEDENTES

Las autoridades de imposición de la ley (LEA) podrían pedir a ATSP que les facilite sus operaciones mediante tratamiento especial en el espacio aéreo y el tránsito aéreo o el suministro de información relacionada con determinados vuelos. Las operaciones de imposición de la ley podrían abarcar actividades locales, tales como policía con helicópteros y RPA, para detener o vigilar una actividad ilegal en tierra o apoyar una operación de imposición de la ley contra actividades criminales transfronterizas. Si se necesitan restricciones en el espacio aéreo y los vuelos para fines de seguridad, ATSP debería aplicar procedimientos para establecer restricciones temporales cuyo alcance y duración deberían ser el mínimo necesario para contener las actividades previstas, teniendo en cuenta las disposiciones de LEA en materia de seguridad de las operaciones aéreas y las operaciones de vuelo normales.

Según la orientación prevista por el Estado, ATSP podría también asistir en la interdicción terrestre y las medidas de respuesta del personal de imposición de la ley a interferencia ilícita a bordo de una aeronave u otra actividad ilegal, incluso si se apunta o dispara contra aeronaves civiles en vuelo con armas pequeñas, láser, sistemas portátiles de defensa antiaérea (MANPADS) o uso ilegal de sistemas de aeronaves no tripuladas. A menudo, esto supone que el personal ATM proporcione “vigilancia en el aire” hasta que las LEA en tierra asuman responsabilidad después del aterrizaje de la aeronave. El apoyo de ATSP a LEA podría también consistir en suministrar, a petición, información sobre planes de vuelo: país de matrícula, explotador, origen y destino. A menudo, una entidad que no sea ATSP se encarga de la tarea de detectar y vigilar aeronaves sospechadas de narcotráfico transfronterizo o por vía terrestre; no obstante, ATSP podría desempeñar funciones consecuentes de apoyo a dichas medidas de vigilancia.

### 34 AMENAZAS DE LÁSER

Los rayos láser pueden causar ceguera temporal o daño permanente a los tejidos humanos, especialmente la retina. La distancia sobre la que pueden utilizarse apuntadores láser va de 2 000 ft a mucho más de 30 km. Cuando se apunten directa o aun indirectamente a un piloto o controlador de tránsito aéreo, algunos láseres pueden causar lesión ocular o discapacidad visual temporal, como ceguera y distracción causadas por destellos, y tener efectos muy graves

Para proteger las operaciones de vuelo contra ataques con rayos láser, la OACI ha establecido SARPS al respecto en el Anexo 14 en que se recomienda establecer zonas protegidas alrededor de los aeródromos. ATSP apoya la protección de dichas zonas revisando las aplicaciones de espectáculos de luz u otras operaciones que puedan emitir luces que podrían poner en peligro las operaciones de vuelo.

Se consiguen fácilmente láseres poderosos y económicos y los incidentes relacionados con el láser se han convertido en un problema importante de seguridad operacional y seguridad de la aviación. ATSP debería supervisar continuamente el uso intencional de láseres contra aeronaves y analizar la tendencia de tales incidentes. Para lograr ese objetivo, en la sección 5.6 del Doc 9815 se recomienda que los Estados contratantes que deseen establecer un sistema de notificación de incidentes, proporcionen medios para supervisar el uso no autorizado de láseres en el espacio aéreo.
La rápida notificación de un incidente facilitará la investigación y las medidas posibles de imposición de la ley contra los infractores. En el Apéndice B del Doc 9815 figuran modelos de informes sobre incidentes.

Cuando ATSP reciba del piloto un informe inicial sobre el uso de láseres, debería asegurarse de que se registre la información siguiente:

1. Hora del suceso;
2. Identidad de la aeronave;
3. Tipo de aeronave;
4. Color del láser (rojo o verde, etc.);
5. Posición/emplazamiento — punto de referencia/distancia radial, aproximación a determinada pista, distancia u orientación respecto al aeropuerto o latitud y longitud, etc.;
6. Altitud;
7. Dirección de la aeronave durante el incidente;
8. Posición del láser en relación con la aeronave;
9. Cabina de pilotaje iluminada — sí/no;
10. Lesiones causadas a la tripulación de vuelo — sí/no;
11. Visión de la tripulación de vuelo perturbada por efectos visuales (deslumbramiento, ceguera causada por destellos, pérdida de adaptación a la oscuridad, molestia causada por el deslumbramiento e imagen secundaria);
12. Intenciones de la tripulación de vuelo (p. Ej., continuar o regresar);
13. Lea notificadas — sí/no (nombre y apellido y número de teléfono, si se conocen);
14. Breve descripción del suceso; y
15. Toda información pertinente.

ATSP debería mantener un relato completo y preciso del suceso durante un plazo convenido después de haberse notificado debidamente a la entidad investigadora.

Los Estados deberían establecer leyes y reglamentos para prohibir el uso intencional de láseres contra aeronaves so pena de sanciones en caso de violación. ATSP podría alentar a los controladores de tránsito aéreo a colaborar con los pilotos y LEA para determinar el origen de los rayos láser utilizados contra aeronaves y proporcionar asistencia, según corresponda, a LEA para localizar e identificar a los presuntos autores.
En este aspecto se seguirá el procedimiento para reportes de amenazas con ases de luz láser.

## 35 AMENAZAS CON SISTEMAS PORTÁTILES DE DEFENSA ANTIAÉREA (MANPADS)

Los MANPADS representan una amenaza importante para la aviación civil. Siendo portátiles y muy perfeccionados, son de difícil detección y pueden causar daños graves aun en el caso de aviones civiles de grandes dimensiones. Muchos de ellos tienen efectos mortales hasta una altitud de unos 15 000 ft desde una distancia de 8 km o más. En la sección siguiente se definen los niveles de alerta para amenazas MANPADS y procedimientos para la notificación de sucesos relacionados con estos últimos.

ATSP debería colaborar con las autoridades estatales y civiles para crear un plan estratégico y procedimientos como respuesta a sucesos MANPADS.

Las amenazas de MANPADS pueden clasificarse según determinados niveles de alerta:

1. Nivel de alerta 1 — aumento de la conciencia, operaciones normales;

2. Nivel de alerta 2 — una amenaza creíble a un aeropuerto, transportista o región específicos. Revisar los planes de contingencia y atenuación (de haberlos); y

3. Nivel de alerta 3 — lanzamiento observado o notificado: implantar todo plan de contingencia o atenuación.

Respuesta al nivel de alerta 1. Este representa el nivel más bajo de alerta a una amenaza MANPADS. Una mayor vigilancia y el reconocimiento por ATSP constituyen un elemento fundamental para impedir o limitar un ataque. El personal ATC que considere que existe o es inminente una actividad sospechosa debería informar a sus supervisores para posibles medidas ulteriores.

Respuesta al nivel de alerta 2. Debería implantarse el nivel de alerta 2 a raíz de la recepción de información relativa a una amenaza MANPADS creíble a un aeropuerto, línea aérea o región específicos. Dicha información debería comunicarse a LEA y entidades de defensa del Estado apropiadas, según corresponda.

Debería también comunicarse información relativa al nivel de la amenaza causada por actividad MANPADS a las entidades siguientes, de conformidad con los SARPS y los planes y procedimientos de respuesta estratégicos:

1. Centro apropiado de operaciones del explotador de aeronaves;

2. Instalación ATC que controle el vuelo en cuestión;

3. Instalaciones ATC adyacentes; y

4. Torre ATC de la instalación o instalaciones afectadas.

Respuesta al nivel de alerta 3. El nivel de alerta 3 debería implantarse después de un ataque observado o notificado. Cuando un lanzamiento de MANPADS es observado por la instalación ATC o notificado a esta última por cualquier aeronave bajo su control, ATSP debería preparar un informe inicial, con los datos siguientes:

1. Distintivo de llamada (si se conoce);

2. Tipo de aeronave (si se conoce);

3. Hora UTC del ataque;

4. Posición/emplazamiento;

5. Altitud; y

Toda información pertinente.

El supervisor de la instalación ATC que reciba el informe o presencie el ataque debería asegurarse de que la información se comunique a las LEA, entidades de defensa y autoridades civiles del Estado apropiadas, según corresponda.

La información relativa a MANPADS debería ser radiodifundida por el servicio automático de información terminal (ATIS) del aeropuerto afectado, de conformidad con los procedimientos de ATSP y de la aviación civil.

## CAPÍTULO 4 CATÁSTROFES Y EMERGENCIAS DE SALUD PÚBLICA

### 36 APOYO DE ATM A LA RESPUESTA Y RECUPERACIÓN EN CASO DE CATÁSTROFE

Las medidas de respuesta y recuperación a raíz de catástrofes causadas por el hombre o naturales casi siempre suponen alguna forma de operaciones aéreas que necesitan servicios ATC. En algunos casos, ATSP puede no estar en condiciones de proporcionar servicios de tránsito aéreo porque la infraestructura de aviación podría estar dañada o destruida. En otros, la infraestructura ATC puede estar intacta, pero podrían necesitarse servicios de seguridad ATC especiales durante la respuesta a la catástrofe o la correspondiente recuperación. Entre los ejemplos de servicios de seguridad ATC figuran los servicios para vuelos de vigilancia encaminados a determinar la amplitud del daño, operaciones de salvamento, transporte aéreo de personal y suministros y evacuación de heridos. En caso de incendios forestales, intervendrán aeronaves de extinción de incendios. En algunas situaciones, pueden utilizarse RPA para vigilar las zonas afectadas y para otros fines relacionados con una catástrofe. La utilización de RPA en tales casos podría exigir la aplicación de procedimientos ATC especiales. Los medios de comunicación también tienen una función legítima durante las catástrofes que podría exigir procedimientos ATC especiales para sus aeronaves. Los vuelos que transporten a personalidades destacadas (VIP) y altos funcionarios estatales para fines de vigilancia o visita podrían exigir coordinación en materia de seguridad y restricciones temporales en el espacio aéreo y los vuelos.

En el presente capítulo se examina la amplia visión descrita en que la seguridad de ATM incluye también aspectos de seguridad relacionados con amenazas involuntarias. Estas incluyen el error humano y las catástrofes naturales o los peligros que destruyen partes del sistema ATM y exigen una seguridad reforzada a fin de garantizar la seguridad de ATM durante su recuperación. Esto permite también prestar servicios específicos de seguridad de ATM en apoyo de las medidas de seguridad nacional e imposición de la ley a raíz de tales peligros o amenazas involuntarias. Aunque la seguridad de la aviación se relaciona principalmente con las amenazas intencionales, la seguridad de la aviación solo constituye uno de los aspectos de la seguridad de ATM.

En el marco de esta última deben considerarse tanto las amenazas intencionales como las amenazas y peligros involuntarios.

Dado que a menudo se intensifican las operaciones de vuelo en una zona de catástrofe, las autoridades competentes a menudo solicitarán a ATSP que limite el tipo y tal vez el número de aeronaves que efectúan operaciones en la zona. Esto exige la aplicación de restricciones temporales en el espacio aéreo y los vuelos. El alcance de las restricciones y las categorías de operaciones que se permitirán deberían establecerse en coordinación con la autoridad encargada de la respuesta a catástrofes. Dicha información debería publicarse en un aviso a los aviadores (NOTAM).

Deberían indicarse las organizaciones competentes con las que se necesitará coordinación para las categorías de crisis y catástrofes que puedan presentarse. Esto debería incluir información de contacto (incluido el contacto después del cierre de la jornada). Al enterarse de una crisis o catástrofe inminente, puede iniciarse de inmediato la coordinación con las autoridades locales, estatales y nacionales competentes, pero esto no será posible en ciertas circunstancias. Por consiguiente, el sistema debería estar en condiciones de responder rápidamente a las solicitudes de apoyo a operaciones de respuesta a crisis y catástrofes.

Durante el suceso, ATSP debería asegurarse de que solo se otorgue a aeronaves autorizadas el permiso de efectuar operaciones en el espacio aéreo restringido para gestión de la crisis y operaciones de recuperación en caso de catástrofe y, según corresponda, se otorgue tratamiento prioritario a las aeronaves autorizadas que participan en dichas operaciones. Las autoridades encargadas de las medidas de respuesta deben determinar la duración de las restricciones relativas al espacio aéreo y los vuelos. Si las operaciones se prolongan, deberían revisarse periódicamente el alcance de las restricciones en el espacio aéreo y las restricciones sobre las categorías de vuelo que se permitan.
Para tal efecto se seguirán los protocolos de respuesta ante catástrofes de la Coordinadora para la Reducción de Desastres CONRED.

## 37 ENFERMEDADES TRANSMISIBLES Y OTROS RIESGOS PARA LA SALUD PÚBLICA A BORDO DE LAS AERONAVES

En el mundo globalizado, las enfermedades pueden propagarse involuntariamente por todas partes debido a los viajes y el comercio internacionales. Una crisis sanitaria en un país puede propagarse rápidamente a otro. La rápida identificación de posibles casos de enfermedades transmisibles y otros riesgos para la salud pública entre los pasajeros que viajan por vía aérea es un elemento crucial para reducir la probabilidad de que dichos casos se conviertan en una emergencia pandémica que podría afectar a la seguridad nacional.

Ningún país está protegido contra la amenaza de terrorismo; además, existe la inquietud permanente respecto a amenazas de terrorismo CBRN cuyos efectos se propagan mediante el uso de personas expuestas o infectadas a bordo de aeronaves comerciales. La posibilidad de una propagación intencional de enfermedades y otros riesgos para la salud pública por intermedio de personas a bordo de las aeronaves constituye una amenaza a la seguridad nacional y la seguridad de la aviación que exige que ATSP tenga conciencia de la situación e intervenga para apoyar los procedimientos de la autoridad médica y las posibles medidas e intervenciones de imposición de la ley o militares. Por consiguiente, los servicios ATM que se exigen en el Capítulo 16 de los Procedimientos para los servicios de navegación aérea — *Gestión del tránsito aéreo* (PANS-ATM) (Doc 4444) para dichas situaciones se incluyen debidamente en el presente manual como servicio relacionado con la seguridad de ATM.

Con objeto de lograr una respuesta eficiente, la planificación de la preparación para un posible

suceso CBRN relacionado con la salud pública debería incluir comunicación y colaboración entre los organismos nacionales y locales de salud pública y seguridad antes de identificar la amenaza.

En el Reglamento Sanitario Internacional (2005) de la Organización Mundial de la Salud (OMS) se especifican los procedimientos para responder a casos en que se sospechen enfermedades transmisibles a bordo de las aeronaves. Incumbe a las autoridades de salud pública, explotadores de aeropuertos y líneas aéreas aplicar la mayoría de dichos procedimientos.

Las líneas aéreas deben proporcionar orientación a las tripulaciones de cabina para la identificación y gestión a bordo de posibles casos de enfermedades transmisibles. En las disposiciones del Anexo 9 — *Facilitación,* y la sección 16.6 de los PANS-ATM (Doc 4444) se exige que la tripulación de vuelo notifique a ATC lo más prontamente posible los casos de enfermedades transmisibles u otros riesgos para la salud pública que se determinen.

Se necesita la información siguiente:

1. Identidad de la aeronave;

2. Aeródromo de salida;

3. Aeródromo de destino;

4. Hora prevista de llegada (ETA);

5. Número de personas a bordo;

6. Número de casos sospechosos a bordo; y

7. Tipo de riesgo para la salud pública, si se conoce.

En la sección 16.6 de los PANS-ATM (Doc 4444) se exige también que, tras recibir dicho aviso de enfermedad transmisible o un riesgo para la salud pública a bordo de una aeronave, la dependencia ATS transmita dicha información, lo antes posible, a las dependencias ATS que presten servicios en el lugar de destino o de salida a menos que existan procedimientos para notificar a la autoridad competente designada por el Estado y al explotador de aeronaves o su representante designado.

Por regla general, la tripulación de cabina no estará en condiciones de identificar determinada enfermedad o efecto CBRN; probablemente solo podrá describir los síntomas observados. A fin de asistir a las autoridades médicas en la evaluación de la respuesta necesaria, dicha descripción debería registrarse exactamente como la ha comunicado la tripulación.

En la sección 16.6 de los PANS-ATM (Doc 4444) se indica también que cuando las dependencias ATS que prestan servicios en los aeródromos de destino y salida reciban un informe relativo a un caso sospechado de enfermedad transmisible u otro riesgo para la salud pública a bordo de una aeronave, proveniente de otra dependencia ATS o de una aeronave o un explotador de aeronaves, deberán transmitir el mensaje, lo antes posible, a la autoridad de salud pública u otra autoridad competente designada por el Estado, al explotador de aeronaves o su representante designado y al explotador del aeropuerto local.

A raíz de la notificación inicial, debería comunicarse al explotador del aeropuerto todo cambio en la ETA de la aeronave.

Los Estados no deberían denegar la entrada a una aeronave debido a un caso notificado de posible enfermedad transmisible. Sin embargo, en el Artículo 28.1 del Reglamento Sanitario Internacional (2005) se especifica que si el punto de entrada previsto no está equipado para aplicar las medidas sanitarias apropiadas exigidas en virtud del reglamento, podrá exigirse que la aeronave se desvíe hacia un aeropuerto de entrada más apropiado, a condición de que esta opción sea operacionalmente viable.
En tal caso se seguirán los protocolos que figuran el manual de Plan de Emergencia del Aeropuerto PEA.

## CAPÍTULO 5 GESTIÓN DEL ESPACIO AÉREO PARA LA SEGURIDAD DE ATM

### 38 VIGILANCIA Y NOTIFICACIÓN DEL SOBREVUELO DE ZONAS DE IDENTIFICACIÓN PARA FINES DE SEGURIDAD

Los Estados contratantes, dentro del espacio aéreo bajo su soberanía, tienen la autoridad legal para permitir o denegar el acceso a su espacio aéreo soberano, de conformidad con las disposiciones del Convenio de Chicago. En las leyes nacionales deberían designarse las autoridades y entidades nacionales a las que incumbe: establecer normas y procedimientos sobre uso del espacio aéreo, autorizar o denegar el acceso al espacio aéreo nacional y resolver aspectos relacionados con autorizaciones diplomáticas y exigencias de seguridad nacional (p. ej., defensa aérea). Puede exigirse que ATSP apoye dichos requisitos de seguridad vigilando y proporcionando información relativa al sobrevuelo de zonas de identificación para fines de seguridad.
Una zona designada de identificación para fines de seguridad es el espacio aéreo por encima de una zona específica de tierra o agua bajo soberanía nacional donde el control de las aeronaves sea necesario por motivos de seguridad nacional. Dichas zonas suelen situarse por encima de límites territoriales y se designan para proteger la soberanía aérea del Estado. Dentro de dichas zonas, se limitan las operaciones de aeronaves a aquellas que satisfagan requisitos específicos, tales como mantenimiento de radiocomunicaciones bidireccionales con ATC, presentación de un plan de vuelo en que se indiquen la hora y el punto de entrada en la zona de identificación para fines de seguridad, utilización de un código especial de transpondedor, notificación de la altitud y salida dentro de un plazo especificado respecto a la hora prevista. Dichos requisitos deben satisfacer lo acordado entre las autoridades respectivas del Estado responsable de la defensa nacional y el organismo estatal responsable de la seguridad de las fronteras.

ATSP debería comunicar a la comunidad de aviación por medio de NOTAM, la publicación de información aeronáutica y otros canales oficiales de comunicación, los requisitos relacionados con la seguridad en el caso de vuelos que entran, salen, atraviesan o efectúan operaciones dentro del espacio aéreo territorial del país. ATSP adquiere, procesa y distribuye información sobre planes de vuelo a las instalaciones aeronáuticas pertinentes. La vigilancia y notificación de información sobre movimientos de aeronaves debería ajustarse a los procedimientos especificados en los procedimientos operacionales normalizados (SOP) de cada instalación ATC.

En algunos casos, ATSP podría detectar en una zona de identificación para fines de seguridad una aeronave que no cumpla los reglamentos. En dicho caso, debería notificar a las organizaciones competentes de defensa aérea según las SOP de la instalación y declarar la aeronave como objeto sospechoso (TOI).

En algunas zonas, podría ser necesario el uso de radar primario para identificar las aeronaves que aplican las reglas de vuelo visual (VFR) y asegurarse de que cumplan los requisitos aplicables.

En ciertas situaciones, las entidades de defensa o seguridad del Estado podrían informar a ATSP acerca de aeronaves que no cumplan los reglamentos. ATSP debería localizar y presentar en la

pantalla la aeronave en el sistema de vigilancia del tránsito aéreo y podría, además, facilitar su identificación y seguimiento. También se le podría solicitar que comunique a los organismos en materia de seguridad la posición, altitud, velocidad aerodinámica y dirección del vuelo. ATSP debería también informar a la instalación ATC del caso, a lo largo de la trayectoria del TOI, a fin de coordinar el seguimiento de la aeronave desconocida hasta que aterrice. De conformidad con los acuerdos entre las autoridades militares y los organismos civiles del Estado, ATSP debería informar a la autoridad designada cuando la aeronave aterrice.

En una situación de emergencia, el piloto al mando tal vez tenga que desviarse de las normas para proteger el vuelo. ATSP debe considerar la seguridad operacional del vuelo y los requisitos de seguridad y aconsejar al piloto al mando que cambie la trayectoria de vuelo en consecuencia.

Si debe interceptarse una aeronave, debe seguirse el Anexo 2 — *Reglamento del aire* (sección 3.8):

La interceptación de aeronaves civiles se regirá por los reglamentos y directrices administrativas apropiados que los Estados contratantes establezcan en cumplimiento del Convenio sobre Aviación Civil Internacional y, especialmente en cumplimiento del Artículo 3 d), en virtud del cual los Estados contratantes se comprometen a tener debidamente en cuenta la seguridad de las aeronaves civiles, cuando establezcan reglamentos aplicables a sus aeronaves de Estado. En consecuencia, al redactar dichos reglamentos y directrices administrativas los Estados tendrán en cuenta las disposiciones que figuran en el Apéndice 1, Sección 2, y en el Apéndice 2, Sección 1.

Reconociendo que es esencial para la seguridad del vuelo que cualquier señal visual utilizada en caso de interceptación, a la que solamente debería recurrirse en última instancia, sea correctamente empleada y comprendida por las aeronaves civiles y militares del mundo entero, el Consejo de la Organización de Aviación Civil Internacional, al adoptar las señales visuales contenidas en el Apéndice 1 de este Anexo, instó a los Estados contratantes a que se aseguren de que sus aeronaves de Estado cumplan estrictamente con dichas señales visuales. Como la interceptación de aeronaves civiles representa en todos los casos un peligro posible, el Consejo ha formulado también recomendaciones especiales e insta a los Estados contratantes a ponerlas en práctica con carácter uniforme. Estas recomendaciones especiales figuran en el Adjunto A.

En caso de interceptación de una aeronave civil su piloto al mando cumplirá con las normas que figuran en el Apéndice 2, Secciones 2 y 3, interpretando y respondiendo a las señales visuales en la forma especificada en el Apéndice 1, Sección 2.

## 39 CONTROL DE SEGURIDAD DE EMERGENCIA DEL TRÁNSITO AÉREO

Convendría que los Estados elaboraran un plan de preparación de emergencia en el que se prescriban las medidas que deben tomar las autoridades nacionales competentes para fines de seguridad nacional a fin de controlar el tránsito aéreo en situaciones de emergencia. En un plan de control de seguridad de emergencia del tránsito aéreo se definirían las autoridades, responsabilidades y procedimientos para identificar y controlar el tránsito aéreo dentro de una zona especificada durante situaciones de emergencia de defensa aérea o nacional. Deberían establecerse en el plan la función ATM, el espacio aéreo y las medidas de seguridad y funciones requeridas de ATSP.

Si las autoridades nacionales deciden imponer medidas de control de seguridad de emergencia del tránsito aéreo, se seguirán los protocolos nacionales relativos a su implantación.

La restricción del tránsito aéreo en respuesta a un ataque o amenaza a la seguridad nacional podría lograrse implantando medidas coordinadas y apropiadas de control del espacio aéreo. Las fases de control convenidas o las medidas solicitadas por autoridades nacionales o militares y

aplicadas por intermedio de ATSP podrían incluir, entre otras cosas, rutas aéreas, corredores y vuelos específicos y autorizaciones de explotadores de aeronaves, planificación de vuelo y restricciones basadas en procedimientos o el cierre total selectivo o sistemático de determinado espacio aéreo.

El control de seguridad de emergencia del tránsito aéreo podría implantarse por fases para lograr una transición fácil de los procedimientos normales de identificación y control de tránsito aéreo a procedimientos más restrictivos de identificación y control exigidos por la situación. Las medidas de control del espacio aéreo dentro de cada fase podrían modificarse, adaptarse o suprimirse, según corresponda, o también implantarse prescindiendo de las mencionadas fases, si así lo dicta la situación. Las fases convenidas podrían seguir determinado modelo de aplicación a zonas de identificación para fines de seguridad, corredores aéreos específicos y todas las zonas controladas por ATSP.

Las prioridades asignadas para misiones de aeronaves, en el plan de control de seguridad de emergencia del tránsito aéreo del Estado, podrían comprender requisitos específicos sobre planes de vuelo, exigir el paso a un código especial de transpondedor, radiocomunicaciones directas con una instalación ATC y la entrada de información específica relativa a la seguridad en la sección de observaciones en el plan de vuelo. La información específica sobre seguridad requerida en el plan de vuelo podría incluirse con los datos de este último y comunicarse de una instalación ATC a la siguiente y a las instalaciones competentes de control de defensa aérea.

Podrían presentarse situaciones que no puedan controlarse de conformidad con una lista de requisitos prioritarios para una emergencia de tránsito aéreo. Constituyen ejemplos de ello las emergencias de aeronaves y los vuelos internacionales de llegada que hayan alcanzado el punto de no retorno, incluidos los vuelos de explotadores de aeronaves internacionales que estén en ruta hacia aeropuertos refugio de conformidad con acuerdos internacionales específicos. Estos sucesos deberían tratarse individualmente mediante coordinación entre ATSP y las autoridades militares competentes considerando la urgencia de la situación en vuelo y las condiciones militares tácticas existentes.

Podrían presentarse situaciones en que la aeronave necesitaría efectuar un vuelo, pero no podrá hacerlo porque carece de prioridad o su ruta de vuelo prevista entra en conflicto con las restricciones de vuelo impuestas. En tales casos, deberían existir y seguirse disposiciones relativas a una solicitud especial de aprobación de vuelo.

Al recibir un mensaje debidamente autenticado para implantar un control de seguridad de emergencia del tránsito aéreo, ATSP debería hacer lo siguiente:

1. Implantar medidas de control del espacio aéreo según las instrucciones recibidas;

2. Comunicar instrucciones a todas las instalaciones ATC dentro de su ámbito de jurisdicción para que implanten el control de seguridad de emergencia del tránsito aéreo y avisar a las instalaciones ATC adyacentes que podrían resultar afectadas; y

3. Informar a las autoridades respectivas del Estado cuando concluyan las medidas de control de seguridad de emergencia del tránsito aéreo o se prevea su conclusión.

Después de aplicar medidas de control de seguridad de emergencia del tránsito aéreo, ATSP debería coordinar los cambios o modificaciones directamente con las autoridades nacionales respectivas.

Cuando se les notifiquen medidas de control de seguridad de emergencia del tránsito aéreo, los controladores de tránsito aéreo deberían hacer lo siguiente:

1. Transmitir instrucciones de seguridad apropiadas en todas las frecuencias disponibles, según los intervalos especificados por el Estado, hasta que se les ordene otra cosa; y

2. Aplicar todas las medidas de control del espacio aéreo según las instrucciones de las autoridades respectivas de ATSP.

## 40 CREACIÓN, PROMULGACIÓN Y VIGILANCIA DE RESTRICCIONES TEMPORALES EN EL ESPACIO AÉREO Y LOS VUELOS

Cada Estado contratante debería determinar las autoridades habilitadas para exigir la creación de restricciones temporales en el espacio aéreo y los vuelos y las circunstancias para su creación. La Dirección General de Aeronáutica Civil debería fomentar procedimientos apropiados ordinarios o urgentes para establecer, publicar e implantar tales restricciones temporales. Constituyen ejemplos de circunstancias que pueden exigir la aplicación de las mismas los grandes eventos deportivos, los viajes de jefes de Estado, asuntos del Estado, eventos de importancia nacional, como las cumbres internacionales, y la respuesta a crisis y catástrofes.

Los sucesos que exigen restricciones temporales en el espacio aéreo y los vuelos generalmente ocurren con algún previo aviso para ATSP, dando habitualmente lugar a un enfoque planificado de antemano para su gestión. ATSP apoya las decisiones de las autoridades competentes asistiendo en la determinación, desde el punto de vista técnico, de las repercusiones operacionales en el transporte aéreo y las operaciones conexas en los aeropuertos y el espacio aéreo, para satisfacer los requisitos de seguridad mediante medidas de facilitación, según lo recomendado en la sección 2.3 del Anexo 17.

Deberían emitirse NOTAM sobre restricciones temporales en el espacio aéreo y los vuelos, de conformidad con el Anexo 15, pudiendo indicarse lo siguiente:

1. Motivo de las restricciones temporales en el espacio aéreo y los vuelos (a menos que sea clasificado);

2. Definición del volumen de espacio aéreo;

3. Hora de entrada en vigor y de expiración (tal vez “hasta nuevo aviso”); y

4. Instrucciones operacionales en que se definan los requisitos para vuelos permitidos dentro del espacio aéreo, procedimientos relativos a la manera en que deben operar y toda aeronave o vuelos específicos que no puedan efectuar operaciones dentro del espacio aéreo durante el período de las restricciones temporales en el espacio aéreo y los vuelos.

Después de haber definido plenamente y coordinado con los organismos en materia de seguridad las restricciones temporales en el espacio aéreo y los vuelos, ATSP las activa y, mediante la publicación de NOTAM, notifica a los usuarios del espacio aéreo las restricciones que deben aplicar al planificar vuelos.

Mientras estén en vigor restricciones temporales en el espacio aéreo y los vuelos, deberían aplicarse procedimientos en que se indiquen en detalle las medidas, funciones, y responsabilidades en materia de vigilancia de dichas restricciones, según la organización del Estado contratante y respecto a las tareas asignadas para vigilar el espacio aéreo. Deberían también proporcionarse procedimientos relativos a enlaces de comunicaciones prioritarias y coordinación para activar las reglas de intervención en relación con los TOI.

**Las restricciones temporales en el espacio aéreo y los vuelos deberían cancelarse lo antes posible.**

## CAPÍTULO 6 ORGANIZACIÓN DE OPERACIONES EFICACES DE SEGURIDAD DE ATM

### 41 ANTECEDENTES

En la norma 3.5 del Anexo 17 al Convenio sobre Aviación Civil Internacional se dispone que cada Estado contratante exigirá que los proveedores de servicios de tránsito aéreo que operan en su Estado establezcan y apliquen disposiciones de seguridad apropiadas para satisfacer los requisitos del programa nacional de seguridad de la aviación civil de este Estado.

Como se explicó en los capítulos anteriores, los servicios de seguridad de ATM cubren una gama aún más amplia de amenazas a la seguridad, que son diversas y dinámicas y a menudo exigen medidas muy rápidas. A fin de ejecutar eficazmente la misión de seguridad, ATSP debería, en la medida de lo posible, prever servicios de seguridad de manera ágil e integrada mediante prácticas que incluyan operaciones tácticas de seguridad, planificación y operaciones estratégicas de seguridad y acuerdos sobre interoperabilidad con las entidades de seguridad. En el presente capítulo se propone una organización de las operaciones y actividades según criterios funcionales, de conformidad con las disposiciones del Anexo 17 y la misión más amplia de seguridad de ATM.

La organización de las funciones de operaciones de seguridad de ATM, ilustrada en la Figura II-6-1, permitiría a ATSP mantener un enfoque y equilibrio apropiados respecto a las necesidades de cada aspecto de la seguridad, como se indica a continuación:

1. Actividades de operaciones estratégicas de seguridad que fortalecen la continuidad del sistema ATM mediante planificación a largo plazo, gestión de crisis, elaboración de procedimientos, funciones de apoyo y análisis;

2. Actividades y operaciones tácticas de seguridad que proporcionan vigilancia diaria de la seguridad de las operaciones del sistema ATM para lograr la conciencia más clara de las situaciones relacionadas con la seguridad y una respuesta inmediata a las mismas; y

Acuerdos sobre interoperabilidad y actividades que apoyan a esta última y colaboración con organismos externos en materia de seguridad, tales como organismos estatales de defensa o imposición de la ley, e intensifican la cooperación y coordinación mediante enlaces integrados.

### 42 PLANIFICACIÓN Y OPERACIONES ESTRATÉGICAS DE SEGURIDAD

La planificación y preparación entre organismos es el mecanismo de facilitación de la colaboración y cooperación con organismos estatales y de defensa para fines de planificación previa de la función de ATSP de suministrar servicios de seguridad de ATM para fines de seguridad nacional, seguridad de la aviación e imposición de la ley. La planificación y preparación entre organismos constituye un elemento estratégico fundamental que permite ejecutar los planes integrados y completos del Estado relativos a las operaciones de seguridad de ATM.

Los planes deberían incluir coordinación con autoridades estatales y, de ser necesario, locales. Además, deberían consultarse las autoridades nacionales de defensa o militares encargadas de la seguridad del espacio aéreo, según lo dispuesto en el NCASP. Los planes deberían incluir preparación de emergencia, análisis de la información proporcionada por el organismo de imposición de la ley y los servicios de inteligencia y aplicación de tecnologías para facilitar la

detección de amenazas y vulnerabilidades.

El componente estratégico de las operaciones de seguridad de ATM se relaciona también con la planificación previa y la preparación para operaciones de gestión de crisis, elaboración de procedimientos para operaciones de seguridad de ATM y apoyo a dichas operaciones.

En la presente sección se destacan elementos que deberían considerarse para cada aspecto de las funciones estratégicas de seguridad.

La planificación y preparación entre organismos debería centrarse en las cuestiones y actividades siguientes:

1. Establecer un plan de respuesta a las amenazas que oriente la respuesta operacional a catástrofes y cualquier fuente de amenazas o ataques intencionales que afecten al sistema ATM;

2. Definir estrategias para atenuar las repercusiones operacionales y económicas de un ataque o catástrofe que podría tener un efecto negativo considerable en el sistema ATM;

3. Definir medidas que permitirán que el sistema ATM y otros elementos críticos gubernamentales y privados relacionados con la aviación que resulten afectados recuperen rápidamente a raíz de un ataque o catástrofe;

Concertar planificación y coordinación estratégicas con organizaciones ATM internacionales y organizaciones militares para optimizar la continuidad de la seguridad de ATM, especialmente entre sistemas ATM adyacentes;

4. Preparar planes de seguridad de ATM sobre:

   a) Brote de una enfermedad transmisible a bordo de una aeronave, causada intencional o involuntariamente, que plantee un riesgo para la salud pública o una emergencia de alcance internacional;

   b) Interceptación en el aire;

   c) Respuesta de procedimientos de seguridad de aeronaves a bordo;

   d) Interdicción y respuesta terrestre en el sector de aviación;

   e) Apoyo de ATM a las operaciones de lucha contra el terrorismo;

   f) Interdicción y neutralización de TOI designados; y

   g) Ataque o amenaza de ataque en el territorio, incluidas amenazas con armas autónomas como MANPADS;

   h) Elaborar e implantar un plan nacional de seguridad de la aviación:

5. Debería aplicarse un enfoque basado en los riesgos para elaborar e implantar medidas encaminadas a reducir las vulnerabilidades y las repercusiones de las correspondientes amenazas en el sistema ATM;

6. En los planes deberían definirse las responsabilidades de ATSP para la coordinación con las autoridades estatales y locales durante situaciones de emergencia, permitir que ATSP tenga acceso a la información de imposición de la ley y servicios de inteligencia y describir

las expectativas de la utilización por ATSP de tecnologías para facilitar la detección de amenazas y vulnerabilidades; y

7. En los planes en que se exijan servicios de gestión del espacio aéreo por ATSP para la seguridad de ATM, debería figurar la coordinación con las autoridades militares responsables de la seguridad del espacio aéreo.

El apoyo a las operaciones de gestión de crisis debería centrarse en las cuestiones y actividades siguientes:

1. Coordinación y gestión de las actividades de planificación de emergencia del sistema ATM para ATSP;

2. Elaboración de planes de contingencia de ATSP como preparación a catástrofes naturales, conflictos militares o actos de interferencia ilícita en la aviación civil:

3. Estos pueden afectar a la capacidad del sistema ATM en materia de operaciones de aeronaves civiles y suministro de servicios de tránsito aéreo y servicios de apoyo; y

4. En los planes debería preverse el uso de personal y activos apropiados;

5. colaboración con organismos apropiados respecto a planes de ejercicios nacionales, regionales y locales para asegurar la preparación operacional de la capacidad en materia de seguridad de ATM y la atenuación de las repercusiones de dichos ejercicios y medidas conexas en la seguridad operacional y eficiencia del sistema ATM;

6. planificación de ejercicios de seguridad de ATM que incluyan situaciones de amenaza a la aviación de nivel táctico:

7. además de someter a prueba la coordinación entre funciones de mando y control de ATSP, los ejercicios deberían incorporar situaciones con activos e instalaciones de aviación reales; y

8. establecimiento de la capacidad de notificar la respuesta a las crisis, reflejando la situación de los empleados de ATSP, los servicios del sistema ATM, el equipo y demás infraestructura ATM fundamental.

Los procedimientos y el apoyo a las operaciones de seguridad suponen la preparación de procedimientos de seguridad de ATM para afrontar, controlar, resolver o vencer las amenazas al sistema ATM y apoyar las operaciones militares y de imposición de la ley en el sistema ATM y deberían abarcar algunos o todos los elementos siguientes:

1. Elaborar planes operacionales detallados y procedimientos de seguridad para sincronizar las responsabilidades respectivas determinadas en los planes de los organismos participantes: esto incluirá planes para identificar y responder a amenazas a la seguridad de la aviación a bordo de las aeronaves, incluidos informes sobre niveles de amenaza, apoderamientos ilícitos posibles o confirmados, terroristas equipados con dispositivos explosivos improvisados (IED) o armas de destrucción masiva, enfermedades endémicas, gestión y solución de situaciones o conductas sospechosas, etc.;

2. Preparar procedimientos para categorizar e identificar vuelos sospechosos designados que no representen una amenaza inmediata a los intereses nacionales, pero que sí exigen atención concentrada, coordinación y posible respuesta;

3. Elaborar procedimientos para establecer, activar, aplicar y levantar restricciones en el espacio aéreo y los vuelos relacionadas con la seguridad dentro del sistema ATM, permitiendo imponer limitaciones a las operaciones de aeronaves;

4. Elaborar procedimientos de vigilancia y alerta para el espacio aéreo afectado por restricciones temporales en el espacio aéreo y los vuelos cuando se prevean o presencien violaciones de restricciones, dando lugar a una situación TOI;

5. Asegurarse de que se apliquen las políticas y procedimientos de seguridad de ICT al tratar información clasificada y confidencial:

6. Varios organismos y departamentos participan en operaciones clasificadas de la aviación y en programas confidenciales que refuerzan la seguridad de un estado. Para lograr dicho apoyo, determinadas personas de la Gerencia de Navegación Aérea debieran estar en niveles apropiados de habilitación de seguridad y recibir capacitación sobre programas clasificados y confidenciales para satisfacer las necesidades de otros organismos y departamentos;

7. Planificar la infraestructura necesaria para apoyar debidamente las operaciones de seguridad de ATM;

8. Proporcionar gestión de programas para elaborar sistemas de vigilancia y seguimiento que permitan identificar más rápidamente, para fines de seguridad, posibles amenazas en vuelo en el espacio aéreo de su territorio y aguas jurisdiccionales.

9. Mejorar la integración de la gestión de crisis mediante instrumentos y sistemas de vigilancia automatizados para mantener la continuidad de las operaciones entre organismos;

10. Implantar programas de aseguramiento de la calidad centrados en la recopilación y análisis de datos de seguridad de ATM a nivel nacional, regional, de instalación e individual. El aseguramiento de la calidad supone también proporcionar orientación específica sobre normas, investigación, notificación y registro, por la instalación, de incidentes relacionados con la seguridad que afecten al sistema ATM;

11. Recopilar y analizar datos relacionados con la seguridad de la aviación; establecer y mantener datos para la información relacionada con la seguridad (tales como incidentes TOI y láser y sus repercusiones en el sistema ATM);

12. Evaluar periódicamente los planes y programas de seguridad de ATM utilizando datos derivados del aseguramiento de la calidad y coordinando con otros departamentos y organismos las actualizaciones necesarias a los planes de seguridad de ATM; y

    Asegurarse de que los procedimientos de las operaciones de seguridad de ATM satisfagan las exigencias de la gestión de riesgos para la seguridad operacional (SRM).

## 42.1 OPERACIONES TÁCTICAS DE SEGURIDAD

Las operaciones tácticas de seguridad de los ATSP apoyan la gestión diaria de las operaciones de seguridad en el dominio aéreo mediante coordinación en tiempo real (o casi real) con los organismos en materia de seguridad. Las funciones de ATSP relativas a las mencionadas operaciones podrían abarcar algunos o todos los elementos siguientes:

1. Medidas para detectar, disuadir y neutralizar amenazas al sistema ATM, reducir vulnerabilidades y minimizar las consecuencias de ataques posibles y acelerar la

recuperación a raíz de los mismos;

2. Identificación de sucesos relacionados con la seguridad de ATM en tiempo real;

3. Respuesta o asistencia operacional táctica inmediata, si corresponde, a las autoridades estatales para responder adecuadamente a casos TOI, lo que podría abarcar algunas de las actividades siguientes, debiendo incluirse en el NCASP la función de ATSP:

   a) Interceptación en el aire y operaciones tierra a aire de las autoridades estatales;

   b) Respuesta de procedimientos de seguridad a bordo;

   c) Interdicción terrestre para fines de procedimientos en plataformas de la aviación y respuesta por autoridades estatales; y

   d) Iniciativas de gestión del espacio aéreo para operaciones estatales de lucha contra el terrorismo e imposición de la ley;

4. Respuesta operacional para proteger al sistema ATM durante un ataque o amenaza de ataque, incluidos ataques con armas autónomas como MANPADS;

5. Recopilación, procesamiento y suministro, a las instalaciones apropiadas de defensa aérea, de datos sobre movimientos en el aire. Esto se lleva a cabo de conformidad con procedimientos mutuamente aceptables para todos los vuelos de aeronaves civiles y militares que exigen identificación en zonas de identificación para fines de seguridad y restricciones temporales en el espacio aéreo y los vuelos;

6. Coordinación apropiada que ATSP debe iniciar rápidamente al recibir notificación u otra información de que está ocurriendo un incidente y que se necesita una respuesta inmediata. Esto protege al sistema ATM contra toda amenaza conexa o cuando se necesiten servicios inmediatos de seguridad de ATM para apoyar a las autoridades al dar respuesta al incidente. Las disposiciones relacionadas con la seguridad de ATM relativas a vuelos que entran, salen, transitan o efectúan operaciones dentro del espacio aéreo de ATSP o en espacio aéreo objeto de restricciones temporales en el espacio aéreo y los vuelos. Entre los medios de notificación podrían figurar NOTAM, sitios Internet oficiales u otros métodos;

7. Coordinación y apoyo a las partes interesadas críticas en materia de seguridad de la aviación durante actividades tácticas relacionadas con la seguridad e incidentes que afecten al sistema ATM. La coordinación puede efectuarse de diversos modos, tales como utilización de líneas de comunicación abierta o colaboración in situ en instalaciones principales de un organismo estatal o de defensa. Esto incluye el establecimiento, organización o cambio en cualquier instalación aeronáutica, servicio, procedimientos o peligro que podría relacionarse con la seguridad de ATM;

8. Asignación de responsabilidades de coordinación de la seguridad del tránsito aéreo a personal en las instalaciones principales que participan en la vigilancia de la seguridad de ATM y la identificación de TOI e inicio de medidas y comunicaciones tácticas apropiadas relativas a sucesos en materia de seguridad de ATM. El personal encargado de coordinar la seguridad del tránsito aéreo debería ser responsable de lo que se indica a continuación y ejercer vigilancia al respecto:

   a) Respuesta a incidentes relacionados con la seguridad de la aviación tales como violaciones de restricciones temporales en el espacio aéreo y los vuelos, informes

de interferencia ilícita a bordo de una aeronave, informes sobre pasajeros insubordinados y niveles correspondientes de amenaza, informes relativos a vuelos de interés especial designados por el Estado, aeronaves objeto de hurto, identificación de TOI, etc.;

b) Colaboración con organismos en materia de seguridad para elaborar restricciones en el espacio aéreo y los vuelos y NOTAM y asegurarse de la distribución oportuna de la información para reducir o atenuar las repercusiones que las medidas puedan tener en las operaciones del sistema ATM;

c) Negociación, designación, establecimiento y publicación de restricciones en el espacio aéreo y los vuelos relacionadas con la seguridad;

d) Recepción, procesamiento y distribución del itinerario de personalidades destacadas;

e) Recepción, procesamiento y publicación de todas las solicitudes para investigar operaciones de vuelo de conformidad con las restricciones temporales en el espacio aéreo y los vuelos;

f) Elaboración, perfeccionamiento y publicación de NOTAM y avisos especiales basados en la seguridad; y

g) Localización, organización y compilación de recursos asociados con catástrofes naturales o causadas por el hombre.

### 42.2 SEGURIDAD ESPECIAL DE LA INTEROPERABILIDAD PARA OPERACIONES CIVILES Y MILITARES.

En esta función se establece una estrecha relación de trabajo con organismos militares y Civiles:

1. Proporcionar enlaces de seguridad de ATM para operaciones confidenciales o clasificadas en el sistema ATM, tales como desplazamientos de personalidades destacadas y grandes eventos políticos o deportivos (p. Ej., Cumbre G-8, Juegos Olímpicos, Copa Mundial);

2. Proporcionar enlaces de seguridad ATM para usuarios militares del sistema ATM, particularmente los responsables de interceptar los TOI;

3. Proporcionar interfaces de seguridad ATM a los organismos gubernamentales responsables de las operaciones de seguridad en el espacio aéreo;

4. Proporcionar interoperabilidad clasificada y no clasificada relacionada con la seguridad de ATM, según corresponda, para apoyar misiones nacionales de defensa y seguridad de la aviación y permitir acciones ATM apropiadas para atenuar las repercusiones, en el sistema ATM, de procedimientos nacionales relacionados con la seguridad;

5. Establecer enlaces con personas o entidades con habilitación de seguridad apropiada que pueden participar en conferencias y coordinación de actividades de defensa aérea con organismos civiles y militares;

6. Cooperar con organismos estatales y regionales o locales para apoyar sus misiones

relacionadas con la seguridad de ATM;

7. Formular recomendaciones para mejorar y aclarar las medidas entre organismos encaminadas a vigilar e investigar los vuelos dentro del sistema ATM para satisfacer los requisitos de seguridad y de otra índole impuestos a los explotadores de aeronaves;

8. Coordinar un plan completo de comunicación entre organismos para el control de seguridad de emergencia del tránsito aéreo:

9. Todos los organismos estatales con una función de seguridad de la aviación deberían poder comunicarse entre sí sobre una respuesta conjunta a emergencias y aprovechar plenamente la información compartida relativa a la situación;

10. Determinar e implantar, si corresponde, medidas de protección de la seguridad del espacio aéreo para todos los sucesos que exijan la aplicación de restricciones en el espacio aéreo y los vuelos relacionadas con la seguridad;

11. Deberían publicarse avisos preliminares antes del suceso, de conformidad con los procedimientos, y revisarse periódicamente las medidas de seguridad de ATM para dichos sucesos;

12. Actuar como punto de contacto con la dependencia encargada de comunicación social de la DGAC para la gestión de relaciones y responsabilidades de seguridad de ATM entre departamentos, organismos y otras entidades estatales:

13. Los acuerdos ya concertados, tales como memorandos de acuerdo (cartas de acuerdo operacional) facilitarán la coordinación de operaciones con recursos compartidos y responsabilidades independientes;

14. Aclarar el carácter del compromiso y objetivo de cada parte respecto a la seguridad de ATM;

15. Preparar respuestas a criterios establecidos relativos a cuestiones operacionales.

16. Proporcionar divulgación y educación sobre procedimientos relacionados con la seguridad y las restricciones en el espacio aéreo y los vuelos. Los funcionarios de seguridad de ATM y los especialistas del personal podrían realizar visitas periódicas a aeropuertos, aeroclubes y explotadores de servicios aeronáuticos en el aeropuerto, con objeto de sensibilizar a los pilotos respecto a las restricciones en el espacio aéreo y los vuelos, relacionadas con la seguridad, y reducir el número de aeronaves que no cumplen las normas, convirtiéndose así en TOI.

## 42.3 ADMINISTRACIÓN DE LAS OPERACIONES DE SEGURIDAD DE ATM

Todas las funciones que se acaban de describir – operaciones estratégicas de seguridad, operaciones tácticas de seguridad y seguridad especial para interoperabilidad – podrían situarse, desde el punto de vista administrativo, en una oficina de operaciones de seguridad de ATM, que serviría como nexo entre las operaciones de seguridad y el sistema ATM y que podría constituir un punto central para las numerosas responsabilidades de ATSP en materia de seguridad de ATM y mejorar la integración de las operaciones de seguridad dentro del espacio aéreo del Estado.

Las funciones de la oficina de seguridad de ATM serían las siguientes:

1. Administrar las medidas de seguridad de ATM, a fin de proteger al Estado y sus intereses contra amenazas relacionadas con operaciones internacionales y nacionales de aviación civil y contra catástrofes;

2. Atenuar las repercusiones de las amenazas contra el sistema ATM y la seguridad operacional y eficiencia de los usuarios del espacio aéreo y participar en las correspondientes medidas de respuesta (tales como restricciones temporales en el espacio aéreo y los vuelos) adoptadas por el gobierno;

3. Proporcionar operaciones eficaces de seguridad de ATM cooperando con organismos externos en materia de seguridad (sector militar, respuesta de emergencia, sector gobernación, organismos afines y otros ATSP).

## APÉNDICES

## APÉNDICE A MECANISMO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD

### 43 INTRODUCCIÓN

La eliminación total de riesgos no es posible; por consiguiente, en la gestión de riesgos para la seguridad, los ATSP deberían aplicar un enfoque basado en los riesgos. En el presente documento, la gestión de riesgos significa el mecanismo de evaluación de riesgos y selección de opciones de atenuación de los mismos considerando los costos y beneficios de las medidas que se adopten. La gestión de riesgos ofrece a los ATSP un enfoque estructurado para tomar decisiones racionales respecto a los mismos.

Una gestión eficaz de los riesgos para la seguridad no funciona en el vacío, pero debe considerarse en el contexto operacional de ATSP. A fin de lograr un enfoque por capas completo para la seguridad de la aviación, los ATSP deberían colaborar estrechamente con otras partes interesadas, incluidas autoridades de aviación, otros organismos nacionales y proveedores de servicios de seguridad.

### 44 MECANISMO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD

El mecanismo de gestión de riesgos para la seguridad abarca varios elementos relacionados entre sí y constituye una actividad continua y repetitiva. En la Figura Ap A-1 se ilustra una vista de alto nivel del mecanismo que las organizaciones ATM pueden aplicar para identificar sistemáticamente los riesgos para la seguridad y determinar opciones de atenuación. Esta metodología es aplicable a la organización en su totalidad o a un componente o instalación en particular.

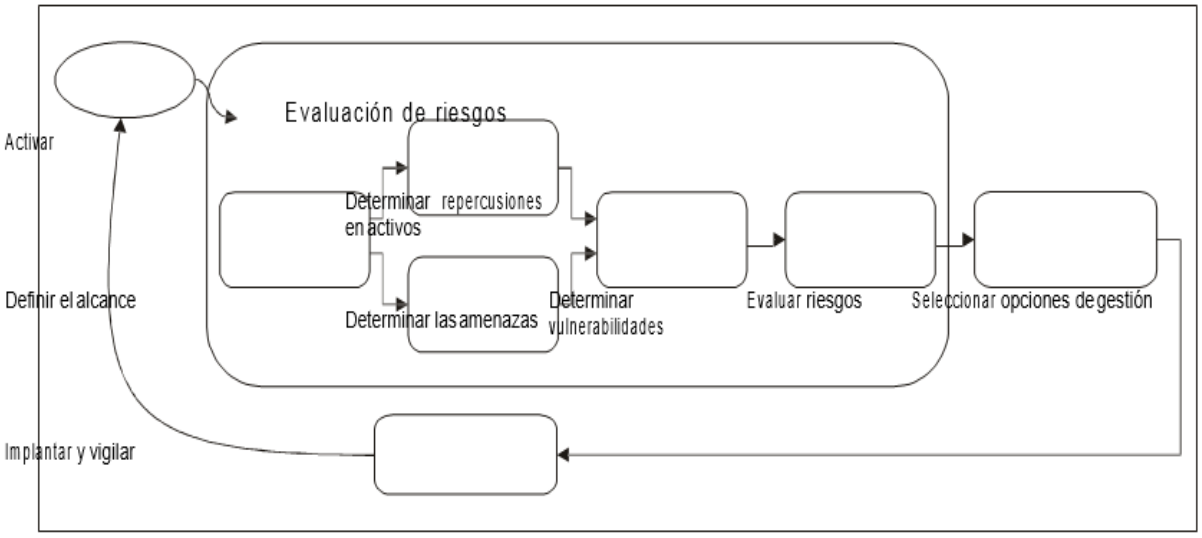


Figura Ap A-1. Mecanismo de gestión de riesgos para la seguridad.

Elementos de activación

El mecanismo de gestión de riesgos debería constituir una actividad continua y repetitiva. Los ATSP deberían determinar elementos de activación para la gestión de riesgos a fin de asegurarse de que la gestión de la seguridad del sistema ATM se actualice continuamente y satisfaga las exigencias del entorno en mutación. Los ATSP podrían evaluar los riesgos para la seguridad como operaciones programadas o a raíz de cambios en factores fundamentales que afectan a la situación del sistema ATM respecto a los riesgos. Entre los elementos de activación comunes figuran los siguientes:

1. Cambio en el entorno de amenazas (tipos de amenazas o frecuencia de sucesos);

2. Incidente relacionado con la seguridad (p. Ej., un ataque que revela una vulnerabilidad imprevista);

3. Modificación de la política de seguridad que pueda conducir a cambios en las prioridades en materia de riesgos o tolerancia a los mismos; y

4. Cambio en el sistema atm o elaboración de otro nuevo.

5. El mecanismo de gestión de riesgos comprende siete etapas:

    a) Etapa 1: Definir el alcance

    b) Etapa 2: Determinar las repercusiones en los activos

    c) Etapa 3: Identificar los agentes de amenaza y determinar la probabilidad de ataques

    d) Etapa 4: Determinar vulnerabilidades

    e) Etapa 5: Evaluar los riesgos

f) Etapa 6: Seleccionar opciones de gestión de riesgos

g) Etapa 7: Implantar y vigilar.

A menudo las etapas 1 a 5 se consideran como mecanismo de evaluación de riesgos que sirve de base, para determinar, evaluar y seleccionar medidas de atenuación en la etapa 6. En la etapa 7 se implantan las medidas de atenuación seleccionadas y se vigila su eficacia para proporcionar información al respecto.

Etapa 1: Determinar el alcance

Esta etapa tiene por objeto asegurarse de que se conozca el alcance del sistema ATM que debe evaluarse y que reúne diversos componentes: personas, información, tecnología, instalaciones, servicios y CNS. El alcance a menudo podría consistir en un conjunto completo o un subconjunto de dichos componentes.

Esta etapa se lleva a cabo definiendo primero los límites del sistema ATM que debe evaluarse, luego documentando los objetivos en materia de seguridad y, por último, describiendo el sistema o subsistema ATM.

La descripción de límites del sistema debería incluir la información siguiente relativa al sistema (o subsistema) ATM que debe evaluarse:

1. Componentes del sistema;

2. Entorno operacional;

3. Usuarios, sus funciones y autoridad;

4. Terceros asociados con el sistema atm, incluidas organizaciones, sus funciones y autoridad;

5. Servicios o infraestructura de apoyo fundamentales, incluida la infraestructura de seguridad y las hipótesis sobre su calidad o seguridad;

6. Servicios proporcionados por los activos y obligaciones conexas en materia de seguridad (incluidos servicios y obligaciones para con terceros);

7. Fase del ciclo de vida útil del sistema (o subsistema) atm que debe evaluarse (p. Ej., diseño, operaciones de instalación, mantenimiento, interrupción del servicio); y

8. Requisitos jurídicos y reglamentarios.

Después de haber definido los límites e interfaces del sistema, ATSP debería determinar los activos dentro de los límites del sistema y describir la arquitectura de este último a fin de determinar las vías (vulnerabilidades) que podrían permitir a las amenazas pasar de los puntos de acceso a los activos.

Las metas en materia de seguridad son propias del sistema o subsistema ATM que se esté evaluando y deben ser lo suficientemente específicas como para corresponder a grupos de activos y categorías de incidentes relacionados con la seguridad.

Etapa 2: Determinar las repercusiones en los activos

En esta etapa se evalúa el efecto de posibles sucesos relacionados con la seguridad en los activos, dentro del alcance. Las repercusiones podrían medirse en relación con lo siguiente:

1. Seguridad operacional;

2. Eficiencia y eficacia;

3. Aspectos financieros y económicos;

4. Confianza del público; y

5. Política.

Las repercusiones se describen mediante una escala cualitativa cuyo nivel mínimo es “efecto mínimo”. A menudo, una escala de cuatro puntos por encima de “efecto mínimo” es suficiente. A continuación se indica un ejemplo de escala relativa a las repercusiones en la eficiencia operacional:

Efecto mínimo — Se prevé que la pérdida cause un efecto mínimo en el rendimiento de la organización.

1. Un activo podría resultar afectado de tal modo que se observará que el rendimiento de la organización se sitúa por debajo de una norma tolerable. Esto debería incluir situaciones en que el mantenimiento del servicio se pierde durante un período prolongado.

2. La pérdida de un grupo de activos causará la interrupción del servicio, que podría deberse a la pérdida de un grupo de activos semejantes o de una serie de sistemas secuenciales. También se aplica a la interrupción de las operaciones si otro incidente ocurre antes de haberse restaurado el funcionamiento del activo o atenuado la pérdida.

3. La pérdida del activo reducirá inmediatamente la capacidad y tendrá repercusiones negativas en la capacidad de proporcionar el servicio requerido.

4. La pérdida causará una interrupción inmediata del servicio.

Etapa 3: Identificar los agentes de amenaza y determinar la probabilidad de ataques

En esta etapa se identifican los agentes de amenaza y se evalúa la probabilidad de los sucesos.

Los ATSP deberían considerar una amplia gama de amenazas. Estas pueden variar debido al carácter de la intención, tales como amenazas intencionales (p. ej., criminales, terroristas), involuntarias (p. ej., accidentes) y catástrofes naturales (p. ej., inundaciones). Las amenazas podrían también variar según el agente (p. ej., externo o interno en la organización).

Es importante no pasar por alto las amenazas internas. En el caso de los sistemas ICT, las amenazas internas son las más graves para la ciberseguridad. Cada punto de acceso legítimo constituye una fuente posible de ataque. Esto incluye a los usuarios u operadores del sistema, otras organizaciones con acceso a distancia o cierto grado de dependencia respecto al sistema, así como los servicios necesarios para el sistema. Estos se determinan a partir de la descripción de límites y se categorizan como posibles agentes de amenaza.

Entre los agentes de amenaza externos figuran terroristas, criminales, extremistas, enemigos, peligros naturales y degradación del servicio (p. ej., interrupción de la alimentación eléctrica). Entre las amenazas intencionales figuran diversos métodos de ataque, tales como bombas, ataques químicos, biológicos, radiológicos y nucleares (CBRN), ciberataques y ataques electrónicos y magnéticos (p. ej., falsificación, interferencia).

Las amenazas deberían organizarse según las categorías de activos. Se indican a continuación ejemplos de amenazas a diferentes categorías de activos:

1. Activos físicos y personal: las amenazas a activos físicos (instalaciones) y personal incluyen fenómenos meteorológicos extremos, catástrofes naturales, IED y amenazas CBRN, chantaje, secuestro y extorsión;

2. Activos ICT: amenazas a los datos o conocimientos de una organización, que pueden también caracterizarse como amenazas a la integridad, confidencialidad y disponibilidad. Las amenazas a los sistemas ICT son más numerosas que las amenazas a sistemas físicos;

3. Activos relacionados con procedimientos: amenazas a documentación y políticas, que pueden causar la supresión, pérdida o corrupción de documentación.

Una vez establecida la lista de posibles agentes de amenaza, debe establecerse la probabilidad de los ataques.

Cada amenaza exige una evaluación de la probabilidad de que la amenaza se convierta en tentativa de ataque por un adversario. En el caso de otros peligros, la amenaza se estima como la probabilidad de que surja un peligro. Respecto a catástrofes naturales y accidentes, ATSP podría tener acceso a estadísticas.

En caso de amenazas intencionales, particularmente de terrorismo, ATSP podría carecer de experiencia o recursos pertinentes y tendrá que pedir ayuda a servicios de inteligencia u organismos de seguridad. A menudo es difícil cuantificar la probabilidad de un ataque a raíz de amenazas intencionales, por lo que se necesitan evaluaciones cualitativas por expertos en el tema. Como para la escala de repercusiones, bastará una escala cualitativa corta de 0 a 5, cuyo nivel más bajo corresponde a “efecto mínimo”.

Etapa 4: Determinar vulnerabilidades

Las vulnerabilidades son características del sistema o de los procedimientos operacionales que podrían ser explotados por agresores o que son susceptibles a peligros naturales (p. ej., huracanes). Por ejemplo, los activos físicos podrían carecer de verjas adecuadas, guardias de seguridad o sistemas de vigilancia; el personal podría carecer de capacitación apropiada sobre procedimientos de seguridad; los sistemas ICT podrían carecer de protección antivirus adecuada; y los activos relacionados con procedimientos podrían tener vulnerabilidades inherentes tales como documentación deficiente (o comunicada de manera no satisfactoria), prácticas negligentes o investigación deficiente del personal.

Los agresores tratan de hallar el medio más fácil para entrar en el sistema. Por consiguiente, al evaluar vulnerabilidades, es importante examinar todas las vías posibles. Por ejemplo, al evaluar el riesgo para ICT, es importante considerar la vulnerabilidad de elementos del sistema no relacionados con ICT (p. ej., descuido de la instrucción en materia de seguridad, que podría permitir un ataque de manipulación por un administrador del sistema).

La probabilidad de un incidente depende de la vulnerabilidad del sistema. Por ello, el evaluador debe examinar los controles de seguridad implantados a lo largo de la vía correspondiente a la amenaza y determinar la manera en que reducen la vulnerabilidad a un ataque. Para determinar el riesgo, se examina la vulnerabilidad a determinada amenaza, la probabilidad de que una amenaza se convierta en un ataque, así como sus repercusiones.

Etapa 5: Evaluar los riesgos

El objetivo de la evaluación de riesgos consiste en establecer una imagen global del peligro para el sistema ATM. Un riesgo es la posibilidad de un resultado negativo y se expresa en relación con la probabilidad de la amenaza, las vulnerabilidades y las repercusiones.

Deberían considerarse todas las combinaciones válidas de amenazas (ataques) y vulnerabilidades del sistema para determinar si existe una vía a través del activo o sistema que permita que un ataque tenga éxito. Los riesgos pueden evaluarse considerando la probabilidad de la amenaza (ataque) o peligro, la vulnerabilidad del activo o sistema respecto a dicha categoría de amenaza y las repercusiones o consecuencias de la pérdida o degradación del activo o sistema.

Etapa 6: Seleccionar opciones de gestión

En esta etapa se determinan y seleccionan las opciones de gestión de los riesgos que se hayan identificado. Se lleva a cabo mediante las actividades siguientes:

1. Determinar si los riesgos identificados son aceptables:

   Esta determinación se basa en el nivel de tolerancia o tendencia al riesgo de ATSP, según lo establecido en la política relativa a la seguridad. Esto debería haberse especificado en esta última respecto al nivel de riesgos y repercusiones. La inclusión del nivel de repercusiones, además del nivel de riesgos, tiene por objeto permitir que ATSP se entere de riesgos poco probables, pero que tienen graves repercusiones.

2. Determinar las opciones de gestión:

   La administración puede seleccionar una de las medidas siguientes en caso de riesgos que excedan el nivel aceptable:

   1. Tolerar (no adoptar ninguna medida);
   2. Tratar (aplicar medidas de control para reducir a un nivel aceptable);
   3. Transferir (transferir a otra dependencia dentro de ATSP o una entidad externa); y
   4. Poner fin (detener la actividad);
   5. Seleccionar opciones de control:

Las opciones de control son contramedidas encaminadas a atenuar los riesgos. Los controles de seguridad podrían tener carácter técnico o basarse en procedimientos o políticas y cubren también una gama de actividades, según el método aplicado para bloquear las vías para las amenazas. Pueden disuadir las amenazas, disminuir la probabilidad de un ataque efectivo reduciendo las vulnerabilidades, disminuir las consecuencias de los ataques o catástrofes, permitir una rápida reacción y respuesta de emergencia a un incidente o que la organización ATSP reanude sus operaciones normales efectivamente mediante planificación de contingencia.

Además, la selección de la opción de control podría considerarse en un contexto más amplio del sistema o subsistema ATM que se esté evaluando o que sea externo respecto a la organización

ATSP. Por ejemplo, una instalación NAVAID situada dentro del perímetro del aeropuerto puede contribuir a las medidas de control del acceso del aeropuerto.

Priorizar las medidas de atenuación:

El establecimiento de prioridades tiene por objeto la toma de decisiones fundadas de asignación de recursos. Una imagen completa del riesgo, acompañada de opciones de control, proporciona a la administración de ATSP una base para establecer prioridades de protección de la infraestructura. La evaluación y selección de opciones de gestión dependen de factores tales como disposiciones legales o reglamentarias, aceptabilidad, viabilidad y costo. Por ejemplo, ATSP podría definir un umbral de activación de medidas. Para todo activo o sistema con un riesgo superior al nivel de activación se implantarían opciones de atenuación. La administración de ATSP podría también priorizar las medidas de atenuación de riesgos en el caso de sistemas cuyo nivel de riesgo se sitúe por debajo del umbral de activación de medidas basándose en consideraciones de orden económico. El equipo de seguridad, los expertos en la materia y la administración superior deberían tomar conjuntamente decisiones definitivas en materia de gestión de riesgos con la participación de los organismos de reglamentación.

Etapa 7: Implantar y vigilar

ATSP debería ejercer vigilancia para evaluar la eficacia de las medidas de atenuación implantadas. Si su rendimiento no permite alcanzar la meta prevista, ATSP debería tomar medidas correctivas. La evaluación y la corrección contribuyen a mejorar continuamente los programas de atenuación de riesgos. Con esta actividad, ATSP recibe información sobre la debida aplicación de las medidas de atenuación implantadas y el logro de los resultados previstos. La eficacia real proporciona una base para establecer responsabilidad, facilitar el diagnóstico de un rendimiento deficiente y permitir que se revisen las metas y objetivos. La vigilancia también advierte a ATSP acerca de indicadores tempranos respecto a aspectos de posibles deficiencias y permite tomar medidas activas de prevención de fallas.

## 45 GESTIÓN DE RIESGOS PARA LA SEGURIDAD, COLABORACIÓN DE LA ORGANIZACIÓN

Gestión de riesgos para la seguridad basada en inteligencia

En el Anexo 17 se alienta a la cooperación internacional y el intercambio de información e inteligencia sobre amenazas. En la norma 3.1.3 se dispone que “cada Estado contratante evaluará constantemente el grado de amenaza para la aviación civil en su territorio y establecerá y aplicará políticas y procedimientos para ajustar en consecuencia los aspectos pertinentes de su programa nacional de seguridad de la aviación basándose en una evaluación de riesgos de seguridad de la aviación realizada por las autoridades nacionales pertinentes”.

La determinación y evaluación de los riesgos para la seguridad dependen en gran medida de la información que puede proceder de diferentes fuentes y antecedentes, incluidos el análisis de datos históricos, amenazas emergentes y tendencias en materia de ataques.

Los ATSP (especialmente los no gubernamentales) solo tendrán acceso limitado a la información pertinente.

Los Estados y los servicios nacionales o regionales de inteligencia deberían intercambiar con los ATSP información pertinente sobre amenazas a la aviación y la navegación aérea y sobre las capacidades o tendencias de ataques emergentes.

A raíz de la Enmienda 12 del Anexo 17, se exige, además, que los Estados compartan con ATSP la parte pertinente del NCASP.

Comités nacionales o locales de seguridad de la aviación

En virtud del Anexo 17, los Estados contratantes deben establecer un comité nacional de seguridad de la aviación civil (o arreglos semejantes) para coordinar las actividades en materia de seguridad entre los departamentos, agencias y otros órganos del Estado, los explotadores de aeropuertos y aeronaves, los ATSP y otras entidades encargadas de implantar diversos aspectos del NCASP o responsables de ellos. Esto constituye la plataforma principal para coordinar las medidas de seguridad de la aviación.

En el mismo contexto, los aeropuertos deberían también designar a una autoridad para coordinar los procedimientos de seguridad y establecer un comité de seguridad aeroportuaria en cada aeropuerto para asistir a la autoridad. Estos arreglos locales amplían la plataforma nacional.

Aunque ATSP no estará siempre situado en un aeropuerto o en su vecindad, debería utilizar dichas plataformas. La colaboración y coordinación eficaz en la organización exigen la participación de todos los actores en estas modalidades de trabajo.

La autoridad competente debería designar a ATSP como miembro del comité nacional o local de seguridad de la aviación pertinente o crear un nuevo comité para colaborar e intercambiar información con el mismo.

La colaboración debería abarcar también la enmienda de los respectivos planes de emergencia locales (incluida la designación de un centro local de operaciones de emergencia y procedimientos de coordinación pertinentes) para incluir respuestas a los ataques contra infraestructura, instalaciones y servicios de ATM.

## APÉNDICE B CIBERSEGURIDAD DE LOS SISTEMAS ICT

### 46 INTRODUCCIÓN

“Ciber” es un prefijo utilizado para describir a una persona, objeto o idea como parte de la edad de computadoras e información, como el “ciberespacio”, medio electrónico en que tiene lugar la comunicación en línea. La arquitectura del sistema ATM sigue evolucionando y convirtiéndose en una arquitectura abierta de cibersistemas interconectados en que se utilizan protocolos normalizados de transmisión de datos y sistemas operacionales de código abierto. La comunidad de aviación civil depende cada día más de la tecnología de la información y de las comunicaciones (ICT) cibernética para llevar a cabo sus misiones y funciones comerciales; además, la interconexión de cibersistemas está aumentando, en tierra, entre partes interesadas y entre sistemas en tierra, aeronaves y el espacio (sistemas de determinación de la posición).

Mientras dicha evolución de la tecnología aumenta la eficiencia de las operaciones, también expone los sistemas de información y comunicaciones a un mayor riesgo en materia de ciberseguridad. Esta se refiere comúnmente a las salvaguardias y medidas que pueden aplicarse para proteger el dominio cibernético contra amenazas asociadas con sus redes e infraestructura de información interdependientes o que podrían causarles daño. La ciberseguridad está encaminada a preservar la integridad y disponibilidad de las redes y la infraestructura, así como la confidencialidad de la información que contienen.

Los ciberataques contra sistemas ICT están ocurriendo constantemente con mayor alcance y perfeccionamiento; la seguridad de pasajeros, tripulaciones y personal de tierra podría verse en peligro si se alteran los sistemas ICT de ATM. Además, la información personal sobre los empleados debería protegerse contra uso y acceso no autorizados.

En el presente capítulo figuran conceptos y definiciones de ciberseguridad de ICT, así como una descripción de los requisitos de seguridad para los cibersistemas ICT críticos de ATSP, basándose en el Doc 8973 — Distribución limitada. En el Apéndice C figura una orientación general sobre seguridad de ICT basada en normas de la Unión Europea (UE), así como una lista completa de controles de seguridad para ICT.

## 47 CONCEPTOS Y DEFINICIONES

Activos cibernéticos de ICT
Los activos cibernéticos de ICT, de ATSP, incluyen información o datos, sistemas de tecnología de la información y sistemas de tecnología de las comunicaciones.

En el presente apéndice los términos “datos” e “información” se utilizan indistintamente. Los activos de información incluyen información operacional e información personal sobre los empleados, generadas, procesadas o transmitidas por ATSP. La información operacional se relaciona con el suministro de servicios de tránsito aéreo y abarca también la información que se intercambia entre ATSP y sus organismos en materia de seguridad, como los organismos nacionales o regionales de seguridad de la aviación y los organismos de seguridad nacional, defensa e imposición de la ley. Parte de dicha información sobre seguridad podría tener carácter clasificado.

Los sistemas de tecnología de la información cibernética incluyen soportes lógicos y físicos. Los primeros abarcan sistemas operacionales, aplicaciones y procesamiento de datos; los segundos, dispositivos de computación, así como sistemas y dispositivos de almacenamiento de datos.

Los cibersistemas de tecnología de la información se refieren a redes (locales, regionales o mundiales, con o sin cables) de dispositivos y sistemas de comunicación.

Objetivos de seguridad de los cibersistemas ICT

La seguridad de los cibersistemas ICT se refiere a la aplicación de controles de seguridad para proteger los cibersistemas ICT de ATM contra degradación intencional o accidental de su integridad, confidencialidad y disponibilidad:

1. Integridad: objetivo de seguridad que garantiza que la información y los sistemas no se modifiquen indebida o accidentalmente. Cuando la integridad resulta comprometida, la información se expone a modificación o destrucción.

2. Confidencialidad: objetivo de seguridad que garantiza que la información no se divulgue a entidades no autorizadas. Cuando la confidencialidad resulta comprometida, es posible que se divulgue información sin autorización. A menudo se garantiza la confidencialidad cifrando los datos en tránsito o almacenados.

3. Disponibilidad: objetivo de seguridad que garantiza la fiabilidad y el acceso oportuno de entidades autorizadas a datos, servicios y recursos. Cuando la disponibilidad resulta comprometida, el sistema puede sufrir una perturbación temporal o la pérdida completa del servicio.

Para proteger los sistemas ICT de ATM, debe también considerarse la seguridad del entorno en que funcionan. Por consiguiente, la seguridad de ICT está también vinculada con la seguridad física, los proveedores, los servicios de infraestructura y terceros con los que ATSP tiene relaciones, tales como autoridades de imposición de la ley, seguridad y reglamentación.

Carácter crítico de los cibersistemas ICT

Por regla general, el carácter crítico se define como la medida en que una organización depende de ICT o de la información para el éxito de una misión o función comercial. En el contexto del presente manual, el carácter crítico se expresa en relación con la misión de ATSP:

Suministro de servicios ATM, incluido el apoyo a la gestión nacional o regional de incidentes relacionados con la seguridad.

Controles de seguridad de los cibersistemas ICT

Los controles de seguridad son salvaguardias o contramedidas implantadas para proteger la integridad, confidencialidad y disponibilidad de los activos ICT y pueden clasificarse en tres categorías:

1. Controles de gestión: centrados en la gestión de riesgos para la seguridad y la gestión de la seguridad de los sistemas;

2. Controles operacionales: salvaguardias o contramedidas implantadas o ejecutadas principalmente por personas; y

3. Controles técnicos: salvaguardias o contramedidas implantadas o ejecutadas principalmente por el sistema mediante mecanismos contenidos en sus componentes.

## 48 REQUISITOS DE SEGURIDAD PARA CIBERSISTEMAS ICT

La presente sección se basa en el Capítulo 18 — “Amenaza de ciberataques contra sistemas críticos de tecnología de la información y las comunicaciones aeronáuticas” del Doc 8973 — Distribución limitada. Se recomienda en este documento que los Estados exijan que los explotadores de la industria de la aviación (incluidos los ATSP) determinen medidas de seguridad para los cibersistemas ICT críticos. Por consiguiente, ATSP debería aplicar dichas medidas como requisitos mínimos de seguridad para ICT. Se ha modificado ligeramente el texto original porque ahora se destina a ATSP.

Determinar los cibersistemas ICT críticos

ATSP debería determinar soportes lógicos y físicos críticos de los cibersistemas ICT utilizados en la infraestructura de su sistema ATM, lo que podría abarcar, entre otras cosas, lo siguiente:

1. Activos y componentes del sistema ATC;

2. Sistemas de mando, control y despacho de seguridad;

3. Sistemas de control del acceso y vigilancia de alarmas;

4. Sistemas de vigilancia por televisión en circuito cerrado;

5. Bases de datos sobre agentes acreditados y expedidores reconocidos; y

6. Dispositivos electrónicos portátiles y no portátiles utilizados para procesar, almacenar y comunicar información crítica de ATSP (p. ej., computadoras de escritorio, portátiles, "subportátiles", de tipo "tableta", teléfonos móviles instalados en plataformas de computación, computadoras de bolsillo, cámaras fotográficas digitales y dispositivos de almacenamiento, incluidos los soportes de tipo USB y las tarjetas de memoria).

Proteger los cibersistemas ICT críticos

ATSP debería implantar medidas de seguridad para cibersistemas ICT, de conformidad con el NCASP y los programas nacionales pertinentes. Los objetivos de dichas medidas deberían ser, a lo mínimo:

1. Proteger los sistemas contra acceso y uso no autorizados;

2. Impedir la alteración de los sistemas; y

3. Detectar ataques contra los sistemas.

La protección física de dichos sistemas debería iniciarse en la etapa de diseño o lo más temprano posible a fin de garantizar su máxima resistencia a ciberataques, lo que puede lograrse mediante un enfoque por capas que incluya, entre otras cosas, lo siguiente:

1. Controles de gestión, como:

   a) Normas, políticas y procedimientos de seguridad;

   b) Contratación, selección y capacitación apropiadas del personal, particularmente de personas con derechos administrativos, así como verificación de antecedentes;

   c) Evaluación de amenazas y riesgos para determinar la vulnerabilidad de un sistema y la probabilidad de ataques;

   d) Control de la calidad, incluidas inspecciones y pruebas; y

   e) Seguridad de la cadena de suministro de soportes físicos y lógicos;

2. controles virtuales o lógicos, tales como:

   a) Cortafuegos;

   b) Cifrado de datos;

   c) Sistemas de detección de intrusos en el sistema; y

   d) Sistemas antivirus;

3. Controles físicos, tales como:

   a) Asegurarse de que los soportes físicos del sistema, particularmente los servidores, estén debidamente protegidos y situados en zonas de acceso controlado;

   b) Implantar sistemas de autenticación, tales como registros o métodos biométricos o

contraseñas, para asegurarse de que únicamente las personas autorizadas tengan acceso al sistema;

c) Limitar el número de personas con derecho de acceso;

d) Exigir la intervención de más de una persona para aprobar el acceso a sistemas críticos;

e) Vigilar y controlar continuamente el acceso a los sistemas;

f) Utilizar sistemas de reserva remotos en caso de pérdida del sistema principal; y

4. Mantener registros de actividades, lo que puede ser útil para fines de auditoria y evaluación, y prever alertas si se detecta actividad que no corresponda a operaciones normales.

La protección de los cibersistemas ict críticos debería formar parte de los mecanismos de evaluación de riesgos establecidos por la autoridad competente, lo que puede lograrse si se incluyen dichos sistemas en las evaluaciones de amenazas (ataques), vulnerabilidades y repercusiones en caso de pérdida de dichos cibersistemas.

ATSP debería adoptar medidas, tales como inspecciones y auditorías, encaminadas a atenuar posibles ciberataques y verificar su aplicación como parte de sus actividades normales de vigilancia del cumplimiento.

## 49 MEDIDAS DE SEGURIDAD PARA LA INFRAESTRUCTURA DE CIBERSISTEMAS ICT CRÍTICOS

Seguridad basada en el diseño

ATSP debería asegurarse de que se incluyan medidas de seguridad en el diseño, implantación y operación de nuevos cibersistemas ICT, incluida la eliminación final de soportes físicos y lógicos. Al modificar sistemas existentes, debería tenerse en cuenta la seguridad, en la medida de lo posible.

ATSP debería también incluir disposiciones de seguridad en las especificaciones relativas a nuevos cibersistemas ICT y su adquisición, exigiendo que sus proveedores proporcionen información sobre los medios de protección de la información y operación del sistema, incluidas las modalidades de apoyo y mantenimiento continuos, *in situ* o a distancia.

Debería programarse y administrarse mantenimiento preventivo; si el apoyo y el mantenimiento son objeto de contratación externa, debería limitarse el número de personas con acceso autorizado a los soportes lógicos y físicos del sistema. Dicha medida contribuirá a impedir el acceso no autorizado al sistema y reducir las posibilidades de interferencia en la integridad del sistema.

Asimismo, el tendido de cables debería diseñarse de modo que no puedan infiltrarse fácilmente los sistemas críticos de información aeronáutica.

Separación entre redes

ATSP debería asegurarse de que las redes utilizadas para cibersistemas ICT críticos de ATC estén separadas de las redes accesibles al público.

Los soportes lógicos y físicos de un sistema ICT moderno no pueden funcionar sin los cables necesarios y la conexión a otra red de sistemas operacionales para facilitar la transmisión e intercambio de datos. Por dicho motivo, deberían examinarse los cibersistemas ICT para asegurarse de que no resulten comprometidos los objetivos de seguridad, debido a la exposición

a redes de comunicaciones no controladas o de acceso libre. Además, deberían establecerse políticas y prácticas apropiadas para reducir a un mínimo las conexiones necesarias. Esta práctica recibe a menudo el nombre de “reforzamiento”.

Las conexiones cibernéticas a redes deberían efectuarse en condiciones controladas en que se conozcan el tipo de información y la frecuencia o método de intercambio de datos entre el sistema y la red. Debería establecerse un sistema de gestión eficaz para dichas interfaces en la red a fin de asegurarse de que todas las conexiones a un sistema sean objeto de documentación, examen y actualización, según corresponda, y se cuente, de ser posible, con protección adecuada contra virus y programas perniciosos.

Además, debería considerarse un enfoque por capas para la gestión de soportes lógicos. Un número limitado de personas debería tener derechos a título de administradores de un cibersistema ICT crítico. El acceso al sistema debería basarse en el principio de necesidad legítima. Así, podrían otorgarse a algunas personas derechos que se limiten a la lectura, mientras que se autorizaría a otras el acceso únicamente a las partes del sistema que se relacionen con sus tareas concretas.

Acceso a distancia

ATSP debería asegurarse de que solo se permita el acceso a distancia a cibersistemas ICT críticos en condiciones establecidas de antemano y seguras y de que los proveedores no tengan acceso no autorizado a dichos sistemas después de su adquisición o instalación.

En la mayoría de los casos, el acceso a distancia a un cibersistema exige que los proveedores tengan un medio apropiado para ello. ATSP debería asegurarse de conocer dicha vía de acceso y de que se concierten el método y las condiciones de entrada. Por ejemplo, debería exigirse que el proveedor notifique al funcionario designado por el explotador cuando el acceso al sistema sea necesario. Podría también generarse automáticamente un correo-e para notificar al mencionado funcionario cada vez que se solicite acceso.

Solo el personal autorizado debería efectuar el mantenimiento de los cibersistemas, según horarios establecidos y aprobados de antemano. ATSP debería solicitar a los proveedores que limiten el número de personas autorizadas para fines de apoyo y mantenimiento del sistema. Dichas personas deberían ser objeto de verificación de antecedentes, incluidos sus antecedentes penales, en la medida en que lo permitan las leyes.

Podrían añadirse a las mencionadas medidas una auditoría apropiada y un sistema de notificación de excepciones que genere un informe automático siempre que tenga lugar una actividad anormal en el cibersistema, como el acceso fuera de las horas normales de trabajo. Por ejemplo, si se trata de entrar fuera de las horas establecidas, debería enviarse un informe de excepción al supervisor responsable del sistema. Dicha persona debería comunicarse con el proveedor para determinar la justificación de la entrada sin acuerdo previo. Asimismo, deberían examinarse regularmente los registros de auditoría para determinar el acceso excepcional y examinar sus circunstancias.

Seguridad de la cadena de suministro de soportes físicos y lógicos

Los cibersistemas ICT deben actualizarse periódicamente debido a cambios en los requisitos operacionales o la modernización de soportes lógicos, exigiendo a menudo que se modifiquen los soportes lógicos o físicos. En cada una de dichas circunstancias, existe la posibilidad de que se introduzcan sin autorización soportes lógicos o físicos que puedan atacar, infiltrar o comprometer la integridad del sistema.

ATSP debería adoptar medidas para asegurarse de que se recurra únicamente a proveedores de confianza y legítimos para adquirir soportes físicos y lógicos para los cibersistemas ICT. En la medida de lo posible, debería aplicarse el concepto de seguridad de la cadena de suministro, cuyo objetivo consiste en asegurarse de que se proteja la integridad de dichos soportes contra manipulaciones a lo largo de la cadena de suministro. Debería exigirse que los proveedores indiquen sus propias medidas de seguridad en la etapa de instalación y también durante toda la vida útil del sistema.

Registros de incidentes de ciberataques

El conocimiento de la amenaza y de los probables métodos de ataque constituye un elemento esencial al elaborar medidas de seguridad apropiadas para proteger a los cibersistemas ICT contra ciberataques. ATSP debería implantar un régimen de notificación de tales incidentes e incluirlo en sus programas de seguridad.

Aspectos de evolución

La seguridad de los cibersistemas ICT desempeñará una función más importante en los futuros sistemas ATM, como NextGen en los Estados Unidos y SESAR en Europa. Dado que los enlaces de comunicación de datos de los cibersistemas ICT reemplazan los actuales canales de comunicaciones vocales, aumenta la necesidad de asegurarse de la oportunidad y fiabilidad de los enlaces de datos dotados de controles de seguridad puesto que serán indispensables para el éxito de los programas.

SWIM brinda la oportunidad de intercambiar, por intermedio de cibersistemas ICT, datos ATM sobre meteorología, afluencia del tránsito aéreo, trayectorias de vuelo y vigilancia en la totalidad de los cibersistemas ICT. La comunicación oportuna, segura y fiable de los datos ATM mediante dichos sistemas reviste suma importancia para el éxito de los sistemas ATM del futuro.

## APÉNDICE C CONTROLES DE SEGURIDAD PARA ICT

### 50 INTRODUCCIÓN

El texto del presente apéndice fue elaborado por EUROCONTROL para facilitar la implantación de las disposiciones reglamentarias relativas a la seguridad de ICT por los ATSP en Europa. Esta orientación fue elaborada teniendo en cuenta dos aspectos:

1 Necesidad de asistir a las organizaciones en la selección de controles apropiados a partir del gran número especificado en las normas internacionales; y

2 Amplia diversidad de organizaciones ATSP y categorías de sistemas ICT.

Para satisfacer ambos aspectos, la presente orientación incluye una lista de controles de seguridad de ICT (Tablas Ap C-1 a C-10), basada en la recopilación y consolidación de las normas internacionales siguientes:

1. Todas las normas pertinentes sobre seguridad de la comunicación de información en ISO/IEC 27001:2005; y

2. Otras normas pertinentes, particularmente en los Objetivos de control para la tecnología de la información y otras afines (COBIT) y el conjunto ISO/IEC 13335-4.

La lista abarca también los mejores métodos de aplicación práctica y actualizada de dichas normas. Al seguir la mencionada orientación, la organización ATSP cumplirá las normas internacionales vigentes.

Los controles de seguridad de ICT se clasifican en seis niveles, según el riesgo para los sistemas de información designados por la organización. El nivel 1 es el de menor riesgo y exige el nivel más bajo de controles básicos; el nivel 6 corresponde al mayor riesgo y exige el nivel más elevado de controles básicos.

### 51 CATEGORÍAS DE CONTROLES

Los controles de seguridad para ICT se dividen en nueve categorías según las funciones de la organización.

Orientación de la organización y controles de políticas

La orientación de la organización y los controles de políticas se relacionan con el conjunto de personas, entidades externas y organizaciones que se adhieren a las políticas y procedimientos de seguridad de determinada organización.

Las políticas de seguridad constituyen un documento aprobado por la administración, distribuido a todos los empleados y entidades externas, que cubre todos los sistemas y describe las responsabilidades de cada una de las partes en relación con el uso de los sistemas previstos en las políticas. Se trata de un documento en evolución sometido a ciclos de revisiones programadas y actualizaciones no programadas, según corresponda, para asegurar la actualidad y eficacia de las políticas que contiene. La política de seguridad es también parte del enfoque de gestión de riesgos para la evaluación y gestión de la seguridad de ICT.

Controles de la cultura y la administración de la organización

El éxito de la elaboración e implantación de un sistema de seguridad de ICT basado en políticas depende en gran medida de la participación y apoyo de la administración a los esfuerzos con un compromiso claro y permanente respecto al mecanismo.

Los controles armonizan los objetivos de las operaciones de la organización con sus objetivos de seguridad, definiéndose debidamente las funciones de la administración y estableciéndose objetivos claros en materia de seguridad de ICT.

Controles relativos a recursos humanos

Los controles relativos a recursos humanos para la seguridad de ICT se relacionan con los empleados y contratistas, así como sus funciones, responsabilidades y aptitud. Se examinan y reducen los riesgos asegurándose de que dichas personas se investiguen debidamente y reciban capacitación para sus funciones. Los riesgos inherentes de hurto y uso indebido de recursos constituyen aspectos de preocupación.

Controles de seguridad física y seguridad relativa al entorno

Estos controles de la seguridad de ICT se relacionan con sus vulnerabilidades respecto a emplazamiento de la instalación, perímetro de seguridad, técnicas de control del acceso y equipo de seguridad diverso que protege la organización y sus activos ICT.

Controles del funcionamiento del sistema ICT

Los controles del funcionamiento del sistema ICT garantizan que se aplique debidamente la seguridad operacional definida en los procedimientos y políticas. La instrucción de los usuarios del sistema permite asegurarse de que entiendan las políticas y cumplan sus obligaciones.

Controles de mecanismos técnicos e infraestructura

Los controles de mecanismos técnicos e infraestructura garantizan que los controles apropiados de la configuración de la red protejan debidamente a esta última y que los controles técnicos seleccionados impidan el acceso a los datos del sistema por entidades no autorizadas.

Suele aplicarse el principio de “menor privilegio” para asegurarse de que una persona o sistema reciba únicamente el acceso necesario para desempeñar su tarea.

Constituyen ejemplos de estos controles los cortafuegos, los sistemas de detección de intrusos, las listas de control del acceso, el cifrado de datos, las contraseñas, la separación de redes y los controles de rutas.

Controles de la adquisición y el desarrollo

Los controles de la adquisición y el desarrollo se establecen aplicando metodologías comprobadas de ingeniería de sistemas para garantizar que la seguridad esté plenamente integrada en todas las fases del ciclo de adquisición y desarrollo.

Controles de la vigilancia y las auditorías

Los controles de la vigilancia y las auditorías se relacionan con el registro de eventos, auditorías y fallas para fines de seguridad. Se utilizan medios de vigilancia de las alertas y alarmas del sistema para detectar las condiciones de alerta y el uso no autorizado del sistema.

Controles del cumplimiento

Los controles del cumplimiento aseguran que el sistema satisface los acuerdos y las disposiciones legales, reglamentarias y contractuales. Dichos controles suelen ejercerse mediante auditorías del sistema.

El establecimiento de categorías de controles según las funciones de la organización permite relacionar las diversas partes funcionales de una organización con un grupo más reducido de controles. Sin embargo, esto no significa que la gestión de riesgos puede centrarse en una sola función de la organización para proteger determinado activo; normalmente, se necesitarán controles procedentes de diversas funciones.

## 52 NIVELES DE CONTROL

Las organizaciones ATSP varían en dimensiones y tipos. Por ejemplo, en Europa puede tratarse de una organización con personal limitado que proporciona una gama limitada de servicios (p. ej., NAVAID) o de organizaciones que administran centros ATC complejos. En algunos Estados, un organismo gubernamental proporciona servicios de tránsito aéreo mediante una gran variedad de sistemas o instalaciones ATM.

A fin de tener en cuenta estas organizaciones ATSP y sistemas ICT, los controles de seguridad se subdividen en seis niveles de rigor creciente. La diferencia principal reside en el nivel de riesgo para el sistema ICT de ATM, que varía según el carácter crítico del servicio proporcionado por la organización ATSP, la vulnerabilidad del sistema y el tipo de amenazas.

Los seis niveles de control (1 a 6) son cumulativos y corresponden a los requisitos básicos de control de ICT para organizaciones ATM. Cada nivel de control tiene un grado más elevado de complejidad de ICT o activos ICT con riesgos crecientes. Por ejemplo, el Nivel 1 es el más bajo y es apropiado para una organización cuyo sistema ICT sea limitado y aislado. El Nivel 6 es el más elevado y exigiría una implantación competente de todos los requisitos de control (Niveles 1 a 6); es apropiado para una organización de defensa nacional o servicios de inteligencia. La diferencia principal reside en el nivel de riesgo para un sistema ICT, que varía según el carácter crítico del servicio proporcionado por la organización ATSP, la vulnerabilidad del sistema ICT y el tipo de amenazas. En la Tabla Ap C-1 se resumen las características generales de cada nivel de control, mientras que en las Tablas Ap C-2 a C-10 se describe detalladamente cada nivel respecto a cada una de las nueve funciones de la organización.

En cada tabla, los niveles de control se describen en orden ascendente (Nivel 1 a Nivel 6). Estos tienen carácter cumulativo, o sea, los controles del nivel superior contienen todos los controles de nivel inferior, además de lo que se especifica para el nivel en cuestión.

Los niveles de control se han diseñado de modo que una organización con una seguridad “equilibrada” tendrá un nivel de control semejante en cada una de sus funciones. Convendría que ATSP revisara su situación en materia de seguridad de ICT evaluando el nivel de control correspondiente a cada una de las nueve categorías. Esta autoevaluación podría revelar aspectos en que los controles no corresponden a su nivel. En la Figura Ap C-1 se ilustra la manera en que el nivel de control podría constituir un medio conveniente para determinar visualmente los aspectos que deben atenderse. En la ilustración, la meta es el Nivel 2. Los niveles de control correspondientes a cada una de las nueve categorías indican que la auditoría y la organización están en los controles de Nivel 1 y que no se satisfacen los elementos básicos.

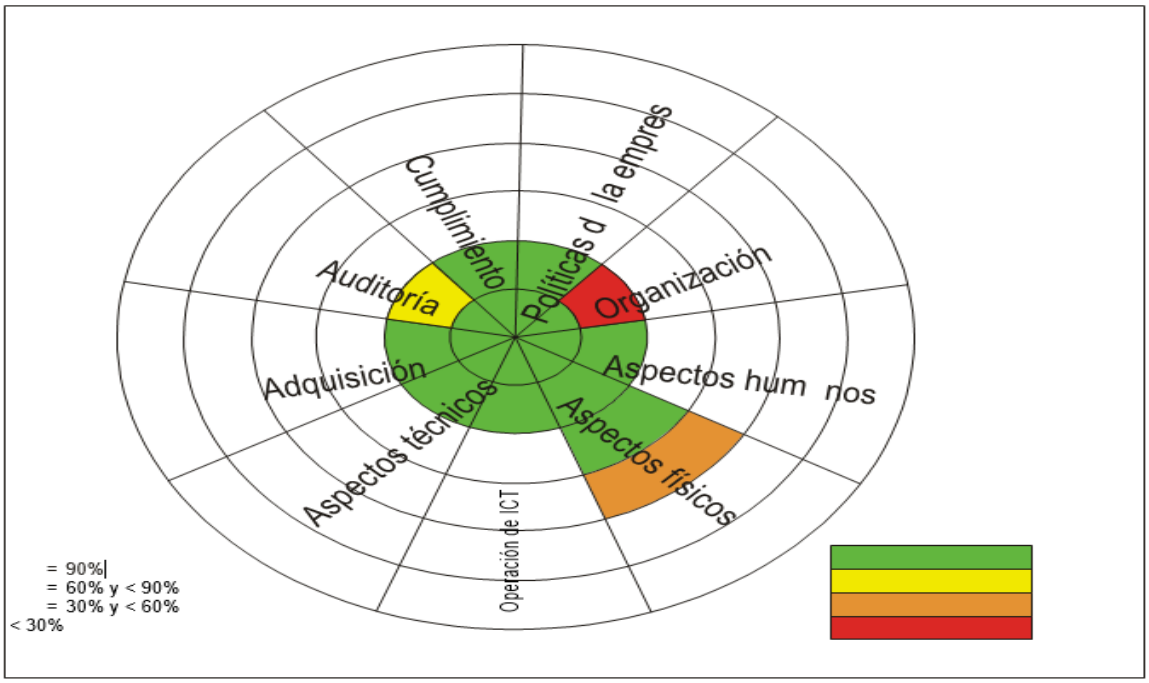


Figura Ap C-1. Ejemplo de presentación gráfica de los niveles de control

**Tabla Ap C-1. Características de los niveles de control**

| | Información | Alcance de la protección | Aislamiento de un activo ICT crítico | Amenaza supuesta |
|---|---|---|---|---|
| Nivel 1 | Utiliza información sensible[1] | Activos de información críticos | Aislado[2] | Amenazas omnipresentes comunes (p. ej., piratas y pequeños criminales) |
| Nivel 2 | Utiliza información sensible | Todos los activos de información | Sistema IT con elevado nivel de conexiones | Amenazas omnipresentes comunes (p. ej., piratas y pequeños |
| Nivel 3 | Para operaciones sensibles | Añade controles de seguridad medianos para activos importantes identificados | Exposición limitada a un entorno de amenaza más elevada, comparada con el conjunto de sistemas ICT de la | Adversarios más sofisticados y con mejores recursos (p. ej., dedicados a crímenes graves u organizados, incluidas ciertas organizaciones terroristas) |
| Nivel 4 | Para operaciones sensibles | Seguridad media para toda la organización[3] | Infraestructura de información sumamente integrada | Adversarios más sofisticados y con mejores recursos (p. ej., dedicados a crímenes graves u organizados, incluidas ciertas organizaciones terroristas) |

| | | | | |
|---|---|---|---|---|
| Nivel 5 | Los activos de información tienen gran valor para la organización y para posibles agresores | Controles de nivel elevado, generalmente específicos para los riesgos y activos | Relativamente aislado | Adversarios con la mayor capacidad, normalmente gobiernos hostiles (p. ej., amenazas reales de gobiernos, terrorismo o espionaje industrial patrocinados por gobiernos; ciertas organizaciones |
| Nivel 6 | Los activos de información tienen gran valor para la organización y para posibles agresores | Reforzar la totalidad de la organización mediante controles de nivel elevado | Activos repartidos que no pueden aislarse suficientemente | Adversarios con la mayor capacidad, normalmente gobiernos hostiles (p. ej., amenazas reales de gobiernos, terrorismo o espionaje industrial patrocinados por gobiernos; ciertas organizaciones |

1. La “información sensible” está definida por la organización en su evaluación de riesgos y abarca la correspondiente a los requisitos legales, tales como la protección de datos.
2. El aislamiento debe confirmarse mediante examen y no solamente enunciarse. Las organizaciones no suelen darse cuenta de
3. “puertas traseras” dejadas por la instalación o proporcionadas, o aun exigidas, para el apoyo por el proveedor o instaladas por el personal para mayor conveniencia. Hasta que se demuestre lo contrario, debe suponerse que los sistemas tienen conexiones externas.
4. Si se contara con un arquitecto para la seguridad, los correspondientes controles se asignarían a sistemas y protección entre Sistemas según una gestión más eficiente y efectiva de la seguridad.

**Tabla Ap C-2. Orientación y políticas de la organización**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | 1.1. La administración aprobará un documento sobre políticas de seguridad de ICT relativo a sistemas críticos y lo publicará y comunicará a todos los empleados y partes externas pertinentes con responsabilidades directamente relacionadas con dichos sistemas.<br><br>Nota En el Nivel 1, el alcance de la mayoría de los controles se limita a sistemas críticos y se modifica la redacción en consecuencia. La restricción se elimina en el Nivel 2. |
| Nivel 2 | El documento sobre políticas de seguridad de ICT cubre todos los sistemas y se comunica a todos los empleados y partes externas pertinentes. Existen también documentos específicos sobre políticas de seguridad del sistema.<br><br>La política de seguridad de ICT se revisará a intervalos programados o si ocurren cambios importantes a fin de mantener su carácter apropiado, adecuado y eficaz. |
| Nivel 3 | 1.4. La administración ha adoptado un método sistemático de gestión de riesgos y lo aplica para la evaluación y gestión de riesgos para la seguridad de ICT. |
| Nivel 4 | No se añaden otros controles en este nivel. |

| | |
|---|---|
| Nivel 5 | No se añaden otros controles en este nivel. |
| Nivel 6 | No se añaden otros controles en este nivel. |

**Tabla Ap C-3. Cultura y administración de la organización**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | La administración apoyará activamente la seguridad dentro de la organización mediante orientación clara, compromiso probado, asignaciones explícitas y reconocimiento de las responsabilidades en materia de seguridad de ICT.<br><br>Nota. — Esto es indispensable, dado que sin el compromiso de la administración superior todo el edificio estaría construido sobre arena.<br><br>Se definirán claramente todas las responsabilidades en materia de seguridad de ICT.<br><br>Se establecerá y aplicará un mecanismo de autorización por la administración en el caso de nuevas instalaciones de procesamiento de la información que comprendan funciones críticas.<br><br>El método de la organización para la gestión de la seguridad de ICT y su implantación (o sea, objetivos de control, controles, políticas, mecanismos y procedimientos para la seguridad de ICT) se revisará internamente cuando ocurran cambios importantes en la aplicación de la seguridad en áreas críticas para las operaciones.<br><br>Los riesgos para la información y las correspondientes instalaciones, planteados por procedimientos operacionales en que participan partes externas, se identificarán y se implantarán controles apropiados antes de autorizar el acceso. |

| Nivel | Requisitos de control |
|---|---|

| | |
|---|---|
| | Se identificarán claramente todos los activos ICT y se establecerá y mantendrá un inventario de todos los activos importantes. Todos los activos de información y de ICT serán propiedad de una parte designada de la organización. Se establecerán, documentarán e implantarán normas relativas al uso aceptable de información y de los activos ICT relacionadas con las instalaciones de procesamiento de la información.<br><br>Nota. — La identificación de los activos ICT es esencial para la gestión de riesgos. Además, es imposible implantar la seguridad o lograr una cultura de la seguridad sin una clara percepción de lo que constituye una conducta aceptable.<br><br>Los sucesos relacionados con la seguridad de ICT que afecten a sistemas críticos se notificarán mediante canales apropiados de la administración lo antes posible.<br><br>Las responsabilidades y procedimientos de gestión se establecerán para asegurar una respuesta rápida, eficaz y ordenada a los incidentes relacionados con la seguridad de ICT.<br><br>Se establecerá y mantendrá un mecanismo controlado para la continuidad de las operaciones en toda la organización, que cubra los requisitos en materia de seguridad de ICT que se necesitan para la continuidad de las operaciones de la organización.<br><br>Nota. — La continuidad de las operaciones se vincula estrechamente a la seguridad. Los dobles objetivos consisten en impedir la pérdida de capacidad crítica para las operaciones y asegurar que las operaciones de contingencia o emergencia no comprometan de manera inaceptable otros objetivos de seguridad.<br><br>Se identificarán los sucesos que pueden causar interrupciones a procedimientos operacionales críticos, así como su probabilidad y repercusiones y sus consecuencias para la seguridad de ICT. |
| Nivel 2 | La administración ha creado un marco y un programa de sensibilización para fomentar un entorno de control positivo en toda la organización. Esto cubre la integridad, valores éticos y competencia de las personas, filosofía de la administración, modo de operar y rendimiento de cuentas. Se otorga atención particular a los aspectos de ICT, incluidas la seguridad y planificación de la continuidad de las operaciones. La administración planifica recursos apropiados para aplicar políticas y asegurar el cumplimiento, de modo que dichos recursos se introducen en las operaciones y forman parte integrante de las mismas. La administración vigila también la oportunidad de aplicación de las políticas. Si bien por regla general la capacitación cae bajo la categoría de recursos humanos, este control se incluye aquí debido a su importancia como instrumento de liderazgo para crear una cultura apropiada de seguridad.<br><br>Se establecerá y aplicará un mecanismo de autorización por la administración en el caso de nuevas instalaciones de procesamiento de la información que comprenda funciones críticas.<br><br>Todos los procedimientos operacionales que pueden apoyar la seguridad de ICT (p. ej., adquisición, cooperación con otras organizaciones) se organizarán para proporcionar dicho apoyo de manera segura.<br><br>El alcance de 2.3, 2.7 y 2.10 se amplía a todos los sistemas y la totalidad de la organización. |

| | |
|---|---|
| Nivel | Requisitos de control |

| | |
|---|---|
| Nivel 3 | Existe una organización oficial de seguridad de ICT que apoya las operaciones. Si los requisitos de la seguridad exceden los niveles básicos, se necesita asistencia especializada.<br><br>Las actividades de seguridad de ICT se coordinarán entre representantes de diferentes partes de la organización que desempeñen funciones y tareas pertinentes.<br><br>Las revisiones de la seguridad, como las indicadas en 2.4, son independientes.<br><br>Deberán satisfacerse todos los requisitos de seguridad establecidos antes de otorgar a los clientes acceso a información o activos de la organización.<br><br>La información se clasificará teniendo en cuenta su valor, requisitos jurídicos, sensibilidad y carácter crítico para la organización (p. ej., aplicando EC 2096/2005). Se elaborará un conjunto apropiado de procedimientos para categorizar y utilizar la información, de conformidad con este plan de clasificación.<br><br>Se exigirá que todos los empleados, contratistas y usuarios externos de sistemas y servicios ICT tomen nota de todas las deficiencias o fallas de la seguridad observadas o sospechadas en los sistemas o servicios y las notifiquen.<br><br>Se contará con mecanismos que permitan cuantificar y vigilar las categorías, volúmenes y costos de los incidentes relacionados con la seguridad de ICT. Cuando las medidas de seguimiento respecto a una persona u organización a raíz de un incidente de seguridad de ICT acarreen procedimientos legales (civiles o criminales), se reunirán, conservarán y presentarán las pruebas para satisfacer las normas relativas a estas últimas enunciadas en la jurisdicción pertinente.<br><br>Nota. — Esto incluye la vigilancia de la utilización aceptable, así como la detección de intrusos, etc.<br><br>Se elaborarán y aplicarán planes para mantener o restaurar las operaciones de sistemas operacionales críticos y asegurar la disponibilidad de información al nivel y en los plazos requeridos a raíz de una interrupción o falla de procedimientos operacionales críticos. Los planes de continuidad de las operaciones se someterán a prueba y se actualizarán periódicamente para asegurarse de que están al día y son eficaces.<br><br>La metodología de gestión de riesgos en 1.4 es fundamental para el procedimiento de decisión en materia de gestión de la seguridad de ICT, desde la selección de controles, adquisición de sistemas y habilitación hasta procedimientos operacionales. El personal de las dependencias operacionales desempeña una función activa en el mecanismo de gestión de riesgos junto con sus colegas técnicos y la administración. |
| Nivel 4 | Se determinarán y revisarán periódicamente las disposiciones de los acuerdos de confidencialidad o no divulgación a fin de reflejar las necesidades de la organización en materia de protección de la información.<br><br>Los acuerdos con terceros relativos a acceso, procesamiento, comunicación o gestión de información o instalaciones de procesamiento de la información de la organización, o la instalación de nuevos productos o servicios para instalaciones de procesamiento de la información, cubrirán todos los requisitos pertinentes en materia de seguridad. |

| Nivel | Requisitos de control |
|---|---|
| | 2.26 Se mantendrá un marco único de planes de continuidad de las operaciones a fin de asegurar que todos los planes sean coherentes, para satisfacer sistemáticamente los requisitos de seguridad de ICT y establecer prioridades relativas a pruebas y mantenimiento. |
| Nivel 5 | 2.27 Contactos apropiados con grupos de interés u otros foros de especialistas en materia de seguridad. |
| Nivel 6 | No se añaden otros controles en este nivel. |

**Tabla Ap C-4. Seguridad relacionada con los recursos humanos**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | Las funciones y responsabilidades en materia de seguridad relacionada con empleados, contratistas y usuarios externos respecto a sistemas críticos se definirán y documentarán de conformidad con la política de seguridad de ICT de la organización. La administración les exigirá que apliquen medidas de seguridad de ICT de conformidad con las políticas y procedimientos establecidos de la organización.<br><br>Se exigen referencias a todos los candidatos para trabajar en áreas sensibles o con responsabilidades concretas de seguridad de ICT.<br><br>Como parte de sus obligaciones contractuales, los empleados, contratistas y usuarios externos que tengan acceso a sistemas ICT críticos firmarán y aceptarán las condiciones de su contrato de empleo, en el que se enunciarán sus responsabilidades y las de la organización en materia de seguridad de ICT.<br><br>Todos los empleados con funciones sensibles en materia de seguridad de la organización y, cuando corresponda, los contratistas y usuarios externos, recibirán capacitación de sensibilización apropiada y actualizaciones periódicas en materia de políticas y procedimientos de la organización, de conformidad con sus funciones y tareas.<br><br>Se definirán y asignarán claramente las responsabilidades para desempeñar funciones de seguridad relacionadas con el cese o cambio de empleo.<br><br>Todos los empleados, contratistas y usuarios externos devolverán todos los activos ICT de la organización que posean y se pondrá fin a todos sus derechos de acceso al concluir su empleo o vencer su contrato o acuerdo. |
| Nivel 2 | El alcance de 3.1, 3.2, 3.3 y 3.4 se amplía a todos los empleados y, cuando corresponda, contratistas y usuarios externos.<br><br>Los empleados investigarán y notarán las violaciones de la seguridad.<br><br>Se brinda a los empleados que dejan su empleo la oportunidad de presentar a la organización sus observaciones sobre aspectos de seguridad de ICT. |

| | |
|---|---|
| Nivel 3 | 3.10 Verificaciones básicas de control de todos los candidatos para un empleo, contratistas y usuarios externos que tengan acceso a sistemas ICT críticos o responsabilidades específicas en materia de seguridad. |

| Nivel | Requisitos de control |
|---|---|
| | Se establecerá un proceso disciplinario oficial para los empleados que hayan violado la seguridad en áreas sensibles.<br><br>Al dejar su empleo, los empleados que trabajen en áreas sensibles o que tengan responsabilidades específicas en materia de seguridad deberán preparar un informe sobre seguridad. |
| Nivel 4 | El alcance de 3.10 y 3.11 se amplía a todos los empleados y, cuando corresponda, contratistas y usuarios externos.<br><br>La seguridad de ICT es una responsabilidad explícita del personal directivo cuyas actitudes y rendimiento en materia de seguridad se notifican en el sistema de evaluación.<br><br>Al dejar su empleo, todos los empleados deberían tener una entrevista relativa a la seguridad. |
| Nivel 5 | Se llevarán a cabo para estas personas verificaciones de antecedentes superiores al nivel básico, como en 3.10.<br><br>Los administradores tienen una responsabilidad oficial respecto al rendimiento en materia de seguridad de ICT dentro de su ámbito de responsabilidad. |
| Nivel 6 | 3.18 El alcance de 3.16 se amplía a todos los empleados y, cuando corresponda, contratistas y usuarios externos. |

**Tabla Ap C-5. Seguridad física y del entorno**

| Nivel | Requisitos de control |
|---|---|

| | |
|---|---|
| Nivel 1 | Se utilizarán perímetros de seguridad (barreras tales como muros, puertas de entrada controladas mediante tarjetas o puestos de recepción atendidos, escolta de visitantes) para proteger las zonas de ICT que contengan información e instalaciones de procesamiento de información de carácter crítico.<br><br>Se establecerá protección física contra daños ocasionados por incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de catástrofes naturales o causadas por el hombre y se aplicará en el caso de instalaciones de procesamiento de información crítica para las operaciones.<br><br>El equipo utilizado para funciones ICT críticas se emplazará o protegerá para reducir los riesgos causados por amenazas y peligros ambientales y las oportunidades de acceso no autorizado. También se protegerá contra fallas de la alimentación eléctrica y otras perturbaciones causadas por fallas de los servicios públicos de apoyo. Se considerará la posibilidad de utilizar una fuente de alimentación ininterrumpible.<br><br>Se mantendrá debidamente el equipo ICT para asegurar su disponibilidad e integridad continuas.<br><br>Se aplicarán medidas de seguridad para el equipo situado fuera del emplazamiento utilizado para funciones críticas, teniendo en cuenta los diversos riesgos que representa el trabajo realizado fuera de los locales de la organización. |
| Nivel | Requisitos de control |
| Nivel 2 | 4.6 El alcance de 4.1 se amplía para cubrir toda la información e instalaciones de procesamiento de la información. Se amplía de manera semejante el alcance de 4.2, 4.3 y 4.5. |
| Nivel 3 | Se protegerán las zonas restringidas controlando debidamente las entradas para asegurarse de que se permita el acceso únicamente a personal autorizado. Se diseñará y aplicará seguridad física para oficinas, salas e instalaciones donde se procesa información sensible o se tenga acceso a la misma. Los puntos de acceso, tales como zonas de entrega y carga y otros puntos por los que personas no autorizadas puedan entrar en los locales, se controlarán y, de ser posible, se aislarán de las instalaciones restringidas de procesamiento de la información para impedir el acceso no autorizado.<br><br>Se protegerán contra daños los cables de alimentación y los medios de telecomunicaciones (físicos y sin cable) que transporten datos y comunicaciones vocales sensibles o críticos para las operaciones o que apoyen dichos servicios ICT.<br><br>Se verificará todo equipo ICT dotado de dispositivos de almacenamiento a fin de asegurarse de que todos los datos sensibles y los soportes lógicos objeto de licencia hayan sido retirados o borrados de manera segura antes de su eliminación final. |
| Nivel 4 | El alcance de 4.7 se amplía a todas las instalaciones de procesamiento de la información y todas las oficinas, salas e instalaciones; 4.8 se amplía a todo el cableado de telecomunicaciones.<br><br>El equipo, la información o los soportes lógicos de ICT no se transportarán fuera de la organización sin autorización previa. |

| | |
|---|---|
| Nivel 5 | 4.12 El cableado de telecomunicaciones que transporte datos críticos o que apoye tales servicios ICT se protegerá contra interceptación. |
| Nivel 6 | 4.13 El alcance de 4.12 se amplía a todo el cableado de telecomunicaciones. Se consulta a las autoridades nacionales. |

**Tabla Ap C-6. Operación de sistemas ICT**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | Los procedimientos operacionales para sistemas ICT críticos se documentarán, mantendrán y se pondrán al alcance de todos los usuarios que los necesiten.<br><br>Se controlarán los cambios en las instalaciones de procesamiento de la información y los sistemas ICT críticos.<br><br>Deberá asegurarse de que los controles de seguridad, definiciones de servicios y niveles de entrega de ICT que consten en todo acuerdo de entrega de servicios por terceros sean implantados, aplicados y mantenidos por estos últimos. Los servicios, informes y registros relacionados con las funciones ICT críticas proporcionadas por terceros serán objeto de vigilancia, revisión y auditorías periódicas.<br><br>Las redes que sean críticas para las operaciones o que transporten información sensible serán objeto de gestión y control adecuados a fin de protegerlas contra amenazas y mantener la seguridad de los sistemas y aplicaciones que las utilicen, incluida la información en tránsito. |

| Nivel | Requisitos de control |
|---|---|

| | |
|---|---|
| | Se implantarán procedimientos para la gestión de dispositivos amovibles. Cuando estos ya no se necesiten, se eliminarán de manera protegida y en condiciones de seguridad.<br><br>Se elaborarán y aplicarán políticas y procedimientos para proteger la información asociada con la interconexión de sistemas ICT que efectúan operaciones sensibles.<br><br>Se establecerán contratos oficiales para concertar acuerdos entre organismos comerciales sobre procedimientos de comunicaciones y normas relativas a la seguridad de los mensajes de operaciones y el almacenamiento de datos. Al realizar operaciones comerciales por Internet, deberán exigirse controles adecuados en las políticas para asegurar el cumplimiento, a nivel mundial, de las leyes y costumbres locales; incumbe a la administración asegurarse de su aplicación. Entre dichos controles figura la verificación de la autenticidad de la contraparte que proporciona instrucciones u operaciones electrónicas, así como la protección de la información electrónica que transita por redes públicas contra actividades fraudulentas, litigios relativos a contratos y divulgación y modificación no autorizadas.<br><br>Se establecerá, documentará y revisará una política de control del acceso para sistemas ICT críticos, basándose en las operaciones y los requisitos de seguridad. Se contará con un procedimiento oficial de registro y supresión de usuarios para otorgar y revocar el acceso a todos los mencionados sistemas y servicios ICT. Se restringirá y controlará la atribución y uso de privilegios. Todos los usuarios de sistemas ICT críticos tendrán un identificador único (identificador de usuario) para uso personal exclusivo. Se seleccionará una técnica apropiada de autenticación para justificar la identidad alegada de un usuario. Las sesiones inactivas se cerrarán al cabo de determinado período de inactividad.<br><br>Se exigirá que los usuarios apliquen buenas prácticas de seguridad al seleccionar y utilizar contraseñas y se aseguren de que el equipo no atendido cuente con protección apropiada.<br><br>Los usuarios de sistemas ICT críticos solo tendrán acceso a los servicios de la red para los que hayan recibido una autorización específica de uso.<br><br>El acceso a los sistemas operacionales se controlará mediante un procedimiento seguro de inicio de sesión.<br><br>La entrada o salida de datos de aplicaciones ICT críticas se validarán para asegurarse de que los datos de entrada sean correctos y apropiados y que la información almacenada se procese de forma correcta y apropiada acorde con las circunstancias. |
| Nivel 2 | El alcance de 5.1 y 5.2 se amplía a todos los procedimientos operacionales e instalaciones de procesamiento de la información, respectivamente.<br><br>El alcance de 5.3 se amplía a todos los acuerdos con terceros para el suministro de IT.<br><br>El alcance de 5.6, 5.8, 5.9 y 5.10 se amplía a todos los sistemas ICT.<br><br>El alcance de 5.4 se amplía a todas las redes.<br><br>La autenticación e integridad de la información procedente del exterior de la organización, recibida por teléfono, mensaje vocal, documentos impresos, facsímil o correo-e, debe verificarse debidamente antes de que puedan tomarse medidas posiblemente críticas. |

| Nivel | Requisitos de control |
|---|---|
| | Los usuarios controlan sistemáticamente la actividad de sus propias cuentas. Se han establecido mecanismos de seguridad de ICT a fin de que puedan supervisar la actividad normal y recibir alertas oportunas sobre actividades inhabituales.<br><br>Se restringirá el acceso de usuarios y personal de apoyo a ICT y funciones de aplicación del sistema, de conformidad con la política establecida de control del acceso. |
| Nivel 3 | El alcance de 5.12 se amplía a todas las aplicaciones apropiadas.<br><br>La administración se asegurará de que la nueva acreditación de la seguridad (p. ej., mediante equipo especial) para sistemas ICT críticos se realice periódicamente para mantener al día el nivel de seguridad aprobado oficialmente y la aceptación del riesgo residual.<br><br>Se separarán las tareas y ámbitos de responsabilidad en zonas protegidas a fin de reducir las posibilidades de modificación no autorizada o involuntaria o el uso indebido de los activos de ICT.<br><br>Se separarán las instalaciones de desarrollo, pruebas y operaciones para reducir los riesgos de acceso o cambios no autorizados en el sistema operacional.<br><br>Se administrarán los cambios en el suministro de servicios ICT críticos, lo que incluye el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de ICT existentes, teniendo en cuenta el nivel crítico de los sistemas y procedimientos operacionales del caso y la evaluación de riesgos.<br><br>Se vigilará y ajustará el uso de recursos para funciones ICT críticas y se prepararán proyecciones relativas a futuros requisitos de capacidad para garantizar el rendimiento requerido del sistema.<br><br>Se establecerán criterios de aceptación basados en análisis oficiales de riesgos en el caso de nuevos sistemas, actualizaciones y nuevas versiones de ICT y se llevarán a cabo pruebas apropiadas de los sistemas durante el desarrollo y antes de su aceptación para funciones críticas. En los Niveles 3 y 4 se necesitan procedimientos más oficiales.<br><br>El mecanismo de control (y eliminación final de) los soportes en 5.5 tiene carácter oficial.<br><br>Se establecerán procedimientos para tratar y almacenar información sensible o crítica a fin de protegerla contra divulgación no autorizada o uso indebido.<br><br>La documentación relativa a sistemas críticos debería protegerse contra acceso no autorizado.<br><br>Se establecerán políticas, procedimientos y controles oficiales para proteger el intercambio de información sensible mediante toda clase de instalaciones de comunicaciones. Se concertarán acuerdos para intercambiar información y soportes lógicos sensibles con partes externas; los soportes que contengan dicha información se protegerán contra acceso no autorizado, uso indebido o corrupción durante su transporte fuera de los límites físicos de la organización.<br><br>Se controlará la atribución de contraseñas para el acceso a sistemas ICT críticos; la administración revisará los derechos de acceso de los usuarios mediante un mecanismo oficial. |

| Nivel | Requisitos de control |
|---|---|
| | Se adoptará en las zonas restringidas una política de “despacho despejado” de papeles y dispositivos amovibles de almacenamiento y una política de “pantallas limpias” para las instalaciones de procesamiento de la información.<br><br>Nota. — En la política de pantalla o despacho despejados, al ausentarse, los usuarios no dejan ningún contenido en sus pantallas ni artículos sobre sus despachos. A menudo, las políticas relativas a las pantallas se aplican para ausencias de unos pocos minutos, mientras que las correspondientes a los despachos podrían exigirse únicamente de noche, a condición de que la sala esté protegida para ausencias temporales durante el día.<br><br>Se elaborarán e implantarán una política, planes y procedimientos operacionales para actividades de teletrabajo.<br><br>Se analizarán los riesgos específicamente antes de autorizar el uso de código móvil en un sistema crítico. La justificación operacional debe ser muy sólida para que se considere semejante autorización. (Esto amplía el control que figura en ISO 27001.) |
| Nivel 4 | El alcance de 5.22 y 5.32 se amplía a toda la organización.<br><br>El alcance de 5.24 se amplía a todos los servicios ICT proporcionados por terceros.<br><br>El alcance de 5.21, 5.25 y 5.26 se amplía a todos los sistemas de procesamiento de la información.<br><br>La administración obtiene una certificación o acreditación independiente de la seguridad y los controles internos antes de implantar nuevos servicios ICT críticos o recurrir a proveedores de servicios ICT, así como recertificación o nueva acreditación de dichos servicios en un ciclo ordinario después de su implantación.<br><br>El alcance de 5.28 se amplía a toda la información intercambiada con partes externas.<br><br>El alcance de 5.29 se amplía a todos los sistemas.<br><br>El mecanismo oficial de 5.31 se amplía a todos los sistemas. |

| | |
|---|---|
| Nivel 5 | Con objeto de reducir al mínimo los riesgos y las posibilidades de uso indebido en una red en funcionamiento, se mantendrán separadas, lógica o físicamente, las zonas operacionales que se ocupan de cuestiones e información sobre operaciones críticas. Las instalaciones de desarrollo se separan de las operacionales.<br><br>Las zonas sometidas a la política de despacho o pantalla despejados (véase 5.32) se verifican de manera ordinaria fuera de las horas de trabajo.<br><br>El acceso a distancia a un sistema crítico se autoriza únicamente en circunstancias excepcionales después de un análisis específico de riesgos.<br><br>Se aplicarán restricciones relativas a las horas de conexión a fin de aumentar la seguridad de las aplicaciones con riesgo elevado.<br><br>El teletrabajo con datos sensibles debería realizarse únicamente desde emplazamientos debidamente protegidos. |
| Nivel | Requisitos de control |
| Nivel 6 | El alcance de 5.43 y 5.45 se amplía a todos los sistemas.<br><br>El teletrabajo debería llevarse a cabo a partir de emplazamientos debidamente protegidos. |

No se recomienda la restricción para sistemas CSC en el caso de 6.1 (como es normal para el Nivel 1) debido al riesgo de propagación del código malicioso entre sistemas. Los productos antivirus comerciales (debidamente actualizados), una buena administración de revisiones, un control apropiado de dispositivos y una elevada penetración de la sensibilización deberían ser adecuados para los niveles básicos.

| | |
|---|---|
| Nivel | Requisitos de control |

| | |
|---|---|
| Nivel 3 | Se contará con mecanismos que impidan la fuga de información de sistemas sensibles.<br><br>En el caso de sistemas ICT críticos, se refuerzan los mecanismos utilizados para implantar 6.1 y 6.2, por ejemplo mediante el uso de “listas blancas” para controlar los códigos ejecutables, verificaciones periódicas y capacitación específica de sensibilización para todos los usuarios. Las defensas deberían someterse a prueba periódicamente.<br><br>Se determinarán las características de seguridad, los niveles de servicio y las disposiciones de la administración respecto a todos los servicios críticos en la red y se incluirán en todo acuerdo relativo a tales servicios proporcionados en la propia empresa o contratados.<br><br>Se controlará el acceso físico y lógico a las entradas de conexión a dispositivos de diagnóstico y configuración en sistemas ICT críticos. Se considerará la identificación automática del equipo (y se adoptará, cuando corresponda) como medio de autenticación de las conexiones a sistemas ICT críticos a partir de emplazamientos y equipo específicos.<br><br>Los sistemas de gestión de contraseñas para sistemas ICT críticos serán interactivos y garantizarán la calidad de las contraseñas.<br><br>Se restringirá el uso de programas de utilidades que podrían invalidar los controles de sistemas y aplicaciones y se controlará estrictamente en el caso de sistemas críticos.<br><br>En todo entorno de teletrabajo con sistemas ICT críticos, existen mecanismos para detectar los intentos por introducirse en sistemas o redes o el ingreso efectivo no autorizado, lo que permite a la organización responder de manera apropiada y efectiva.<br><br>Se incorporarán verificaciones de validación en las aplicaciones críticas para detectar toda corrupción de la información debida a errores de procesamiento o actos deliberados.<br><br>Se determinarán normas para asegurar la autenticidad y proteger la integridad de los mensajes en aplicaciones críticas y se determinarán y aplicarán controles apropiados.<br><br>Se elaborará y aplicará una política relativa al uso de controles criptográficos para proteger la información.<br><br>El uso de técnicas criptográficas por la organización exigirá una gestión sólida. |
| Nivel 4 | El alcance de 6.10, 6.12, 6.13, 6.14 y 6.15 se amplía a todos los sistemas.<br><br>El alcance de 6.11 se amplía a todos los servicios en la red.<br><br>Se protegerá debidamente la información en los mensajes electrónicos.<br><br>El alcance de 6.16 y 6.17 se amplía a todas las aplicaciones apropiadas.<br><br>Existe una infraestructura apropiada de identificación en toda la organización que sirve de fundamento para las decisiones relativas a autenticación y control del acceso. |

| Nivel | Requisitos de control |
|---|---|
| Nivel 5 | 6.25 Se instalarán controles estrictos de encaminamiento para redes conectadas a sistemas sensibles para asegurarse de que las conexiones de computadoras y la circulación de información no violen la política de control del acceso a aplicaciones operacionales. Se exige un aislamiento efectivo respecto a vías no fiables.<br><br>Los sistemas sensibles contarán con un entorno de computación exclusivo (aislado). |
| Nivel 6 | 6.26 El alcance de 6.25 se amplía a todos los sistemas. |

**Tabla C-8. Adquisición, desarrollo y mantenimiento**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | Al enunciarse requisitos operacionales para nuevos sistemas ICT o mejoras de sistemas ICT existentes para funciones críticas, se especificarán los requisitos correspondientes a controles de seguridad.<br><br>Se establecerán procedimientos para controlar la instalación de soportes lógicos en sistemas operacionales con funciones críticas.<br><br>Cuando se modifiquen sistemas operacionales, se revisarán y someterán a prueba sus aplicaciones críticas a fin de asegurarse de que no afecten a las operaciones o la seguridad de la organización.<br><br>Deberían obtenerse e instalarse oportunamente actualizaciones de seguridad para sistemas críticos.<br><br>Se efectuarán y someterán a prueba periódicamente copias de salvaguardia de la información y los soportes lógicos críticos de conformidad con la correspondiente política. |
| Nivel 2 | El alcance de 7.1, 7.2, 7.3 y 7.4 se amplía a todos los sistemas ICT.<br><br>La administración ha implantado procedimientos para asegurarse de que los responsables de operaciones y los usuarios acepten oficialmente los resultados de las pruebas y el nivel de seguridad para los sistemas ICT, así como el correspondiente riesgo residual. Estos procedimientos reflejan las funciones y responsabilidades convenidas de los usuarios y del personal de desarrollo de sistemas, gestión de redes y operaciones del sistema, teniendo en cuenta los aspectos de separación, supervisión y control.<br><br>Los administradores de ICT se han asegurado de que el personal de mantenimiento cuente con asignaciones específicas y que su trabajo sea objeto de vigilancia apropiada. Además, se controla su derecho de acceso a fin de evitar el riesgo de acceso no autorizado a sistemas automatizados.<br><br>El alcance de 7.5 se amplía a la totalidad de la información y los soportes lógicos. |

| | |
|---|---|
| Nivel 3 | 7.10 La seguridad de ICT basada en la gestión de riesgos está integrada en la gestión de proyectos de la organización y sus métodos de control de la calidad. |

| Nivel | Requisitos de control |
|---|---|
| | Los datos para pruebas de funciones ICT críticas se seleccionarán cuidadosamente, se protegerán y controlarán y se limitará el acceso a los códigos de fuente de programas. Este requisito es de difícil interpretación porque una interpretación rigurosa prohibiría el uso de sistemas operacionales de propiedad exclusiva y soportes lógicos de fuente abierta. Los elementos fundamentales son los siguientes:<br><br>los soportes lógicos se someten a pruebas cuidadosas y apropiadas;<br>la fuente de todo soporte lógico se considera como suficientemente fiable para la aplicación concreta; y<br>la información detallada sobre configuración del sistema debería estar protegida.<br><br>La implantación de modificaciones en sistemas ICT críticos se controla mediante procedimientos oficiales apropiados, que incluyen una evaluación de riesgos para la seguridad.<br><br>Se desaconseja modificar los conjuntos de soportes lógicos en sistemas ICT críticos; conviene limitarse a cambios necesarios y controlar todos los cambios estrictamente.<br><br>Se obtendrá información oportuna sobre vulnerabilidades técnicas de los sistemas ICT en uso, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán medidas apropiadas para afrontar el riesgo correspondiente.<br><br>Se establece el almacenamiento externo de soportes de salvaguardia, documentación y otros recursos ICT críticos para apoyar los planes de recuperación y continuidad de operaciones. Los propietarios de procedimientos operacionales y el personal de funciones ICT participan en la determinación de los recursos de salvaguardia que se conservarán en almacenes externos. La instalación externa de almacenamiento tiene un entorno apropiado para los dispositivos y otros recursos almacenados y un nivel de seguridad acorde con el que se necesita para proteger los recursos de salvaguardia contra acceso no autorizado, hurto o daño. Los administradores de ICT se asegurarán de que se evalúen periódicamente, al menos anualmente, los arreglos externos respecto a contenido, protección del entorno y seguridad. |
| Nivel 4 | El alcance de 7.11 se amplía a todos los programas de aplicaciones y sistemas.<br><br>El alcance de 7.12 se amplía a todos los sistemas.<br><br>Las modificaciones de conjuntos de soportes lógicos en todos los sistemas ICT se limitarán a cambios necesarios y todos los cambios se controlarán estrictamente. |
| Nivel 5 | 7.19 La organización supervisará y vigilará el desarrollo de soportes lógicos contratados para sistemas ICT críticos. |
| Nivel 6 | 7.20 El alcance de 7.19 se amplía a todos los sistemas. |

**Tabla C-9. Vigilancia y auditoría**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | Para todos los sistemas ICT críticos, se mantendrán registros de auditorías relativos a actividades de los usuarios, excepciones y sucesos relacionados con la seguridad de ICT y se conservarán durante un período convenido para facilitar futuras investigaciones y la vigilancia en materia de control del acceso.<br><br>Se registrarán las actividades de los administradores y operadores del sistema en el caso de sistemas ICT críticos.<br><br>Se registrarán y analizarán las faltas relacionadas con sistemas críticos y se tomarán medidas apropiadas al respecto.<br><br>Se planificarán y acordarán cuidadosamente los requisitos y actividades de auditoría mediante verificaciones de sistemas operacionales ICT críticos para minimizar el riesgo de perturbación de procedimientos operacionales.<br><br>Se protegerá el acceso a los instrumentos de auditoria de sistemas ICT críticos para impedir todo posible uso indebido o interferencia. |
| Nivel 2 | El alcance de 8.1, 8.2, 8.3, 8.4 y 8.5 se amplía a todos los sistemas.<br><br>Se han implantado políticas y técnicas relativas a la utilización y vigilancia de las utilidades de los sistemas y la evaluación de su uso. Las responsabilidades relativas al uso de utilidades de soportes lógicos sensibles han sido claramente definidas y comprendidas por sus diseñadores y se vigila y registra el uso de las utilidades. |
| Nivel 3 | Se establecerán procedimientos para vigilar el uso de instalaciones de procesamiento de información crítica y se examinarán periódicamente los resultados de dicha vigilancia.<br><br>Los instrumentos de registro y la información sobre sistemas ICT críticos que figure en los registros se protegerán contra alteración y acceso no autorizado.<br><br>La vigilancia de la red se utilizará para determinar las deficiencias en su configuración actual. Permitirá una nueva configuración a raíz de un análisis del tráfico en la red y facilitará la identificación de agresores. |
| Nivel 4 | El alcance de 8.8 y 8.9 se amplía a todos los sistemas ICT y sus instalaciones de procesamiento de la información.<br><br>Se cuenta con mecanismos para detectar los intentos por introducirse en sistemas o redes o el ingreso efectivo no autorizado, lo que permite a la organización responder de manera apropiada y efectiva. |
| Nivel 5 | 8.13 Los relojes de todos los sistemas pertinentes de procesamiento de la información en una organización o dominio de seguridad se sincronizarán con una fuente precisa de la hora. |
| Nivel 6 | No se añaden otros controles en este nivel. |

**Tabla C-10. Cumplimiento**

| Nivel | Requisitos de control |
|---|---|
| Nivel 1 | Todas las disposiciones estatutarias, reglamentarias y contractuales pertinentes y los métodos de la organización para satisfacerlas se definirán explícitamente, se documentarán y se mantendrán actualizadas para cada sistema ICT y la organización en conjunto.<br><br>Los registros importantes se protegen contra pérdida, destrucción y falsificación, de conformidad con las disposiciones estatutarias, reglamentarias, contractuales y operacionales.<br><br>La protección y privacidad de los datos se garantizan según lo dispuesto en la legislación, reglamentos y, si corresponde, cláusulas contractuales pertinentes.<br><br>Los administradores se asegurarán de que todos los procedimientos de seguridad de ICT dentro de su ámbito de responsabilidad se apliquen debidamente para lograr que se cumplan las políticas y normas de seguridad. |
| Nivel 2 | Se aplican procedimientos apropiados para asegurar el cumplimiento de las disposiciones legislativas, reglamentarias y contractuales relativas al uso de material respecto al cual puedan existir derechos de propiedad intelectual y el uso de soportes lógicos de propiedad exclusiva.<br><br>Existen reglas precisas en que se impide el uso de instalaciones de procesamiento de la información para fines no autorizados, que se supone todos los usuarios deben obedecer, reforzadas por un proceso disciplinario. En 15.1.5 de la norma ISO 27001 solo se indica que "Se disuadirá a los usuarios…". |
| Nivel 3 | Se utilizan controles criptográficos de conformidad con todos los acuerdos, leyes y reglamentos pertinentes.<br><br>Se refuerzan las normas que figuran en 9.6 mediante verificaciones técnicas y físicas y un estricto proceso disciplinario.<br><br>Se verifican periódicamente los sistemas ICT respecto al cumplimiento de las normas de implantación de la seguridad. |
| Nivel 4 | No se añaden otros controles en este nivel. |
| Nivel 5 | No se añaden otros controles en este nivel. |
| Nivel 6 | No se añaden otros controles en este nivel. |

## APÉNDICE D: EJEMPLOS NACIONALES Y REGIONALES DE SUMINISTRO DE SERVICIOS DE SEGURIDAD PARA ATM

En el presente apéndice figura información sobre procedimientos y prácticas actualmente utilizados que los Estados y administraciones de aviación civil pueden considerar al reglamentar los servicios de seguridad de ATM de los ATSP. El apéndice se divide en tres secciones en que se examinan los servicios de seguridad de ATM de EUROCONTROL, Reino Unido y Estados Unidos para la gestión de incidentes en vuelo y la coordinación de la gestión de crisis.

### 53 MARCO EUROPEO DE GESTIÓN DE INCIDENTES EN VUELO RELACIONADOS CON LA SEGURIDAD

EUROCONTROL y la OTAN han creado un concepto operacional para incidentes en vuelo relacionados con la seguridad en Europa que permite coordinar sus medidas durante tales sucesos. En el presente apéndice se describe dicho concepto.

Los trágicos acontecimientos del 11 de septiembre de 2001 han cambiado a fondo la manera de afrontar los incidentes en vuelo relacionados con la seguridad cuando el mundo presenció una dimensión de terrorismo sin precedentes: la utilización de aeronaves civiles como armas de destrucción masiva. En Europa, la nueva amenaza se llamó “Renegade”. Desde entonces, las autoridades nacionales de seguridad toman medidas más activas ante cualquier indicación que podría dar lugar a inquietud respecto a la seguridad, o sea, COMLOSS con la aeronave o desconexión o ajuste incorrecto del transponedor. Como ejemplo, en la mayoría de los países europeos el número de interceptaciones por COMLOSS ha duplicado, por lo menos, después de dicho 11 de septiembre.

Respuesta europea

A la luz de la nueva amenaza “Renegade”, se han revisado los procedimientos nacionales de respuesta a incidentes en vuelo relacionados con la seguridad. En numerosos casos se han concertado acuerdos bilaterales para coordinar más eficazmente los incidentes transfronterizos. Sin embargo, la dimensión internacional de los incidentes en vuelo relacionados con la seguridad exige armonización a nivel europeo. A título de ejemplo, en la Figura Ap D-1 se ilustran las derrotas de las aeronaves el 11 de septiembre sobre un mapa de Europa Central, lo que indica que tres o cuatro Estados resultan afectados por un incidente de poca duración.

Para tener en cuenta la dimensión internacional del problema “Renegade”, EUROCONTROL y la OTAN han creado el Grupo OTAN-EUROCONTROL de coordinación de la seguridad en la gestión del tránsito aéreo (ATM) (NEASCOG) cuya misión consiste en asegurar la estrecha coordinación necesaria y el desarrollo de todas las actividades de seguridad conexas con miras a lograr puntos de vista convergentes entre los países miembros de cada organización.

La situación en que se utiliza una aeronave civil como arma para perpetrar un ataque terrorista suele llamarse “Renegade”.

A este respecto, NEASCOG fomenta, desarrolla y apoya medidas de seguridad paneuropeas eficaces, a saber:

1. Crear un punto central regional europeo para información ATM relativa a intereses civiles y militares; y

2. Otorgar prioridad a la validación de comunicaciones aeroterrestres de gran capacidad para la

transmisión de la voz en el puesto de pilotaje, datos de vuelo e información vídeo de a bordo en formato cifrado.

Explicación del problema

Los incidentes en vuelo relacionados con la seguridad son sucesos urgentes que exigen una sólida coordinación entre diferentes actores y la reunión y validación de información casi en tiempo real para apoyar la toma de decisiones.

Los principales aspectos que deben considerarse durante un incidente relacionado con la seguridad son:

1 Sensibilización óptima: identificación de aeronaves sospechosas, notificación de incidentes, difusión de la información y mantenimiento de la sensibilización;

2 Requisitos de información: se necesita información pertinente para la gestión y solución de un incidente;

3 Factor tiempo: la información necesaria debe llegar al destinatario pertinente a tiempo para que pueda proporcionar una respuesta adecuada; y

4 Apoyo tecnológico: la automatización y el cifrado facilitan el intercambio de información, reducen los plazos y protegen la confidencialidad.

Los requisitos en materia de información sobre incidentes en vuelo relacionados con la seguridad se obtienen de las autoridades nacionales. Se indican a continuación elementos de información pertinentes:

1. Determinar si la conducta es sospechosa. Se han determinado diversos criterios para una conducta sospechosa, pero la lista no es exhaustiva. La capacitación, la sensibilización respecto a la seguridad y el juicio de pilotos y controladores constituyen, por consiguiente, un factor fundamental;

2. Reunir información acerca del suceso. La información sobre la situación a bordo es fundamental. El piloto al mando (PIC) es el actor principal y deben aplicarse medidas para apoyarlo, de ser posible, de conformidad con situaciones predefinidas. Sin embargo, es indispensable asegurarse de la legitimidad del PIC. Son también importantes otros elementos de información acerca del vuelo:

   a) Tipo de aeronave;

   b) Nacionalidad;

   c) Explotador;

   d) Pasajeros a bordo y su nacionalidad;

   e) Personalidades destacadas; y

   f) Niños;

3. Evaluar el riesgo. La evaluación de riesgos debería incluir el examen de la amenaza real

planteada por la aeronave basándose en factores como resistencia, objetivos al alcance, conducta de la aeronave (p. Ej., descenso marcado), confirmación de la intención del pic y los pilotos legítimos.

Suministro de soluciones: marco

El concepto de alto nivel de gestión de incidentes relacionados con la seguridad en el espacio aéreo (ASSIM) de NEASCOG constituye un marco para afrontar incidentes en vuelo relacionados con la seguridad. Su objetivo consiste en apoyar el mecanismo de toma de decisiones proporcionando a las autoridades nacionales responsables de la seguridad del espacio aéreo[2] información fiable en tiempo real acerca de los incidentes relacionados con la seguridad en el espacio aéreo.

Otros actores que se consideran en el concepto de alto nivel ASSIM son: centros nacionales de defensa aérea, centros adyacentes de defensa aérea, ATC civil, centros de operaciones de líneas aéreas y las aeronaves (véase la Figura Ap D-2).

Uno de los dominios que deben considerarse en el concepto ASSIM consiste en el apoyo técnico (instrumento ASSIM) que permite la difusión de la información en forma protegida y en tiempo real.

Seguridad del espacio aéreo: protección del espacio aéreo contra uso no autorizado, intrusión, actividades ilegales o toda violación. Esto exige la gestión del espacio aéreo para impedir, detectar y resolver en lo posible las amenazas en el aire.

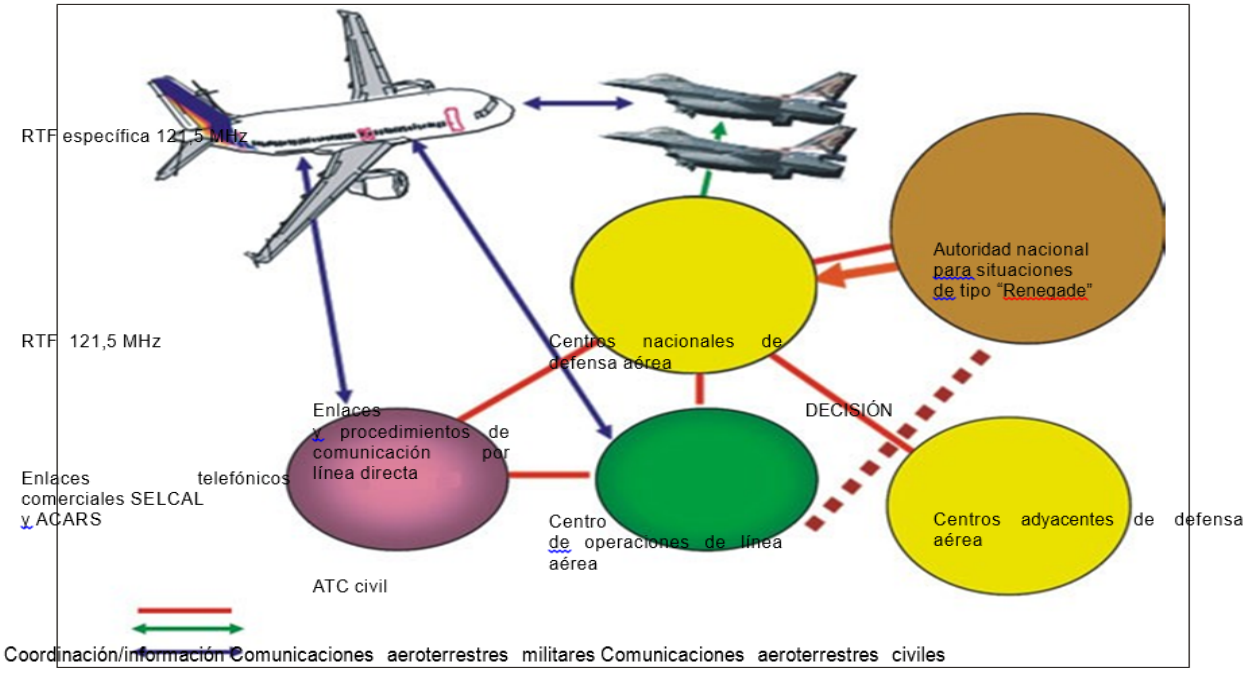


**Figura Ap D-2. Concepto de alto nivel de gestión de incidentes en el espacio aéreo relacionados con la seguridad**

Apoyo técnico (instrumento de apoyo ASSIM)

Un aspecto fundamental de ASSIM consiste en reunir y difundir oportunamente la información necesaria. En el concepto ASSIM las autoridades gubernamentales nacionales (NGA) se consideran como usuario. Los demás actores deberían desempeñar una función de apoyo a estas últimas y facilitar el procedimiento de toma de decisiones.

Por consiguiente, un instrumento ASSIM debería elaborarse teniendo en cuenta las necesidades precisas de NGA. Un instrumento ASSIM automatizado favorecería claramente el mecanismo nacional de toma de decisiones al reunir y difundir información protegida (o sea, cifrada) en tiempo real. Si un incidente alcanza el nivel de NGA, se necesitan inmediatamente conjuntos predefinidos de elementos de información; solo un instrumento automatizado puede satisfacer esta exigencia, especialmente en una situación de sucesos múltiples.

Desde el punto de vista pragmático y económico, los productos disponibles en el comercio (COTS) deberían constituir la mejor opción para el instrumento ASSIM.

Componentes del instrumento de apoyo ASSIM

Teniendo en cuenta la información proporcionada en los párrafos precedentes, los dos aspectos fundamentales de la gestión de incidentes en vuelo relacionados con la seguridad son:

1. Disponibilidad en tiempo real de información protegida sobre la situación a bordo; y

2. Intercambio en tiempo real de información sobre seguridad, incluida la situación a bordo.

La tecnología permite adquirir información sobre la situación a bordo e intercambiar información relativa a la seguridad mediante una red. EUROCONTROL y la OTAN participan en dos proyectos piloto en que se consideran ambos aspectos a fin evaluar la viabilidad y las opciones de implantación.

Adquisición de información de a bordo

La seguridad en vuelo puede reforzarse proporcionando, de aire a tierra, información cifrada en tiempo real (voz, datos y vídeo) que presentaría a las autoridades de seguridad una imagen de la situación netamente mejorada en caso de interferencia ilícita en una aeronave en vuelo (véase la Figura Ap D-3).

La disponibilidad de radioespectro apropiado es crítica para todos los sistemas que transmiten o reciben señales. Esto significa que todo nuevo sistema aeronáutico debe funcionar dentro del espectro aeronáutico existente y ser compatible con otros sistemas

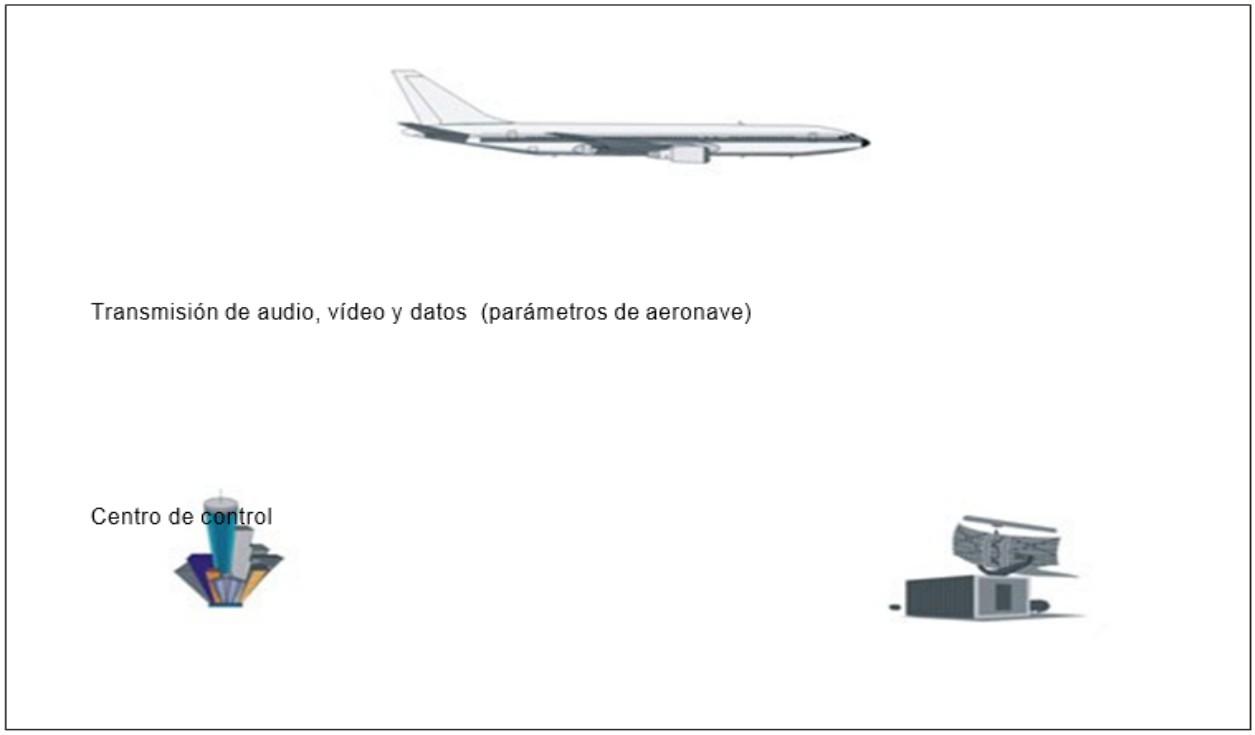


**Figura Ap D-3. Adquisición de información de a bordo**

Intercambio de información relativa a la seguridad

Una vez adquirida información relativa a la seguridad, la segunda etapa consiste en compartirla con todos los actores que se relacionen con incidentes en vuelo. Esto mejora la capacidad para evaluar la situación, tomar medidas apropiadas y facilitar y apoyar el mecanismo de toma de decisiones. Sin embargo, la información debe compartirse de manera segura para proteger la privacidad y confidencialidad.

El proyecto actual depende de la tecnología de infraestructura de clave pública (PKI), que se utiliza cada vez más en entornos civiles y militares (véase la Figura Ap D-4). PKI contribuye una solución a diversos problemas básicos de confianza y fiabilidad en el mundo electrónico, incluido lo siguiente:

1. Identificación de usuarios;

2. Autenticación, integridad y no repudiación mediante firma digital;

3. Privacidad y confidencialidad mediante cifrado;

4. Información protegida contra manipulación; y

5. Información protegida contra repudiación.

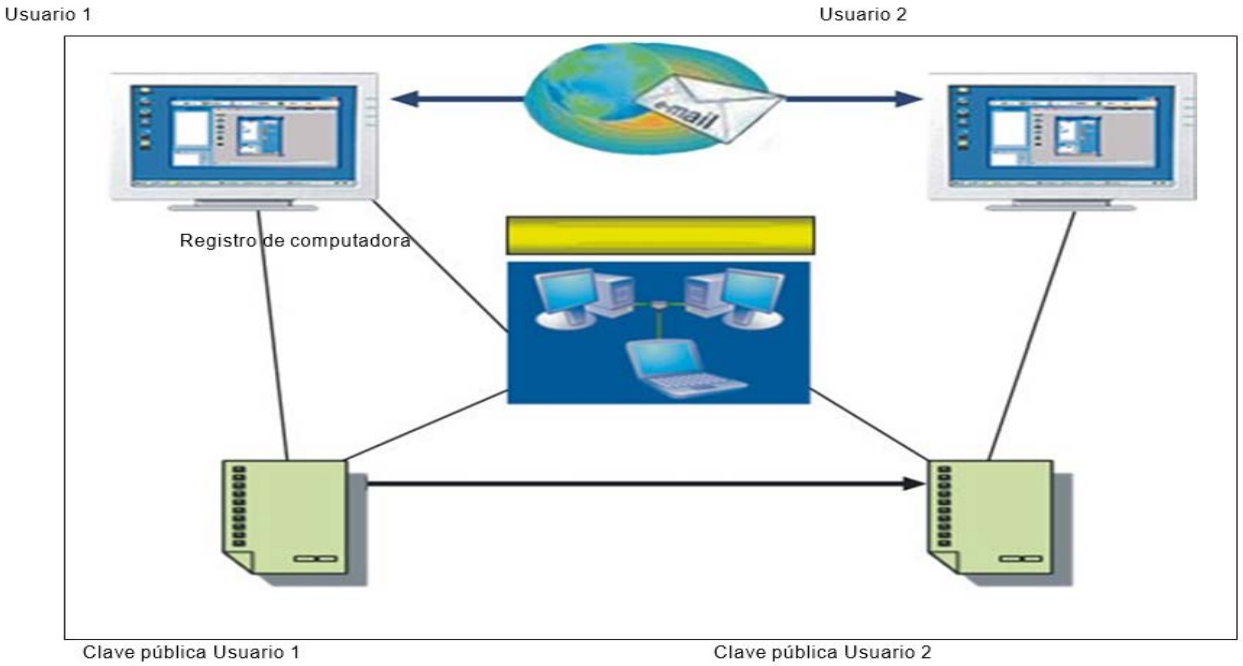


**Figura Ap D-4. Marco seguro para correo-e**

PKI ofrece un entorno seguro (cifrado PKI) para intercambiar información relacionada con la seguridad y tiene también la ventaja de que puede ponerse en comunicación con cualquier otra aplicación de seguridad basada en el protocolo de Internet (IP) ofreciendo compatibilidad, por ejemplo, con el componente de a bordo.

## 53.1 PROCEDIMIENTOS PARA SUCESOS EN VUELO RELACIONADOS CON LA SEGURIDAD EN EL REINO UNIDO

UK NATS, ATSP del Reino Unido (RU), ha publicado procedimientos de seguridad para afrontar sucesos en vuelo relacionados con la seguridad, tales como secuestros, amenazas de bomba o irregularidades como pérdida de comunicaciones o cambio no autorizado de código de transpondedor. Los correspondientes procedimientos se presentan aquí como referencia para Estados miembros que deseen examinar los procedimientos de otros ATSP.

La orientación siguiente permitiría a los explotadores de aeronaves, evaluadores de amenazas y pilotos entender los procedimientos que las autoridades competentes del RU aplicarán para afrontar sucesos de a bordo relacionados con la seguridad. El objetivo global consiste en identificar, contener y resolver tales situaciones de manera apropiada y lo más rápidamente posible en condiciones de seguridad.

Para fines de seguridad nacional, los organismos de ATC y defensa aérea (AD) vigilan el espacio aéreo del RU y sus aproximaciones para determinar la presencia de indicaciones de actividad sospechosa que puedan señalar un suceso a bordo en curso relacionado con la seguridad, de modo que puedan tomarse medidas apropiadas para afrontar la situación. Semejante suceso ocurre cuando una aeronave es objeto de una amenaza real o supuesta, que puede consistir en un secuestro, alerta de bomba u otra perturbación a bordo, o que la

aeronave se perciba como una amenaza para el RU. En ambos casos, los procedimientos aplicados para determinar la certeza, carácter y alcance de la amenaza serán similares. Sin embargo, los procedimientos aplicados para afrontar cada categoría de amenaza probablemente serán diferentes.

Si se considera que un suceso en el aire relacionado con la seguridad plantea una amenaza al RU, es probable que la autoridad de defensa aérea (ADA), conferida al Centro nacional de operaciones aéreas (NAOC) de la base de la Fuerza Aérea Real (RAF) en High Wycombe, pueda utilizar aeronaves y otros medios de alerta de reacción rápida (QRA) para obtener más amplia información y tomar las medidas necesarias para resolver la situación. Esta podría evolucionar rápidamente, por lo que es indispensable comunicar la información oportunamente y cumplir las instrucciones.

Los procedimientos descritos aquí pertenecen al Gobierno del RU y contienen medidas para diversos organismos, principalmente el Ministerio de Defensa (MoD), NATS, el Departamento de transporte (DfT) y el Servicio de policía metropolitana. Estos procedimientos se revisan periódicamente y se aplican cuando una aeronave, sea cual fuere su nacionalidad, entra, sale o sobrevuela el RU, y se aplican a todo el espacio aéreo del RU, o sea, las FIR y las regiones superiores de información de vuelo (UIR) London y Scottish y el área de control oceánico de Shanwick.

Identificación y señalamiento de secuestros y situaciones relacionadas con la seguridad

Situación de secuestro verificada. De ser posible, la identidad de una aeronave objeto de secuestro debería comunicarse al personal de ATC mediante selección, por la tripulación de vuelo, del código 7500 en Modo 3/A en el transpondedor de la aeronave o una declaración en la frecuencia de la instalación de transmisión radioeléctrica (RTF).

Otros indicadores de alerta de seguridad. Existe una gama de indicadores de aeronaves o actividades de piloto sospechosas que podrían señalar a ATC y a los organismos de defensa aérea un suceso posible relacionado con la seguridad e iniciar procedimientos de intervención. Entre dichos indicadores figuran los siguientes:

1. Perfil de vuelo no autorizado, o sea, violación del espacio aéreo;

2. Desviación no autorizada, en el plano horizontal o vertical, respecto al perfil de vuelo autorizado;

3. Negativa o incapacidad de acatar las instrucciones de ATC, incluida la guía vertical, sin motivo válido;

4. Pérdida de contacto RTF, particularmente en relación con la desviación del perfil de vuelo;

5. Cambios no autorizados en el código SSR o uso prolongado de IDENT;

6. Uso, por la tripulación de vuelo, de fraseología no normalizada u otras tentativas disimuladas para destacar la situación (p. Ej., cambio marcado en las inflexiones de la voz o voz diferente, etc.);

7. Notificación de una amenaza o incidente procedente de fuentes oficiales o no oficiales;

8. Transmisión RTF abierta desde el puesto de pilotaje;

9. Transmisión RTF no relacionada con ATC (p. Ej., una declaración política); y

10. Amenaza, concreta o no, comunicada por intermedio de terceros (p. Ej., la policía o el público).

Los últimos tres elementos que preceden pueden significar que se ignora la identidad de la aeronave hasta que se aclaren otros factores. Tal vez los elementos individuales no constituyan, de por sí, actividades sospechosas del piloto o la aeronave. No obstante, una combinación de los mismos puede considerarse como un suceso inhabitual, a raíz de lo cual ATC tomaría medidas de alerta apropiadas.

Responsabilidades del piloto al mando y el explotador de aeronaves

Cuando exista información relativa a una amenaza real o supuesta a la seguridad de una aeronave, debería ser comunicada inmediatamente, por el piloto al mando, a la dependencia ATC correspondiente o, por el explotador de aeronaves, a las autoridades de seguridad civil del RU, según corresponda. Un asesor de amenazas capacitado de la línea aérea debería evaluar la amenaza y comunicar la serie de conclusiones o códigos a las autoridades de seguridad civil del RU, lo antes posible. La información relativa a la integridad del puesto de pilotaje debería proporcionarse a ATC oportunamente. Esto permitiría a los organismos de defensa estatal del RU aplicar la gestión más apropiada para la situación.

Es indispensable utilizar debidamente fraseología RTF y códigos en Modo 3/A del radar secundario de vigilancia (SSR) con objetivos especiales. En caso de amenaza real a la seguridad, el piloto al mando no debería utilizar llamadas con prefijo PAN o MAYDAY aisladamente para comunicar la amenaza a ATC. Los pormenores de la amenaza a la seguridad deberían comunicarse en la misma transmisión. Si el piloto al mando no percibe una amenaza a la seguridad de la aeronave, debería aplicar el uso apropiado de PAN (posible asistencia necesaria – ningún peligro inminente para la vida humana) o MAYDAY (llamada de socorro – peligro inminente para la vida humana) si necesita alguna forma de tratamiento prioritario por parte de ATC hasta el lugar de destino o un aeropuerto de desviación.

Debería encarecerse a las tripulaciones de vuelo a que vigilen la frecuencia de emergencia 121,5 MHz en todo momento, lo que aumenta la posibilidad de captar transmisiones de ATC, que esté tratando de reestablecer contacto con la aeronave. Por su parte, las aeronaves militares transmiten simultáneamente en 121,5, además de las frecuencias ATC normalizadas. Sí, por cualquier motivo, las tripulaciones de vuelo se encuentran sin la frecuencia apropiada, se les aconseja también solicitar asistencia de ATC utilizando 121,5 MHz.

La combinación de llamadas RTF correctas y uso de códigos en Modo A permitirá a ATC tomar medidas apropiadas para la situación.

Comunicaciones

ATC. En cuanto se reciba notificación de un suceso, la dependencia ATC correspondiente comunicará la información al supervisor de operaciones ATC en un centro de control de área (ACC) de tránsito aéreo principal. Incumbe entonces al supervisor notificar a los organismos de defensa militar del RU por intermedio de la organización ATC militar. Luego, ADA-RU militar notificará a los organismos gubernamentales apropiados del RU, incluidas las organizaciones civiles y de imposición de la ley.

La policía:

1. Contribuye al establecimiento de la imagen de la situación basándose en datos de los servicios de inteligencia y participa en la evaluación de la amenaza de bomba;

2. Actúa como punto de contacto único (SPOC) para la transmisión de información en tiempo real entre ADA-RU y la fuerza policial responsable en el aeropuerto que recibe la amenaza;

3. Establece una respuesta eficaz y flexible de la policía, que sea apropiada para la amenaza o incidente; y

4. Investiga los crímenes.

El organismo de imposición de la ley utiliza una sala de reserva como despacho de guardia para recibir llamadas y proporcionar a ADA-RU toda información sobre un incidente en el aire relacionado con la seguridad, del que la policía se haya enterado.

La sala de reserva sirve también de SPOC para las fuerzas policiales que reciban llamadas mediante teléfonos móviles de pasajeros o tripulantes a bordo de una aeronave en situación “Renegade” o de parientes de los pasajeros que estén en tierra y comuniquen tal información. Dichas llamadas, que podrían contener datos o información vitales, se retransmiten a ADA-RU para facilitar la evaluación del incidente en curso.

A medida que avanza el suceso, ATC civil, ATC militar y ADA-RU coordinarán sus acciones y, cuando la autoridad competente adopte decisiones, implantarán todas las directrices operacionales. ADA mantendrá enlace con los organismos civiles y de imposición de la ley y estos seguirán proporcionando datos e información, a medida que los obtengan, para facilitar la toma de decisiones por ADA.

Si se necesita o debe comunicarse información específica sobre un suceso, los organismos de seguridad civil podrían comunicarse con los explotadores de aeronaves por intermedio de los centros de operaciones o personal pertinente (p. ej., evaluadores de amenazas). Podrían utilizarse dichos canales al tratar de determinar la seguridad e integridad del puesto de pilotaje o el carácter o grado de la amenaza planteada a una aeronave o por esta última. Este canal de comunicación es vital para determinar el carácter y alcance de la amenaza.

Por consiguiente, es indispensable que el explotador de aeronaves proporcione a los organismos de seguridad civil un número de contacto permanente (24/7) para su centro de operaciones de manera que el personal pueda comunicarse inmediatamente con a) la línea aérea cuando trate de informar acerca de la pérdida de comunicaciones y solicitar medidas al respecto y b) un asesor de amenazas capacitado que pueda asistir a los organismos gubernamentales del RU para responder adecuada y oportunamente a la situación a medida que progrese.

Si se carece de un evaluador de amenazas capacitado o de un punto de contacto en el centro de operaciones, se limita considerablemente la capacidad de una línea aérea de participar en lo que podría constituir un mecanismo dinámico y en mutación de toma de decisiones o contribuir al mismo.

Los centros de operaciones de las líneas aéreas y los evaluadores de amenazas que tengan que comunicar o recibir información oportuna para contribuir a la gestión efectiva de una situación de crisis deberían tener una lista preparada de números de teléfono e información de contacto con los organismos de seguridad civil disponible.

Medidas tomadas por la autoridad de defensa aérea (y organismos asociados) del RU

Cuando se le notifique un posible incidente o amenaza en vuelo, ADA-RU determina las medidas iniciales que deben tomarse para garantizar la seguridad del espacio aéreo del RU. Antes de formular una declaración oficial sobre un incidente relacionado con la seguridad, ADA-RU podría adoptar ciertas medidas para preparar las fuerzas de defensa aérea. Esto podría incluir órdenes a las aeronaves QRA respecto a un estado más elevado de preparación o el envío de aeronaves QRA para interceptar la aeronave relacionada con el incidente.

Una vez notificado por ADA-RU, el organismo de seguridad civil hará todo lo posible para comunicarse con el centro de operaciones de la línea aérea o el evaluador de amenazas. También tratará de obtener la ayuda de ambos para asegurarse de que toda respuesta de los organismos gubernamentales del RU sea oportuna, adecuada y efectiva. Es indispensable que el personal de la línea aérea entienda que esto constituye una oportunidad clave para influenciar o servir de base para el mecanismo de toma de decisiones, permitiendo así que ATC restablezca las comunicaciones con la aeronave o evalúe la amenaza. La falta de disponibilidad o de respuesta oportuna podría limitar las opciones al alcance del gobierno del RU al considerar la mejor manera de responder a una situación en rápida mutación y dinámica.

Cuando ADA-RU inicia el lanzamiento de aeronaves QRA, el supervisor militar en los centros de control de tránsito aéreo (ATCC) apropiados se comunicará por teléfono con las autoridades de seguridad civil. Se iniciará el plan de notificación de la policía y se pondrá al supervisor militar en enlace con el centro de control de la fuerza de la policía responsable del aeropuerto donde aterrizará la aeronave.

Este método de suministro de información en tiempo real facilita la respuesta en tierra por la policía y permite la reevaluación continua de la amenaza (en particular por el evaluador de la línea aérea) a fin de que la fuerza en el punto de destino aplique la respuesta más apropiada y proporcionada de la policía. El objetivo de dicha respuesta consiste en proteger vidas humanas, reducir las lesiones a lo mínimo, asegurar un rápido retorno a la situación normal y conservar las pruebas.

Si ADA-RU ordena la interceptación de una aeronave civil, las aeronaves QRA se le acercarán por el lado izquierdo tratando de establecer contacto con el puesto de pilotaje mediante radiocomunicaciones VHF; las aeronaves militares transmitirán simultáneamente en 121,5 MHz, además de las frecuencias ATC normalizadas.

Las comunicaciones vocales con el puesto de pilotaje y el cumplimiento o incumplimiento de las señales de interceptación permitirán a ADA-RU determinar la intención de las personas que controlan la aeronave. Las conclusiones de ADA-RU se comunicarán al gobierno de este último, que determinará las medidas adicionales que deberían tomarse. Dichas medidas podrían dar lugar a la desviación de la aeronave hacia un puerto de alternativa que no será el aeropuerto de destino previsto.

Falsas alarmas

Siguen generándose periódicamente falsas alarmas que, en la mayoría de los casos, se deben a lo siguiente:

1. Aeronaves civiles que efectúan operaciones de vuelo controlado que no mantengan

una escucha continua en la radiofrecuencia apropiada de la dependencia ATC correspondiente ni establecen comunicaciones bidireccionales con la misma, según corresponda, al aproximarse o entrar en el espacio aéreo del RU; o

2. Con menor frecuencia, amenazas de bomba formuladas contra aeronaves en vuelo cuando no puede establecerse contacto con evaluadores de amenazas capacitados de la línea aérea o cuando estos no puedan contribuir a la comprensión o codificación del carácter y gravedad de la amenaza.

Los colegas de la OTAN u otros organismos ATC alertarán también a ADA-RU o a los organismos ATC de este último si una aeronave, que esté a punto de aterrizar o sobrevolar el RU, pierde las comunicaciones durante un largo período o afronta una posible situación de amenaza. Esto puede activar las medidas de ADA-RU descritas en las secciones anteriores. Así, una pérdida de comunicaciones, combinada con la desviación de la aeronave respecto a su plan de vuelo, probablemente activará el lanzamiento inmediato de aeronaves QRA, lo que podría dar lugar a la interceptación y desviación de la aeronave.

ADA-RU podría tratar de comunicarse con el comandante de cualquier aeronave que haya activado una alerta (independientemente de las medidas tomadas posteriormente) después del aterrizaje. Podrían solicitarse otras medidas, por intermedio de las autoridades nacionales competentes, si se sospecha negligencia o no se explica la pérdida de comunicaciones. La incapacidad de una línea aérea de contribuir a la comprensión de la amenaza por el gobierno del RU de manera oportuna, p. ej., manteniendo disponible a un asesor de amenazas capacitado, podría incitar al gobierno del RU a solicitar una aclaración de la capacidad de la línea aérea en materia de planificación de contingencia.

Se reconoce que seguirán produciéndose falsas alarmas debido a errores de los operadores o fallas de comunicaciones basadas en tierra o en RTF. No obstante, debe tenerse en cuenta que desperdician los recursos de la industria y el gobierno del RU y pueden plantear un peligro para las personas a bordo y el RU de manera más general.

El organismo de seguridad del gobierno del RU solicitará una explicación de las falsas alarmas, particularmente las que hayan ocasionado el lanzamiento de aeronaves QRA y podría solicitar una copia del informe interno sobre el incidente y los pormenores de las medidas correctivas adoptadas para evitar que se repita. En colaboración con la Asociación de pilotos de líneas aéreas británicas, se ha elaborado un formulario de notificación que los pilotos que hayan tenido incidentes COMLOSS pueden llenar para facilitar toda investigación subsiguiente.

Dominio de la situación

Como parte de la reacción a situaciones relacionadas con la seguridad en el aire, podrían tomarse decisiones relativas a rutas, perfil de vuelo y destino (incluida la posible espera en el aire) fuera de los arreglos normales del explotador de aeronaves o piloto al mando. Si ATC o ADA-RU consideran justificado preguntarse si la comunicación desde el puesto de pilotaje se está haciendo bajo coacción, podrían darse instrucciones a la aeronave para que efectúe determinadas maniobras. Es indispensable seguir las instrucciones comunicadas por ATC o por medio de señales normalizadas de los procedimientos de interceptación de la OACI.

Cabe señalar que ciertas categorías de información podrían ocultarse al piloto al mando durante sucesos semejantes y que las autoridades competentes del RU podrían no aprobar ciertas solicitudes formuladas por el explotador de aeronaves o el piloto al mando.

Como parte de la respuesta, podría encargarse a ATC que aplique medidas para alejar el tráfico del espacio aéreo. Estas medidas podrían afectar a otras aeronaves en las cercanías, incluso en tierra; además, podrían suspenderse los planes de vuelo vigentes. ATC podría exigir la desviación hacia aeropuertos de alternativa o retirar autorizaciones. Durante tales períodos, la seguridad de vuelo de todas las aeronaves seguirá siendo de suma importancia y, por ello, podría otorgarse a las aeronaves autorizaciones ATC no normalizadas.

El alcance, secuencia y prioridad de toda restricción temporal en el espacio aéreo y los vuelos quedará a discreción del supervisor del ACC responsable, que coordinará sus medidas con las autoridades de defensa civil competentes. Se otorgará prioridad a alejar al tráfico de todo espacio aéreo reglamentado por el que se prevé que avance la aeronave del caso. El supervisor del ACC responsable actuará como coordinador global del procedimiento necesario de evacuación del espacio aéreo y aplicará métodos como los siguientes:

1. Cancelar todas las autorizaciones de ATC pertinentes en el espacio aéreo que probablemente quedaría afectado por el incidente;

2. Aplicar medidas de gestión de afluencia del tránsito aéreo (ATFM);

3. Coordinar las medidas con las dependencias ATC adyacentes, prestando particular atención a los efectos en las operaciones aeroportuarias (p. Ej., cese de la espera en el aire, desviaciones, etc.), así como la capacidad de dichas dependencias para participar en la transferencia del tránsito en el caso de sectores afectados;

4. Modificar temporalmente las rutas de las aeronaves para evitar la aeronave sospechosa y su avance;

5. Cancelar o enmendar los arreglos de coordinación de ATC; y

De ser necesario, DFT podría ordenar el cierre del espacio aéreo del RU exigiéndose para ello que todas las aeronaves cumplan las instrucciones dadas por ATC.

Puntos fundamentales para pilotos, explotadores de aeronaves y evaluadores de amenazas

Para evitar un incidente, los pilotos, explotadores de aeronaves y evaluadores de amenazas deberían asegurarse de que:

1. Las comunicaciones con ATC se mantengan sin interrupción;

2. Los organismos de seguridad civil tengan información de contacto permanente (24/7) con el centro de operaciones de la línea aérea; y

3. Un evaluador de amenazas capacitado esté en servicio de manera permanente.

Para asegurarse de la gestión más apropiada de todo incidente, el gobierno del RU aconseja a los pilotos y explotadores de aeronaves que:

1. Estén atentos a situaciones posibles, tales como pérdida de comunicaciones bidireccionales o selección accidental del código 7500 en Modo 3/A, que podrían indicar una posible alerta de seguridad para ATC, y tomen todas las precauciones necesarias para evitar que esto suceda;

2. Comuniquen claramente a todas las partes cuando, a juicio del piloto, exista una amenaza real o supuesta relacionada con la seguridad de la aeronave o el RU;

3. Establezcan contacto con el centro de operaciones de la línea aérea, lo antes posible, para asegurarse de que se intercambie toda la información pertinente de manera oportuna, comunicándose, de ser necesario, con un asesor de amenazas capacitado de la línea aérea;

4. Comuniquen voluntariamente información sobre integridad del puesto de pilotaje y carácter exacto de la amenaza o problema a ATC y al centro de operaciones de la línea aérea, de manera oportuna, clara y concisa;

5. Utilicen fraseología RTF apropiada y códigos de objetivo especial en Modo 3/A de SSR; y

6. Cumplan las instrucciones gubernamentales comunicadas por radiotelefonía o mediante señales visuales de interceptación.

Recuperación de la situación

No se reanudarán las operaciones ATC normales hasta que así lo autorice la autoridad competente. ATSP podría ocuparse de las medidas de recuperación subsiguientes necesarias para el sistema ATC global.
Notificación de incidentes de pérdida de comunicaciones en vuelo

ATC civil y ATC militar del RU vigilan constantemente las comunicaciones previstas entre ATC y una aeronave en vuelo. La pérdida de comunicaciones constituye un ejemplo posible de conducta sospechosa que podría indicar un posible incidente en vuelo relacionado con la seguridad. El formulario del Informe sobre incidentes de pérdida de comunicaciones en vuelo, del RU, permite a las tripulaciones de vuelo notificar tales incidentes de modo que a) se registre información correcta sobre los pormenores exactos del incidente, y b) puedan tomarse las medidas necesarias para reducir la posibilidad de una repetición.

En el formulario figuran elementos relativos a los datos siguientes:

1. Fecha
2. Hora UTC
3. Explotador (línea aérea)
4. Número de vuelo
5. Distintivo de llamada de la aeronave (si es diferente)
6. Aeropuerto de salida y destino
7. Código squawk/SSR en Modo 3/A
8. Tipo de aeronave
9. Matrícula/marca de matrícula
10. Altitud (en el momento del incidente): FL/ft
11. Velocidad (en el momento del incidente): Mach, número de millas marinas
12. Fase de vuelo
13. Emplazamiento
14. Ruta
15. Condiciones meteorológicas
16. Frecuencia en el canal (mhz)
17. Controlado por (sector ATC)
18. Descripción del incidente
19. Causas: a) error del piloto; b) error de transferencia de ATC; c) problemas técnicos; d)

cualquier otra causa - se ruega especificar:

20. ¿Trató ATC la retransmisión de aeronave a aeronave? - resultados obtenidos (de ser el caso):
21. ¿Se trató de establecer comunicaciones de tierra a aeronave en 121,5 mhz?
22. ¿Se han tratado otros métodos de comunicación [sistema de direccionamiento e informe para comunicaciones de aeronaves (ACARS), satélite, frecuencia de la empresa, etc.]?
23. Toda información pertinente
24. Información para contacto (nombre y apellido, teléfono o dirección de correo-e).

## 53.2 PROCEDIMIENTOS DE LA RED DE SUCESOS EN EL TERRITORIO NACIONAL DE LOS ESTADOS UNIDOS

Los Estados Unidos han elaborado procedimientos para la coordinación y gestión de sucesos relacionados con la seguridad de ATM en su espacio aéreo mediante la Red de sucesos en el territorio nacional (DEN). En la presente sección figura una reseña de dichos procedimientos.

En la mañana del 11 de septiembre de 2001, se estableció una conferencia telefónica entre varias instalaciones ATC de la Administración Federal de Aviación (FAA), el Centro de mando del sistema de control de tránsito aéreo (ATCSCC) de la FAA y el Sector de defensa aérea del Nordeste (NEADS) para coordinar la información sobre las aeronaves secuestradas. Dicha conferencia original, iniciada para coordinar la seguridad del Sistema del espacio aéreo nacional (NAS), se ha convertido en lo que ahora se llama DEN y constituye actualmente la principal red de coordinación de la seguridad de ATM en los Estados Unidos.

DEN es una conferencia telefónica entre organismos, permanente (24/7) y no clasificada, utilizada por Seguridad de las operaciones del sistema, de la FAA, para coordinar en tiempo real sucesos relacionados con la seguridad en el sistema ATM de los Estados Unidos. La información se comparte mediante DEN, de modo que todos los organismos pertinentes a nivel federal, estatal, tribal y local puedan juntarse para analizar posibles incidentes relacionados con la seguridad y establecer una respuesta de colaboración entre organismos para la gestión de sucesos.

La FAA fue creada en 1958 a fin de servir de punto central para la aviación en los Estados Unidos. La Ley sobre seguridad del territorio nacional de 2002, la Ley sobre seguridad de la aviación y el transporte de 2001 y la creación del Departamento de seguridad del territorio nacional (DHS) y de la Administración de seguridad del transporte (TSA) no modificaron la función de la FAA. Esta sigue siendo la única autoridad en materia de gestión del espacio aéreo, la reglamentación del tránsito aéreo y el uso del espacio aéreo. TSA colabora estrechamente con la FAA, la consulta y coordina sus operaciones con ella, según corresponda, respecto a todas las cuestiones relacionadas con la seguridad de la aviación.

En circunstancias que podrían afectar a la defensa nacional, el Administrador de la FAA de común acuerdo con el Secretario de Defensa – decide establecer zonas en el espacio aéreo que son necesarias para la defensa nacional. En los estatutos se dispone explícitamente la transferencia de una función, poder, actividad o instalación de la FAA al sector militar en caso de guerra. No existe ninguna otra disposición relativa al traslado de cualquier función, poder, actividad o instalación de la FAA a otro organismo o entidad gubernamental.

La utilización de DEN permite reconocer y preservar las funciones y conocimientos

respectivos del Departamento de defensa (DOD), TSA, FAA y organismos de imposición de la ley. DEN permite coordinar las medidas y actividades más eficaces de suministro de servicios de seguridad de ATM para seguridad nacional, seguridad de la aviación e imposición de la ley.

DEN es un entorno abierto de tipo foro y la comunicación debe ser bidireccional para ser eficaz. Todas las instalaciones ATC de la FAA y más de 60 otros organismos y entidades participan en DEN. Mientras algunas instalaciones, organismos y entidades no participan necesariamente el 100% del tiempo, deben responder a las cuestiones y proporcionar información cuando se les solicite.

El personal de ATC comunica información relacionada con la seguridad de ATM por medio de DEN, de conformidad con los protocolos de la FAA. La información que se comunica incluye, entre otras cosas:

1. Aeronaves en situación de secuestro;
2. Informes sobre pasajeros insubordinados o interferencia con miembros de la tripulación;
3. Aeronaves con transpondedor inutilizable cerca de la zona de reglas de vuelo especiales (SFRA) de Washington, D.C.;
4. Comunicaciones de aeronave pérdidas o no establecidas (NORDO);
5. Una aeronave atraviesa una zona de identificación de defensa aérea (ADIZ) costera y no aterriza en el aeropuerto de entrada;
6. Actividades incoherentes o anormales de la aeronave;
7. La aeronave se desvía de la ruta de vuelo y no regresa a la misma cuando así se le pide;
8. Toda situación que pueda indicar una actividad sospechosa de la aeronave o una amenaza a aeronaves o instalaciones ATC;
9. Información relativa a objetos sospechosos (TOI);
10. Incidentes relacionados con rayos láser y otros incidentes de tierra a aire que afectan a las aeronaves;
11. Informes sobre posibles enfermedades transmisibles y otros riesgos para la salud pública a bordo de aeronaves; y
12. Información sobre la situación de una instalación ATC.
13. Otros organismos deben comunicar a DEN información sobre:
14. Penetración no identificada en Washington, D.C., SFRA y ADIZ costera;
15. Informes sobre pasajeros insubordinados o interferencia con miembros de la tripulación;
16. Pasajeros sin derecho de viajar a bordo de aeronaves que se acercan a los Estados Unidos;
17. Información no clasificada relacionada con la seguridad de NAS;
18. Incidentes o accidentes de aeronaves (aeronaves que no reciban servicios ATC);
19. Amenazas de bomba;
20. Interceptación de aeronaves sospechosas con equipo de DOD y DHS;
21. Incidentes relacionados con la seguridad en los aeropuertos (incluidos los relativos a rayos láser e incidentes de tierra a aire que afectan a las aeronaves);
22. Informes sobre aeronaves que merodean en las cercanías de instalaciones sensibles, p. Ej., centrales nucleares; y
23. Informes sobre una enfermedad transmisible u otro riesgo para la salud pública a bordo de una aeronave.

Además de los elementos mencionados, los organismos deben informar a DEN al adoptar una medida a raíz de información recibida por su intermedio.

Coordinadores de la seguridad del tránsito aéreo (ATSC), Seguridad de las operaciones del sistema, de la FAA

Sede de la FAA
Se ha delegado en los ATSC, en la Sede de la FAA, la autoridad de dirigir y establecer coordinación con todas las instalaciones de tránsito aéreo y las oficinas regionales para garantizar la seguridad operacional y la protección del sistema. Para ello, los ATSC facilitan la interacción de las instalaciones de tránsito aéreo con los numerosos organismos gubernamentales que consultan los datos de DEN.

Los ATSC cuentan con numerosos años de experiencia aeronáutica, incluso en ATC militar y civil. Todos los ATSC han sido controladores de tránsito aéreo en la FAA o instalaciones militares. Muchos de ellos tienen experiencia como supervisores de una instalación de la FAA o como administradores de una instalación o comandantes militares.

Región de los Estados Unidos continentales (CONR)
Se asigna a ATSC de la FAA a fin de que trabajen en CONR para facilitar las operaciones de DEN y mantener coordinación directa con los oficiales de mando de combate.

Centro de coordinación de la región de la Capital Nacional (NCRCC)
La misión principal del NCRCC consiste en facilitar una rápida coordinación e intercambio de información entre los organismos participantes que protegen la región de la Capital Nacional (NCR), Washington, D.C. Los ATSC desempeñan funciones de seguridad de ATM que permiten a dichos organismos ejercer sus propias responsabilidades de seguridad del aire o de defensa para la prevención, disuasión o, de ser necesario, interdicción de amenazas aéreas a la NCR.

Mando de la defensa aeroespacial norteamericana (NORAD)
Se asigna a ATSC de la FAA a fin de que trabajen en NORAD para facilitar las operaciones DEN y mantener coordinación directa con los directores del mando.

Instalaciones ATC de la FAA
El sistema ATC de los Estados Unidos es una amplia red de personas y equipo que garantiza la operación segura y protegida de las aeronaves comerciales, militares y privadas. Los controladores de tránsito aéreo coordinan el movimiento del tráfico aéreo para asegurarse de que los aviones mantengan distancia segura entre sí. La seguridad operacional constituye su principal responsabilidad, pero los controladores deben también dirigir las aeronaves eficientemente para minimizar las demoras y notificar a DEN todo problema relacionado con la seguridad de ATM.

Los controladores de terminal regulan el tráfico aeroportuario a través de espacio aéreo designado; otros regulan las llegadas y salidas en los aeropuertos. Después de cada salida de aeronave, los controladores de la torre del aeropuerto notifican a los controladores en ruta que luego se hacen cargo.

Existen 20 centros de control de tránsito en rutas aéreas (ARTCC) situados por todo el país, contando cada uno de ellos entre 300 y 700 controladores; más de 150 de ellos permanecen en servicio durante las horas de máxima actividad en las instalaciones de mayor intensidad de tránsito. Se asigna a cada ARTCC determinado espacio aéreo que contiene numerosas rutas diferentes. Los controladores en ruta trabajan en equipos hasta de tres miembros, según la intensidad del tránsito. Cada equipo tiene responsabilidad respecto a un sector del espacio aéreo del ARTCC.
Por ejemplo, un equipo podría tener la responsabilidad relativa a todas las aeronaves que se sitúen entre 50 y 160 km al norte de un aeropuerto y que vuelen a una altitud de 6 000 a 18 000 ft. ATCSCC de la FAA supervisa la totalidad de ATC. También administra ATC dentro de los ARTCC cuando surgen problemas (condiciones meteorológicas adversas, exceso de

tránsito y pistas inutilizables).

Los ATSC de la FAA mantienen relaciones con estas instalaciones ATC en tiempo real por intermedio de DEN respecto a todas las cuestiones de seguridad de ATM. Centro de operaciones de Washington, Sede de la FAA

El Complejo del centro de operaciones de Washington (WOCC) es la piedra angular del Sistema de mando, control y comunicaciones de la FAA. El personal de WOCC está capacitado para satisfacer todos los requisitos operacionales de la FAA. El personal está específicamente estructurado para apoyar a todos los sectores de la FAA que tienen responsabilidad operacional para responder a sucesos relacionados con: catástrofes naturales, seguridad de las instalaciones, materiales peligrosos, accidentes e incidentes de aeronave, cuestiones de certificación de aeronaves, operaciones de tránsito aéreo, transporte espacial comercial, asuntos públicos, cuestiones relacionadas con el Congreso, relaciones con la Junta nacional de seguridad del transporte (NTSB) y situaciones internacionales.

Entre las responsabilidades operacionales del WOCC, las operaciones de tránsito aéreo siempre ocupan el primer puesto en la carga de trabajo diaria. La atmósfera a raíz del 11 de septiembre de 2001 destacó aún más la necesidad de contar con una respuesta en tiempo real para el tránsito aéreo a fin de facilitar una gestión rápida y breve de las crisis. Por consiguiente, los ATC de la Sede de la FAA están de servicio todo el tiempo en el WOCC para la gestión de DEN, para facilitar respuestas rápidas al Administrador y ejecutivos superiores respecto a cuestiones de seguridad de ATM y satisfacer solicitudes operacionales. El personal de WOCC asiste a los ATSC para intercambiar información crítica, verificar a los participantes en DEN y facilitar la conexión de todos los participantes a DEN.

### 53.3 CENTRO DE GESTIÓN DE LA RESPUESTA A INCIDENTES DE ORGANIZACIÓN DEL TRÁNSITO AÉREO (ATO) (AIRMAC) DE LA SEDE DE LA FAA

Cuando lo active la Seguridad de las operaciones del sistema de tránsito aéreo, de la Sede de la FAA, AIRMAC se junta a DEN y actúa como coordinador de ATO para cuestiones de seguridad de ATM relativas a la gestión de crisis nacionales e internacionales o actividades de socorro en caso de catástrofe, que afecten a los Estados Unidos o sus intereses. Si la seguridad de ATM exige una amplia gestión del espacio aéreo, se activa la Célula de respuesta para el acceso al espacio aéreo (AARC), que funciona dentro de AIRMAC. AARC administra las operaciones en el espacio aéreo por medio de comunicaciones directas con los oficiales de enlace de la FAA encargados de la seguridad del tránsito aéreo despachados a la Agencia federal de gestión de emergencias (FEMA) y a todos los centros operacionales conjuntos establecidos para la crisis o catástrofe. Además, AIRMAC vigila la respuesta y las medidas de recuperación. Basándose en información recibida de DOD, DHS y otros organismos asociados, AIRMAC ajusta las restricciones en el espacio aéreo para garantizar la seguridad, protección y eficacia de las operaciones de respuesta y recuperación.

## 54 APROBACIÓN DEL MANUAL DEL DEPARTAMENTO DE INVENTARIOS

**Aprobado Por:**

**Nombre**: A.T.M. Mynor Xoy

**Nombre del Puesto**: Gerencia de Navegación Aérea

***Firma y Sello:***


## 55 PERSONAL QUE PARTICIPÓ EN LA COORDINACIÓN Y ELABORACIÓN DEL MANUAL

***Nombre***: A.T.M. Mynor Xoy
***Puesto***: Gerencia de Navegación Aérea

**Nombre:** A.T.M. Juan Carlos Alvarado
**Puesto:** Coordinador de la Gestión de la Seguridad Operacional SMS/ATS

***Nombre***: Carlos Alfredo Porta
***Puesto***: Asistente Administrativo (UP)

# MANUAL DE SEGURIDAD DE LA GESTIÓN DE TRÁNSITO AÉREO

## DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

Original
Este manual será revisado y actualizado cada dos (2) años o cuando se considere necesario, de acuerdo a las disposiciones de los Servicios de Navegación Aérea
Año 2018