

**Doc 9859**  
**AN/474**



# Manual de gestión de la seguridad operacional

---

Aprobado por el Secretario General  
y publicado bajo su responsabilidad

Segunda edición — 2009

Organización de Aviación Civil Internacional



**Doc 9859**  
**AN/474**



# **Manual de gestión de la seguridad operacional**

---

Aprobado por el Secretario General  
y publicado bajo su responsabilidad

Segunda edición — 2009

**Organización de Aviación Civil Internacional**

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

La información sobre pedidos y una lista completa de los agentes de ventas y librerías, pueden obtenerse en el sitio web de la OACI:  
[www.icao.int](http://www.icao.int).

*Segunda edición 2009*

**Doc 9859, *Manual de gestión de la seguridad operacional***

Núm. de pedido: 9859  
ISBN 978-92-9231-480-4

© OACI 2010

Reservados todos los derechos. No está permitida la reproducción, de ninguna parte de esta publicación, ni su tratamiento informático, ni su transmisión, de ninguna forma ni por ningún medio, sin la autorización previa y por escrito de la Organización de Aviación Civil Internacional.

## **ENMIENDAS**

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de publicaciones de la OACI*; el Catálogo y sus suplementos pueden consultarse en el sitio web de la OACI: [www.icao.int](http://www.icao.int). Las casillas en blanco facilitan la anotación de estas enmiendas.

### **REGISTRO DE ENMIENDAS Y CORRIGENDOS**

ENMIENDAS		
Núm.	Fecha	Anotada por

CORRIGENDOS		
Núm.	Fecha	Anotado por



# ÍNDICE

	<i>Página</i>
<b>ACRÓNIMOS Y ABREVIATURAS .....</b>	<b>(ix)</b>
<b>Capítulo 1. PANORAMA GENERAL DEL MANUAL .....</b>	<b>1-1</b>
1.1 Generalidades .....	1-1
1.2 Objetivos .....	1-1
1.3 Concepto .....	1-1
1.4 Contenido .....	1-1
1.5 Estructura .....	1-3
<b>Capítulo 2. CONCEPTOS BÁSICOS DE SEGURIDAD OPERACIONAL .....</b>	<b>2-1</b>
2.1 Objetivo y contenido .....	2-1
2.2 El concepto de seguridad operacional .....	2-1
2.3 Evolución del pensamiento sobre seguridad operacional .....	2-2
2.4 Causalidad de los accidentes — El modelo de Reason .....	2-5
2.5 El accidente de organización .....	2-7
2.6 Las personas, el contexto y la seguridad operacional — El modelo Shel .....	2-9
2.7 Errores y violaciones .....	2-16
2.8 Cultura de organización (corporativa) .....	2-25
2.9 Investigación de seguridad operacional .....	2-33
<b>Capítulo 3. INTRODUCCIÓN A LA GESTIÓN DE LA SEGURIDAD OPERACIONAL .....</b>	<b>3-1</b>
3.1 Objetivo y contenido .....	3-1
3.2 El estereotipo de la seguridad operacional .....	3-1
3.3 El dilema gerencial .....	3-2
3.4 Necesidad de la gestión de la seguridad operacional .....	3-5
3.5 Estrategias para la gestión de la seguridad operacional .....	3-10
3.6 El imperativo de cambio .....	3-14
3.7 Gestión de la seguridad operacional — Ocho pilares básicos .....	3-15
3.8 Cuatro responsabilidades para gestionar la seguridad operacional .....	3-16
<b>Capítulo 4. PELIGROS .....</b>	<b>4-1</b>
4.1 Objetivo y contenido .....	4-1
4.2 Peligros y consecuencias .....	4-1
4.3 Primer fundamento — Comprensión de los peligros .....	4-3
4.4 Segundo fundamento — Identificación de peligros .....	4-4
4.5 Tercer fundamento — Análisis de peligros .....	4-6
4.6 Cuarto fundamento — Documentación de los peligros .....	4-8

	<i>Página</i>
Apéndice 1 del Capítulo 4. Análisis de la información de seguridad operacional .....	4-AP 1-1
Apéndice 2 del Capítulo 4. Gestión de la información de seguridad operacional .....	4-AP 2-1
<b>Capítulo 5. RIESGOS DE SEGURIDAD OPERACIONAL .....</b>	<b>5-1</b>
5.1 Objetivo y contenido .....	5-1
5.2 Definición de riesgo de seguridad operacional .....	5-1
5.3 Primer fundamento — Gestión de los riesgos de seguridad operacional .....	5-3
5.4 Segundo fundamento — Probabilidad de los riesgos de seguridad operacional .....	5-6
5.5 Tercer fundamento — Gravedad de los riesgos de seguridad operacional .....	5-7
5.6 Cuarto fundamento — Tolerabilidad de los riesgos de seguridad operacional .....	5-8
5.7 Quinto fundamento — Control/mitigación de los riesgos de seguridad operacional .....	5-9
5.8 Los cinco fundamentos de la gestión de los riesgos de seguridad operacional — Resumen .....	5-15
Apéndice 1 del Capítulo 5. Plan de construcción en el Aeropuerto internacional de Acullá .....	5-AP 1-1
Apéndice 2 del Capítulo 5. Operaciones en pistas convergentes .....	5-AP 2-1
Apéndice 3 del Capítulo 5. Operaciones comerciales en el Aeropuerto internacional de Ciudad Andes .	5-AP 3-1
<b>Capítulo 6. REQUISITOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL DE LA OACI.....</b>	<b>6-1</b>
6.1 Objetivo y contenido .....	6-1
6.2 SARPS de la OACI sobre gestión de la seguridad operacional — Generalidades .....	6-1
6.3 Programa estatal de seguridad operacional (SSP) .....	6-2
6.4 Nivel aceptable de seguridad operacional (ALoS) .....	6-3
6.5 Sistema de gestión de la seguridad operacional (SMS) .....	6-11
6.6 Eficacia de la seguridad operacional del SMS .....	6-12
6.7 Responsabilidad y rendición de cuentas de la administración .....	6-15
6.8 Relación entre un SSP y un SMS .....	6-15
6.9 Cumplimiento y eficacia .....	6-18
<b>Capítulo 7. INTRODUCCIÓN A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) .....</b>	<b>7-1</b>
7.1 Objetivo y contenido .....	7-1
7.2 Conceptos introductorios .....	7-1
7.3 Características del SMS .....	7-4
7.4 Descripción del sistema .....	7-5
7.5 Análisis de las carencias .....	7-7
7.6 SMS y QMS .....	7-9
7.7 SSP/SMS y el proceso de investigación de accidentes .....	7-11
7.8 Integración de los sistemas de gestión .....	7-12
7.9 Aclaración de términos .....	7-13
7.10 Diferencia entre consignas de seguridad operacional y principios de seguridad operacional .....	7-13



	<i>Página</i>
Apéndice 1 del Capítulo 7. Orientación sobre descripción del sistema .....	7-AP 1-1
Apéndice 2 del Capítulo 7 Orientación sobre la elaboración de un análisis de carencias del SMS para proveedores de servicios .....	7-AP 2-1
<b>Capítulo 8. PLANIFICACIÓN DEL SMS .....</b>	<b>8-1</b>
8.1 Objetivo y contenido .....	8-1
8.2 Componentes y elementos del SMS .....	8-1
8.3 Marco SMS de la OACI .....	8-3
8.4 Responsabilidad y compromiso de la administración .....	8-3
8.5 Responsabilidades respecto de la seguridad operacional .....	8-6
8.6 Designación del personal clave de seguridad operacional .....	8-9
8.7 Coordinación del plan de respuesta ante emergencias .....	8-12
8.8 Documentación SMS .....	8-12
8.9 Plan de implantación del SMS .....	8-13
Apéndice 1 del Capítulo 8. Marco para los sistemas de gestión de la seguridad operacional (SMS) .....	8-AP 1-1
Apéndice 2 del Capítulo 8. Ejemplo de descripción de tareas para un gerente de seguridad operacional .....	8-AP 2-1
<b>Capítulo 9. FUNCIONAMIENTO DEL SMS .....</b>	<b>9-1</b>
9.1 Objetivo y contenido .....	9-1
9.2 Gestión de riesgos de seguridad operacional — Generalidades .....	9-1
9.3 Identificación de peligros .....	9-2
9.4 Evaluación y mitigación de riesgos .....	9-3
9.5 Garantía de la seguridad operacional — Generalidades .....	9-3
9.6 Supervisión y medición de la eficacia de la seguridad operacional .....	9-5
9.7 Protección de las fuentes de información de seguridad operacional .....	9-9
9.8 Gestión del cambio .....	9-12
9.9 Mejora continua del SMS .....	9-14
9.10 Relación entre gestión de riesgos de seguridad operacional (SRM) y garantía de la seguridad operacional (SA) .....	9-15
9.11 Promoción de la seguridad operacional — Instrucción y educación .....	9-16
9.12 Promoción de la seguridad operacional — Comunicación de la seguridad operacional .....	9-18
<b>Capítulo 10. ENFOQUE EN FASES DE LA IMPLANTACIÓN DEL SMS .....</b>	<b>10-1</b>
10.1 Objetivo y contenido .....	10-1
10.2 Por qué adoptar un enfoque en fases de la implantación del SMS .....	10-1
10.3 Fase I — Planificación de la implantación del SMS .....	10-2
10.4 Fase II — Procesos reactivos de gestión de la seguridad operacional .....	10-3
10.5 Fase III — Procesos proactivos y predictivos de gestión de la seguridad operacional .....	10-4
10.6 Fase IV — Garantía de la seguridad operacional .....	10-4

	<i>Página</i>
Apéndice 1 del Capítulo 10. Orientación para la elaboración de un reglamento del Estado sobre el SMS .....	10-AP 1-1
Apéndice 2 del Capítulo 10. Orientación sobre la elaboración de un plan de implantación del SMS para proveedores de servicios .....	10-AP 2-1
<b>Capítulo 11. PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP) .....</b>	<b>11-1</b>
11.1 Objetivo y contenido .....	11-1
11.2 Componentes y elementos de un SSP .....	11-1
11.3 El marco para SSP de la OACI .....	11-3
11.4 Elaboración de un SSP .....	11-3
11.5 Implantación del SSP .....	11-5
11.6 Función del SSP en apoyo de la implantación del SMS .....	11-5
Apéndice 1 del Capítulo 11. Marco para el programa estatal de seguridad operacional (SSP) .....	11-AP 1-1
Apéndice 2 del Capítulo 11. Orientación sobre la elaboración de una declaración estatal de política de seguridad operacional .....	11-AP 2-1
Apéndice 3 del Capítulo 11. Orientación sobre la elaboración de un análisis de las carencias del programa estatal de seguridad operacional (SSP) .....	11-AP 3-1
Apéndice 4 del Capítulo 11. Orientación para la elaboración de una política de cumplimiento y procedimientos de cumplimiento del Estado en un entorno SMS .....	11-AP 4-1
Apéndice 5 del Capítulo 11. Orientación sobre la elaboración de un plan de implantación del SSP .....	11-AP 5-1
<b>Adjuntos:</b>	
A — Sistema de notificación de datos sobre accidentes/incidentes (ADREP) de la OACI .....	AD A-1
B — Plan de respuesta ante emergencias .....	AD B-1
C — Textos de orientación conexos de la OACI .....	AD C-1

# ACRÓNIMOS Y ABREVIATURAS

AAC	Administración de aviación civil
ADREP	Sistema de notificación de datos sobre accidentes/incidentes (OACI)
AEP	Plan de emergencia de aeródromo
AIRPROX	Proximidad de aeronaves (cuasi colisión)
ALARP	Tan bajo como sea razonable en la práctica
ALoS	Nivel aceptable de seguridad operacional
AMJ	Texto de consulta (JAR)
AMO	Organismo de mantenimiento reconocido
AOC	Certificado de explotador de servicios aéreos
ASDE	Equipo de detección en la superficie del aeropuerto
ASR	Informe de seguridad aérea
ATC	Control de tránsito aéreo
ATCO	Controlador de tránsito aéreo
ATM	Gestión del tránsito aéreo
ATS	Servicios de tránsito aéreo
CDA	Llegadas en descenso constante
CEO	Director general
CFIT	Impacto contra el suelo sin pérdida de control
CIP	Persona comercialmente importante
Cir	Circular
CMC	Centro de gestión de crisis
CRDA	Ayuda de presentación de pistas convergentes
CRM	Gestión de recursos de tripulación
CVR	Registrador de la voz en el puesto de pilotaje
DME	Equipo radiotelemétrico
Doc	Documento
ERP	Plan de respuesta ante emergencias
FDA	Análisis de datos de vuelo
FDM	Vigilancia de datos de vuelo
FDR	Registrador de datos de vuelo
FOD	Daño por objetos (restos, desechos) extraños
ft	Pies
GPS	Sistema mundial de determinación de la posición
ILS	Sistema de aterrizaje por instrumentos
IMC	Condiciones meteorológicas de vuelo por instrumentos
ISO	Organización Internacional de Normalización
kg	Kilogramos
LOFT	Instrucción de vuelo orientada a las líneas aéreas

---

LOSA	Auditoría de la seguridad de las operaciones de ruta
m	Metros
MDA	Altitud mínima de descenso
MEL	Lista de equipo mínimo
MOR	Informe obligatorio de sucesos
MRM	Gestión de recursos de mantenimiento
NM	Millas marinas
OJT	Instrucción en el puesto de trabajo
PC	Computadora personal
QA	Garantía de calidad
QC	Control de calidad
QMS	Sistema de gestión de la calidad
RVSM	Separación vertical mínima reducida
SA	Garantía de la seguridad operacional
SAG	Grupo de acción de seguridad operacional
SARPS	Normas y métodos recomendados (OACI)
SDCPS	Sistemas de recopilación y procesamiento de datos de seguridad operacional
SHEL	Soporte lógico/soporte físico/entorno/elemento humano
SMM	Manual de gestión de la seguridad operacional
SMS	Sistemas de gestión de la seguridad operacional
SMSM	Manual de sistemas de gestión de la seguridad operacional
SOPs	Procedimientos operacionales normalizados
SRB	Junta de control de la seguridad operacional
SRM	Gestión de riesgos de seguridad operacional
SSP	Programa estatal de seguridad operacional
TLH	Peligro de máximo nivel
TRM	Gestión de recursos de equipo
USOAP	Programa universal de auditoría de la vigilancia de la seguridad operacional (OACI)
VIP	Persona muy importante
VMC	Condiciones meteorológicas de vuelo visual
VOR	Radiofaro omnidireccional en muy alta frecuencia

---

# Capítulo 1

## PANORAMA GENERAL DEL MANUAL

### 1.1 GENERALIDADES

El presente manual está dirigido a proporcionar a los Estados orientación para elaborar el marco normativo y los textos de orientación de apoyo para la implantación de sistemas de gestión de la seguridad operacional (SMS) por los proveedores de servicios. También brinda orientación para la elaboración de un programa estatal de seguridad operacional (SSP), con arreglo a las normas y métodos recomendados internacionales (SARPS) que figuran en el Anexo 1 — *Licencias al personal*, Anexo 6 — *Operación de aeronaves*, Anexo 8 — *Aeronavegabilidad*, Anexo 11 — *Servicios de tránsito aéreo*, Anexo 13 — *Investigación de accidentes e incidentes de aviación* y Anexo 14 — *Aeródromos*.

### 1.2 OBJETIVOS

El objetivo de este manual es proporcionar a los Estados:

- a) conocimiento de los conceptos de gestión de la seguridad operacional, las normas y métodos recomendados (SARPS) de la OACI sobre gestión de la seguridad operacional que figuran en los Anexos 1, 6, 8, 11, 13 y 14, y textos de orientación conexos;
- b) orientación sobre cómo aceptar y supervisar la implantación de los componentes clave de un SMS de conformidad con los SARPS pertinentes de la OACI; y
- c) orientación sobre cómo elaborar e implantar un SSP de conformidad con los SARPS pertinentes de la OACI.

### 1.3 CONCEPTO

El concepto subyacente en este manual es el de bucle continuo (véase la Figura 1-1). El manual presenta inicialmente conceptos básicos de seguridad operacional, como fundamento para comprender la necesidad de un SMS y de un SSP. Luego el manual analiza cómo estos conceptos de seguridad operacional están abarcados en los SARPS de la OACI que figuran en los Anexos 1, 6, 8, 11, 13 y 14. A partir de allí, el manual reseña un enfoque de principios de la implantación de un SMS por los proveedores de servicios y de la implantación gradual y mantenimiento de un SSP, con énfasis en la función que desempeñan las administraciones de aviación civil en apoyar la implantación de SMS por los proveedores de servicios.

### 1.4 CONTENIDO

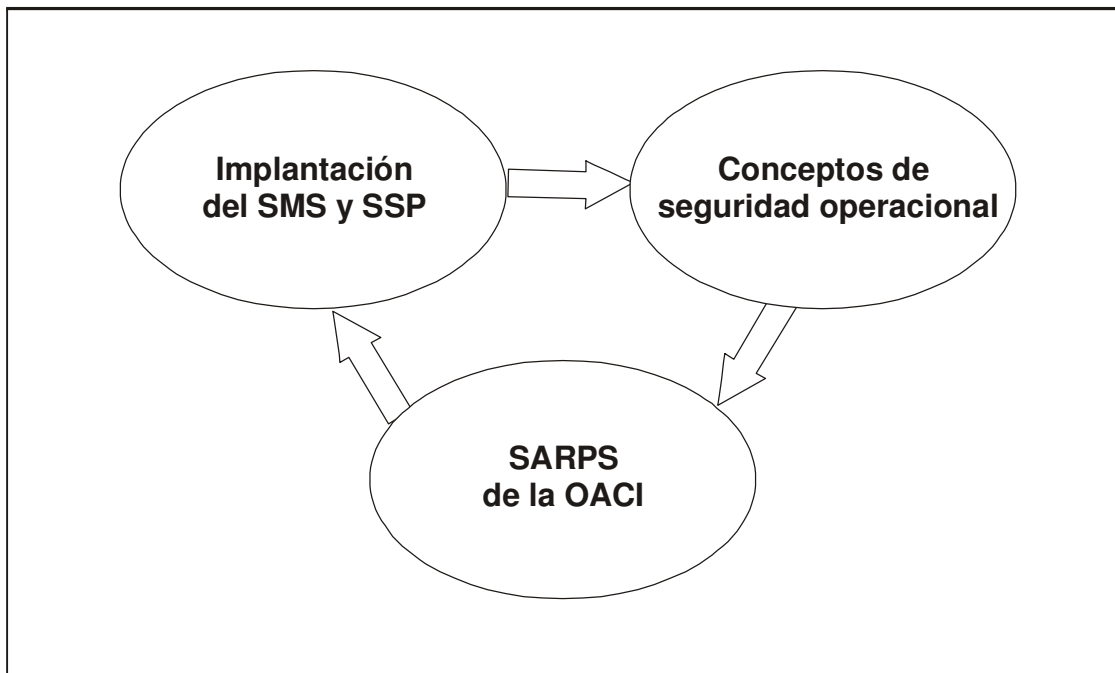
1.4.1 El manual está integrado por once capítulos, a saber:

- a) Capítulo 1 — Panorama general del manual;
- b) Capítulo 2 — Conceptos básicos de seguridad operacional;

- c) Capítulo 3 – Introducción a la gestión de la seguridad operacional;
- d) Capítulo 4 — Peligros;
- e) Capítulo 5 — Riesgos de seguridad operacional;
- f) Capítulo 6 — Requisitos de gestión de la seguridad operacional de la OACI;
- g) Capítulo 7 — Introducción a los sistemas de gestión de la seguridad operacional (SMS);
- h) Capítulo 8 — Planificación del SMS;
- i) Capítulo 9 — Funcionamiento del SMS;
- j) Capítulo 10 — Enfoque en fases de la implantación del SMS; y
- k) Capítulo 11 — Programa estatal de seguridad operacional (SSP).

1.4.2 El manual también contiene varios apéndices con ejemplos prácticos e información relacionada directamente con la implantación y mantenimiento de un SMS y un SSP. Estos apéndices se incluyen inmediatamente después del capítulo en que se trata la actividad que ellos apoyan y deberían considerarse como de conocimiento obligatorio.

1.4.3 El manual también comprende adjuntos con información útil no directamente relacionada con la implantación de SMS o SSP. Estos adjuntos figuran al final del manual y deberían considerarse como de conocimiento útil.



**Figura 1-1. Concepto de bucle continuo empleado en este manual**

## 1.5 ESTRUCTURA

1.5.1 En este manual se aplica un enfoque de construcción modular. En el Capítulo 2 se establecen los fundamentos, analizando conceptos de seguridad operacional contemporáneos. El Capítulo 3 introduce los aspectos básicos de la gestión de la seguridad operacional, con énfasis en las razones para gestionar dicha seguridad. Los Capítulos 4 y 5 introducen el marco dogmático subyacente en la gestión de riesgos para la seguridad operacional y explican sus dos conceptos básicos: peligros y riesgos para la seguridad operacional. Por último, los Capítulos 6 al 11 presentan un enfoque de principios respecto del diseño, la implantación y el mantenimiento de los procesos de gestión de la seguridad operacional utilizando el SSP y el SMS como los sistemas para gestionar la seguridad operacional dentro de los Estados y organizaciones, respectivamente. Estos capítulos también introducen la noción de gestión de la seguridad operacional como una actividad sistemática.

1.5.2 El Capítulo 11, sobre el programa estatal de seguridad operacional, se proporciona como texto de orientación provisional mientras la OACI y los Estados adquieren más experiencia sobre el desarrollo e implantación de un SSP, tras lo cual se elaborará un manual dedicado al programa estatal de seguridad operacional. Más orientación detallada sobre la elaboración e implantación de un SSP puede obtenerse del curso de capacitación en SSP de la OACI, que puede descargarse de [www.icao.int/fsix](http://www.icao.int/fsix) o [www.icao.int/anb/safetymanagement](http://www.icao.int/anb/safetymanagement).

1.5.3 Esta segunda edición del *Manual de gestión de la seguridad operacional* (Doc 9859) sustituye en su totalidad a la primera edición, publicada en 2006. También sustituye al *Manual de prevención de accidentes* (Doc 9422), que es obsoleto.

---





## Capítulo 2

# CONCEPTOS BÁSICOS DE SEGURIDAD OPERACIONAL

### 2.1 OBJETIVO Y CONTENIDO

2.1.1 En este capítulo se examinan las virtudes y defectos de los enfoques tradicionales de la seguridad operacional y se proponen nuevas perspectivas y conceptos en los que se basa un enfoque contemporáneo de la seguridad operacional.

2.1.2 El capítulo comprende los temas siguientes:

- a) El concepto de seguridad operacional;
- b) La evolución del pensamiento sobre seguridad operacional;
- c) Causalidad de los accidentes — El modelo de Reason;
- d) El accidente de organización;
- e) Las personas, el contexto y la seguridad operacional — El modelo SHELL;
- f) Errores y violaciones;
- g) Cultura de organización; y
- h) Investigaciones de seguridad operacional.

### 2.2 EL CONCEPTO DE SEGURIDAD OPERACIONAL

2.2.1 Dependiendo de la perspectiva, el concepto de seguridad operacional en la aviación puede tener connotaciones diferentes, a saber:

- a) ningún accidente o incidente grave — opinión que sostiene ampliamente el público viajero;
- b) ausencia de peligros o riesgos, es decir de aquellos factores que causan o que probablemente causen daños;
- c) actitud de los empleados de las organizaciones aeronáuticas respecto de actos y condiciones inseguras;
- d) modos de evitar errores; y
- e) cumplimiento de las normas.

2.2.2 Cualquiera sea la connotación, todas tienen un carácter subyacente común: la posibilidad del control absoluto. La ausencia de accidentes, de peligros, etc., transmite la idea de que sería posible — por diseño o intervención — tener bajo control, en los contextos operacionales de la aviación, todas las variables que puedan precipitar resultados malos o perjudiciales. No obstante, si bien la eliminación de accidentes o incidentes graves y el logro del control absoluto son ciertamente deseables, son también objetivos que no pueden lograrse en contextos operacionales abiertos y dinámicos. Los peligros son componentes integrales de los contextos operacionales aeronáuticos. En la aviación ocurrirán fallas y errores operacionales, a pesar de los mejores y más logrados esfuerzos por evitarlos. Ninguna actividad humana o sistema artificial puede garantizarse como absolutamente libre de peligros y errores operacionales.

2.2.3 Por consiguiente, la seguridad operacional es un concepto que debe comprender aspectos relativos más que absolutos, según el cual los riesgos para la seguridad operacional que surgen de las consecuencias de los peligros en contextos operacionales deben ser aceptables en un sistema inherentemente seguro. El aspecto principal sigue siendo todavía el control, pero el control relativo más que el absoluto. En la medida en que los riesgos para la seguridad operacional y los errores operacionales se mantienen bajo un grado razonable de control, un sistema tan abierto y dinámico como la aviación civil comercial se puede considerar seguro. En otras palabras, los riesgos para la seguridad operacional y los errores operacionales que se controlan a un grado razonable son aceptables en un sistema inherentemente seguro.

2.2.4 La seguridad operacional se considera cada vez más como resultado de la gestión de ciertos procesos de una organización, cuyo objetivo es mantener bajo control de la organización los riesgos para la seguridad operacional planteados por las consecuencias de los peligros en los contextos operacionales. Así pues, para los fines de este manual, se considera que la seguridad operacional tiene el significado siguiente:

**Seguridad operacional.** Estado en que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel aceptable, o por debajo del mismo, por medio de un proceso continuo de identificación de peligros y gestión de riesgos.

## 2.3 EVOLUCIÓN DEL PENSAMIENTO SOBRE SEGURIDAD OPERACIONAL

2.3.1 Durante sus primeros años, la aviación comercial fue una actividad relativamente poco reglamentada, caracterizada por tecnología precaria, ausencia de infraestructura adecuada, vigilancia limitada, comprensión insuficiente de los peligros subyacentes en las operaciones aeronáuticas y demandas de producción que no correspondían a los medios y recursos verdaderamente disponibles para satisfacerlas.

2.3.2 Es una premisa en teoría de la seguridad operacional de sistemas que los sistemas de producción que establecen objetivos de producción ambiciosos sin introducir los medios y recursos necesarios para lograrlos desarrollan un potencial de fallas frecuentes. Por consiguiente, no sorprende que los primeros días de la aviación comercial estuvieran caracterizados por una elevada frecuencia de accidentes, que la prioridad principal de los primeros procesos de seguridad operacional fuera la prevención de accidentes y que la investigación de accidentes fuera el medio principal de dicha prevención. En esos tempranos días, la investigación de accidentes, perjudicada por la ausencia de apoyo tecnológico más allá del básico, era una tarea intimidante.

2.3.3 Las mejoras tecnológicas (debidas en no pequeña medida a la investigación de accidentes), conjuntamente con el desarrollo final de una infraestructura apropiada, condujeron a una disminución gradual pero firme de la frecuencia de accidentes, así como a un impulso normativo cada vez mayor. Ya en los años 50, la aviación se estaba transformando (en términos de accidentes) en una de las industrias más seguras, pero también en una de las más estrictamente reglamentadas.

2.3.4 Esto resultó en la noción que todavía permanece de que la seguridad operacional puede garantizarse en la medida en que se sigan las reglas y que la desviación con respecto de las reglas conduce necesariamente a fallas de seguridad. Sin negar la inmensa importancia del cumplimiento de las normas, sus limitaciones como fundamento de la seguridad operacional se han venido reconociendo cada vez más, en particular a medida que aumenta la complejidad de las operaciones aeronáuticas. Es sencillamente imposible proporcionar orientación sobre todos los escenarios operacionales concebibles en un sistema operacional tan abierto y dinámico como la aviación.

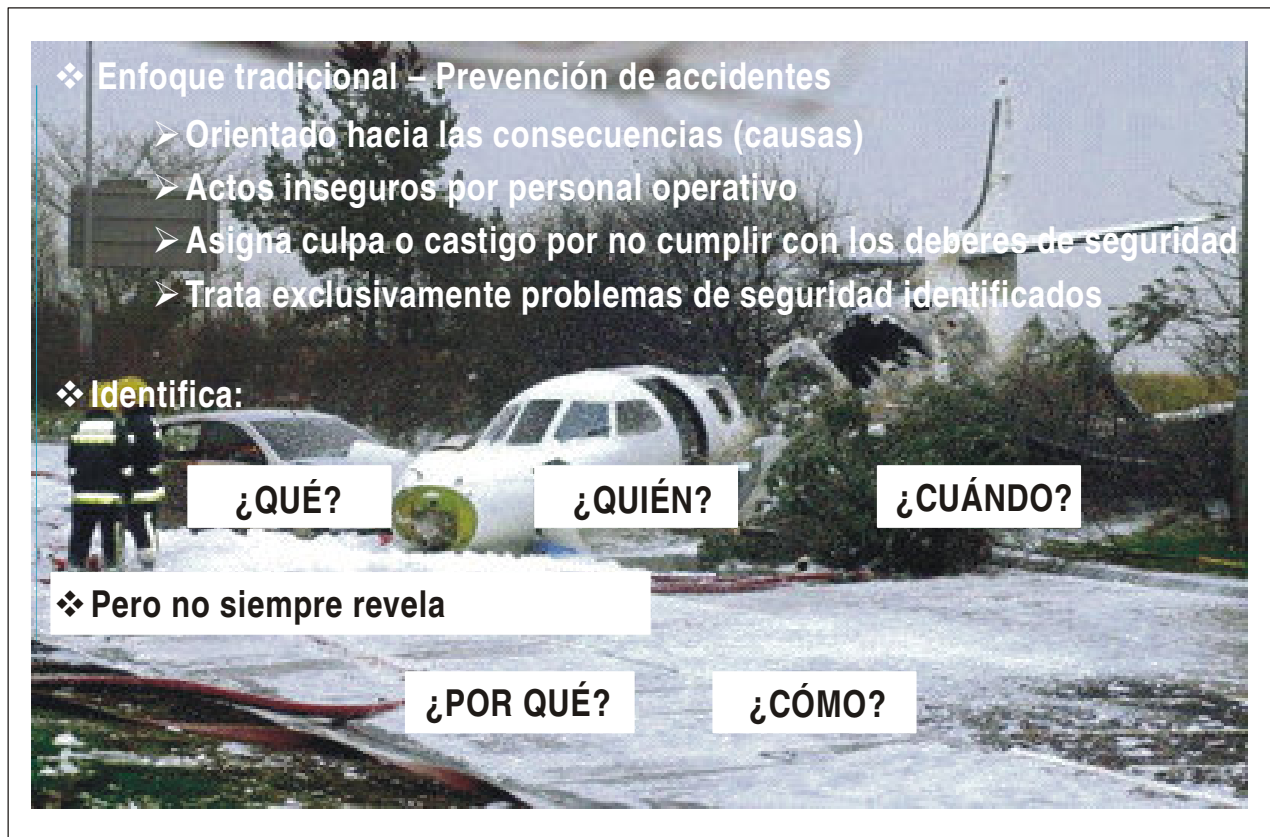
2.3.5 Los procesos son motivados por las creencias. Por lo tanto, en la creencia de que el cumplimiento de las normas era la clave de la seguridad operacional de la aviación, los primeros procesos de seguridad se ampliaron para abarcar el cumplimiento de las normas y la vigilancia. Este nuevo proceso de seguridad operacional se concentró en los resultados (es decir accidentes o incidentes de cierta magnitud) y se basaba en la investigación de accidentes para determinar las causas, incluyendo la posibilidad de fallas tecnológicas. Si estas fallas tecnológicas no eran evidentes, la atención se dirigía a la posibilidad de que el personal operacional no hubiera respetado las reglas.

2.3.6 La investigación de accidentes procuraba encontrar un punto o puntos en la cadena de sucesos en los que las personas directamente involucradas en la falla de seguridad no hubieran hecho lo que se suponía que hicieran, o hubieran hecho algo que no se suponía que hicieran, o una combinación de ambos. En ausencia de fallas tecnológicas, las investigaciones procurarían determinar actos contrarios a la seguridad por parte del personal operacional, es decir acciones u omisiones que pudieran relacionarse directamente con el resultado que se estaba investigando. Una vez que dichas acciones u omisiones se identificaban y relacionaban en retrospectiva, con la falla de seguridad, la consecuencia inevitable era la atribución de culpas en diferentes grados y matices, para castigar al culpable por no haber “cumplido con los deberes de seguridad”.

2.3.7 Un aspecto característico de este enfoque era producir recomendaciones de seguridad operacional dirigidas al problema de seguridad operacional inmediato y específico determinado como causa de la falla de seguridad, con carácter casi exclusivo. Poco hincapié se hacía en las condiciones peligrosas que, aunque presentes, no eran “causa” del suceso bajo investigación, aunque tuvieran posibilidades de perjudicar a las operaciones aeronáuticas en circunstancias distintas.

2.3.8 Si bien esta perspectiva era bastante eficaz en la determinación de “qué” sucedió, “quién” lo hizo y “cuándo” sucedió, era considerablemente menos eficaz en determinar “por qué” y “cómo” había sucedido (véase la Figura 2-1). Si bien en determinado momento era importante entender “qué”, “quién” y “cuándo”, se hizo cada vez más necesario comprender “por qué” y “cómo” para entender plenamente las fallas de seguridad operacional. En los últimos años, se ha avanzado considerablemente en el logro de esta comprensión. En retrospectiva, es evidente que las ideas sobre seguridad operacional de la aviación han experimentado una evolución considerable en los últimos cincuenta años.

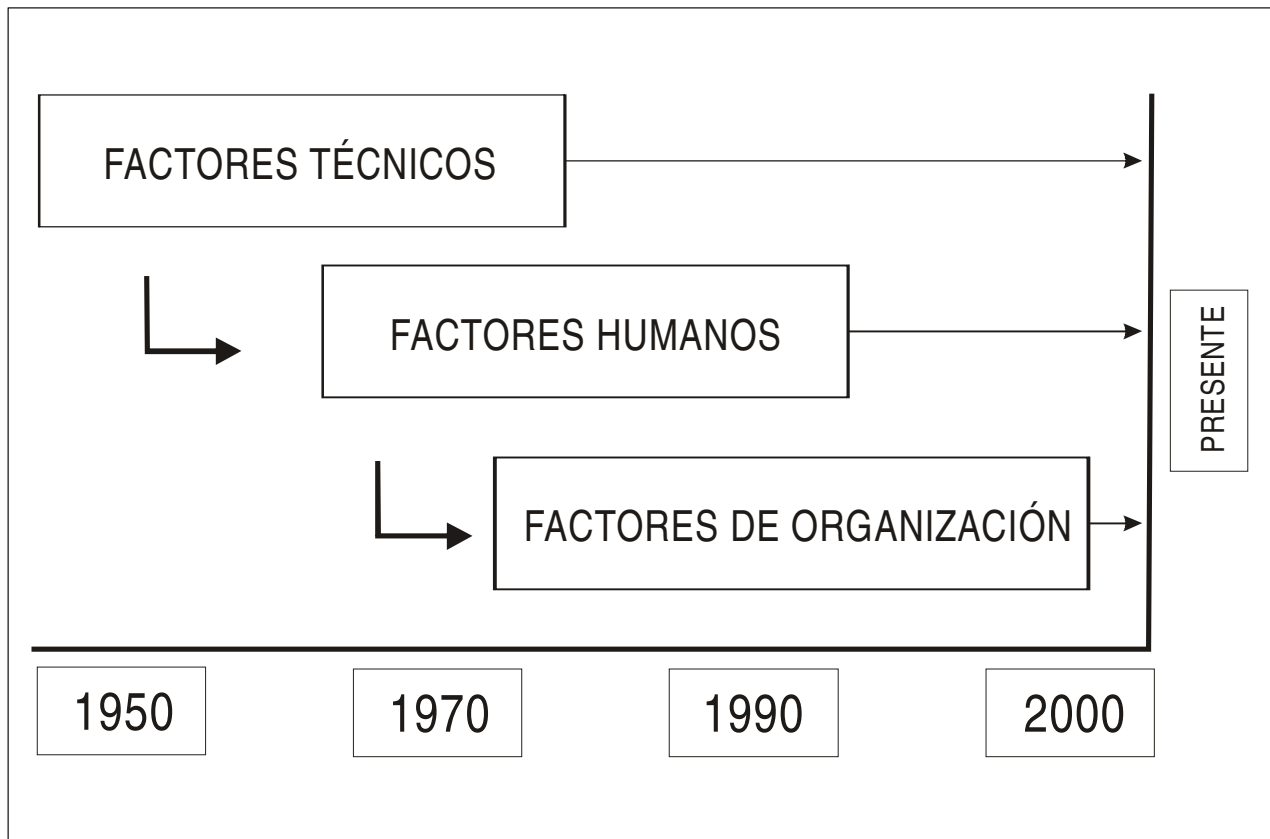
2.3.9 Los primeros días de la aviación, antes e inmediatamente después de la Segunda Guerra Mundial hasta los años 1970, pueden caracterizarse como la “era técnica” en que las preocupaciones de seguridad operacional se relacionaban principalmente con factores técnicos. La aviación estaba surgiendo como una industria del transporte de masas, pero la tecnología para apoyar sus operaciones no estaba plenamente desarrollada y las fallas tecnológicas eran el factor recurrente en las fallas de seguridad operacional. Las actividades de seguridad operacional se concentraban correctamente en la investigación y mejora de los factores técnicos.



**Figura 2-1. Enfoque tradicional — Prevención de accidentes**

2.3.10 A comienzos del decenio de 1970, se dieron importantes avances tecnológicos con la introducción de motores de reacción, radar (tanto de a bordo como terrestre), piloto automático, directores de vuelo, capacidades mejoradas de navegación y comunicaciones y tecnologías similares de ampliación de la performance, tanto en el aire como en tierra. Esto indicó el comienzo de la “era humana”, y el centro de atención de las actividades de seguridad operacional pasó a la actuación humana y a los factores humanos, con el surgimiento de la gestión de recursos de tripulación (CRM), la instrucción de vuelo orientada a las líneas aéreas (LOFT), la automatización centrada en el ser humano y otras intervenciones en materia de actuación humana. El período entre la mitad de los años 70 a la mitad de los años 90 se ha denominado “la era dorada” de los factores humanos en la aviación, en referencia a la enorme inversión de la industria para lograr el control del evasivo y ubicuo error humano. No obstante, a pesar de la masiva inversión de recursos en la mitigación de errores, para mediados de los años 90 la actuación humana seguía señalándose como el factor recurrente en las fallas de seguridad operacional (véase la Figura 2-2).

2.3.11 La carencia de las actividades de factores humanos durante una parte considerable de la “era dorada” es que tendían a concentrarse en el individuo, con muy poca atención al contexto operacional en el cual los individuos realizaban sus tareas. Sólo a comienzos de los años 90 se reconoció por primera vez que los individuos no funcionan en el vacío, sino dentro de contextos operacionales definidos. Si bien se disponía de literatura científica respecto a cómo las características de un contexto operacional pueden influir en la actuación humana y crear sucesos y resultados, no fue sino hasta los años 90 que la aviación reconoció dicho hecho. Esto señaló el comienzo de la “era de la organización” en la que la seguridad operacional comenzó a verse desde una perspectiva de sistema, para abarcar los factores de organización, humanos y técnicos. También en ese momento la aviación incorporó la noción de accidente de organización.



**Figura 2-2. Evolución del pensamiento en materia de seguridad operacional**

## 2.4 CAUSALIDAD DE LOS ACCIDENTES — EL MODELO DE REASON

2.4.1 La aceptación en toda la industria del concepto de accidente de organización fue posible gracias a un sencillo pero gráficamente poderoso modelo elaborado por el Profesor James Reason, que proporcionó un medio para comprender cómo la aviación (o cualquier otro sistema de producción) funciona con éxito o se dirige al fracaso. Con arreglo a este modelo, los accidentes se producen cuando cierto número de factores permiten que ocurran — siendo cada uno de ellos necesario pero en sí no suficiente para quebrar las defensas del sistema. Debido a que los sistemas complejos como la aviación están extremadamente bien defendidos por capas de defensas profundas, las fallas en un punto único rara vez tienen consecuencias en el sistema aeronáutico. Las fallas de equipo o los errores operacionales nunca son la causa del quiebre de las defensas de seguridad operacional, sino más bien los elementos activadores. Los quiebres de las defensas de seguridad operacional son una consecuencia tardía de decisiones tomadas a los más altos niveles del sistema, que permanecen latentes hasta que sus efectos o posibilidades perjudiciales se ven activadas por conjuntos específicos de circunstancias operacionales. En tales circunstancias específicas, las fallas humanas o las fallas activas a nivel operacional actúan de desencadenantes de las condiciones latentes que llevan a facilitar la quiebra de las defensas de seguridad operacional inherentes del sistema. En el concepto presentado por el modelo de Reason, todos los accidentes comprenden una combinación de condiciones activas y latentes.

2.4.2 Las fallas activas son acciones u omisiones, incluyendo errores y violaciones, que tienen consecuencias adversas inmediatas. En general y en retrospectiva se les considera actos inseguros. Las fallas activas se relacionan generalmente con el personal de primera línea (pilotos, controladores de tránsito aéreo, mecánicos de mantenimiento de

aeronaves, etc.) y pueden resultar en consecuencias perjudiciales. Tienen la posibilidad de penetrar las diversas defensas para proteger el sistema de aviación creadas por la administración de la empresa, las autoridades de reglamentación, etc. Las fallas activas pueden ser resultado de errores normales o de desviaciones respecto de procedimientos y prácticas prescritos. El modelo de Reason reconoce que en el lugar de trabajo hay muchas condiciones que conducen a errores o violaciones y que pueden afectar al comportamiento individual o de equipo.

2.4.3 Las fallas activas del personal operacional tienen lugar en un contexto operacional que incluye condiciones latentes. Las condiciones latentes son condiciones presentes en el sistema mucho antes de que se experimente un resultado perjudicial y que llegan a ser evidentes cuando actúan factores de activación locales. Sus consecuencias pueden permanecer latentes durante mucho tiempo. Individualmente, estas condiciones latentes generalmente no se perciben como perjudiciales, puesto que, en primer lugar, no se perciben como fallas.

2.4.4 Las condiciones latentes solo pueden llegar a ser evidentes una vez que se han quebrado las defensas del sistema. Estas condiciones son creadas generalmente por personas que están muy lejos, en tiempo y espacio, del accidente. El personal que ejecuta las operaciones hereda condiciones latentes del sistema, como las creadas por un diseño deficiente del equipo o de las tareas; objetivos incompatibles (p. ej., servicio a tiempo o bien seguridad operacional); defectos de organización (p. ej., comunicaciones internas deficientes); o malas decisiones de la administración (p. ej., postergación de una cuestión de mantenimiento). La perspectiva subyacente del tratamiento de accidentes de organización procura identificar y mitigar estas condiciones latentes en todo el sistema, en vez de realizar actividades localizadas para minimizar las fallas activas de los individuos. Las fallas activas son solo síntomas, y no causas, de los problemas de seguridad operacional.

2.4.5 Aun en las organizaciones mejor dirigidas, la mayoría de las condiciones latentes comienzan en quienes toman decisiones. Este personal directivo también está sujeto a limitaciones y predisposiciones humanas normales, así como a limitaciones de tiempo, presupuestarias y políticas. Dado que estas carencias no siempre pueden evitarse, deben adoptarse medidas para detectarlas y reducir sus consecuencias perjudiciales.

2.4.6 Las decisiones de los supervisores de la línea aérea pueden traducirse en instrucción inadecuada, programación deficiente o negligencia respecto a precauciones en el lugar de trabajo. También pueden conducir a conocimientos y competencias inadecuados o procedimientos operacionales improcedentes. La forma en que los supervisores y la organización en su totalidad desempeñan sus funciones establece las condiciones en que se produce un error o una violación. Por ejemplo: ¿cuán eficaz es la administración con respecto a establecer objetivos de trabajo realizables, organizar tareas y recursos, manejar los asuntos cotidianos y comunicar interna y externamente? Las decisiones adoptadas por la administración de la empresa y las autoridades normativas son demasiado a menudo la consecuencia de recursos inadecuados. No obstante, evitar los costos iniciales de reforzar la seguridad operacional del sistema puede allanar el camino hacia el accidente de organización.

2.4.7 En la Figura 2-3 se muestra el modelo de Reason que ayuda a comprender la interrelación de los factores de organización y de gestión (es decir, factores sistémicos) en la causalidad de los accidentes. En el sistema de la aviación hay varias defensas incorporadas para proteger contra fluctuaciones en la actuación humana o decisiones deficientes en todos los niveles del sistema (es decir, en el lugar de trabajo, en los niveles de supervisión y en la administración superior). Las defensas son recursos proporcionados por el sistema para proteger contra los riesgos para la seguridad operacional que generan y deben controlar las organizaciones involucradas en actividades de producción. Este modelo muestra que, si bien los factores de organización, incluyendo las decisiones de la administración, pueden crear condiciones latentes que podrían conducir a un quiebre en las defensas del sistema, estos factores también contribuyen a la solidez de dichas defensas.

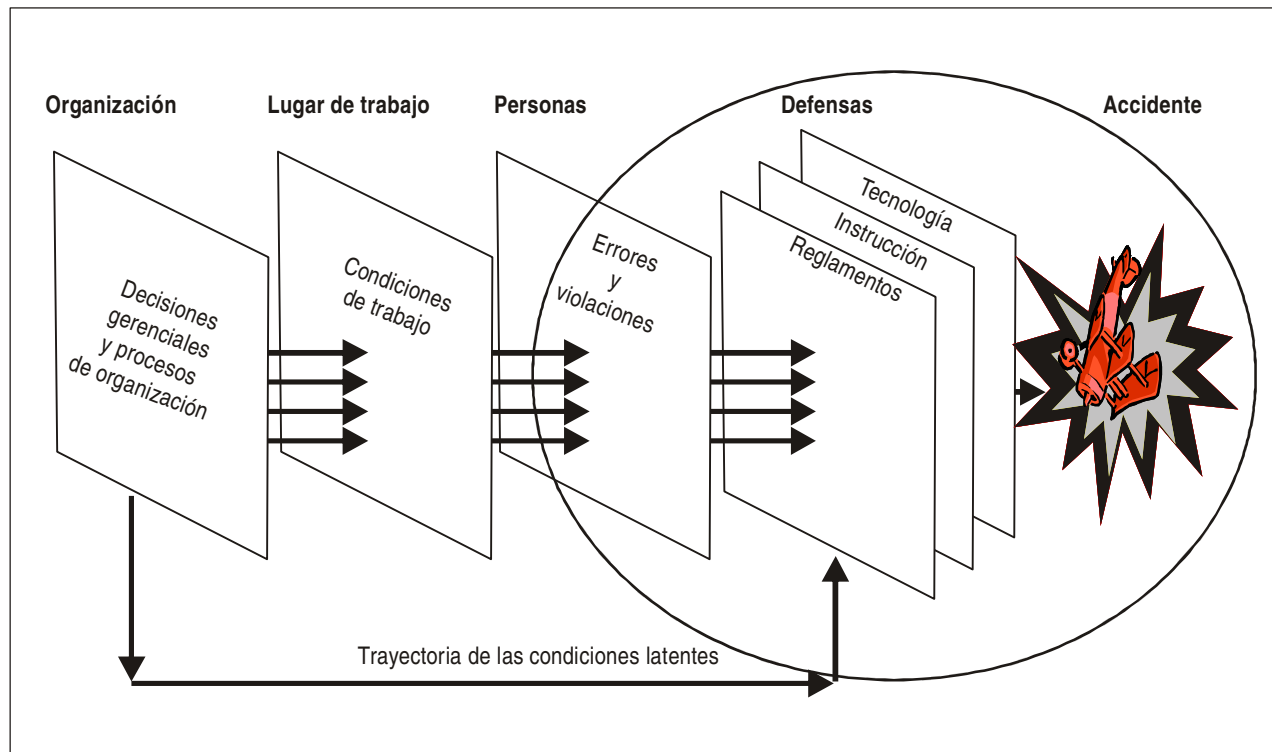


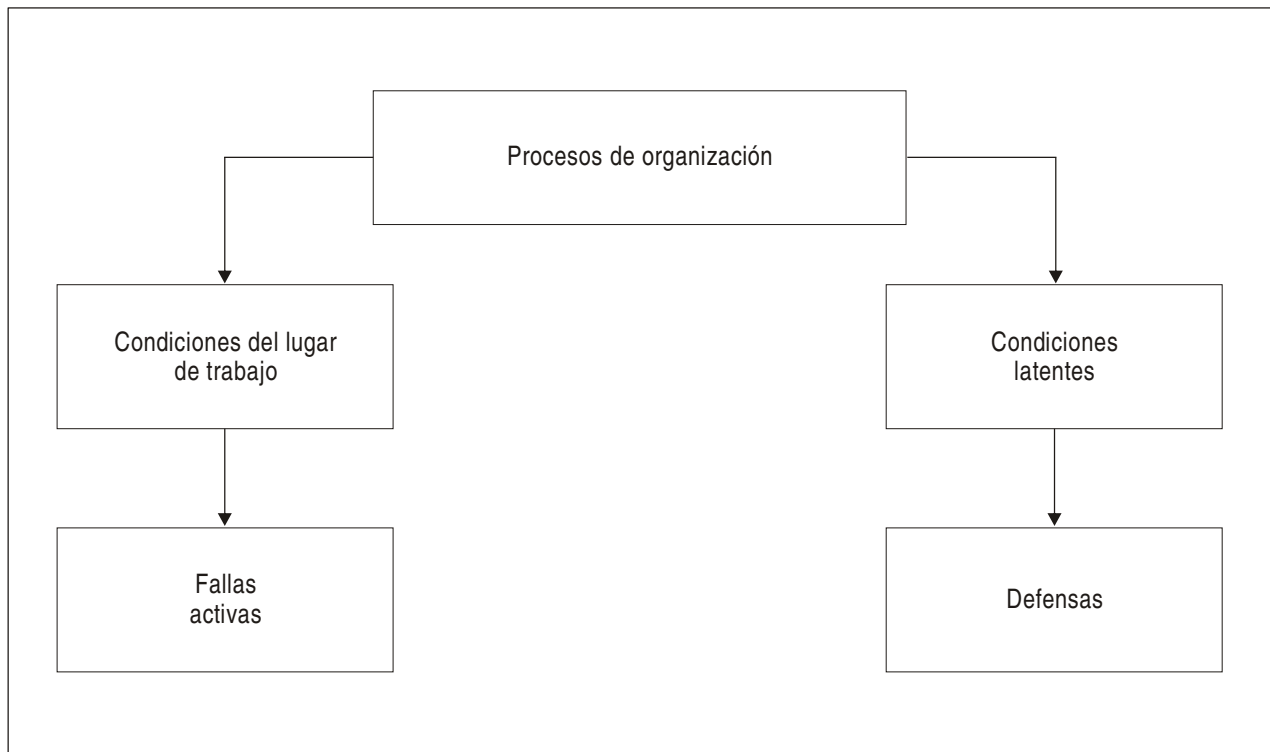
Figura 2-3. Concepto de causalidad de accidentes

## 2.5 EL ACCIDENTE DE ORGANIZACIÓN

2.5.1 La noción de accidente de organización en que se basa el modelo de Reason puede comprenderse mejor mediante un enfoque de elementos básicos integrado por cinco bloques (véase la Figura 2-4).

2.5.2 El bloque superior representa los procesos de la organización. Estos son actividades sobre las cuales cualquier organización tiene un grado razonable de control directo. Los ejemplos típicos son: formulación de políticas, planificación, comunicación, asignación de recursos, supervisión y así sucesivamente. Incuestionablemente, los dos procesos de organización fundamentales, por lo que hace a la seguridad operacional, son la asignación de recursos y la comunicación. Las carencias o deficiencias en estos procesos de organización fomentan un doble camino hacia el fracaso.

2.5.3 Un camino es el de las condiciones latentes. Entre las condiciones latentes están: deficiencias en el diseño del equipo, procedimientos operacionales normalizados incompletos o incorrectos y deficiencias en la instrucción. En términos genéricos, las condiciones latentes pueden agruparse en dos grandes conglomerados. Un grupo es la identificación de peligro y la gestión de riesgos de la seguridad operacional inadecuadas por las cuales los riesgos de seguridad operacional de las consecuencias de los peligros no se mantienen bajo control, sino que transitan libremente por el sistema hasta activarse finalmente por medio de elementos desencadenantes operacionales.



**Figura 2-4. El accidente de organización**

2.5.4 El segundo grupo se conoce como normalización de la desviación, una noción que, en términos sencillos, es indicativa de contextos operacionales en los que la excepción pasa a ser la regla. En este caso, la asignación de recursos es defectuosa al extremo. Como consecuencia de la falta de recursos, la única forma de que el personal operacional, directamente responsable de la eficacia real de las actividades de producción, puede realizar con éxito esas actividades es tomando atajos que entrañan una violación constante de reglas y procedimientos.

2.5.5 Las condiciones latentes tienen todo el potencial de quebrar las defensas del sistema de aviación. Normalmente, las defensas en aviación pueden agruparse en tres grandes rubros: tecnología, instrucción y reglamentación. Las defensas son normalmente la última red de seguridad operacional para contener a las condiciones latentes, así como a las consecuencias de lapsos en la actuación humana. La mayoría, si no la totalidad, de las estrategias de mitigación contra los riesgos de seguridad operacional de las consecuencias de los peligros se basan en el fortalecimiento de las defensas existentes o en la creación de defensas nuevas.

2.5.6 El otro camino que se origina en los procesos de organización es el camino de las condiciones en el lugar de trabajo. Estas condiciones son factores que influyen directamente en la eficacia de las personas en los lugares de trabajo de la aviación. Las condiciones en los lugares de trabajo son principalmente intuitivas en el sentido de que todas las personas con experiencia operacional las han experimentado en diversos grados, y comprenden: estabilidad laboral, calificaciones y experiencia, moral, credibilidad de la supervisión y factores ergonómicos tradicionales como la iluminación, la calefacción y el aire acondicionado.

2.5.7 Las condiciones en el lugar de trabajo inferiores al nivel óptimo fomentan las fallas activas del personal operacional. Las fallas activas pueden considerarse como errores o como violaciones. La diferencia entre ambos es el componente de motivación. Una persona que trata de hacer lo mejor posible para realizar una tarea, siguiendo las reglas



y procedimientos según la instrucción recibida, pero que no satisface el objetivo de la tarea en cuestión comete un error. Una persona que, al realizar una tarea, se desvía voluntariamente de las reglas, procedimientos o instrucción recibida comete una violación. Así pues, la diferencia básica entre errores y violaciones es la intención.

2.5.8 Desde la perspectiva del accidente de organización, las tareas de seguridad operacional deberían vigilar los procesos de organización para identificar condiciones latentes y reforzar las defensas. Estas actividades de seguridad operacional también deberían mejorar las condiciones del lugar de trabajo para contener las fallas activas, porque es la concatenación de todos estos factores lo que produce las fallas de seguridad operacional (véase la Figura 2-5).

## 2.6 LAS PERSONAS, EL CONTEXTO Y LA SEGURIDAD OPERACIONAL — EL MODELO SHEL

2.6.1 Los lugares de trabajo de la aviación son contextos operacionales complejos con múltiples componentes y características. Sus funciones y actuación involucran relaciones complejas entre sus muchos componentes para que el sistema pueda lograr sus objetivos de producción.

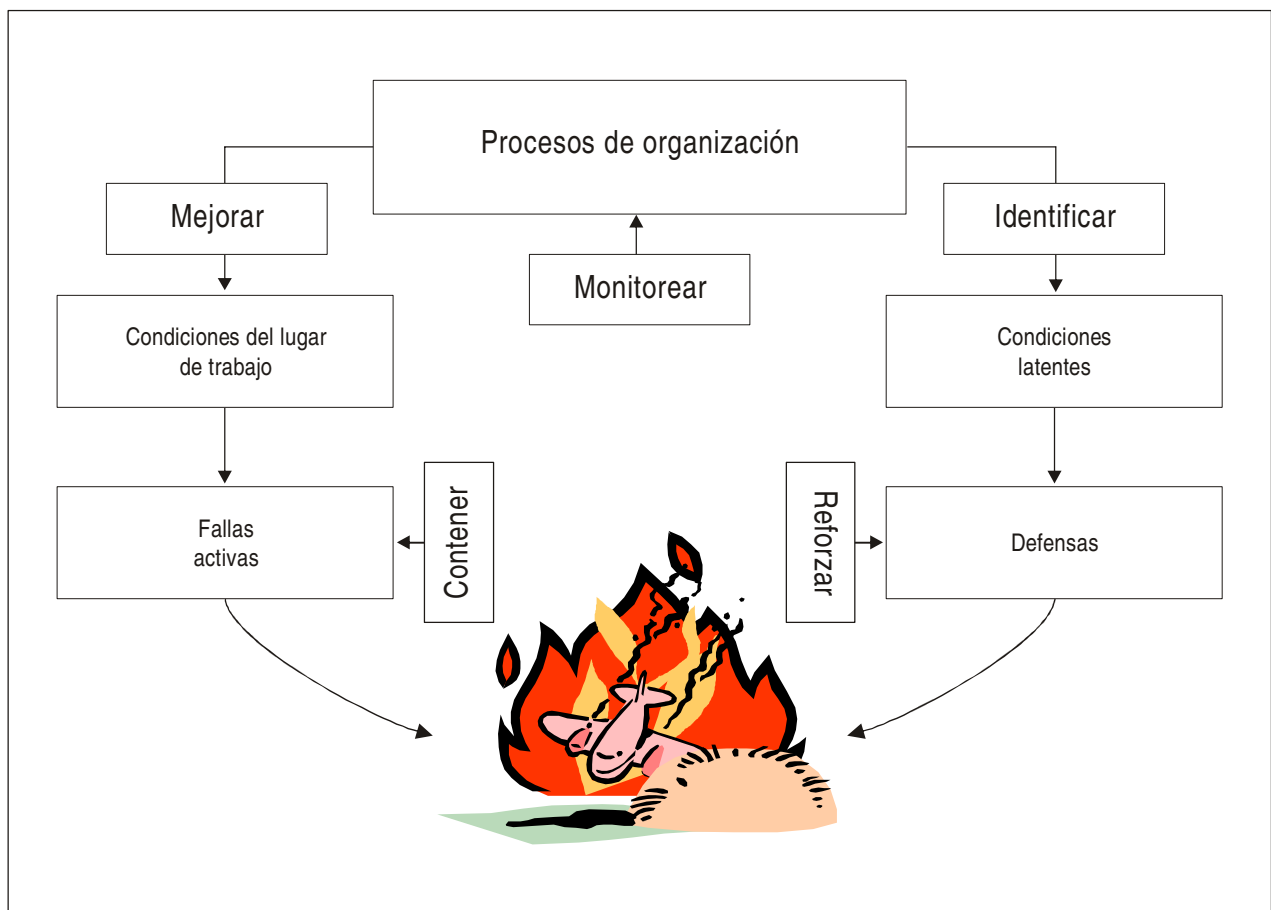


Figura 2-5. Perspectiva del accidente de organización

2.6.2 Para comprender la contribución humana a la seguridad operacional y apoyar la actuación operacional humana necesaria para lograr los objetivos de producción del sistema, es necesario comprender cómo la actuación operacional humana puede verse afectada por los diversos componentes y características del contexto operacional y las interrelaciones entre componentes, características y personas.

2.6.3 Un ejemplo muy sencillo se presenta en la Figura 2-6. El cavernícola representa el personal operacional, y la misión (u objetivo de producción del sistema) consiste en entregar paquetes al otro lado de las montañas. Los diferentes componentes y características de contexto operacional y su interacción con el cavernícola y entre sí influirán en la seguridad operacional y eficiencia de la entrega de los paquetes. Así pues, la interacción del cavernícola con los leones puede tener efectos perjudiciales para dicha entrega, a menos que el cavernícola esté adecuadamente equipado para enfrentar a los leones.

2.6.4 La travesía de las montañas por un camino probablemente ondulado y no pavimentado, sin calzado impedirá la actuación eficiente (demoras en la entrega de los paquetes) y puede conducir a heridas, planteando con ello preocupaciones de seguridad operacional. Enfrentar las posibles condiciones meteorológicas adversas sin equipo de lluvia también es una fuente de posibles deficiencias en seguridad operacional y eficacia.

2.6.5 Es evidente que la adecuada consideración y análisis del contexto operacional es una fuente de valiosa información para comprender la actuación operacional, apoyarla y mejorarla.



Fuente: Dedale

**Figura 2-6. Las personas y la seguridad operacional**

2.6.6 La necesidad de comprender la actuación operacional dentro del contexto de las operaciones en el que tiene lugar queda más ilustrado con otro ejemplo en la Figura 2-7A.

2.6.7 En este caso, el objetivo de producción del sistema es la entrega de paquetes por corredores entre los puntos A y B. Es una hipótesis básica del diseño del sistema que los corredores seguirán la ruta más corta, representada por la línea de trazo lleno.

2.6.8 No se escatiman inversiones en recursos para optimizar el sistema. Los mejores recursos humanos disponibles, en este caso los corredores, se seleccionan, entrenan, adoctrinan y equipan con el mejor calzado deportivo disponible (tecnología). Como parte del diseño del sistema, se incluye la vigilancia de las operaciones en tiempo real. Una vez completadas las etapas de diseño, se inician las operaciones. Poco después de la puesta en marcha del sistema, se inicia la vigilancia de las operaciones en tiempo real. Para gran desazón de los administradores del sistema, la vigilancia en tiempo real revela que la mayoría de los corredores no siguen el trayecto previsto, a lo largo de la línea recta, sino un trayecto en zigzag. Como consecuencia, se producen demoras en la entrega y también ocurren incidentes (véase la Figura 2-7B).

2.6.9 En este punto, los administradores del sistema tienen dos opciones. Una de ellas es seguir la perspectiva tradicional analizada en 2.3.6 — exhortar y recordar a los corredores a que hagan lo que saben y para lo que han sido entrenados y asignar culpas castigando a los corredores por no rendir según lo previsto. La otra opción consiste en analizar el contexto operacional para ver si hay componentes y características del contexto que puedan ser fuente de interacciones adversas con los corredores. Siguiendo la segunda opción, se conseguirá valiosa información sobre ciertos componentes y características del contexto (Figura 2-7C), que permitirá reajustar las hipótesis de diseño y elaborar estrategias de mitigación para los riesgos de seguridad operacional de las consecuencias de componentes y características imprevistas del contexto. En otras palabras, adquiriendo información sobre los peligros (se analiza en el Capítulo 4) en el contexto operacional y comprendiendo sus interacciones con las personas, los gestores del sistema pueden traerlo nuevamente bajo el control de la organización.

2.6.10 Por ello se propone que una adecuada comprensión de la actuación operacional y de los errores operacionales no puede lograrse sin una adecuada comprensión del contexto operacional en que tienen lugar la actuación operacional y los errores. Esta comprensión no puede lograrse a menos que se establezca una clara diferenciación entre procesos y resultados. Hay tendencia a asignar una simetría a las causas y consecuencias de los errores operacionales que, en la práctica real, no existe. El mismo error puede tener consecuencias considerablemente diferentes, dependiendo del contexto en que tiene lugar el error operacional. Las consecuencias de los errores operacionales no dependen de las personas sino del contexto (Figura 2-8). Este concepto tiene consecuencias importantes en las estrategias de mitigación: las estrategias de mitigación de errores eficaces y efectivas se dirigen a cambiar las características y componentes del contexto operacional que magnifican las consecuencias de los errores, en vez de cambiar a las personas.

2.6.11 La Figura 2-8 ilustra también un escenario en el que podrían aplicarse las dos opciones administrativas analizadas en 2.3.6. La aplicación del enfoque tradicional llevaría a producir recordatorios sobre tener cuidado al apoyarse (o no apoyarse) en alféizares de ventanas y los peligros de empujar macetas de flores hacia afuera, volver a redactar los procedimientos con arreglo a los efectos anteriores o castigos por empujar macetas de flores fuera de la ventana (no actuar según lo previsto o no actuar con seguridad). Por otra parte, el enfoque de organización llevaría a instalar una red de contención bajo la ventana, ensanchar el alféizar, utilizar macetas de flores de tipo frangible, desviar el tránsito bajo la ventana o, en circunstancias extremas, poner una cerca alrededor de ésta. El argumento básico es que eliminando o modificando las características que llevan a errores en el contexto operacional, se consigue una reducción exponencial de la probabilidad y gravedad de las consecuencias de los errores operacionales.

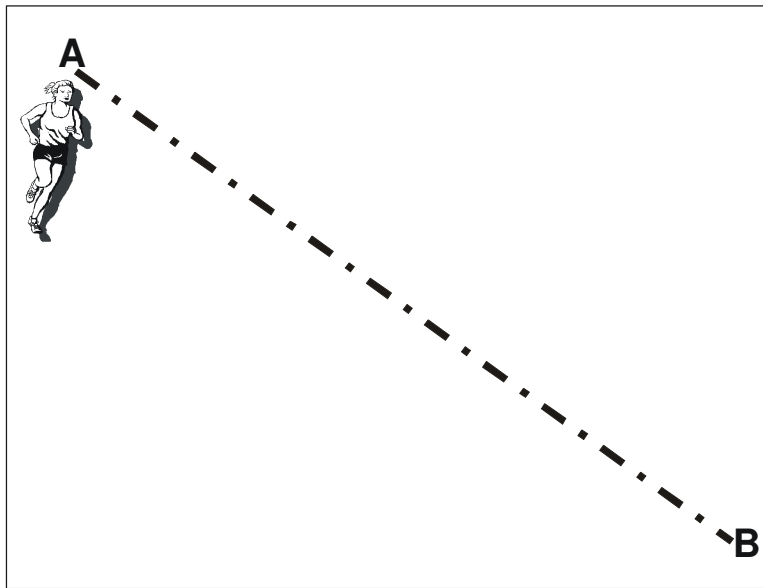


Figura 2-7A. Comprender la actuación humana

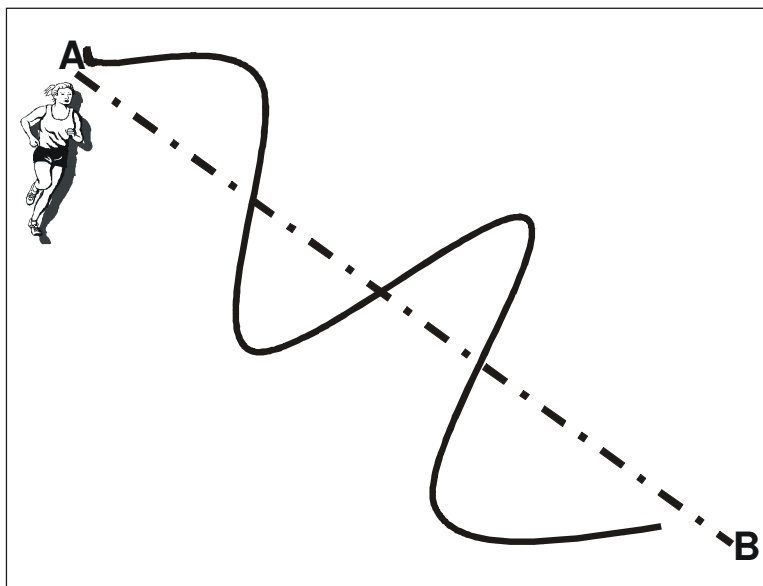


Figura 2-7B. Comprender la actuación humana

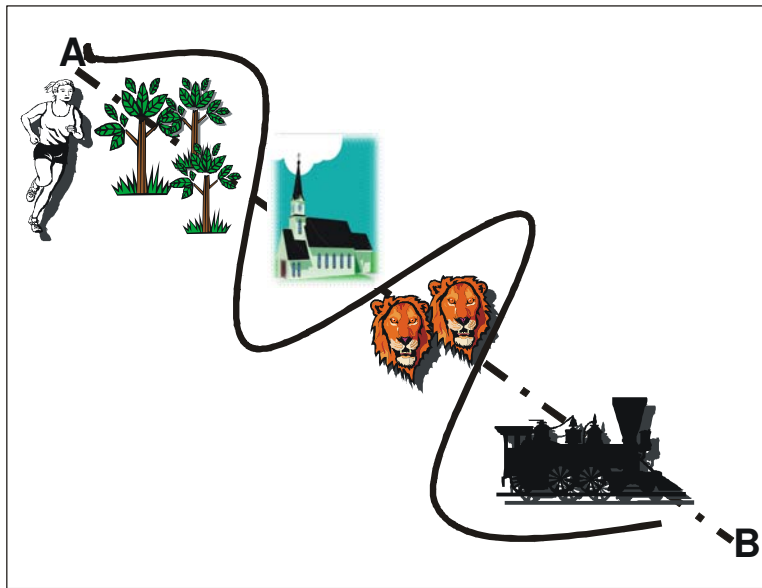


Figura 2-7C. Comprender la actuación humana

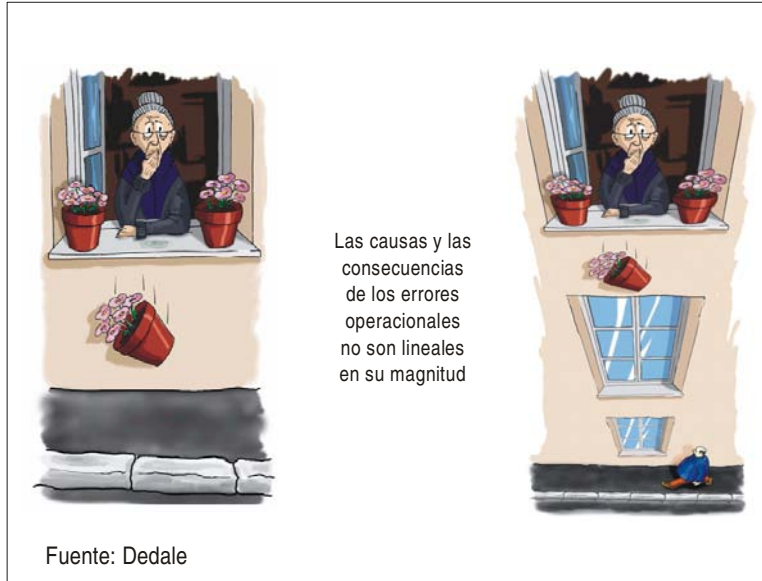


Figura 2-8. Procesos y consecuencias

2.6.12 Una herramienta conceptual sencilla aunque visualmente poderosa para el análisis de los componentes y características de los contextos operacionales y sus posibles interacciones con las personas es el modelo SHEL. El modelo SHEL [a veces conocido como modelo SHEL(L)] puede aplicarse para ayudar a visualizar las interrelaciones entre los diversos componentes y características del sistema aeronáutico. Este modelo pone énfasis en el individuo y en las interfaces del ser humano con los otros componentes y características del sistema de aviación. Su nombre deriva de las letras iniciales de sus cuatro componentes (en inglés):

- a) (S) Software (soporte lógico-procedimientos, instrucción, apoyo, etc.);
- b) (H) Hardware (soporte físico-máquinas y equipo);
- c) (E) Environment (entorno-circunstancias operacionales en que debe funcionar el resto del sistema L-H-S); y
- d) (L) Liveware (elemento humano-personas en el lugar de trabajo).

2.6.13 La Figura 2-9 ilustra el modelo SHEL. Este diagrama de bloques está orientado a facilitar una comprensión básica de la relación de los individuos con los componentes y características del lugar de trabajo.

2.6.14 **Personas en el lugar de trabajo.** En el centro del modelo SHEL están las personas que realizan las operaciones. Aunque el ser humano es notablemente adaptable, está sujeto a variaciones considerables en su actuación. Los seres humanos no están normalizados en el mismo grado que las máquinas y los equipos, de manera que los bordes de este bloque no son simples y rectos. La gente no dialoga perfectamente con los diversos componentes del mundo en que trabaja. Para evitar tensiones que pueden comprometer la actuación humana, deben comprenderse los efectos de las irregularidades en las interfaces entre los diversos bloques SHEL y el bloque central. Para evitar tensiones en el sistema, los otros componentes deben ajustarse cuidadosamente a los seres humanos.

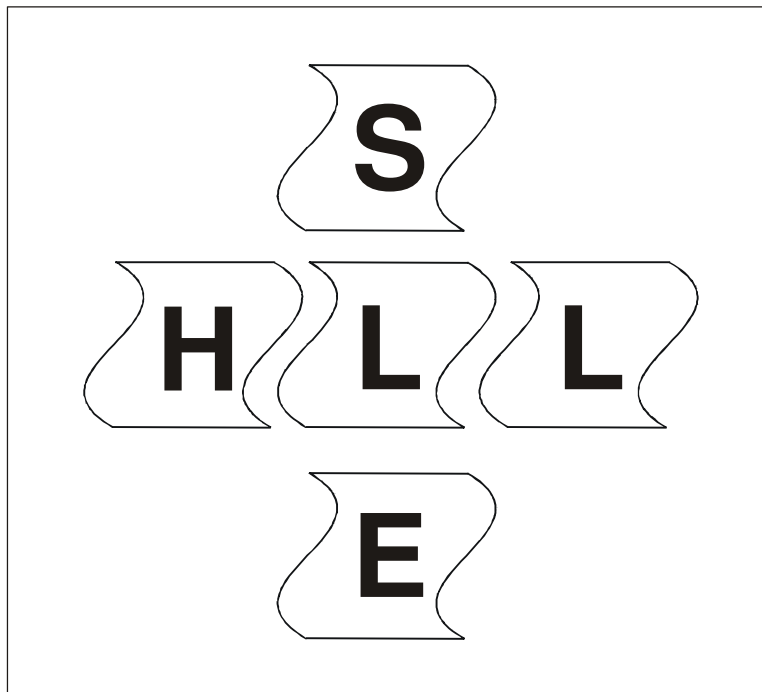


Figura 2-9. El modelo SHEL

2.6.15 Diversos factores ponen los bordes irregulares sobre el bloque L de personas en el lugar de trabajo. Algunos de los factores más importantes que afectan a la actuación individual son los siguientes:

- a) **Factores físicos.** Incluyen las capacidades físicas del individuo para realizar las tareas necesarias, por ejemplo, fuerza, altura, alcance, visión y oído.
- b) **Factores fisiológicos.** Incluyen aquellos factores que afectan a los procesos físicos internos del ser humano y que pueden comprometer la actuación física y cognitiva de una persona, p. ej., disponibilidad de oxígeno, salud y estado físico generales, enfermedad, uso de tabaco, drogas o alcohol, estrés personal, fatiga y embarazo.
- c) **Factores psicológicos.** Incluyen aquellos factores que afectan a la disposición psicológica del individuo para enfrentar todas las circunstancias que puedan presentarse, p. ej., instrucción, conocimientos y experiencia adecuados y carga de trabajo.
- d) **Factores psicosociales.** Incluyen todos aquellos factores externos en el sistema social de los individuos que ejercen presión sobre ellos, en su trabajo y en situaciones ajenas al trabajo, p. ej., una discusión con un supervisor, conflictos laborales, la muerte de algún familiar, problemas financieros personales o tensiones en el hogar.

2.6.16 El modelo SHELL es particularmente útil para visualizar las interfaces entre los diversos componentes del sistema de aviación, que incluyen:

- a) **Elemento humano-soporte físico (L-H).** Cuando se habla de factores humanos, la interfaz entre el ser humano y la tecnología es uno de los que se considera más comúnmente. Esta interfaz determina la forma en que el humano interactúa en relación con el entorno físico de trabajo, p. ej., el diseño de los asientos para que sea adecuado a las características del cuerpo humano, las presentaciones para ajustarse a las características sensoriales y de procesamiento de la información del usuario, y movimiento, codificación y emplazamiento de los controles adecuados para el usuario. Sin embargo, hay una tendencia humana natural a adaptarse a las disparidades entre L y H. Esta tendencia puede encubrir graves deficiencias que sólo se ponen en evidencia después de un accidente.
- b) **Elemento humano-soporte lógico (L-S).** La interfaz L-S es la relación entre el ser humano y los sistemas de apoyo en el lugar de trabajo, p. ej., reglamentos, manuales, listas de verificación, publicaciones, procedimientos operacionales normalizados (SOP) y soporte lógico de computadora. Incluye también cuestiones de "facilidad para el usuario" tales como aceptación general, precisión, formato y presentación, vocabulario, claridad y simbología.
- c) **Elemento humano-elemento humano (L-L).** La interfaz L-L es la relación entre el ser humano y otras personas en el lugar de trabajo. Las tripulaciones de vuelo, los controladores de tránsito aéreo, los mecánicos de mantenimiento de aeronaves y demás personal de operaciones funcionan como grupo, y las influencias del grupo desempeñan una función en la determinación del comportamiento y la actuación del ser humano. El advenimiento de la gestión de recursos de tripulación (CRM) ha hecho que se prestara mucha atención a esta interfaz. La instrucción en CRM y su extensión a los servicios de tránsito aéreo (ATS) [gestión de recursos de equipo (TRM)] y el mantenimiento [gestión de recursos de mantenimiento (MRM)] fomenta el trabajo de equipo y se concentra en la gestión de los errores operacionales. Las relaciones entre el personal y los administradores también quedan comprendidas en el ámbito de esta interfaz, puesto que la cultura, el ambiente y las presiones operacionales de la empresa pueden afectar considerablemente la actuación humana.
- d) **Elemento humano-entorno (L-E).** Esta interfaz involucra una relación entre el individuo y los entornos interno y externo. El entorno laboral interno comprende aspectos físicos como la temperatura, luz ambiente, ruido, vibración y calidad del aire. El entorno externo comprende elementos como la visibilidad, turbulencia y terreno. El ambiente de trabajo en aviación de veinticuatro horas cada día de la semana incluye perturbaciones a los ritmos biológicos normales, p. ej., la estructura del

sueño. Además, el sistema de aviación funciona en un contexto de amplias limitaciones políticas y económicas que, a su vez, afectan el ambiente general de la empresa. Se incluyen aquí factores como la pertinencia de las instalaciones físicas y de la infraestructura de apoyo, la situación financiera local y la eficacia de los reglamentos. Así como el ambiente de trabajo inmediato puede crear presiones para tomar el camino más corto, una infraestructura de apoyo inadecuada también puede comprometer la calidad de la toma de decisiones.

2.6.17 Es necesario tener cuidado para que los errores operacionales no “se filtren por las grietas” de las interfaces. En la mayoría de los casos, los bordes irregulares de estas interfaces pueden manejarse, por ejemplo:

- a) El diseñador puede asegurar la fiabilidad de la performance del equipo en condiciones de funcionamiento específicas.
- b) Durante el proceso de certificación, la autoridad de reglamentación puede definir las condiciones en que se puede usar el equipo.
- c) La administración de la organización puede especificar los procedimientos operacionales normalizados (SOP) y proveer la instrucción inicial y periódica para el uso seguro del equipo.
- d) Los operadores de equipos individuales pueden familiarizarse con ellos y adquirir confianza para emplearlos con seguridad en todas las condiciones operacionales exigidas.

## 2.7 ERRORES Y VIOLACIONES

### Errores operacionales

2.7.1 El crecimiento que ha experimentado la industria de la aviación en las dos últimas décadas habría sido imposible si no se hubiera contado con tecnología avanzada para apoyar la creciente demanda de servicios. En las industrias de producción intensiva como la aviación moderna, la tecnología es fundamental para satisfacer necesidades relativas a la prestación de los servicios. Este es un punto fundamental que a menudo se deja de lado en los análisis de seguridad operacional. La introducción de tecnología no se dirige principalmente a mejorar la seguridad operacional; la introducción de tecnología se dirige principalmente a satisfacer la demanda de una mayor prestación de servicios, manteniendo los márgenes de seguridad operacional existentes.

2.7.2 Así pues, la tecnología se introduce con carácter masivo para satisfacer las demandas de producción. Un resultado de esta introducción masiva de tecnología dirigida a mejorar la prestación de servicios es que la interfaz elemento humano-soporte físico del modelo SHELL se deja de lado o no siempre se considera en la medida que debería hacerse. Como consecuencia, puede introducirse prematuramente tecnología que no está suficientemente desarrollada, lo que conduce a fallas imprevistas.

2.7.3 Si bien la introducción de tecnología no plenamente desarrollada es una consecuencia inevitable de las necesidades de cualquier industria de producción masiva, su pertinencia para la gestión de la seguridad operacional no puede dejarse de lado. El personal de operaciones debe interactuar diariamente con la tecnología en el desempeño de sus funciones para lograr la prestación de servicios. Si la interfaz soporte físico-elemento humano no se considera adecuadamente durante el diseño de la tecnología, y si las consecuencias operacionales de las interacciones entre las personas y la tecnología se desatienden, el resultado es obvio: errores operacionales.

2.7.4 La perspectiva de los errores operacionales como una propiedad emergente de los sistemas integrados por ser humano/tecnología plantea una perspectiva considerablemente distinta de la gestión de la seguridad opera-



cional cuando se compara con la perspectiva tradicional, basada en la psicología, de los errores operacionales. Con arreglo a la perspectiva basada en la psicología, la fuente del error “reside” en la persona, y es consecuencia de mecanismos psicosociales específicos explorados y explicados por las diversas ramas de investigación y la psicología aplicada.

2.7.5 Intentar prever y mitigar eficazmente los errores operacionales siguiendo una perspectiva basada en la psicología es extremadamente difícil, si no lisa y llanamente imposible. La selección puede filtrar individuos sin los rasgos básicos necesarios para las tareas y el comportamiento puede verse influido por la instrucción y la reglamentación. No obstante, las carencias de esta perspectiva, desde el punto de vista estrictamente operacional, son claras: es imposible prever de manera sistemática las flaquezas humanas típicas como la distracción, el cansancio y los olvidos, y la forma en que pueden interactuar con componentes y características de un contexto operacional en determinadas condiciones específicas. Las estrategias de mitigación basadas en el individuo se consideran mitigaciones “blandas”, debido a que, cuando menos se espera, surgirán deficiencias en la actuación humana, no necesariamente en situaciones exigentes, liberando su potencial perjudicial.

2.7.6 La perspectiva de errores operacionales como propiedad emergente de los sistemas ser humano/tecnología traslada la fuente del error operacional del ser humano para colocarla directamente en el mundo físico, en la interfaz L/H. Una disparidad en esta interfaz es la fuente del error operacional. Como parte del mundo físico, la fuente del error operacional se hace entonces visible y puede articularse en términos operacionales (un conmutador está parcialmente oculto por una palanca haciendo difícil observar su posición correcta durante operaciones nocturnas) por oposición a términos científicos (limitaciones perceptuales). Por consiguiente, la fuente del error operacional puede preverse y mitigarse mediante intervenciones operacionales. No hay mucho que la gestión de la seguridad operacional pueda lograr con respecto a las limitaciones de percepción del ser humano, pero hay un conjunto de opciones disponibles mediante la gestión de la seguridad operacional para contraatacar las consecuencias de un diseño que incluya un conmutador parcialmente oculto.

2.7.7 Es parte de la tradición de seguridad operacional de la aviación considerar los errores operacionales como factor contribuyente en la mayoría de los accidentes de aviación. Esta opinión, basada en la perspectiva psicológica analizada anteriormente, representa los errores operacionales como forma de comportamiento adoptada voluntariamente por el personal operacional, como si éste tuviera una clara opción entre cometer un error operacional o no y adoptara voluntariamente la primera posibilidad. Además, un error operacional se considera indicativo de una actuación subnormal, fallas de carácter, falta de profesionalismo, ausencia de disciplina y atributos similares desarrollados a lo largo de años de comprensión parcial de la actuación humana. Si bien son convenientes para describir sucesos y expeditivos para culpar personas, estas atribuciones no llegan a comprender y explicar los errores operacionales.

2.7.8 Si se sigue la perspectiva alternativa respecto de los errores operacionales analizada, considerándolos como una propiedad emergente de los sistemas humano/tecnología y ubicando la fuente de los errores en la disparidad de la interfaz L/H, resulta evidente que aún el personal más competente puede cometer errores operacionales. Estos son entonces aceptados como componente normal de cualquier sistema donde interactúen los seres humanos con la tecnología y no considerados como algún tipo de comportamiento aberrante. Los errores pueden considerarse más bien como producto secundario natural de las interacciones entre los humanos y la tecnología durante actividades laborales dirigidas a la prestación de servicios en cualquier sistema de producción. Los errores operacionales se aceptan como componente normal de cualquier sistema en que interactúen humanos y tecnología, y para controlarlos se establecen estrategias de seguridad operacional.

2.7.9 Dada la inevitabilidad de las disparidades en las interfaces del modelo SHEL en operaciones de aviación, el ámbito para los errores operacionales en la industria es enorme. Para la gestión de la seguridad operacional resulta fundamental comprender la forma en que estas disparidades pueden afectar al humano medio en su trabajo. Sólo entonces pueden implantarse medidas eficaces para controlar los efectos de los errores operacionales en la seguridad.

2.7.10 Es un error común de percepción establecer una relación lineal entre los errores operacionales y la inmediatez y magnitud de sus consecuencias. Este error de percepción se analiza en 2.6.10 y 2.6.11 en términos de errores operacionales y la magnitud de sus consecuencias. El análisis señala que no hay simetría entre los errores operacionales y la magnitud de sus posibles consecuencias. Además establece que la magnitud de las consecuencias de los errores operacionales es una función del contexto operacional en que tienen lugar dichos errores, en vez de una consecuencia de los propios errores. En lo que sigue, continúa un análisis en términos de errores operacionales y la inmediatez de sus consecuencias.

2.7.11 Es un hecho estadístico que en la aviación se cometen diariamente millones de errores operacionales antes de que ocurra una falla importante de la seguridad operacional (véase la Figura 2-10). Aparte de fluctuaciones anuales menores, las estadísticas de la industria proponen en forma coherente una proporción de accidentes inferior a un accidente mortal por millón de salidas para la última década. Para expresarlo de otra manera, en las operaciones de líneas aéreas comerciales de todo el mundo, una vez cada millón de ciclos de producción se comete un error operacional que desarrolla un potencial perjudicial lo suficientemente fuerte como para penetrar las defensas del sistema y generar una importante falla de seguridad operacional. No obstante, las disparidades en las interfaces del modelo SHEL generan decenas de miles de errores operacionales diariamente durante el curso de las operaciones de aviación normales. No obstante, estos errores operacionales son contenidos por las defensas incorporadas en el sistema de aviación y su potencial perjudicial se ve mitigado, impidiendo así que tengan consecuencias negativas. En otras palabras, el control de los errores operacionales tiene lugar con carácter cotidiano a través de la actuación eficaz de las defensas del sistema de aviación.

2.7.12 Se presenta un escenario operacional sencillo para explicar la asimetría entre los errores operacionales y la inmediatez de sus consecuencias (Figura 2-11A). Después de la puesta en marcha de los motores, la tripulación de vuelo omite seleccionar el reglaje apropiado de los flaps para el despegue durante la revisión posterior al arranque de los motores, según se indica en los procedimientos operacionales normalizados. Con ello, se ha cometido un error operacional, pero no hay consecuencias inmediatas. El error operacional ha penetrado la primera capa de defensa (SOP, secuencia de verificación por la tripulación de vuelo después del arranque de los motores), pero su potencial perjudicial está todavía latente. No hay consecuencias inmediatas; el error operacional sólo permanece en el sistema, con carácter latente.

2.7.13 La tripulación de vuelo aplica la lista de verificación posterior al arranque de los motores, pero no detecta el reglaje incorrecto de los flaps y la aeronave inicia su rodaje para la salida. Entonces se pierde una segunda oportunidad de recuperarse de las consecuencias del error operacional, que continúa permaneciendo en el sistema, aún con carácter inofensivo. No obstante, el sistema está ahora en un estado de desviación o no deseado (es decir la aeronave en rodaje de salida con un reglaje de flaps incorrecto). La tripulación de vuelo recorre la lista de verificación de rodaje y la lista de verificación antes del despegue. En ambas ocasiones, se pasa por alto el reglaje incorrecto de los flaps. Con ello se pierden más oportunidades de recuperarse de las consecuencias del error operacional. Este permanece sin consecuencias, pero el estado de desviación o el estado no deseado del sistema, aumenta.

2.7.14 La tripulación de vuelo inicia el recorrido de despegue, y suena la alarma de configuración de despegue. La tripulación de vuelo no identifica la razón de la alarma y continúa el recorrido. El error operacional todavía carece de consecuencias pero el estado no deseado del sistema ha avanzado ahora a un estado de amplificación. La aeronave despegue con una configuración de flaps incorrecta. El sistema ha avanzado ahora a un estado de deterioro, pero todavía puede concebirse que la tripulación de vuelo se recupere del estado no deseado. La aeronave no puede sostener el vuelo debido al incorrecto reglaje de los flaps y se precipita al suelo. Sólo en ese momento, después de quebrar un número considerable de defensas incorporadas en el sistema, el error operacional desarrolla su completo potencial perjudicial y pasa a tener graves consecuencias. El sistema experimenta una falla catastrófica.



Figura 2-10. Errores operacionales y seguridad — Una relación no lineal

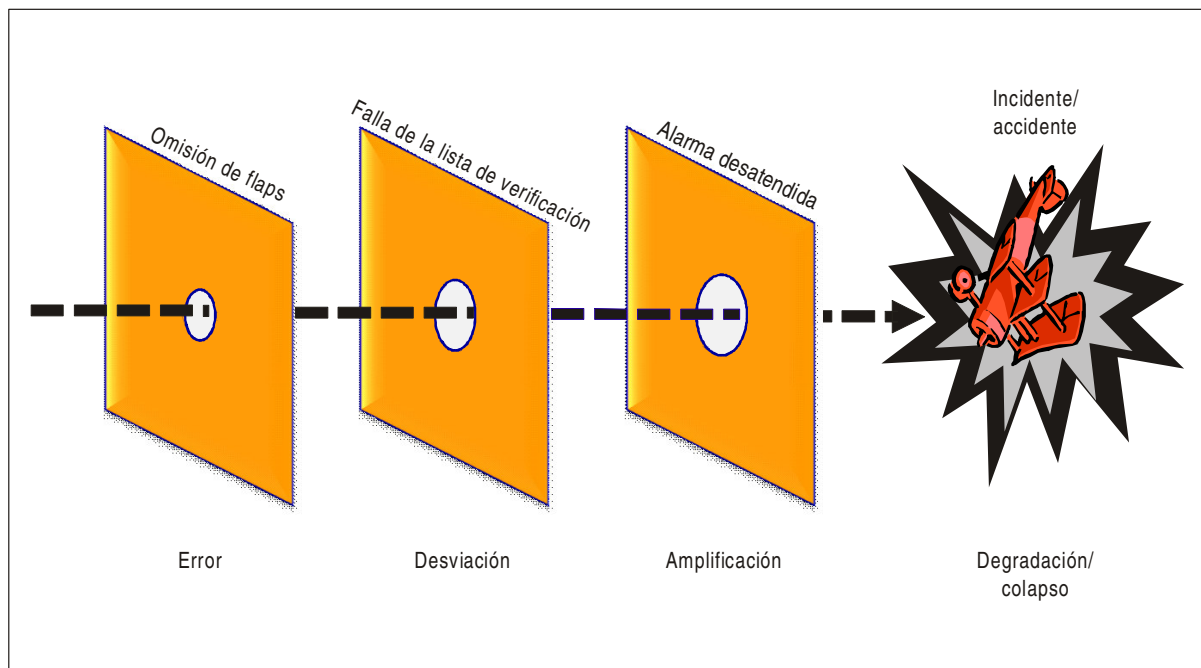
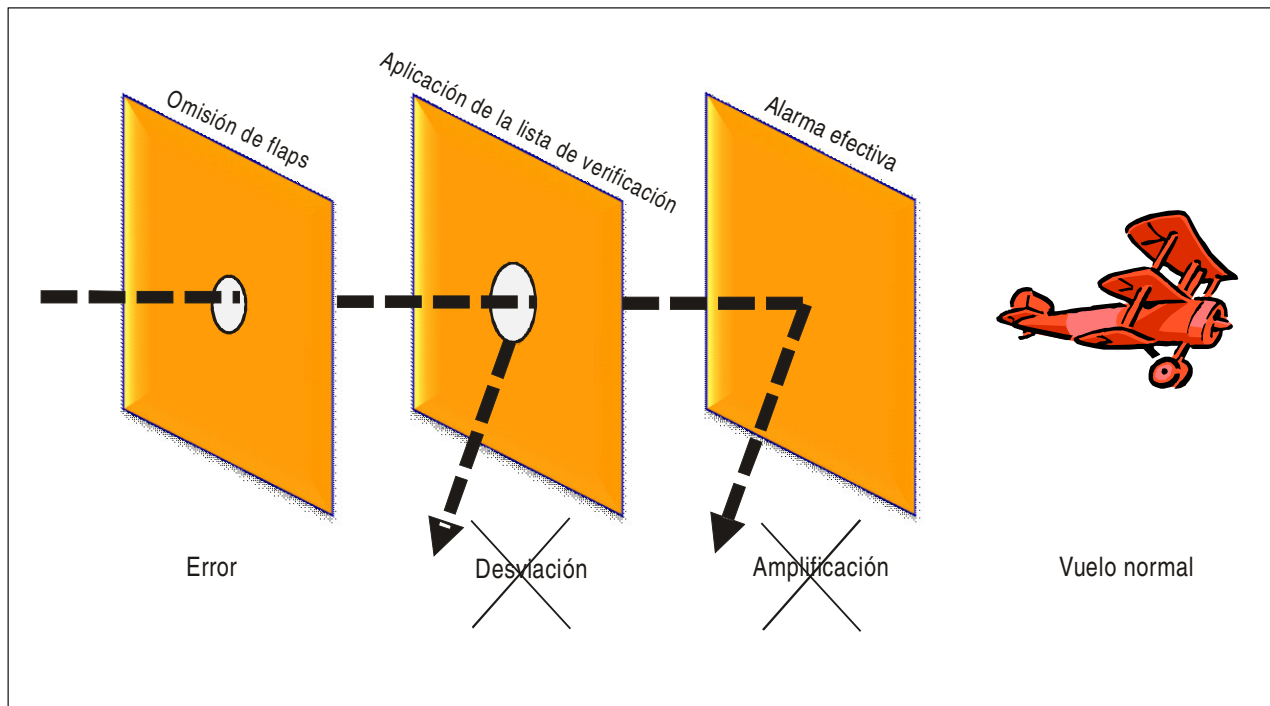


Figura 2-11A. Investigación de sucesos importantes — Uno en un millón de vuelos



**Figura 2-11B. Gestión de la seguridad operacional — En casi todos los vuelos**

2.7.15 Obsérvese el lapso de tiempo relativamente considerable entre el momento en que la tripulación de vuelo comete el error operacional y la materialización de su potencial perjudicial irrecuperable. También obsérvese el número de oportunidades de recuperarse de las consecuencias del error operacional mediante las defensas incorporadas en el sistema. Este período de tiempo es el tiempo con que cuenta el sistema para controlar las consecuencias de los errores operacionales y es conmensurable con la profundidad y la eficacia de las defensas del sistema. Es el período de tiempo a través del cual la gestión de la seguridad operacional funciona con considerable posibilidad de éxito.

2.7.16 Cuantas más defensas incorporadas y capas de contención tenga el sistema, y más eficaz sea su actuación, mayores serán las posibilidades de controlar las consecuencias de los errores operacionales. La inversa también es verdadera.

2.7.17 Desde el punto de vista de este análisis, una conclusión es clara: el escenario planteado en 2.7.12 a 2.7.14 es — inevitablemente — lo que la mayoría de las investigaciones de accidentes encontrarían: errores operacionales no gestionados que condujeron a fallas catastróficas del sistema. Esta es una información valiosa sobre las fallas humanas y del sistema; información que indica lo que falló, lo que no funcionó, y qué defensas no funcionaron como debieran. Si bien es valiosa como elemento básico, esta información no es suficiente para comprender plenamente las fallas de seguridad operacional y debería complementarse con información de fuentes alternativas.

2.7.18 Consideremos una versión modificada del escenario planteado en 2.7.12 a 2.7.14 (Figura 2-11B). Obsérvese que hay por lo menos cuatro oportunidades obvias en que las defensas podrían haberse activado para contener el potencial perjudicial del error operacional inicial (omisión de seleccionar el reglaje de flaps para despegue en la verificación posterior al arranque de los motores por la tripulación de vuelo):

- a) la lista de verificación posterior al arranque;
- b) la lista de verificación de rodaje;
- c) la lista de verificación antes del despegue; y
- d) la advertencia de configuración de despegue.

2.7.19 Hay otras instancias, no tan obvias pero sin embargo posibles, en que podrían haberse activado las defensas: advertencias del personal de plataforma, advertencias de tripulaciones de vuelo en aeronaves similares, avisos del personal ATC, etc. La actuación eficaz de las defensas en cualquiera de estas instancias podría haber controlado las consecuencias del error operacional inicial y restaurar la condición normal del sistema. El potencial perjudicial del error operacional podría haberse eliminado en cada instancia haciendo, para fines prácticos, desaparecer el error operacional.

2.7.20 El argumento aquí presentado es que los escenarios en que los errores operacionales provocan fallas catastróficas son raros, mientras que los escenarios en que los errores operacionales inducen estados no deseados del sistema (desviación/deterioro) son frecuentes. Estos escenarios captan información sobre lo que inicialmente no funcionó, pero principalmente sobre lo que funcionó posteriormente, incluyendo defensas que actuaron como debían. Este es el tipo de información que recogen las fuentes de información de seguridad operacional, alternativas y complementarias a la investigación de accidentes. La información de una investigación de accidentes identificaría por cierto las cuatro instancias en que deberían haberse activado las defensas, pero muy probablemente sólo describirá por qué no lo hicieron.

2.7.21 Las fuentes de información adicionales mencionadas identificarían las instancias en las cuales deberían haberse activado las defensas describiendo por qué y cómo lo hicieron. Estas fuentes caracterizan los éxitos y, por ello, la integración de la información de accidentes con la información de estas fuentes alternativas proporciona un panorama más completo de los problemas de seguridad operacional específicos. Además, dado que escenarios como el planteado anteriormente son frecuentes, estas fuentes alternativas de información de seguridad operacional, si se utilizan, pueden proporcionar un volumen considerable de información constante para complementar la información más esporádica proporcionada por los accidentes y permitir el logro de una comprensión más completa sobre la posibilidad de fallas de seguridad operacional. La conclusión que puede extraerse de este segundo escenario es que la flexibilidad de la seguridad operacional no es tanto cuestión de performance operacional sin errores, sino más bien una cuestión de gestión eficaz del error operacional.

### Tres estrategias para controlar los errores operacionales

2.7.22 Las tres estrategias básicas para controlar los errores operacionales se basan en las tres defensas básicas del sistema de aviación: tecnología, instrucción y reglamentación (incluso procedimientos).

2.7.23 Las **estrategias de reducción** intervienen directamente en la fuente del error operacional reduciendo o eliminando los factores que contribuyen a dicho error. Entre estas estrategias está el mejoramiento del acceso a los componentes de las aeronaves para el mantenimiento, la mejora de la iluminación en la cual se realiza la tarea, y la reducción de las distracciones del entorno, es decir:

- a) diseño centrado en el ser humano;
- b) factores ergonómicos; y
- c) instrucción.

2.7.24 Las **estrategias de captura** suponen que el error operacional ya se ha cometido. La intención es: “capturar” el error operacional antes de que se hagan sentir las consecuencias adversas del mismo. Las estrategias de captura son diferentes de las estrategias de reducción en el sentido de que no sirven directamente para eliminar el error; es decir:

- a) lista de verificación;
- b) tarjetas de tarea; y
- c) fichas de progreso de vuelo.

2.7.25 Las **estrategias de tolerancia** se refieren a la capacidad de un sistema de aceptar un error operacional sin consecuencias graves. Un ejemplo de medida para aumentar la tolerancia del sistema frente a errores operacionales es la incorporación de sistemas hidráulicos o eléctricos múltiples en una aeronave para proporcionar redundancia, o un programa de inspección estructural que proporcione múltiples oportunidades de detectar una grieta debida a la fatiga de materiales antes de que alcance una longitud crítica, es decir:

- a) redundancias del sistema; y
- b) inspecciones estructurales.

2.7.26 La gestión de los errores operacionales no debe limitarse al personal de operaciones. La actuación de dicho personal, según se muestra en el modelo SHELL, se ve influida por factores de organización, reglamentación y entorno. Por ejemplo, procesos de organización como las comunicaciones inadecuadas, procedimientos ambiguos, programación ilógica, recursos insuficientes y presupuesto no realista, constituyen los caldos de cultivo para los errores operacionales. Como ya se analizó, todos estos son procedimientos sobre los cuales una organización debe tener un grado razonable de control directo.

### Errores y violaciones

2.7.27 Hasta ahora, el análisis de esta sección se ha concentrado en los errores operacionales, que se han caracterizado como componente normal de cualquier sistema en que interactúen las personas y la tecnología para lograr los objetivos de producción del sistema. El análisis se centrará ahora en las violaciones, que son muy diferentes de los errores operacionales. Ambos pueden conducir a fallas del sistema y pueden resultar en situaciones de consecuencias graves. Para la gestión de la seguridad operacional es fundamental contar con una clara diferenciación entre errores operacionales y violaciones, y una plena comprensión de los mismos.

2.7.28 La diferencia fundamental entre errores operacionales y violaciones reside en la intención. Mientras que el error no es intencional, una violación es un acto deliberado. Las personas que cometen errores operacionales están tratando de hacer lo correcto, pero por las diversas razones analizadas anteriormente no logran sus objetivos. Las personas que cometen violaciones, por otra parte saben que están adoptando un comportamiento que entraña una desviación de procedimientos, protocolos, normas o prácticas establecidos, pero a pesar de ello continúan haciéndolo.

2.7.29 Por ejemplo, un controlador permite a una aeronave descender a través del nivel de una aeronave en crucero cuando la distancia DME entre ellas es de 18 NM, y esto ocurre en circunstancias en que la separación mínima correcta es de 20 NM. Si el controlador se equivocó al calcular la diferencia en las distancias DME comunicadas por los pilotos, esto sería un error operacional. Si el controlador calculó la distancia correctamente y permitió que la aeronave en descenso continuara a través del nivel de la aeronave en crucero sabiendo que no existían las mínimas de separación requeridas, esto sería una violación.

2.7.30 En la aviación, la mayoría de las violaciones son resultado de procedimientos deficientes o poco realistas cuando se han elaborado “soluciones” para evitar las dificultades de una tarea. La mayoría surgen de un genuino deseo de hacer un buen trabajo. Rara vez se deben a negligencias. Hay dos tipos generales de violaciones: violaciones de situación y violaciones de rutina.

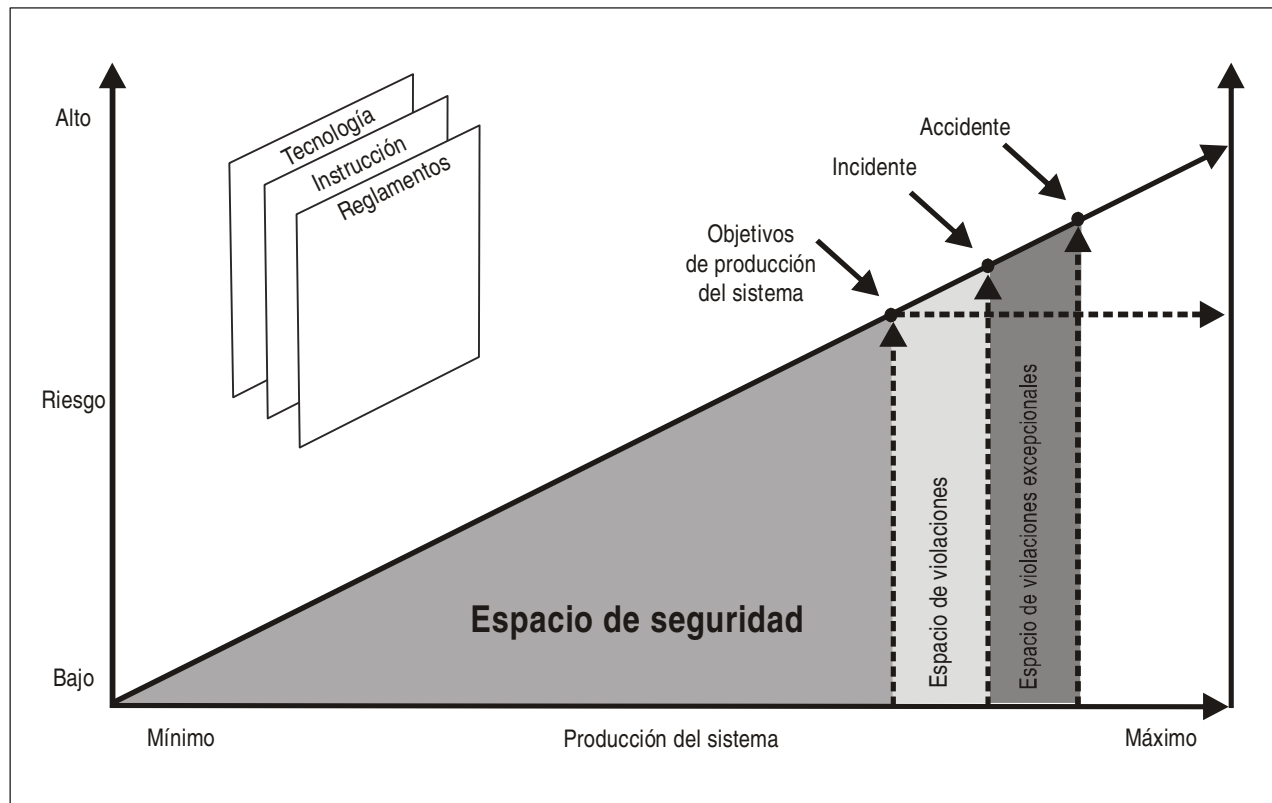
2.7.31 Las **violaciones de situación** ocurren debido a los factores particulares que existen en el momento, como la presión del tiempo o la elevada carga de trabajo. A pesar de saber que se está incurriendo en una violación, la orientación hacia el objetivo y el cumplimiento de una misión llevan a la gente a desviarse de las normas, en la creencia de que dicha desviación no tiene consecuencias adversas.

2.7.32 Las **violaciones de rutina** son violaciones que han pasado a ser la “forma normal de actuar” dentro de un grupo de trabajo. Ocurren cuando el grupo de trabajo tiene dificultades en seguir procedimientos establecidos para realizar la tarea, debido a aspectos de carácter práctico, deficiencias en el diseño de la interfaz humano-tecnología y así sucesivamente, e inventan y adoptan informalmente procedimientos “mejores” que finalmente se transforman en rutina. Esta es la noción de normalización de la desviación a que se hizo referencia en 2.5.4. Las violaciones de rutina se consideran rara vez como tales por el grupo de trabajo, debido a que su objetivo es realizar la tarea. Se consideran como mecanismos de “optimización”, dado que se dirigen a ahorrar tiempo y esfuerzo simplificando una tarea (aun si ello entraña tomar atajos).

2.7.33 Un tercer tipo de violación, a menudo se pasa por alto, son las **violaciones inducidas por la organización**, que pueden considerarse como una extensión de las violaciones de rutina. El pleno potencial del mensaje de seguridad operacional que las violaciones pueden transmitir puede comprenderse solamente cuando se le considera frente a las demandas impuestas por la organización respecto de la prestación de los servicios para la cual se creó la propia organización. En la Figura 2-12 se muestra la relación entre las dos consideraciones básicas que una organización debe sopesar y equilibrar en relación con la prestación de sus servicios y cuando defina sus procedimientos de trabajo: producción del sistema y riesgos de seguridad operacional conexos.

2.7.34 En toda organización dedicada a la prestación de servicios, la producción del sistema y los riesgos de seguridad operacional están entrelazados. A medida que aumentan las demandas de producción del sistema (prestación de servicios), también aumentan los riesgos de seguridad operacional relacionados con dicha prestación, debido al aumento de la exposición. Por consiguiente, como se ilustra en la Figura 2-12, la producción mínima del sistema se correlaciona con el menor riesgo de seguridad operacional, mientras que la producción máxima del sistema se relaciona con el riesgo de seguridad operacional más elevado. La operación continua expuesta a los mayores riesgos de seguridad operacional no es deseable, no sólo desde el punto de vista de la seguridad operacional sino también desde un punto de vista financiero. Así pues, las organizaciones sopesan la producción deseable y el riesgo de seguridad operacional tolerable y definen una producción del sistema inferior al máximo posible, pero que se correlaciona con un nivel tolerable de riesgo de seguridad. Al hacerlo, la organización define sus objetivos de producción como una función de equilibrar la producción aceptable con el riesgo de seguridad operacional aceptable.

2.7.35 Una decisión fundamental relacionada con el proceso de definir objetivos de producción (convenidos sobre la base de un equilibrio entre producción del sistema en riesgos de seguridad) es el establecimiento de las defensas que la organización necesita elaborar para protegerse de los riesgos de seguridad operacional que generará en la producción. Como ya se analizó, las tres defensas básicas del sistema de aviación son la tecnología, la instrucción y los reglamentos (incluso los procedimientos). Por lo tanto, cuando define sus objetivos de producción, la organización también debe definir las herramientas (tecnología) necesarias para lograr en forma segura y eficaz la prestación de servicios; cómo fomentar el comportamiento que sus trabajadores deben exhibir para usar en forma segura y eficiente las herramientas (instrucción); y el conjunto de normas y procedimientos que dictan la actuación de los trabajadores (reglamentos).



**Figura 2-12. Comprender las violaciones**

2.7.36 Así pues, la producción del sistema, el nivel de riesgo de seguridad y las defensas convergen en el punto en que se definen los objetivos de producción de la organización. También establecen los límites de lo que podría denominarse el “espacio de seguridad operacional de la organización”. Este espacio de seguridad operacional representa una zona protegida, la zona dentro de la cual las defensas que la organización ha erigido garantizan la máxima capacidad de reacción frente a los riesgos de seguridad operacional que la organización enfrentará en la entrega del producto del sistema en términos de objetivos de producción.

2.7.37 La razón de la máxima capacidad de reacción proporcionada por ese espacio de seguridad operacional es que las defensas erigidas por la organización son conmensurables con la producción planificada del sistema, lo que a su vez es conmensurable con el riesgo de seguridad operacional tolerable. En otras palabras, los recursos asignados por la organización para proteger son apropiados y conmensurables con las actividades relacionadas con la prestación de los servicios. Esto no significa que la organización no pueda experimentar un accidente, dado que éstos son sucesos aleatorios que resultan de la concatenación de circunstancias imprevisibles. Significa que la organización cuenta con arreglos de gestión de la seguridad operacional que garantizan un nivel aceptable de control de los riesgos de seguridad durante la prestación de los servicios, en circunstancias previsibles. En términos sencillos, la organización ha hecho todo lo posible en términos de seguridad operacional.

2.7.38 Dado el carácter dinámico de la aviación, las organizaciones aeronáuticas pueden enfrentar ocasionalmente demandas transitorias a corto plazo para aumentar su producción (es decir aumentar la prestación de servicios) durante breves períodos de tiempo, por ejemplo, variaciones estacionales de la demanda de asientos, circunstancias específicas como eventos deportivos mundiales, y así sucesivamente. Para mantener intacta la zona de seguridad operacional, la organización debería examinar y volver a disponer o modificar su asignación de recursos existente, así como fortalecer las defensas existentes para contrarrestar el aumento de la producción y su consecuente aumento del nivel de riesgo de seguridad.



2.7.39 Lamentablemente, el historial de la aviación sugiere otra cosa. Con demasiada frecuencia, como lo muestran los antecedentes de fallas de seguridad operacional, las organizaciones aeronáuticas tratan de enfrentar los períodos breves de mayor producción del sistema “estirando” las defensas: recurriendo a horas extraordinarias en vez de contratar personal adicional, lo que lleva a un aumento de la carga de trabajo y la fatiga; utilizando la tecnología en formas “más eficientes” en vez de incorporar tecnología adicional; “optimizando” procedimientos y recursos sin revisar los procedimientos operacionales normalizados y las normas, etc.

2.7.40 Lo que se logra efectivamente con este estiramiento de las defensas es colocar a la organización fuera del espacio de seguridad operacional, en primer lugar en el espacio de violación y, finalmente, en el espacio de violación excepcional. En otras palabras, para lograr la mayor producción con los mismos recursos, el personal operacional debe desviarse de procedimientos establecidos tomando atajos o desviaciones aprobadas por la organización. El personal operacional no elige participar en dichos atajos, la organización lo hace. La expresión familiar “dar una mano a la compañía” describe en forma elocuente la situación en que se obliga a las personas a participar en desviaciones aprobadas por una organización para entregar un producto de sistema inconmensurable con los recursos asignados a esos efectos.

2.7.41 Normalmente, los incidentes proporcionan pruebas concretas de que la organización ha ingresado en el espacio de violación. Una organización consciente volverá entonces a evaluar su asignación de recursos para ampliar su espacio de seguridad a efectos de mantener la armonía entre la producción del sistema, el riesgo de seguridad tolerable y las defensas o, si no puede hacerlo, volverá al espacio de seguridad establecido reduciendo la producción del sistema. Algunas organizaciones ignorarán los avisos proporcionados por los incidentes, persistirán en su conducta e inevitablemente ingresarán al espacio de violación excepcional. Un accidente es entonces un resultado probable.

## 2.8 CULTURA DE ORGANIZACIÓN (CORPORATIVA)

2.8.1 La cultura puede describirse en los términos más sencillos como “programación colectiva de la mente”. Una de las descripciones más gráficas de la cultura la presenta como “soporte lógico de la mente”. La cultura influye en los valores, las creencias y los comportamientos que compartimos con otros miembros de los diversos grupos sociales a que pertenecemos. La cultura sirve para vincularnos como miembros de grupos y proporciona claves sobre la forma de comportarse tanto en situaciones normales como inhabituales. La cultura establece las reglas del juego, o el marco para todas nuestras interacciones interpersonales. Es la suma total de la forma en que las personas llevan adelante sus asuntos en un medio social particular y proporciona un contexto en que las cosas ocurren. En términos de gestión de la seguridad operacional, comprender la cultura es tan importante como comprender el contexto, dado que la cultura es un determinante importante de la actuación humana.

2.8.2 Un peligro latente al estudiar la cultura y, en particular, aspectos transculturales que podrían afectar la seguridad operacional de la aviación, es caer en la trampa de formular involuntariamente juicios de valor y presentar una cultura particular como quizás “mejor” o “más adecuada” que otra, o proponer que una cultura particular es “mala” o “inadecuada” para determinadas propuestas de seguridad. Esto es impropio e infructuoso, debido a que el estudio de aspectos transculturales se refiere — en términos de seguridad operacional — a las diferencias, y no a juicios de valor. Las culturas son en verdad diferentes, y cada una de ellas tiene importantes puntos fuertes así como puntos débiles identificables. La finalidad de las consideraciones transculturales serias, cuando se aplican a la gestión de la seguridad operacional, es basarse en las fuerzas culturales combinadas, en la medida en que se relacionan con las prácticas de seguridad, reduciendo al mínimo los efectos de las debilidades culturales combinadas.

2.8.3 Las organizaciones, en tantos grupos de personas, no son inmunes a las consideraciones culturales. El comportamiento de la organización está sujeto a influencias culturales en cada uno de sus niveles. Los tres niveles de cultura que siguen (Figura 2-13) son importantes para las iniciativas de gestión de la seguridad operacional, dado que los tres son determinantes del comportamiento de la organización:

- a) La **cultura nacional** diferencia las características y los sistemas de valores propios de las diversas naciones. Las personas de diferentes nacionalidades son diferentes en cuanto a la forma en que responden a la autoridad, enfrentan la incertidumbre y la ambigüedad y expresan su individualidad. No todos los individuos están atentos a las necesidades colectivas del grupo (equipo u organización) del mismo modo. En las culturas colectivistas, se acepta la condición desigual y la deferencia a los líderes. Estos factores pueden afectar la disposición de los individuos a objetar decisiones o acciones de sus mayores — lo que es una consideración importante en cuanto al trabajo en equipo, por ejemplo. La asignación de tareas mezclando culturas nacionales también puede afectar la actuación del equipo cuando se crean malentendidos.

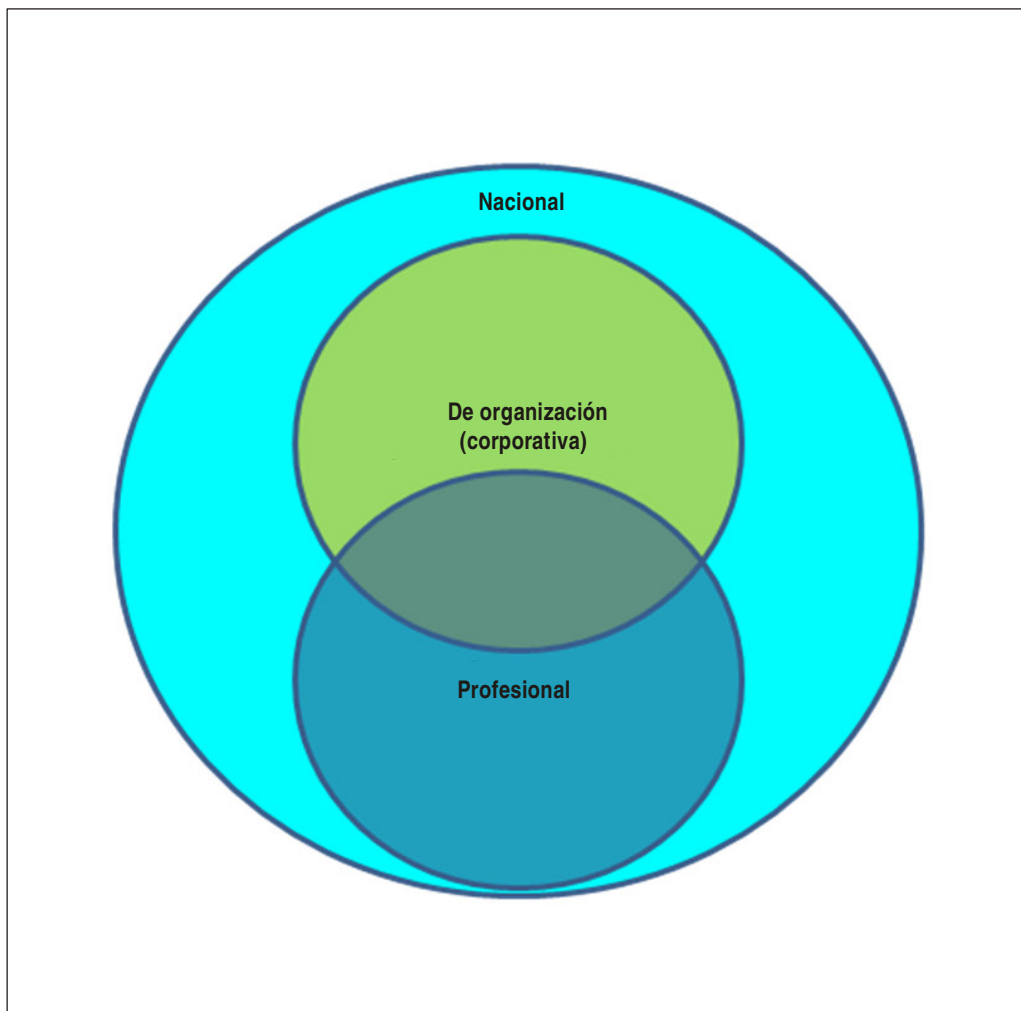


Figura 2-13. Tres culturas diferentes

- b) La **cultura profesional** diferencia las características y los sistemas de valores de grupos profesionales particulares (el comportamiento típico de los pilotos con respecto a los controladores de tránsito aéreo, o al de los mecánicos de mantenimiento de aeronaves). Por medio de la selección, educación e instrucción del personal, la experiencia en el trabajo, las presiones de los colegas, etc., los profesionales (médicos, abogados, pilotos, controladores) tienden a adoptar el sistema de valores y a desarrollar modelos de comportamiento conformes a los de sus pares; aprenden a “caminar y hablar” del mismo modo. Generalmente comparten un orgullo en su profesión y están motivados para sobresalir en ella. Por otra parte, frecuentemente tienen un sentido de invulnerabilidad personal, considerando que su actuación personal no resulta afectada por los problemas personales, y que no cometen errores en situaciones de mucho estrés.
- c) La **cultura de organización (corporativa)** diferencia las características y los sistemas de valores de cada organización (el comportamiento de los miembros de una empresa en comparación con los de otra empresa, o del gobierno en comparación con los del sector privado). Las organizaciones protegen las culturas nacionales y profesionales. Por ejemplo, en una línea aérea, los pilotos pueden provenir de sectores profesionales diferentes (experiencia militar o civil, de operaciones complementarias o en zonas remotas o de una gran empresa de transporte aéreo). También pueden provenir de diferentes organizaciones debido a las fusiones de empresas o despidos.

2.8.4 Los tres conjuntos culturales descritos anteriormente interactúan en contextos operacionales. Estas interacciones determinan por ejemplo la forma en que:

- a) los empleados noveles se relacionarán con los más antiguos;
- b) se comparte una información;
- c) reaccionará el personal sometido a condiciones operacionales exigentes;
- d) se adoptarán tecnologías particulares;
- e) se ejercerá la autoridad y cómo reaccionarán las organizaciones ante los errores operacionales (sancionar a los transgresores o aprender de la experiencia);
- f) se aplica la automatización;
- g) se elaboran los procedimientos (SOP);
- h) se prepara, presenta y recibe la documentación;
- i) se elabora e imparte la instrucción;
- j) se asignan las tareas;
- k) se relacionarán los diferentes grupos de trabajo (pilotos, ATC, personal de mantenimiento, tripulación de cabina); y
- l) se relacionarán la administración y los sindicatos.

En otras palabras, la cultura repercute en prácticamente cada tipo de transacción interpersonal o entre organizaciones. Además, las consideraciones culturales se infiltran en el diseño de equipo y herramientas. La tecnología puede parecer neutra desde el punto de vista cultural, pero refleja las tendencias del fabricante (considérese la predominancia del inglés implícita en gran parte del soporte lógico de computadoras en todo el mundo). Aun así, no hay una cultura correcta y una cultura equivocada; las culturas son lo que son y cada una de ellas posee una combinación de puntos fuertes y débiles.

2.8.5 El mayor ámbito para crear y nutrir una cultura eficaz y generadora para la gestión de la seguridad operacional se encuentra a nivel de la organización. El personal operacional de la aviación está influenciado en su comportamiento diario por el sistema de valores de la organización a la que pertenece. La organización, ¿reconoce los méritos de seguridad, promueve la iniciativa individual, alienta o desalienta la tolerancia a los riesgos de seguridad, aplica el estricto cumplimiento de los SOP, tolera las violaciones de los SOP o promueve comunicaciones abiertas en ambos sentidos? Así pues, la organización es un determinante importante del comportamiento de los empleados cuando realicen actividades operacionales que apoyen la prestación de los servicios para los cuales existe la organización. La cultura de la organización establece los límites del comportamiento humano en el lugar de trabajo estableciendo las normas y las limitaciones. Así pues, la cultura de organización constituye una piedra angular para la toma de decisiones de administración y de los empleados: “así es como hacemos aquí las cosas, y cómo hablamos sobre cómo hacemos aquí las cosas”.

2.8.6 La cultura de organización consiste en creencias, prácticas y actitudes compartidas. El tono de la cultura de organización eficaz y generadora lo establecen y alimentan las palabras y acciones del personal directivo de alto nivel. La cultura de la organización es la atmósfera que crea la administración y que da forma a las actitudes de los trabajadores con respecto a, entre otras cosas, las prácticas de seguridad operacional. La cultura de organización resulta afectada por factores como:

- a) políticas y procedimientos;
- b) prácticas de supervisión;
- c) planificación y objetivos de la seguridad operacional;
- d) medidas en respuesta a comportamientos inseguros;
- e) instrucción y motivación del personal; y
- f) participación o adhesión de los empleados.

2.8.7 La responsabilidad final del establecimiento y cumplimiento de prácticas de seguridad operacional bien fundadas corresponde a los directores y gerentes de la organización — ya sea una línea aérea, un aeródromo, un ATS o un AMO. La ética de seguridad operacional de una organización se establece desde el principio por la medida en que la administración superior acepta la responsabilidad de las operaciones seguras y de la gestión de los problemas de seguridad emergentes.

2.8.8 El modo en que la administración enfrenta las actividades cotidianas es fundamental para una cultura de organización generativa en la gestión de la seguridad. ¿Se sacan las conclusiones correctas de las experiencias de trabajo reales y se adoptan las medidas apropiadas? ¿Participan constructivamente los miembros del personal en este proceso o sienten que son víctimas de medidas unilaterales de la administración?

2.8.9 La relación que la administración de la línea aérea tiene con los representantes de la autoridad de reglamentación también indica si existe una cultura de organización sana. Esta relación debería distinguirse por la cortesía profesional, pero con suficiente distancia como para no comprometer la rendición de cuentas. La apertura, más que el estricto cumplimiento de los reglamentos, conducirá a una mejor comunicación en materia de seguridad operacional. El primer enfoque alienta el diálogo constructivo, mientras que el segundo incita a ocultar o a ignorar los verdaderos problemas de seguridad operacional.

2.8.10 Aunque el cumplimiento de los reglamentos de seguridad operacional es fundamental para la seguridad de las operaciones, el pensamiento contemporáneo es que se necesita mucho más que eso. Las organizaciones que cumplen simplemente con las normas mínimas establecidas por los reglamentos no están en buena posición para identificar los problemas de seguridad operacional que surgen.

2.8.11 Un modo eficaz de promover las operaciones seguras es garantizar que el explotador ha desarrollado un entorno operacional donde todo el personal se siente responsable y tiene en cuenta las repercusiones de la seguridad operacional en todo lo que hace. Esta forma de pensar debe estar tan arraigada en sus actividades que verdaderamente llegue a ser “la forma en que hacemos aquí las cosas”. Todas las decisiones, sean del consejo de administración, de un conductor en la plataforma o de un mecánico de mantenimiento, deben tomarse teniendo en cuenta las repercusiones sobre la seguridad operacional.

2.8.12 Un entorno operacional de este tipo debe tener su origen en los niveles superiores y descansa en un elevado grado de confianza y respeto entre los trabajadores y la administración. Los trabajadores deben creer y sentir que tendrán apoyo en cualquier decisión que tomen a favor de la seguridad operacional. También deben entender que las violaciones deliberadas de la seguridad operacional que ponen en peligro las operaciones no serán toleradas.

### **Notificación efectiva de seguridad operacional**

2.8.13 Uno de los aspectos más influyentes de una cultura de organización en términos de la gestión de la seguridad operacional es que da forma a procedimientos y prácticas de notificar los problemas de seguridad operacional por el personal. La identificación de peligros es una actividad fundamental para la gestión de la seguridad operacional. Nadie está en mejor posición para informar de la existencia de peligros y de lo que funciona bien o no lo hace, que el personal de operaciones, que tiene que vivir cotidianamente con los peligros y enfrentarlos. La notificación efectiva de seguridad operacional de peligros por parte del personal es, por consiguiente, una piedra fundamental de la gestión de la seguridad operacional. Por consiguiente, un entorno operacional en el cual el personal se ha instruido y se ve constantemente alentado a notificar los peligros es el requisito previo para una efectiva notificación de seguridad operacional.

2.8.14 La notificación efectiva de seguridad operacional se apoya en ciertos atributos básicos a saber:

- a) la administración superior pone mucho énfasis en la identificación de peligros como parte de la estrategia para la gestión de la seguridad operacional, y como consecuencia existe una conciencia de la importancia de comunicar la información sobre peligros a todos los niveles de la organización;
- b) la administración superior y el personal de operaciones tiene una opinión realista de los peligros enfrentados por las actividades de prestación de servicios de la organización y, en consecuencia, existen reglas realistas sobre los peligros y posibles fuentes de daños;
- c) la administración superior define los requisitos operacionales necesarios para apoyar la notificación activa de los peligros, asegura que se registren adecuadamente los datos de seguridad clave, demuestra una actitud receptiva hacia la notificación de peligros por el personal de operaciones e implanta medidas para contener las consecuencias de los peligros;
- d) la administración superior asegura que los datos de seguridad operacional fundamentales son protegidos adecuadamente y promueve un sistema de verificaciones y compensaciones de modo que quienes notifiquen peligros sientan confianza en que la notificación de los mismos no será utilizada para otros fines distintos de los previstos (la gestión de la seguridad operacional);
- e) el personal está capacitado formalmente para reconocer y notificar peligros y comprender la incidencia y consecuencias de los peligros en las actividades relacionadas con la prestación de servicios; y
- f) hay una baja incidencia de comportamiento peligroso y existe una ética de la seguridad operacional que desalienta tales comportamientos.

### Notificación efectiva de seguridad operacional — Cinco características básicas

2.8.15 Existen cinco características básicas universalmente relacionadas con los sistemas de notificación efectiva de seguridad operacional (Figura 2-14). Estas cinco características se relacionan con los atributos básicos de la notificación efectiva de seguridad operacional presentados en 2.8.14:

- a) **Buena voluntad.** Como consecuencia de actividades deliberadas de la administración superior para definir los requisitos operacionales necesarios para apoyar la notificación activa de peligros y garantizar que se registran adecuadamente los datos de seguridad fundamentales, el personal de operaciones está dispuesto a notificar peligros, errores operacionales que puedan surgir de la exposición a peligros, así como sus experiencias personales según corresponda.
- b) **Información.** Como consecuencia de la instrucción formal para reconocer y notificar peligros y comprender la incidencia y las consecuencias de los peligros en las actividades dirigidas a la prestación de los servicios, el personal de operaciones conoce los factores humanos, técnicos y de organización que determinan la seguridad operacional del sistema en su totalidad.

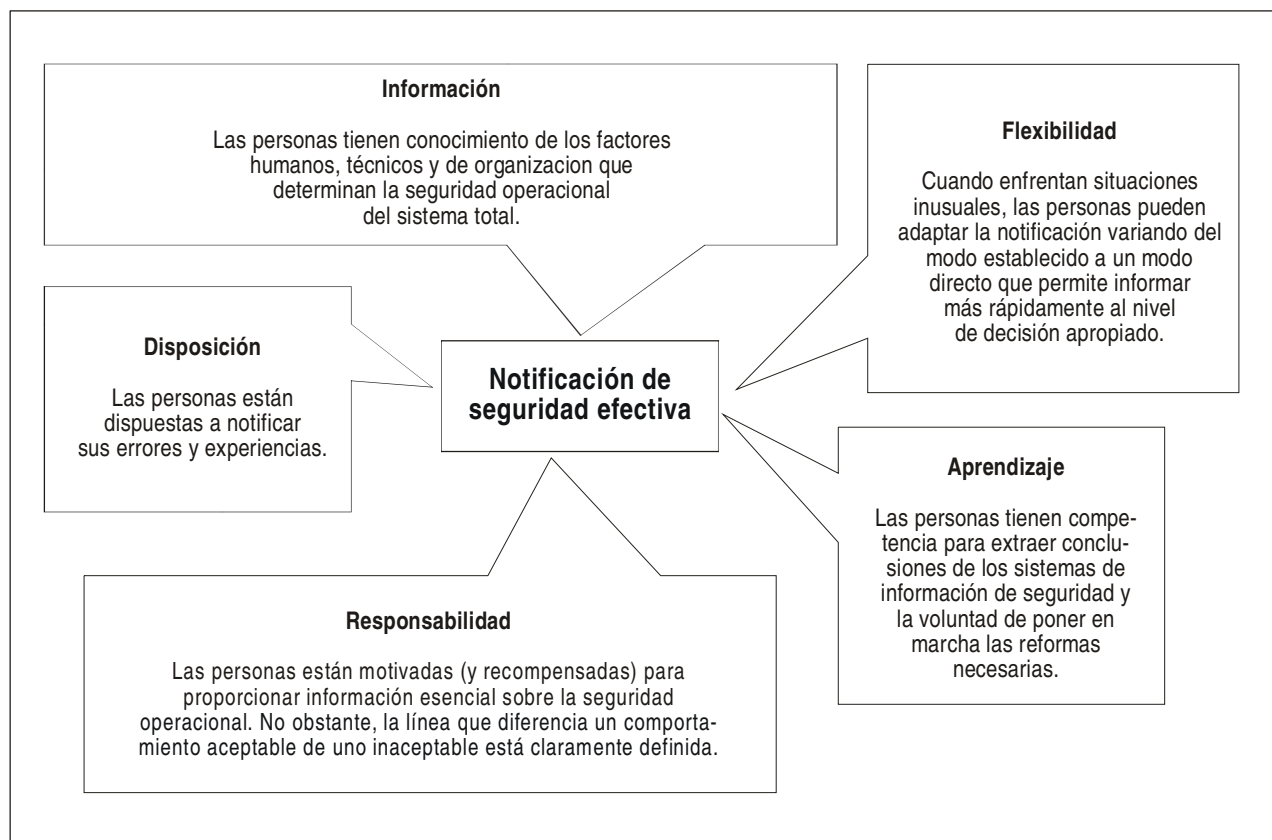


Figura 2-14. Notificación de seguridad efectiva — Cinco características básicas

- c) **Flexibilidad.** Como consecuencia del mantenimiento de opiniones realistas sobre los peligros subyacentes en las actividades de prestación de servicios de la organización y la elaboración de reglas realistas sobre los peligros y posibles fuentes de daños, el personal de operaciones puede adaptar la notificación de peligros cuando enfrente circunstancias inusuales, pasando del modo establecido a un modo directo que permita que la información llegue rápidamente al nivel apropiado de toma de decisiones.
- d) **Aprendizaje.** Como consecuencia de la conciencia de la importancia de comunicar la información sobre peligros a todos los niveles de la organización, el personal de operaciones tiene la competencia para extraer conclusiones de los sistemas de información de seguridad operacional, y la organización tiene la voluntad de implantar reformas importantes.
- e) **Responsabilidad.** Como consecuencia de la protección adecuada de los datos de seguridad operacional fundamentales y el fomento de un sistema de verificaciones y equilibrios que garantice que quienes notifiquen los peligros tengan confianza en que dicha notificación no se utilizará con otros fines que los previstos, se alienta (y recompensa) al personal de operaciones a que proporcione información de seguridad operacional fundamental relativa a los peligros. No obstante, hay una clara línea que diferencia entre actuación operacional aceptable y actuación inaceptable.

2.8.16 La notificación eficaz de seguridad operacional es una piedra fundamental de la gestión de la seguridad operacional. Una vez notificados, los datos sobre peligros se transforman en información de seguridad operacional. Por consiguiente, la notificación eficaz de seguridad operacional es la puerta para la adquisición de datos de seguridad. Una vez adquiridos, dichos datos deben gestionarse. La gestión de los datos de seguridad operacional se basa en tres etapas claramente definidas. Las dos primeras son la recolección de datos de seguridad operacional sobre peligros y el análisis de los datos de seguridad, para transformarlos en información. La tercera y frecuentemente no tenida en cuenta, es la mitigación o las actividades de respuesta a los peligros adoptadas por la organización como consecuencia de la información de seguridad operacional elaborada. La respuesta de la organización respecto de la información de seguridad sobre peligros puede variar desde una mitigación activa a una desatención lisa y llana.

2.8.17 La literatura sobre organizaciones propone tres caracterizaciones de las mismas, dependiendo de la forma en que responden a la información sobre peligros y a la gestión de la información de seguridad operacional:

- a) patológica — oculta la información;
- b) burocrática — restringe la información; y
- c) generadora — valora la información.

2.8.18 En la Tabla 2-1 se presenta una matriz de aspectos clave en la gestión de la información de seguridad en términos de las tres caracterizaciones de organización presentadas en 2.8.17.

	<i>Patológica</i>	<i>Burocrática</i>	<i>Generadora</i>
Información	Escondida	Ignorada	Buscada
Mensajeros	Eliminados	Tolerados	Entrenados
Responsabilidades	Disimuladas	Encapsuladas	Compartidas
Informes	Evitados	Permitidos	Recompensados
Fallas	Encubiertas	Disculpadas	Analizadas
Ideas nuevas	Restringidas	Problemáticas	Bienvenidas
Organización resultante	Organización conflictiva	Organización burocrática	Organización confiable
<i>Fuente: Ron Westrum</i>			

**Tabla 2-1. Tres posibles culturas de organización**

### **Notificación efectiva de seguridad operacional y cultura**

2.8.19 Los sistemas de notificación voluntaria que se elaboraron por primera vez a finales de los años 1970 se concentraban en la notificación de errores operacionales resultantes de condiciones o circunstancias existentes. La notificación efectiva de seguridad operacional, como se describe en este manual, va más allá procurando encontrar e identificar las causas de esos errores operacionales de modo que puedan eliminarse antes de que sucedan o mitigarse. Esto ha llevado a los sistemas de notificación voluntaria que también incluyen la notificación de peligros. Como regla general, lo que hay que gestionar es el peligro, y es más práctico, fácil y en gran medida eficaz, hacer la operación más segura que hacer la gente más segura. Por lo tanto, la identificación sistemática de peligros y otras deficiencias de seguridad puede aportar mucho más a la gestión de la seguridad operacional que la sola notificación de errores. No obstante, la diferencia entre notificación de errores y notificación de peligros es fundamental y puede conducir a problemas de implantación que deben reconocerse y tratarse. Una diferencia importante es que si bien la notificación de peligros es predictiva y debería ser objetiva y neutral, la notificación de errores es reactiva y puede incriminar al informante o a la persona sobre quien se informa, lo que podría conducir a la atribución de culpas y a la imposición de sanciones.

2.8.20 La notificación efectiva de seguridad operacional se basa en una notificación voluntaria de errores y peligros por las personas. Estas personas son principalmente miembros del personal de operaciones que coexisten con los peligros o los encuentran. No obstante, debido a que un peligro puede también ser más obvio para una persona no familiarizada o no conectada con una operación (y las circunstancias en las que se realice) no debería haber restricciones sobre quienes pueden informar y sobre qué. La notificación no debería desalentarse en modo alguno; de ahí que la protección de los informantes y las fuentes de información de seguridad fue, y sigue siendo, un aspecto clave y a menudo contencioso para establecer ambos tipos de sistemas de notificación, y podría constituir un obstáculo importante para el avance y el éxito de la gestión de la seguridad operacional.

2.8.21 Los intentos de proteger la información de seguridad operacional y al informante respecto de sanciones se desarrollaron empleando el término cultura, por ejemplo, "cultura no punitiva", "cultura sin atribución de culpa" y últimamente "cultura de la seguridad operacional" o "cultura de justicia". La palabra *cultura* tiene significados específicos y el contexto en que se use en este caso puede llevar a errores de percepción y de comprensión. No obstante, los términos cultura de seguridad operacional y cultura de justicia han pasado a ser ampliamente aceptados, aunque no



definidos universalmente, para describir el contexto en que las prácticas de seguridad se fomentan dentro de una organización. Estas prácticas de seguridad operacional comprenden una serie de procesos, procedimientos y políticas de la organización dirigidas a lograr un resultado específico, la identificación de peligros. Los procesos (notificación eficaz de seguridad operacional), procedimientos (sistema de notificación de peligros) y políticas (política de seguridad operacional, tratamiento justo de los informantes, etc.) son ideas y comportamientos complejos y específicos que pueden agruparse en forma de hacerlos fácilmente comprensibles a una gran audiencia y, con ello, más fáciles de aplicar en gran escala. No obstante, su contenido y aplicación reflejarán la cultura, en el verdadero sentido de la palabra, del estado u organización que los elabore. La adopción mundial de una única cultura de seguridad operacional de justicia común podría considerarse discriminatoria, quizás incluso discutible, si la cultura local no es la misma.

2.8.22 La política de seguridad operacional debería fomentar activamente la notificación efectiva de seguridad operacional y, definiendo la línea entre la actuación aceptable (a menudo errores no intencionales) y la actuación inaceptable (como negligencia, descuido, violaciones o sabotaje), proporcionar una justa protección a los informantes. No obstante, es posible que una cultura de seguridad operacional o de justicia no impida la “criminalización del error”, lo cual está legal, ética y moralmente dentro de los derechos soberanos de todos los Estados, siempre que se respeten los acuerdos internacionales establecidos. Una investigación judicial, y consecuencias de algún tipo, podrían esperarse después de un accidente o incidente grave especialmente si la falla del sistema resultó en pérdida de vidas o daño a propiedades, aunque no haya existido negligencia ni mala intención. Por consiguiente, podría existir un problema potencial si los informes voluntarios sobre peligros, que se relacionan con deficiencias latentes de un sistema o su performance, se tratan de la misma forma que los relativos a investigaciones de accidentes e incidentes graves. La intención de proteger los informes sobre peligros no debería disputar la legitimidad de una investigación judicial o demandar inmunidad indebida. No obstante, los argumentos jurídicos normalmente tienen precedencia sobre cualquier argumento técnico o relacionado con la seguridad.

2.8.23 Los Estados y organizaciones deberían tener en cuenta las ventajas y desventajas de adoptar una cultura de seguridad operacional y de justicia, y cualquier consecuencia cultural y jurídica. Para fines relacionados con la gestión de la seguridad operacional, el proceso que debe promoverse, alimentarse y defenderse es la notificación eficaz de seguridad operacional; la “criminalización del error” tiene menos relevancia. La notificación eficaz de la seguridad operacional puede lograrse en muchas formas diferentes y aplicando varias estrategias diferentes. Cómo se logra debería dejarse a las preferencias, posibilidades y limitaciones del contexto operacional específico en vez de proponer soluciones generales con la posibilidad de chocar con la cultura local.

## 2.9 INVESTIGACIÓN DE SEGURIDAD OPERACIONAL

2.9.1 La investigación de los sucesos de seguridad operacional es un componente importante de la gestión de la seguridad operacional. En el Capítulo 7 se caracteriza el proceso de investigación de accidentes como el guardameta final de la seguridad del sistema. El valor de la investigación de seguridad operacional es proporcional al enfoque con arreglo al cual se lleva a cabo la investigación.

2.9.2 El enfoque tradicional analizado en 2.3.8 describe lo que se conoce como investigación de seguridad operacional con fines “funerarios”:

- a) dejar atrás las pérdidas;
- b) reafirmar la confianza y la fe en el sistema;
- c) reanudar las actividades normales; y
- d) cumplir fines políticos.

2.9.3 El concepto de causalidad del suceso que se describe en la Sección 2.4, y la noción de accidente de organización analizada en la Sección 2.5, se relacionan con lo que se conoce como investigación de seguridad operacional para mejorar la fiabilidad del sistema:

- a) para aprender sobre las vulnerabilidades del sistema;
- b) para elaborar estrategias de cambio; y
- c) para establecer prioridades en las inversiones de recursos de seguridad operacional.

2.9.4 Para cerrar este capítulo, se presenta esquemáticamente un ejemplo de cada enfoque de la investigación de seguridad operacional. Ambos ejemplos se refieren a la investigación de accidentes.

### **Investigación de seguridad operacional con fines funerarios**

#### **2.9.5 Hechos**

- Un carguero cuatrimotor turbohélice de vieja generación con dos tripulantes como únicos ocupantes opera en condiciones graves de engelamiento durante un vuelo nocturno interno.
- Como consecuencia de la acumulación de hielo, se apagan los motores 2 y 3, y siete minutos después falla el motor 4. La tripulación logra volver a encender el motor número 2.
- La aeronave presenta ahora una condición de considerable asimetría de potencia, con ambos motores de la izquierda funcionando y los dos de la derecha fuera de servicio. La tripulación experimenta graves dificultades en controlar la aeronave.
- Debido a la alta demanda impuesta a las fuentes de energía eléctrica restantes, no es posible repartir la carga eléctrica y el sistema eléctrico pasa a utilizar la batería. La tripulación queda con instrumentación de emergencia limitada para mantener el control de la aeronave, radiocomunicaciones limitadas y capacidades de navegación también limitadas.
- Al intentar realizar un aterrizaje de emergencia, se agota la energía de la batería y se pierde toda energía eléctrica.
- Todo lo que queda a la tripulación de vuelo es el giróscopo de emergencia autoalimentado, una linterna y los instrumentos de los motores también autoalimentados.
- La tripulación de vuelo no puede mantener el vuelo controlado y la aeronave se estrella fuera de control.

#### **2.9.6 Conclusiones de la investigación de seguridad operacional**

- La tripulación de vuelo no usó el radar meteorológico para evitar las condiciones de engelamiento.
- La tripulación de vuelo no consultó la lista de verificación de emergencia para resolver las fallas de los motores y del sistema eléctrico.
- La tripulación de vuelo se vio enfrentada a una situación exigente que requería decisiones y medidas claras.

- La aeronave volaba en condiciones de engelamiento que excedían las condiciones de certificación de los motores.
- La tripulación de vuelo no solicitó desviación a un aeródromo cercano.
- La tripulación de vuelo no utilizó la fraseología correcta para declarar la emergencia.
- La tripulación de vuelo ejerció una pobre gestión de los recursos de tripulación (CRM).
- Hubo un mal manejo de los sistemas de la aeronave.
- La presentación de la información visual en la lista de verificación de emergencia fue deficiente.
- Hubo problemas respecto de procedimientos internos de garantía de la calidad para operaciones de vuelo.

### 2.9.7 **Causas**

- falla múltiple de motores;
- realización incompleta de ejercicios de emergencia;
- medidas de la tripulación de vuelo para controlar y volver a encender los motores;
- resistencia al avance por las hélices no perfiladas;
- peso del hielo;
- CRM deficiente;
- falta de planes de contingencia; y
- pérdida de conocimiento de la situación.

### 2.9.8 **Recomendaciones de la seguridad operacional**

- La autoridad debería recordar a los pilotos que usaran fraseología correcta.
- La autoridad debería investigar la forma más eficaz de presentar el material de referencia de emergencia.

### **Investigación de seguridad operacional para mejorar la fiabilidad del sistema**

### 2.9.9 **Hechos**

- Una aeronave biturbohélice de transporte regional de vieja generación en vuelo regular de transporte de pasajeros realiza una aproximación que no es de precisión en condiciones meteorológicas marginales a un aeródromo remoto no controlado y sin radar.
- La tripulación de vuelo realiza una aproximación directa, en vez de seguir el completo procedimiento de aproximación publicado.

- Al alcanzar la MDA, la tripulación no adquiere referencias visuales.
- La tripulación de vuelo abandona la MDA sin haber adquirido referencias visuales y continúa el aterrizaje.
- La aeronave se estrella contra el terreno poco antes de la pista.

#### 2.9.10 **Conclusiones de la investigación de seguridad operacional**

- La tripulación de vuelo cometió numerosos errores y violaciones.

##### **Pero:**

- La integración de la tripulación de vuelo, si bien legal, no era favorable teniendo en cuenta las exigentes condiciones de vuelo.
- Con arreglo a la práctica de la compañía, el piloto realizó una aproximación rectilínea directa, lo que iba contra los reglamentos.
- El Estado no disponía de normas para operaciones de transporte complementario.
- En el Estado no había supervisión de las instalaciones de tránsito aéreo.
- Las autoridades habían pasado por alto violaciones anteriores de la seguridad operacional por el explotador.
- La legislación del Estado estaba desactualizada.
- La autoridad tenía objetivos conflictivos, es decir facilitar el desarrollo de la industria versus necesidades de vigilancia de la seguridad operacional.
- La autoridad carecía de recursos para cumplir sus responsabilidades.
- No había una política aeronáutica del Estado para apoyar a la autoridad.
- Había deficiencias en el sistema de instrucción del Estado.

#### 2.9.11 **Causas**

- la decisión de la tripulación de continuar la aproximación por debajo de la MDA sin contacto visual;
- la decisión estuvo influida por presiones operacionales; y
- la decisión estuvo influida por la deficiente cultura de seguridad operacional de la línea aérea.

#### 2.9.12 **Recomendaciones de seguridad operacional**

- El informe comprende varias recomendaciones de primera línea respecto de la actuación de la tripulación de vuelo.

- El informe también contiene recomendaciones con respecto a:
    - revisar el proceso de otorgar AOC por la autoridad;
    - revisar el sistema de instrucción del Estado;
    - definir una política aeronáutica que proporcione apoyo a las actividades de la administración aeronáutica;
    - reformar la legislación aeronáutica existente;
    - reforzar la legislación existente como medida provisional; y
    - mejorar los sistemas de investigación de accidentes y los procesos de inspección de aeronaves y aerovías.
-



## Capítulo 3

# INTRODUCCIÓN A LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

### 3.1 OBJETIVO Y CONTENIDO

3.1.1 En este capítulo se analiza la necesidad de una gestión de la seguridad operacional así como las correspondientes estrategias y características básicas. El capítulo trata de las diferencias entre la gestión de la seguridad operacional como un proceso de la organización y la prevención de accidentes como actividad correctiva.

3.1.2 El capítulo comprende los temas siguientes:

- a) el estereotipo de la seguridad operacional;
- b) el dilema gerencial;
- c) necesidad de la gestión de la seguridad operacional;
- d) estrategias para la gestión de la seguridad operacional;
- e) el imperativo de cambio;
- f) gestión de la seguridad operacional — ocho pilares básicos; y
- g) cuatro responsabilidades para gestionar la seguridad operacional.

### 3.2 EL ESTEREOTIPO DE LA SEGURIDAD OPERACIONAL

3.2.1 La aviación ha estado impregnada por una percepción errónea respecto del lugar que le cabe a la seguridad operacional, en términos de prioridad, en el espectro de objetivos que persiguen las organizaciones aeronáuticas, independientemente del carácter de los servicios que dichas organizaciones podrían prestar. Esta percepción errónea se ha transformado en un estereotipo aceptado universalmente: en aviación, la seguridad operacional es la primera prioridad. Si bien son social, ética y moralmente impecables debido a su reconocimiento inherente del valor supremo de la vida humana, el estereotipo y la visión que transmite pierden validez cuando se les considera desde la perspectiva de que la gestión de la seguridad operacional es un proceso de organización.

3.2.2 Todas las organizaciones de aviación, independientemente de su carácter, tienen un componente empresarial en mayor o menor grado. Así pues, todas las organizaciones de aviación pueden considerarse como empresas. Corresponde entonces plantearse una sencilla pregunta para arrojar luz sobre la veracidad o no del estereotipo de seguridad operacional: ¿cuál es el objetivo fundamental de una organización empresarial? La respuesta a esta pregunta es obvia: prestar el servicio para el cual se creó la organización en primer lugar, alcanzar objetivos de producción y finalmente producir dividendos para los accionistas.

3.2.3 No hay ninguna organización de aviación que se haya creado para brindar solamente seguridad. Aún las organizaciones que se desempeñan como guardianes de la seguridad operacional de la aviación están sujetas a limitaciones de eficacia, internas o externas, dictadas por sus partes interesadas. Esto comprende la Organización de Aviación Civil Internacional, las administraciones de aviación civil nacionales y supra nacionales, las organizaciones de comercio internacional y las organizaciones internacionales que bregan por la seguridad operacional.

3.2.4 En el Capítulo 2 se analiza la forma en que la seguridad operacional se ve cada vez más como consecuencia de la gestión de ciertos procesos de organización, con el objetivo final de mantener los riesgos de seguridad de las consecuencias de los peligros en contextos operacionales bajo control de la organización. La gestión de procesos de organización específicos, la mayoría de carácter empresarial, es una condición necesaria para permitir a las organizaciones alcanzar sus objetivos de producción mediante la prestación de servicios. Estos procesos de organización, incluyendo las comunicaciones, la asignación de recursos, la planificación y la supervisión, también se analizaron en el Capítulo 2. La gestión de estos procesos se realiza mediante funciones empresariales básicas y sistemas de gestión, como la gestión financiera, la gestión de recursos humanos y la gestión jurídica.

3.2.5 La perspectiva que se presenta en este manual es que la seguridad operacional no es la primera prioridad de las organizaciones de aviación. La gestión de la seguridad operacional es solo otro proceso de organización que permite a las organizaciones aeronáuticas lograr sus objetivos empresariales mediante la prestación de sus servicios. Por consiguiente, la gestión de la seguridad operacional es solo otra función empresarial básica que debe considerarse al mismo nivel y con la misma importancia que otras funciones empresariales básicas y se realiza mediante un sistema de gestión especializado (sistema de gestión de la seguridad operacional o SMS, que se analiza en el Capítulo 7).

### 3.3 EL DILEMA GERENCIAL

3.3.1 La perspectiva de la gestión de la seguridad operacional como proceso de organización y de la gestión de la seguridad operacional como función empresarial básica coloca claramente la responsabilidad por la seguridad operacional y la responsabilidad de la función a los más altos niveles de las organizaciones aeronáuticas (sin negar la importancia de la responsabilidad individual en la prestación de los servicios). En ninguna parte son más evidentes estas responsabilidades que en las decisiones respecto a la asignación de recursos.

3.3.2 Los recursos disponibles para las organizaciones aeronáuticas son finitos. No hay organización de aviación con recursos infinitos. Los recursos son esenciales para realizar las funciones empresariales básicas de una organización que directa o indirectamente apoyen la prestación de servicios. Por consiguiente, la asignación de recursos es uno de los procesos más importantes, si no el más importante, de la organización de los cuales la administración superior es responsable.

3.3.3 A menos que la organización adhiera al concepto de gestión de la seguridad operacional como función empresarial básica, es posible que exista una competencia perjudicial en la asignación de recursos para realizar las funciones empresariales básicas que directa e indirectamente apoyan la prestación de servicios. Dicha competencia puede llevar a un dilema gerencial que ha sido denominado "dilema de las dos P".

3.3.4 En términos sencillos, el "dilema de las dos P" puede caracterizarse como el conflicto que surgiría a nivel de la administración superior de la organización debido a la percepción de que los recursos deben asignarse a uno solo de los objetivos que se consideran excluyentes: objetivos de producción (prestación de servicios) u objetivos de protección (seguridad operacional).

3.3.5 En la Figura 3-1A se muestra una asignación equilibrada de recursos a los objetivos de producción y de protección resultante de los procesos de toma de decisiones en la organización basados en la gestión de la seguridad operacional como función empresarial básica (es decir, sólo otra función empresarial básica). Debido a que la gestión de la seguridad operacional se considera como solamente otro proceso de la organización y sólo otra función



empresarial básica, la seguridad operacional y la eficacia no están en conflicto sino estrechamente entrelazadas. Esto resulta en una asignación equilibrada de los recursos para garantizar que la organización está protegida mientras produce. En este caso, se ha enfrentado con éxito el “dilema de las dos P”. En realidad, puede argumentarse que en este caso el dilema no existe.

3.3.6 Lamentablemente, la historia de la aviación muestra que la resolución efectiva del dilema no ha sido algo común. Lo que la historia muestra es una tendencia de las organizaciones a caer en un desequilibrio en la asignación de recursos debido a la percepción de esa competencia entre la producción y la protección. En casos en que dicha competencia surge, la protección es normalmente la perdedora, pues las organizaciones privilegian los objetivos de producción (aunque plantean muchos argumentos en contrario). Inevitablemente, según se muestra en la Figura 3-1B, esta toma de decisiones parcial por parte de la organización conduce a una catástrofe. Sólo es cuestión de tiempo.

3.3.7 En la Figura 3-1C se muestra una alternativa a la asignación parcial de recursos analizada en los dos párrafos precedentes. En este caso, la inclinación en la asignación de recursos se da hacia el platillo de la balanza que representa la protección, lo que conduce a la bancarrota. Aunque esta alternativa es difícil de encontrar en los anales de la historia aeronáutica, sirve no obstante de alerta sobre la importancia de una adopción de decisiones sensata por parte de la organización con respecto a la asignación de recursos. En análisis final, es claro que el desarrollo del “dilema de las dos P” desaparece con una perspectiva de organización que se concentre en la gestión de la seguridad operacional como función empresarial básica, al mismo nivel y con la misma importancia que otros procesos empresariales básicos. De esta forma, la gestión de la seguridad operacional pasa a ser parte del tejido de la organización, y se garantiza una asignación de recursos conmensurable con los recursos generales disponibles en la organización.

3.3.8 El fundamento de la gestión de la seguridad operacional como función empresarial básica puede ampliarse a un argumento final que resulta considerablemente pertinente a los procesos subyacentes de la identificación de peligros y la gestión de riesgos de seguridad, así como las actividades y funciones operacionales involucradas en la gestión de la seguridad operacional (se analizan en los Capítulos 4 y 5).

3.3.9 Dado que el objetivo principal de las organizaciones de aviación es la prestación de servicios, la oportuna y eficaz prestación de los servicios puede a veces entrar en conflicto con consideraciones de seguridad operacional. Por ejemplo, debido a la necesidad de cumplir su horario, un avión debe aterrizar en un aeropuerto determinado a una hora determinada independientemente de las condiciones meteorológicas, el volumen del tránsito, las limitaciones aeroportuarias y limitaciones similares que se relacionan absolutamente con la prestación del servicio. Si las consideraciones de eficiencia en la prestación del servicio (necesidad de cumplir un horario) desaparecen, la seguridad operacional (condiciones meteorológicas adversas, alto volumen de tránsito, limitaciones aeroportuarias) cesarían de ser un factor. La operación se realizaría solamente cuando las limitaciones han desaparecido. No obstante, esto no es práctico debido a que destruiría la viabilidad de la industria de la aviación. Por consiguiente, las operaciones aeronáuticas deben realizarse en las condiciones dictadas no tanto por las consideraciones de seguridad operacional sino más bien por consideraciones de prestación de servicios.

3.3.10 El corolario es claro: los aspectos de seguridad operacional de la aviación no son ni inherentes ni condición natural de las operaciones de aviación, sino un producto colateral de la necesidad y la realización de actividades relacionadas con la producción o prestación de servicios. Esto refuerza la idea de gestión de la seguridad operacional como función empresarial básica que conduce a un análisis de los recursos y objetivos de una organización para lograr una asignación equilibrada y realista de los recursos entre los objetivos de protección y los de producción, en apoyo de las necesidades generales de la prestación de servicios por la organización.

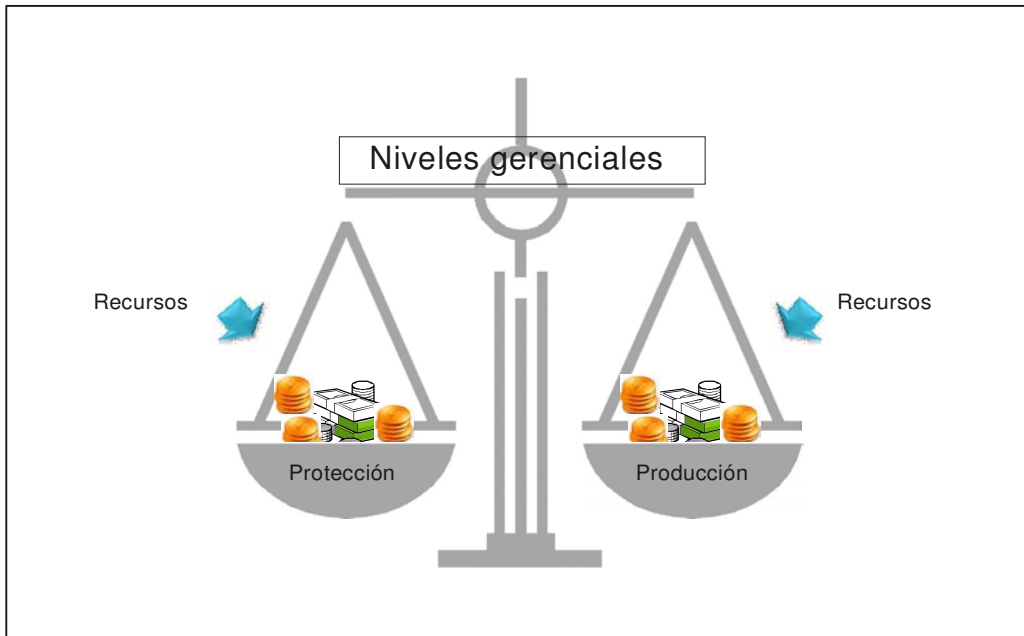


Figura 3-1A. El dilema gerencial

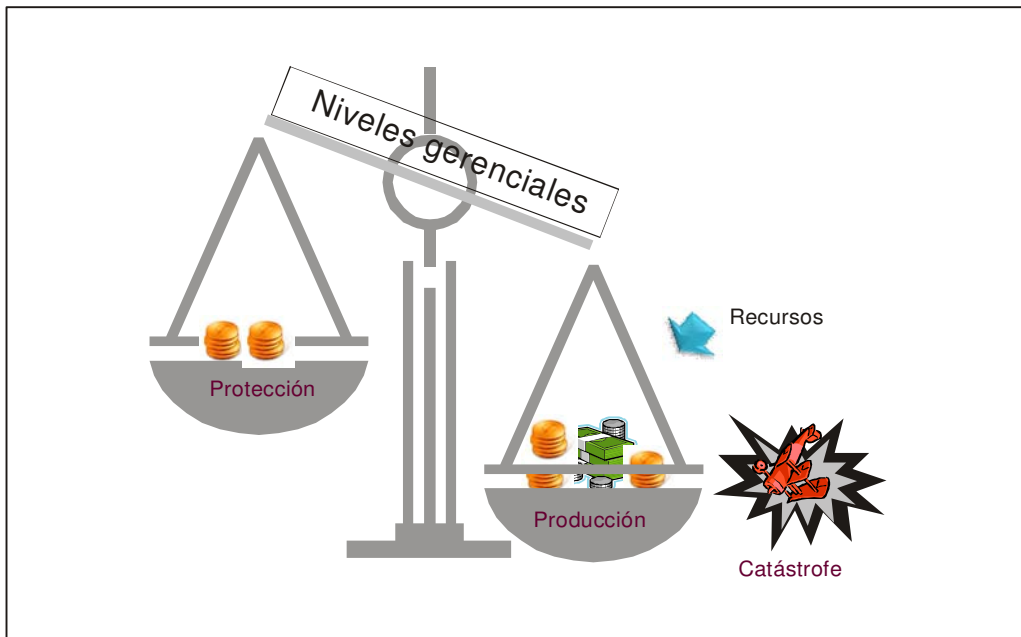
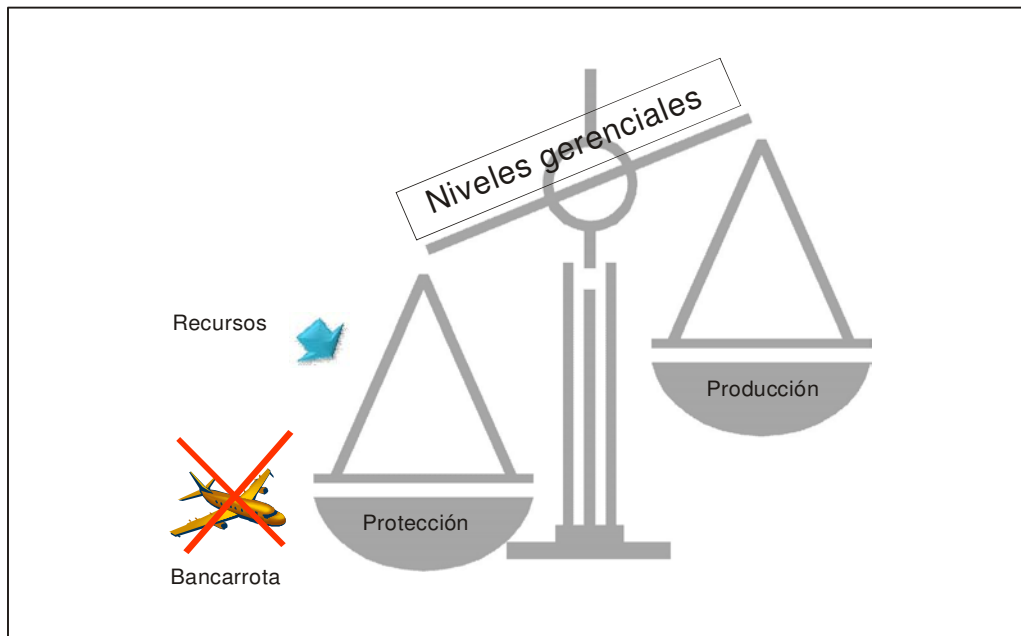


Figura 3-1B. El dilema gerencial



**Figura 3-1C. El dilema gerencial**

### 3.4 NECESIDAD DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

3.4.1 Tradicionalmente, la necesidad de la gestión de la seguridad operacional se ha justificado sobre la base del crecimiento previsto de la industria y de la posibilidad de un aumento en los accidentes como consecuencia de tal crecimiento. Si bien la reducción de los accidentes seguirá siempre siendo una prioridad de la aviación, hay razones más apremiantes que las proyecciones estadísticas que fundamentan la transición a un entorno de gestión de la seguridad operacional en la aviación civil internacional de todo el mundo.

3.4.2 La aviación es sin duda el modo de transporte masivo más seguro y uno de los sistemas sociotécnicos de producción más seguros en la historia de la humanidad. Este logro toma particular relevancia cuando se considera la juventud de la industria de la aviación, que se mide en décadas, frente a otras industrias cuyas historias abarcan siglos. Es un tributo a la comunidad de la seguridad operacional de la aviación y su incesante dedicación el hecho de que en solamente un siglo la aviación haya progresado, desde una perspectiva de seguridad operacional, de un sistema frágil al primer sistema ultraseguro en la historia del transporte. En retrospectiva, la historia de la fiabilidad de la seguridad operacional de la aviación puede dividirse (al igual que la evolución del pensamiento sobre seguridad de la aviación analizada en el Capítulo 2) en tres eras distintas, cada una de ellas con atributos fundamentalmente diferentes.

3.4.3 En la primera era, que abarca desde los días pioneros de comienzos de los años 1900 hasta aproximadamente el final de los años sesenta (la era técnica presentada en el Capítulo 2), la aviación podía caracterizarse como un sistema frágil desde el punto de vista de la fiabilidad de la seguridad. Las fallas de seguridad operacional, si bien no constituían sucesos diarios, no eran infrecuentes. Era lógico entonces que la comprensión de la seguridad operacional y las estrategias de prevención se derivaran principalmente de las investigaciones de accidentes. Realmente no existía un sistema propiamente dicho sino que la industria funcionaba porque los individuos literalmente se encargaban de hacerla avanzar. El foco de la seguridad operacional estaba en los individuos y en la gestión individual de los riesgos de seguridad, que a su vez se basaba en los elementos proporcionados por programas de instrucción intensivos.

3.4.4 Durante la segunda era, de comienzos de los años setenta hasta mediados de los noventa (la era humana), la aviación no sólo pasó a ser un sistema, sino un sistema seguro. La frecuencia de las fallas de seguridad operacional disminuyó considerablemente y se desarrolló gradualmente una comprensión más global de la seguridad operacional que iba más allá de los individuos para examinar el sistema más amplio. Naturalmente, esto condujo a una búsqueda de experiencias de seguridad operacional más allá de las obtenidas en investigaciones de accidentes, y entonces el énfasis se volcó a la investigación de incidentes. Este cambio a una perspectiva más amplia de la seguridad y la investigación de incidentes estuvo acompañado por la introducción masiva de tecnología (como la única forma de satisfacer la creciente demanda de producción del sistema) y el correspondiente aumento múltiple de los reglamentos de seguridad operacional.

3.4.5 Desde mediados de los años noventa al presente (la era de organización), la aviación ingresó en su tercera era de fiabilidad de la seguridad operacional, pasando a ser un sistema ultraseguro (es decir un sistema que experimenta menos de una falla catastrófica de la seguridad operacional cada millón de ciclos de producción). Desde una perspectiva mundial y no obstante excepciones regionales, los accidentes pasaron a ser infrecuentes al punto de considerarse sucesos excepcionales, o anomalías del sistema. Los incidentes graves también disminuyeron y se vieron más apartados entre sí. En concierto con esta reducción de los sucesos se consolidó el viraje hacia una perspectiva más amplia y sistémica de la seguridad operacional que había comenzado durante la era anterior. Para esta consolidación fue fundamental la adopción de un enfoque más comercial de la gestión de la seguridad operacional, basado en la recolección y análisis regular de datos operacionales diarios. Este enfoque más comercial de la seguridad operacional constituye el fundamento de los sistemas de gestión de la seguridad operacional (SMS) que se analizan en el Capítulo 7. En términos sencillos, SMS es la aplicación de prácticas de gestión comercial a la gestión de la seguridad operacional. La Figura 3-2 ilustra la evolución de la seguridad operacional relatada anteriormente.

3.4.6 La aplicación de prácticas de gestión comercial a la seguridad operacional de la aviación, con su subyacente recolección y análisis regular de datos operacionales, tiene como objetivo la creación del espacio de seguridad operacional referido en el Capítulo 2. Dentro de ese espacio de seguridad, la organización puede moverse libremente en la prestación de sus servicios, con la seguridad de que está dentro de un espacio de resistencia máxima frente a los riesgos de seguridad operacional de las consecuencias de los peligros que existen en el contexto en el que debe funcionar para prestar sus servicios.

3.4.7 La importancia de una asignación equilibrada de recursos para lograr los objetivos de protección y producción e impedir así que surja el “dilema de las dos P”, ya se ha analizado. Como ampliación de ese análisis, la noción de producción y protección es pertinente para la definición de los límites del espacio de la seguridad operacional de una organización según se muestra en la Figura 3-3.

3.4.8 Se recordará que la toma de decisiones de la organización que conduce a una asignación excesiva de recursos a la protección puede tener consecuencias sobre el estado financiero de la organización y, por lo menos teóricamente, podría conducir en última instancia a la bancarrota. Por lo tanto es esencial definir límites, límites que, si la organización se les aproxima en su movimiento dentro del espacio de seguridad, pueden proporcionar aviso anticipado de que se está creando o ya existe una situación de asignación desequilibrada de los recursos. Existen dos lados del espacio de seguridad operacional, o dos límites: el límite financiero y el límite de seguridad operacional.

3.4.9 El límite financiero es definido por la administración financiera de la organización. Para desarrollar un sistema de aviso temprano de que la organización se acerca al límite financiero, la administración de finanzas no tiene en cuenta el peor resultado posible (bancarrota). Las prácticas de gestión financiera se basan en la recolección y el análisis diario de indicadores financieros específicos: tendencias del mercado, cambios en los precios de los artículos y recursos externos necesarios para que la organización pueda prestar sus servicios. Al hacerlo, la administración financiera no sólo define el límite financiero del espacio en seguridad operacional, sino que también reajusta constantemente su posición.

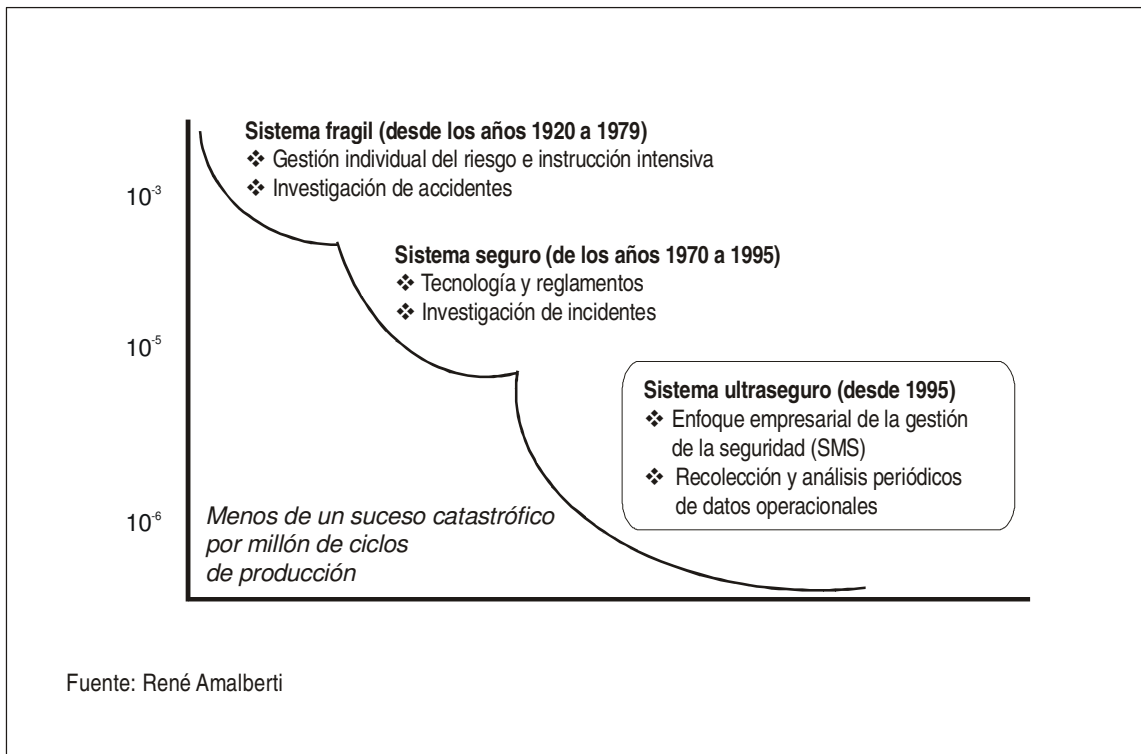


Figura 3-2. El primer sistema industrial ultraseguro

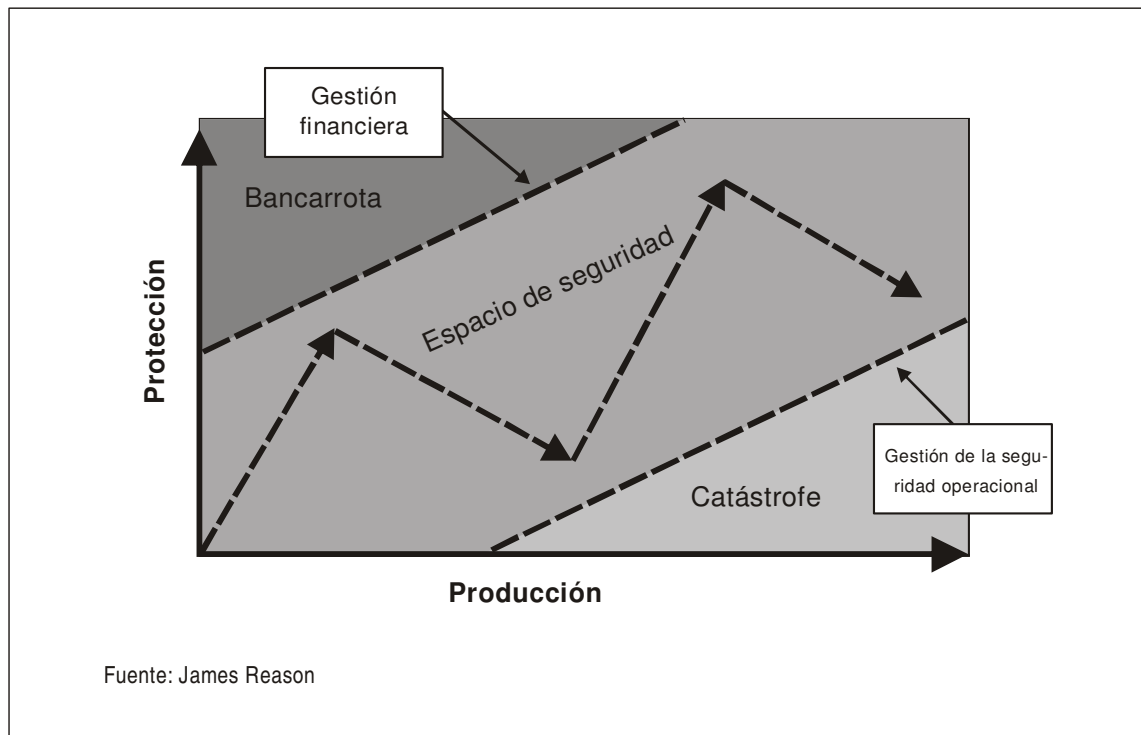


Figura 3-3. El espacio de seguridad operacional

3.4.10 Se recordará también que la toma de decisiones en la organización que conduce a una asignación excesiva de recursos al sector de producción puede tener consecuencias sobre la actuación de la organización en materia de seguridad operacional y podría conducir en última instancia a la catástrofe. Por consiguiente, es esencial que se defina un límite de seguridad operacional que proporcione un aviso temprano de que existe o se está desarrollando una situación de asignación desequilibrada de recursos, en este caso con respecto a la protección. El “límite de seguridad operacional” del espacio de seguridad operacional debería ser definido por la administración de seguridad de la organización.

3.4.11 Este límite es fundamental para alertar a la organización de que se privilegian los objetivos de producción, lo que en última instancia podría conducir a la catástrofe. Lamentablemente, no hay paralelismo entre las prácticas empleadas por la administración financiera y por la administración de seguridad operacional. Debido a la noción profundamente enraizada de que la seguridad operacional equivale a la ausencia de accidentes o incidentes graves, el límite de seguridad del espacio de seguridad operacional raramente existe en las organizaciones de aviación. En realidad, puede afirmarse que pocas o ninguna organizaciones de aviación han desarrollado efectivamente un espacio de seguridad operacional.

3.4.12 Aunque existen avisos tempranos y banderas de alerta, en el ámbito de la seguridad operacional, en su mayoría son ignorados o no reconocidos y las organizaciones se enteran de que han desequilibrado la asignación de recursos cuando experimentan un accidente o un incidente grave. Así pues, a diferencia de la administración financiera, en la perspectiva de la seguridad operacional como ausencia de accidentes o incidentes graves, la organización busca tener en los resultados peores (o más bien en la ausencia de ellos) una indicación de que la gestión de la seguridad operacional ha sido exitosa. Este enfoque no es gestión de la seguridad operacional sino más bien control de daños. Las organizaciones de aviación deben adoptar un enfoque de gestión de la seguridad para garantizar que se define el límite de seguridad para cerrar el círculo con el “límite financiero” y definir así el espacio de seguridad operacional de la organización.

3.4.13 La evolución de la fiabilidad de la seguridad operacional analizada en 3.4.3 a 3.4.5 apoya la necesidad de elaborar medios adicionales y alternativos de la recolección de datos de seguridad, más allá de los informes de accidentes e incidentes. Hasta finales de los años setenta la recopilación de datos de seguridad operacional se hacía mayormente mediante la investigación de accidentes e incidentes y se hizo cada vez más escasa a medida que las mejoras en la seguridad llevaban a una reducción en la cantidad de accidentes. Además, en términos de adquisición de datos de seguridad operacional, los procesos de investigación de accidentes e incidentes graves son reactivos: necesitan un activador (una falla de seguridad) para el proceso de recolección de datos de seguridad operacional.

3.4.14 Como consecuencia de la necesidad de mantener un volumen constante de datos de seguridad operacional, los datos de accidentes e incidentes graves se complementaron con datos de seguridad operacional obtenidos de sistemas de recolección ampliados. En los sistemas ampliados, se dispone de datos de seguridad operacional de sucesos de poca gravedad mediante programas de notificación obligatoria o voluntaria. En términos de adquisición de datos de seguridad, estos nuevos sistemas son proactivos, dado que los sucesos activadores requeridos para iniciar el proceso de recolección de datos de seguridad tienen consecuencias considerablemente menores que los que activan el proceso de captura de datos de seguridad en accidentes e incidentes graves. No obstante, sigue siendo cierto que los datos de seguridad operacional obtenidos con los programas de notificación pasan a estar disponibles solamente después de que deficiencias de seguridad operacional originan un suceso de consecuencias leves.

3.4.15 A comienzos de los años noventa, se hizo evidente que para sostener la seguridad operacional en el sistema ultraseguro a fin de apoyar el enfoque comercial de la seguridad en que se basa el SMS, se necesitaban grandes volúmenes de datos de seguridad, adquiridos sin necesidad de sucesos activadores. Esto condujo al desarrollo de sistemas de recolección de datos de seguridad operacional predictivos, para complementar los sistemas de recolección de datos de seguridad operacional existentes que tenían carácter proactivo y reactivo. Con ese fin, se introdujeron sistemas electrónicos de adquisición de datos y programas de autonotificación sin riesgos, para recoger datos de seguridad de operaciones normales sin necesidad de sucesos activadores para iniciar el proceso de recolección de datos. La más reciente adición a los sistemas predictivos de recolección de datos de seguridad operacional son los sistemas de adquisición de datos basados en la observación directa por parte del personal operacional durante operaciones normales.

3.4.16 Existe una sólida justificación para recoger datos de seguridad de las operaciones normales de aviación. A pesar de su excelencia en la materia, el sistema de aviación, al igual que cualquier otro sistema artificial, está lejos de ser perfecto. La aviación es un sistema abierto; funciona en un entorno natural no controlado y está sujeto a perturbaciones ambientales. Es sencillamente imposible diseñar desde el comienzo un sistema abierto perfecto, aunque más no sea porque es imposible prever todas las posibles interacciones operacionales entre personas, tecnología y el contexto en que tienen lugar las operaciones aeronáuticas. La vigilancia de las operaciones normales en tiempo real permite identificar y corregir carencias y deficiencias que no se previeron durante el diseño del sistema. Este argumento se presenta con más detalle en 3.4.17 a 3.4.19.

### La deriva práctica

3.4.17 Durante las primeras etapas del diseño de un sistema, dos cuestiones principales ocupan la mente de los diseñadores, teniendo en cuenta los objetivos de producción declarados del sistema:

- a) ¿qué recursos se necesitan para lograr esos objetivos de producción? y
- b) ¿cómo puede protegerse el sistema de peligros durante las operaciones necesarias para lograr los objetivos de producción?

Los diseñadores del sistema utilizan métodos diferentes para responder a estas cuestiones. Uno de esos métodos consiste en definir escenarios plausibles (tantos como sea posible) de interacciones operacionales entre personas, tecnología y el contexto operacional, a efectos de identificar posibles peligros en dichas interacciones.

3.4.18 El resultado final del proceso es un diseño inicial del sistema basado en tres hipótesis básicas: la tecnología necesaria para lograr los objetivos de producción del sistema, la instrucción necesaria para que las personas puedan operar adecuadamente la tecnología, y los reglamentos y procedimientos que rigen el comportamiento del sistema y de las personas. Esta hipótesis son el fundamento de la actuación teórica (o ideal) del sistema. Para fines de esta explicación, la actuación ideal o teórica del sistema (es decir cómo debería funcionar el sistema) puede representarse gráficamente como una línea recta (Figura 3-4).

3.4.19 Se ensayan las hipótesis, se valida la actuación teórica y, en última instancia, el sistema pasa a ser operacional. Una vez instalado, el sistema actúa según el diseño, la mayoría de las veces con arreglo a la actuación teórica. No obstante, a menudo la actuación operacional es distinta de la actuación teórica. En otras palabras, una vez que los sistemas pasan a ser operacionales, se desarrolla gradual pero inexorablemente una deriva progresiva de la actuación teórica prevista con arreglo a las hipótesis de diseño del sistema hacia la actuación operacional del mismo, como consecuencia de las operaciones en la vida real. Dado que esta deriva es consecuencia de la práctica diaria, se le conoce como “deriva práctica”.

3.4.20 Una deriva práctica desde una actuación teórica a una actuación operacional real es inevitable en cualquier sistema, independientemente de lo cuidadosa y bien concebida que haya sido la planificación de diseño. Las razones de la deriva práctica son múltiples: tecnología que no siempre funciona con arreglo a lo previsto; procedimientos que no pueden ejecutarse según lo previsto en condiciones operacionales dinámicas; reglamentos que no tienen plenamente en cuenta las limitaciones de contexto; introducción de cambios sutiles en el sistema después de su diseño sin la correspondiente reevaluación de su impacto en las hipótesis básicas del diseño; adición de nuevos componentes al sistema sin una adecuada evaluación de seguridad de los peligros que dichos componentes pueden introducir; interacción con otros sistemas y así sucesivamente. Así pues, cabe afirmar que en todo sistema, las personas realizan las actividades dirigidas a la prestación de servicios dentro de la deriva. No obstante, permanece el hecho de que a pesar de todas las carencias del sistema que condujeron a la deriva, las personas que operan dentro de dicha deriva hacen que el sistema funcione con carácter cotidiano. Los individuos aplican adaptaciones locales y estrategias personales (que encarnan la experiencia colectiva de profesionales operacionales de la aviación), superando así las carencias del sistema. Este proceso de adaptación se refleja en la expresión familiar “la forma en que trabajamos aquí, más allá de lo que diga el libro”.

3.4.21 La captación de lo que tiene lugar dentro de la deriva práctica mediante medios formales (p. ej., obteniendo formalmente conocimientos colectivos) tiene un considerable potencial de aprendizaje sobre adaptaciones exitosas de seguridad y, por consiguiente, para el control de los riesgos de seguridad operacional. La captación oficial de experiencia y conocimientos colectivos puede transformarse en intervenciones formales para el rediseño o mejora del sistema, si se aplica con arreglo a principios dicho potencial de aprendizaje. En el lado negativo, la proliferación descontrolada de adaptaciones locales y estrategias personales pueden hacer que la deriva práctica se aleje demasiado de la actuación teórica prevista, en la medida en que un incidente o accidente se hace posible. La Figura 3-4 ilustra la noción de la deriva práctica planteada en este párrafo.

### 3.5 ESTRATEGIAS PARA LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

3.5.1 Es inevitable el desarrollo de la deriva práctica. Todas las organizaciones de aviación, incluso las más sólidas y resistentes, realizan sus operaciones diarias dentro de la deriva práctica. La deriva práctica es sencillamente inherente al carácter de los sistemas de producción sociotécnicos, dinámicos y abiertos, de los cuales la aviación es un ejemplo principal. Con carácter cotidiano, en su prestación de servicios, las organizaciones navegan por la deriva práctica buscando colocarse tan lejos como sea posible de los puntos en que dicha deriva está en su máximo, y tan cerca como sea posible de su punto de origen. Durante esta navegación diaria, las organizaciones deben superar “corrientes” u obstáculos potencialmente opuestos: estos son los peligros que surgen como consecuencia de una asignación desequilibrada de recursos para apoyar las necesidades de la organización y de la no resolución del “dilema de las dos P”.

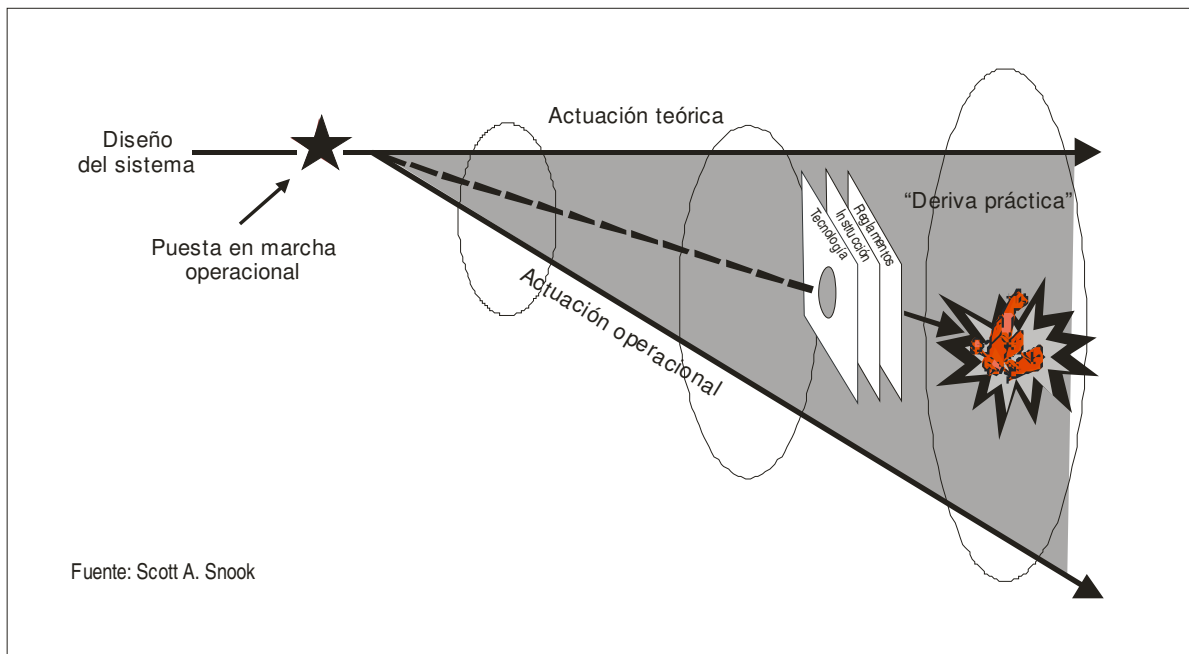


Figura 3-4. La deriva práctica



3.5.2 Para navegar con éxito en la deriva práctica, las organizaciones necesitan ayudas para la navegación que generen la información necesaria para enfrentar corrientes y obstáculos (véase la Figura 3-5). Estas ayudas para la navegación captan datos operacionales que, una vez analizados, informarán a las organizaciones sobre los mejores pasajes a través de las corrientes y obstáculos. Existen varias ayudas para la navegación disponibles a las organizaciones aeronáuticas que pueden agruparse en tres tipos según la gravedad de las consecuencias del suceso activador que inició el proceso de captación de datos de seguridad: reactivas, proactivas y predictivas.

3.5.3 Las ayudas para la navegación **reactivas** requieren que ocurra un suceso activador muy grave que a menudo puede tener considerables consecuencias perjudiciales, a efectos de iniciar el proceso de captación de datos de seguridad operacional. Las ayudas para la navegación reactivas se basan en la noción de esperar hasta que “algo se rompa para arreglarlo”. Son muy apropiadas para situaciones que entrañen fallas de tecnología o sucesos inusuales. Las ayudas para la navegación reactivas son parte integral de una gestión de la seguridad operacional madura. La contribución de estas ayudas a la gestión de la seguridad operacional depende, no obstante, de la medida en que la información que generan va más allá de las causas que activaron el suceso, y la asignación de culpas, e incluyen factores contribuyentes y conclusiones respecto de los riesgos de seguridad. La investigación de accidentes e incidentes graves es un ejemplo de ayuda para la navegación reactiva.

3.5.4 Las ayudas para la navegación **proactivas** exigen que tenga lugar un suceso activador menos grave, probablemente con poca o ninguna consecuencia, a efectos de iniciar el proceso de captación de datos de seguridad. Las ayudas para la navegación proactivas se tratan en la noción de que las fallas del sistema pueden minimizarse mediante la identificación de riesgos de seguridad operacional dentro del sistema antes de que ocurra la falla y adoptando las medidas necesarias para mitigar dichos riesgos. Los sistemas de notificación obligatoria o voluntaria, las auditorías de la seguridad operacional y las encuestas de la seguridad operacional son ejemplos de ayudas para la navegación proactivas.

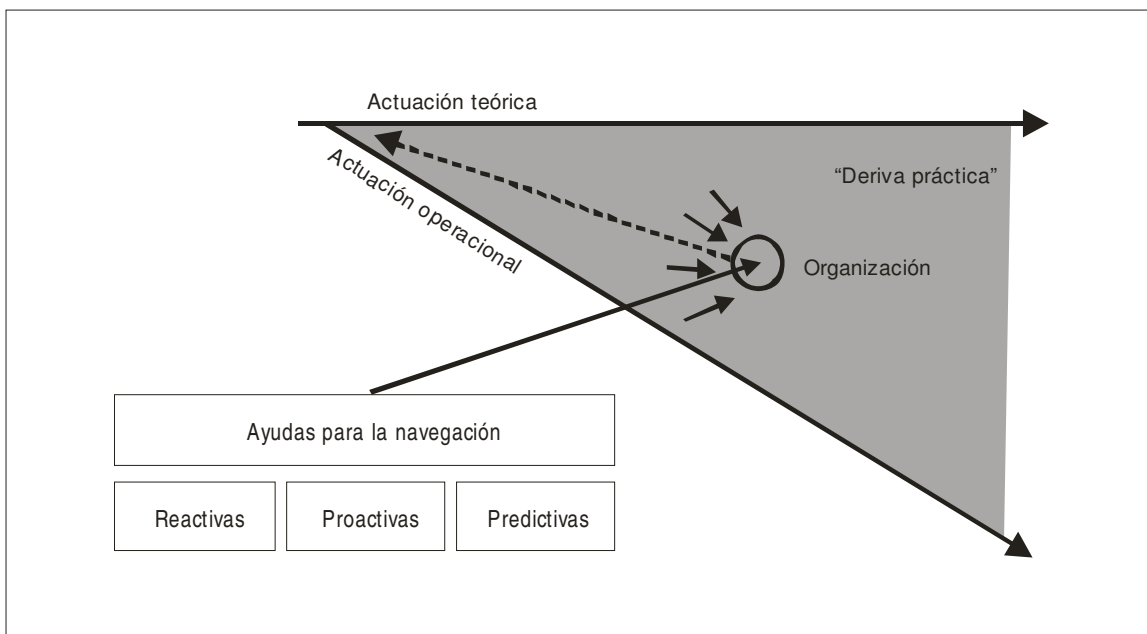


Figura 3-5. Navegando la deriva práctica

3.5.5 Las ayudas para la navegación **predictivas** no requieren que tenga lugar un suceso activador para iniciar el proceso de captación de datos de seguridad operacional. Los datos operacionales ordinarios se captan continuamente y en tiempo real. Las ayudas para la navegación predictivas se basan en la noción de que la mejor forma de lograr la gestión de la seguridad operacional es tratar de encontrar los problemas, y no esperar a que se presenten. Por consiguiente, los sistemas predictivos de captura de datos de seguridad operacional procuran agresivamente obtener información de seguridad que pueda ser indicativa de riesgos de seguridad operacional emergentes de una variedad de fuentes.

3.5.6 Los sistemas predictivos de recopilación de datos de seguridad son esencialmente sistemas estadísticos, mediante los cuales se recoge y analiza un considerable volumen de datos operacionales que individualmente en su mayoría carecen de significado, y se combinan con datos de los sistemas reactivos y proactivos de recopilación de datos. El agregado de los datos conduce así al desarrollo de una muy completa información que permite a las organizaciones navegar en torno de obstáculos y corrientes y colocarse en los lugares óptimos dentro de la deriva. Los sistemas de notificación de peligros, el análisis de datos de vuelo y la vigilancia normal de las operaciones son ejemplos de ayudas para la navegación predictivas.

3.5.7 Los sistemas de captura de datos de seguridad, reactivos, proactivos y predictivos, proporcionan datos de seguridad operacional para estrategias equivalentes de gestión de la seguridad operacional, reactivas, proactivas y predictivas, que a su vez son base de métodos de mitigación específicos reactivos, proactivos y predictivos. Un resumen de las estrategias de gestión de la seguridad operacional, según se vieron en los párrafos anteriores, se presenta en la Figura 3-6.

3.5.8 La gestión madura de la seguridad operacional exige la integración de sistemas de captura de datos de seguridad reactivos, proactivos y predictivos, una juiciosa combinación de estrategias de mitigación reactivas, proactivas y predictivas y la elaboración de métodos de mitigación reactivos, proactivos y predictivos. No obstante, es importante tener en cuenta que, al elaborar las estrategias de mitigación, cada uno de los tres sistemas de captura de datos de seguridad analizados recoge datos de seguridad operacional en diferentes niveles de la deriva operacional. Es igualmente importante tener en cuenta que cada una de las tres estrategias y métodos de mitigación interviene en niveles diferentes de la deriva práctica.

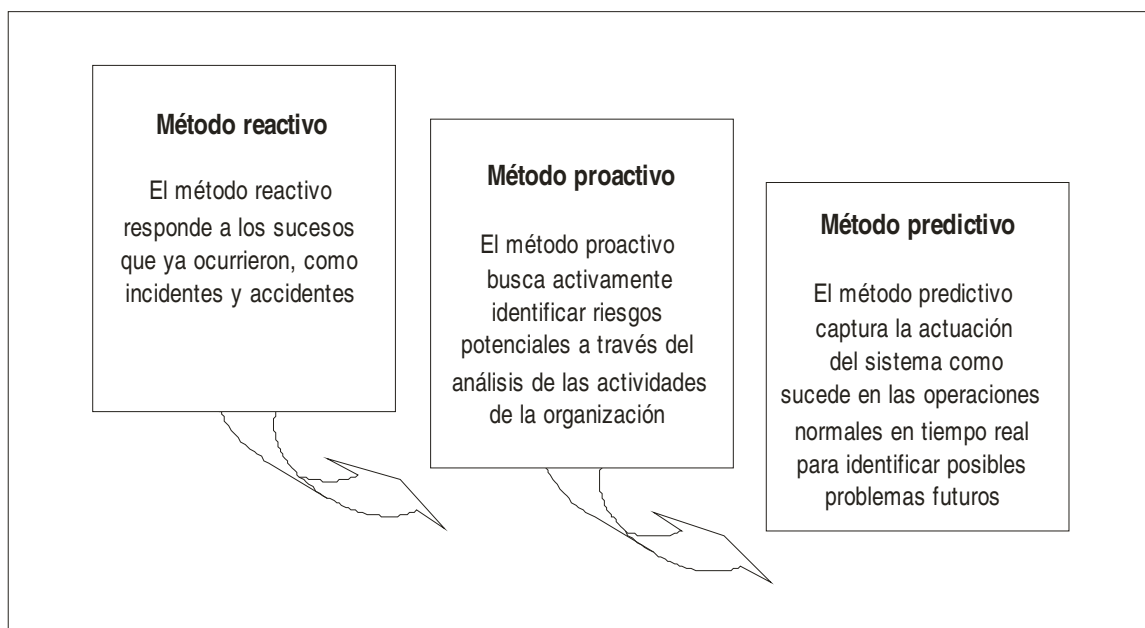


Figura 3-6. Estrategias de gestión de la seguridad operacional

3.5.9 Para ilustrar lo anterior, debemos regresar a la deriva práctica según se representó en la Figura 3-7. Existen peligros con carácter continuo a lo largo de la deriva práctica. Si no se contienen, viajarán a lo largo de la deriva con cada vez mayor potencial perjudicial. Cerca del punto de origen o surgimiento de la deriva práctica, los peligros son relativamente inocuos porque no han tenido oportunidad de desarrollar su potencial perjudicial. Cuanto más avanzan los peligros sin contención a lo largo de la deriva práctica, más impulso cobran y aumentan su potencial perjudicial. A medida que los peligros se aproximan al punto de mayor anchura de la deriva práctica, han desarrollado su potencial perjudicial máximo, incluyendo la posibilidad de fallas graves. Por consiguiente, es fundamental que la gestión de la seguridad operacional capture los peligros tan cerca como sea posible del punto de surgimiento de la deriva práctica.

3.5.10 Los sistemas, estrategias y métodos predictivos de captura de datos de seguridad operacional funcionan relativamente cerca del origen o punto de surgimiento de la deriva práctica. Este es un nivel de intervención muy elevado y muy eficiente. La razón de la elevada eficiencia de los sistemas, estrategias y métodos predictivos de captura de datos de seguridad es doble: por un lado, enfrentan los peligros cuando están en su infancia, no han tenido oportunidad de comenzar a desarrollar su potencial perjudicial y, por consiguiente, son más fáciles de contener. Debido a esto, las mitigaciones elaboradas a partir de los datos de seguridad operacional predictivos se transforman en redes o filtros de contención tan ajustados que bloquean casi totalmente el pasaje de los peligros emergentes hacia más adelante del continuo de la deriva práctica.

3.5.11 Los sistemas, estrategias y métodos proactivos de captura de datos de seguridad operacional también se aplican en las primeras partes de la deriva práctica y del continuo de peligros, pero no tan cerca del origen o surgimiento de la deriva práctica como los sistemas, estrategias y métodos predictivos. También se trata de un elevado nivel de intervención muy eficiente. No obstante, los peligros han tenido la oportunidad de comenzar a desarrollar su potencial perjudicial. Debido a esto, las mitigaciones elaboradas a partir de los datos de seguridad operacional proactivos se transforman en redes o filtros de contención que, si bien son de textura ajustada, permiten el pasaje de peligros en desarrollo hacia más adelante del continuo.

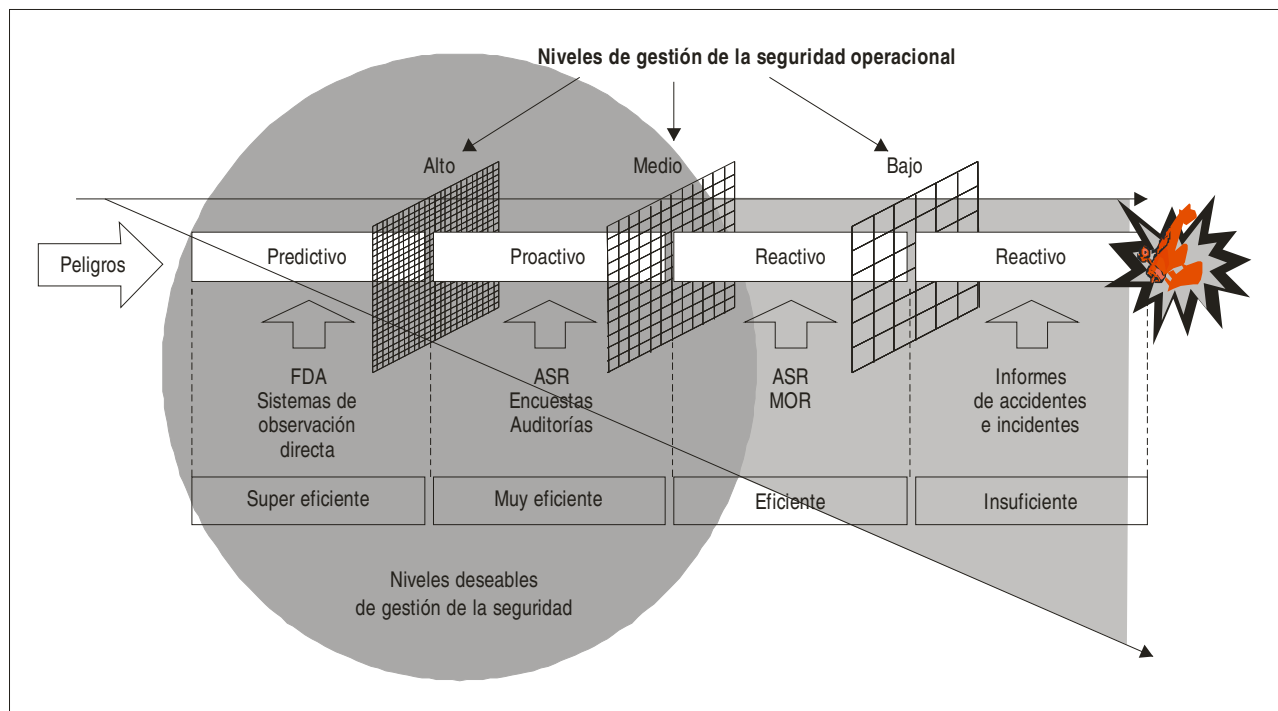


Figura 3-7. Estrategias — Niveles de intervención y herramientas

3.5.12 Los sistemas, estrategias y métodos reactivos de captura de datos de seguridad operacional funcionan en dos niveles de la deriva práctica. Algunos, como los sistemas de notificación obligatoria de sucesos, funcionan en un nivel de intervención medio. Se trata también de un nivel eficiente, pero los peligros han continuado creciendo en su potencial perjudicial. Las mitigaciones elaboradas a partir de este primer nivel de datos de seguridad operacional reactivos pasan a ser redes o filtros de contención con una textura más abierta que puede ser penetrada frecuentemente por los peligros. En el nivel más bajo de los sistemas, estrategias y métodos reactivos de captura de datos de seguridad operacional, la investigación de accidentes e incidentes graves se realiza con carácter de reparación de daños. La información obtenida a partir de datos de seguridad operacional puramente reactivos es insuficiente para la gestión de la seguridad operacional.

### 3.6 EL IMPERATIVO DE CAMBIO

3.6.1 A medida que continúan creciendo las actividades y la complejidad de la aviación mundial, los contextos operacionales profundamente modificados con sus nuevos retos hacen que los métodos tradicionales de gestionar la seguridad operacional a un nivel aceptable sean menos efectivos y eficaces. Es necesario contar con métodos diferentes y evolucionados de comprender y gestionar la seguridad operacional. Actualmente se registra una transición en la aviación civil internacional que refleja un cambio significativo con respecto al paradigma abrazado por las actividades de seguridad operacional del pasado.

3.6.2 Como ya se analizó, el paradigma tradicional de seguridad operacional se basaba en el proceso de investigación de accidentes e incidentes graves como principal intervención y método de seguridad, desarrollado a partir de tres hipótesis básicas:

- a) el sistema de aviación funciona la mayoría del tiempo según las especificaciones de diseño (actuación básica);
- b) el cumplimiento de los reglamentos garantiza la actuación básica del sistema y, por consiguiente, garantiza la seguridad operacional (basada en el cumplimiento); y
- c) debido a que el cumplimiento de las normas garantiza la actuación básica del sistema, las desviaciones menores y casi sin consecuencias durante las operaciones ordinarias (es decir procesos) no importan, y sólo las desviaciones mayores que lleven a consecuencias perjudiciales (es decir resultados) importan (orientada a los resultados).

3.6.3 En contraste, está evolucionando un paradigma de seguridad operacional contemporáneo, que es el apoyado por este manual. Se basa en la noción de gestión de la seguridad operacional mediante el control de los procesos, más allá de la investigación de sucesos, y se apoya en tres hipótesis básicas:

- a) el sistema de aviación no funciona la mayoría del tiempo según especificaciones de diseño (la actuación operacional real conduce a la deriva práctica);
- b) en vez de basarse exclusivamente en el cumplimiento de las normas, la actuación en tiempo real del sistema se vigila constantemente (basado en la eficacia); y
- c) las desviaciones menores y sin consecuencia durante las operaciones ordinarias se monitorean y analizan constantemente (orientada a los procesos).

### 3.7 GESTIÓN DE LA SEGURIDAD OPERACIONAL — OCHO PILARES BÁSICOS

3.7.1 Ocho elementos básicos y genéricos son el fundamento del proceso de gestión de la seguridad operacional, a saber:

- a) **El compromiso de la administración superior con la gestión de la seguridad operacional.** La gestión de la seguridad operacional, al igual que cualquier otra actividad de gestión, exige la asignación de recursos. Esta asignación de recursos es, en todas las organizaciones, una función de la administración superior, de ahí la necesidad del compromiso de dicha administración con la gestión de la seguridad operacional. En lenguaje claro: sin dinero no hay seguridad operacional.
- b) **Notificación efectiva de seguridad operacional.** Se sabe que “no se puede gestionar lo que no puede medirse”. Para gestionar la seguridad operacional, las organizaciones deben adquirir datos de seguridad sobre peligros que permitan realizar mediciones. La mayoría de tales datos se adquirirá mediante acciones voluntarias y de autonotificación del personal operacional. Por consiguiente, es fundamental que las organizaciones desarrollen entornos de trabajo en que tenga lugar la notificación efectiva de seguridad operacional por parte del personal.
- c) **Supervisión continua** mediante sistemas que recojan datos de seguridad operacional sobre peligros durante operaciones normales. La recolección de datos de seguridad es solo el primer paso. Más allá de la recolección, las organizaciones deben analizar y extraer información de seguridad a partir de los datos, porque datos recogidos y relegados a un cajón equivalen a ausencia de datos. Además, es fundamental compartir la información e inteligencia de seguridad operacional obtenidas con quienes operan el sistema diariamente porque son quienes están en constante contacto con los peligros, cuyas consecuencias procura mitigar la notificación eficaz de la seguridad operacional.
- d) **Investigación de sucesos de seguridad operacional** con el objetivo de identificar deficiencias de seguridad operacional del sistema en vez de asignar culpas. Identificar “quién lo hizo” no es tan importante como aprender “por qué sucedió”. La resistencia del sistema puede reforzarse mucho más eficazmente eliminando las deficiencias que eliminando individuos supuestamente “ineptos”.
- e) **Compartir las lecciones de seguridad operacional aprendidas y las mejores prácticas** mediante el intercambio activo de información de seguridad. Otro aforismo bien conocido ilustra elocuentemente la necesidad de compartir datos e intercambiar información de seguridad: “aprende de los errores de los demás, no vas a vivir lo suficiente como para cometerlos todos tú mismo”. La excelente tradición de la industria de la aviación de compartir datos de seguridad operacional debe mantenerse y, si es posible, reforzarse.
- f) **Integración de la instrucción en seguridad para el personal operacional.** Rara vez los programas de instrucción del personal operacional incluyen instrucción especial en seguridad operacional. Se supone que como la “seguridad operacional es responsabilidad de todos”, el personal de operaciones está integrado por expertos en seguridad operacional por derecho propio. La falacia de este razonamiento es evidente y se discute en el Capítulo 7. Hay una necesidad urgente de incluir instrucción especial que trate los aspectos básicos de la gestión de la seguridad operacional en todos los niveles de instrucción del personal.
- g) **Implantación efectiva de procedimientos operacionales normalizados (SOP)**, incluyendo el uso de listas de verificación y reuniones de información. Ya sea en el puesto de pilotaje, en una sala de control de tránsito aéreo, en un taller de mantenimiento o en la plataforma de un aeródromo, los SOP, las listas de verificación y reuniones de información están entre los mecanismos de seguridad operacional más efectivos con que cuenta el personal en el cumplimiento de sus responsabilidades diarias. También constituyen un poderoso mandato de la organización con respecto a la forma en que la administración

superior quiere que se realicen las operaciones. El valor de seguridad operacional de SOP, listas de verificación y reuniones de información realistas, adecuadamente escritos y constantemente cumplidos, no debería subestimarse jamás.

- h) **Mejora continua del nivel general de seguridad operacional.** La gestión de la seguridad operacional no es cuestión de un día. Es una actividad continua que sólo puede tener éxito si se la mejora constantemente.

3.7.2 El resultado de implantar estos ocho elementos básicos será una cultura de organización que fomente prácticas seguras, aliente la comunicación efectiva en seguridad operacional y gestione activamente dicha seguridad.

### 3.8 CUATRO RESPONSABILIDADES PARA GESTIONAR LA SEGURIDAD OPERACIONAL

3.8.1 Las responsabilidades para gestionar la seguridad operacional pueden agruparse en cuatro áreas genéricas y básicas, como sigue:

- a) **Definición de políticas y procedimientos respecto de la seguridad operacional.** Las políticas y los procedimientos son mandatos de la organización que reflejan la forma en que la administración superior desea que las operaciones se realicen. Por consiguiente, es esencial contar con una definición clara de políticas y procedimientos para brindar al personal operacional orientación clara sobre el comportamiento operacional que la organización espera del personal en las operaciones cotidianas.
- b) **Asignación de recursos para actividades de gestión de la seguridad operacional.** La gestión de la seguridad operacional requiere recursos. La asignación de recursos es una función administrativa. La administración tiene la autoridad y, por ello, la responsabilidad de asignar los recursos para mitigar los riesgos de seguridad operacional de las consecuencias de los peligros que amenazan las capacidades de la organización.
- c) **Adopción de mejores prácticas de la industria.** La tradición de la aviación con respecto a la excelencia en materia de seguridad operacional ha llevado al continuo desarrollo de sólidas prácticas de seguridad. Además, la aviación tiene una tradición con respecto al intercambio de información de seguridad operacional por canales tanto institucionales como informales. Estas dos características positivas deberían reforzarse y practicarse para fomentar la adopción de mejores prácticas de la industria.
- d) **Incorporación de reglamentos que rigen la seguridad operacional de la aviación civil.** Podría haber un error de percepción de que la gestión de la seguridad operacional hará redundantes o innecesarios los marcos normativos vigentes. Esta percepción errónea debe rechazarse en los términos más enérgicos. Siempre habrá necesidad de contar con un marco normativo como fundamento para las actividades de gestión de la seguridad operacional. En realidad, la gestión sensata de la seguridad operacional sólo puede desarrollarse a partir de reglamentos sensatos.

3.8.2 En resumen, la gestión de la seguridad operacional:

- a) abarca toda la operación;
- b) se concentra en procesos, haciendo una clara diferenciación entre procesos y resultados;
- c) se basa en datos;

- d) entraña supervisión constante;
  - e) está estrictamente documentada;
  - f) apunta al mejoramiento gradual en oposición a cambios abruptos; y
  - g) se basa en planificación estratégica en oposición a iniciativas parciales.
-





# Capítulo 4

## PELIGROS

### 4.1 OBJETIVO Y CONTENIDO

En este capítulo se presentan los fundamentos de la identificación y análisis de peligros y se abarcan los temas siguientes:

- a) peligros y consecuencias;
- b) primer fundamento — comprensión de los peligros;
- c) segundo fundamento — identificación de los peligros;
- d) tercer fundamento — análisis de peligros; y
- e) cuarto fundamento — documentación de los peligros.

### 4.2 PELIGROS Y CONSECUENCIAS

4.2.1 La identificación de peligros y la gestión de riesgos de seguridad operacional son los procesos centrales involucrados en la gestión de la seguridad operacional. No son nuevos ni se han elaborado como consecuencia del reciente interés en la gestión de la seguridad operacional y, en particular, en los sistemas de gestión de la seguridad operacional (SMS). La identificación de peligros y la gestión de riesgos de seguridad operacional son componentes dogmáticos en los que se basa el concepto total de seguridad operacional del sistema. Se trata de un enfoque totalmente incluyente y basado en conceptos de ingeniería que contribuyen al diseño del sistema y que fue elaborado hace más de cuarenta años. La diferencia entre la seguridad operacional del sistema tradicional y la gestión actual de la seguridad operacional es que, debido a sus fundamentos de ingeniería, la seguridad operacional del sistema se concentraba principalmente en las consecuencias para la seguridad de los aspectos y componentes técnicos del sistema en consideración, a veces a expensas del componente humano. Por otra parte, la gestión de la seguridad operacional se basa en el dogma de la seguridad operacional del sistema (identificación de peligros y gestión de riesgos de seguridad), y amplía la perspectiva para incluir los factores humanos y la actuación humana como consideraciones fundamentales de seguridad operacional durante el diseño y el funcionamiento del sistema.

4.2.2 La diferencia entre peligros y riesgos de seguridad operacional es a menudo fuente de dificultades y confusión. Para desarrollar prácticas de gestión de la seguridad operacional que sean pertinentes y efectivas, es esencial una clara comprensión de lo que constituye un peligro y lo que es un riesgo de seguridad operacional. En este capítulo se analizan exclusivamente los peligros, mientras que en el Capítulo 5 se analizan los riesgos de seguridad operacional. Para analizar los peligros y contribuir a la comprensión de la diferencia entre estos y los riesgos de seguridad, el tratamiento del tema divide el concepto general de peligro en dos componentes: el peligro en sí y sus consecuencias. Una clara comprensión de las diferencias entre estos dos componentes es también fundamental para la práctica de la gestión de la seguridad operacional.

4.2.3 Un peligro se define como una condición o un objeto que podría provocar lesiones al personal, daños al equipo o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita. Los sistemas en los que las personas deben interactuar activa y estrechamente con la tecnología para lograr los objetivos de producción mediante la prestación de servicios se conocen como sistemas sociotécnicos. Así pues, todas las organizaciones de aviación son sistemas sociotécnicos. Los peligros son componentes o elementos normales de los sistemas sociotécnicos. Son integrales a los contextos en que se produce la prestación de servicios por sistemas de producción sociotécnicos. Por sí mismos, los peligros no son “cosas malas”. Los peligros no son necesariamente componentes perjudiciales o negativos de un sistema. Sólo cuando los peligros interactúan con las operaciones del sistema dirigidas a la prestación de servicios, su potencial perjudicial puede transformarse en un problema de seguridad operacional.

4.2.4 Consideremos, por ejemplo, el viento, un componente normal del entorno natural. El viento es un peligro: es una condición con posibilidad de provocar lesiones al personal, daños al equipo o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita. Un viento de 15 nudos, por sí mismo, no necesariamente tendría el potencial de provocar daños durante operaciones aeronáuticas. En realidad, un viento de 15 nudos que sople directamente a lo largo de la pista contribuirá a mejorar la performance de las aeronaves durante la salida. No obstante, cuando un viento de 15 nudos sopla en dirección perpendicular a una pista en la que se realizará un aterrizaje o un despegue, se transforma en viento transversal. Es sólo entonces, cuando el peligro interactúa con las operaciones del sistema (despegue o aterrizaje de un avión) dirigidas a la prestación de un servicio (la necesidad de transportar pasajeros o carga hacia o desde el aeródromo particular cumpliendo un horario), que su potencial de producir daños pasa a ser un problema de seguridad operacional (una excursión lateral de la pista debido a que el piloto puede no controlar el avión como consecuencia del viento transversal). Este ejemplo ilustra el análisis de 4.2.3: un peligro no debería considerarse necesariamente como “cosa mala” o algo con connotaciones negativas. Los peligros son parte integral de los contextos operacionales, y sus consecuencias pueden tratarse mediante diversas estrategias de mitigación para contener el potencial perjudicial del peligro, lo que se analizará más adelante en este manual.

4.2.5 Una consecuencia se define como el posible resultado de un peligro. El potencial perjudicial de un peligro se materializa mediante una o varias consecuencias. En el ejemplo anterior del viento transversal, una consecuencia del peligro “viento transversal” podría ser “la pérdida de control lateral”. Otra consecuencia más grave podría ser la “excursión lateral de la pista”. Una consecuencia aún más grave podría ser “daños al tren de aterrizaje”. Por consiguiente, es importante describir todas las consecuencias posibles de un peligro durante el análisis del peligro y no sólo las más obvias o inmediatas.

4.2.6 El análisis de las consecuencias de los peligros nos lleva a tener en cuenta dos puntos importantes. En primer lugar, los peligros se dan en el presente. En la mayoría de los casos, son parte del contexto operacional y por lo tanto están presentes en el lugar de trabajo antes de que el personal “se presente a trabajar”. Como componentes físicos del contexto operacional o del lugar de trabajo, la mayoría de los peligros son, y deberían ser, detectables mediante auditorías. Por el contrario, las consecuencias pertenecen al futuro. No se materializan hasta que los peligros interactúan con ciertas operaciones del sistema dirigidas a la prestación de servicios. Como consecuencia de esta interacción los peligros pueden desencadenar su potencial perjudicial. Esto trae a colación un aspecto esencial de la gestión de la seguridad operacional: las estrategias de mitigación deberían dirigirse a contener en forma proactiva el potencial perjudicial de los peligros y no esperar hasta que las consecuencias de estos se materialicen y posteriormente tratarlas en forma reactiva.

4.2.7 En segundo lugar, para fines de gestión de seguridad operacional, las consecuencias de los peligros deberían describirse en términos operacionales. Muchos peligros tienen el potencial de producir la consecuencia final y más extrema (la pérdida de vidas humanas). La mayoría de los peligros dan a la pérdida de bienes, daños ecológicos y consecuencias similares de alto nivel. No obstante, describir las consecuencias de los peligros en términos extremos hace difícil diseñar estrategias de mitigación, excepto la cancelación de la operación. Para diseñar estrategias de mitigación que enfrenten los problemas de seguridad operacional subyacentes en las consecuencias operacionales no extremas y de bajo nivel del peligro (por ejemplo, el viento transversal), dichas consecuencias deben describirse en términos operacionales (excursión lateral de la pista), y no en términos extremos (pérdidas de vida).

4.2.8 En el Capítulo 2 se analiza la seguridad operacional como condición del riesgo de seguridad operacional controlado. La descripción de las consecuencias de los peligros que puedan afectar una operación particular es parte de la evaluación de los riesgos de seguridad operacional de las consecuencias de los peligros (analizados en el Capítulo 5). La evaluación de los riesgos de seguridad operacional de las consecuencias de los peligros permite a la organización tomar decisiones informadas sobre si puede lograr el control de los riesgos de seguridad operacional y continuar así la operación. Si las consecuencias del peligro (viento transversal) se describen en términos extremos (pérdida de vidas) en vez de términos operacionales (excursión lateral de la pista), la evaluación del riesgo de seguridad operacional no tiene en general sentido dado que la condición de control de los riesgos de seguridad operacional probablemente no se alcance, a menos que se incurra en gastos formidables y su mitigación probable será la cancelación de toda la operación.

### 4.3 PRIMER FUNDAMENTO — COMPRENSIÓN DE LOS PELIGROS

4.3.1 Como ya se analizó, existe una tendencia a confundir los peligros con sus consecuencias. Cuando esto sucede, la descripción del peligro en términos operacionales refleja las consecuencias más bien que el propio peligro. En otras palabras, no es raro ver que los peligros se describen como sus consecuencias.

4.3.2 Declarar y denominar un peligro como una de sus consecuencias tiene la posibilidad no sólo de ocultar el carácter verdadero y el potencial perjudicial del peligro en cuestión, sino también interferir con la identificación de otras consecuencias importantes del peligro.

4.3.3 Por un lado, la correcta declaración y denominación de los peligros permite identificar el carácter y el potencial perjudicial del peligro, deducir correctamente las fuentes o mecanismos del peligro y, lo que es más importante, evaluar los resultados (diferentes de los extremos) en términos de la magnitud de las pérdidas posibles, que constituye uno de los objetivos finales de la gestión de riesgo de la seguridad operacional según se analiza en el Capítulo 5.

4.3.4 Se presenta otro ejemplo para ilustrar la diferencia entre peligros y consecuencias. Un aeródromo opera con su sistema de señalización en mal estado. Esto complica la tarea de la navegación en tierra para los usuarios del aeródromo, tanto aeronaves como vehículos terrestres. En este caso, la nominación correcta del peligro podría ser “señalización del aeródromo no clara” (es decir, una condición con potencial de provocar lesiones al personal, daños al equipo o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita). Como resultado de este peligro, son posibles muchas consecuencias. Una consecuencia (es decir un resultado posible) del peligro (señalización de aeródromo no clara) podría ser “incursión en la pista”. Pero puede haber también otras consecuencias: vehículos terrestres que ingresen en áreas restringidas, aeronaves en rodaje hacia calles de rodaje erróneas, colisiones entre aeronaves, colisión entre vehículos terrestres, colisión entre aeronaves y vehículos terrestres, y así sucesivamente. Así pues, denominar el peligro como “incursión en la pista” en vez de “señalización de aeródromo no clara” oculta el carácter del peligro e interfiere con la identificación de otras consecuencias importantes. Esto conducirá probablemente a estrategias de mitigación parciales o incompletas.

4.3.5 Los peligros pueden agruparse en tres familias genéricas: peligros naturales, peligros técnicos y peligros económicos.

4.3.6 Los **peligros naturales** son consecuencia del hábitat o entorno en el que se realizan las operaciones dirigidas a la prestación de servicios. Los ejemplos de peligros naturales comprenden:

- a) condiciones meteorológicas o sucesos climáticos violentos (p. ej., huracanes, tormentas invernales, sequías, tornados, tormentas eléctricas, rayos y relámpagos y cizalladura del viento);

- b) condiciones meteorológicas adversas (p. ej., engelamiento, precipitación engelante, lluvia fuerte, nieve, vientos y restricciones a la visibilidad);
- c) sucesos geofísicos (p. ej., terremotos, volcanes, tsunamis, inundaciones y deslizamientos de tierra);
- d) condiciones geográficas (p. ej., terreno adverso o grandes masas de agua);
- e) sucesos ambientales (p. ej., incendios, actividades de fauna silvestre e infestación por insectos o plagas); o
- f) sucesos de salud pública (p. ej., epidemias de gripe u otras enfermedades).

4.3.7 Los **peligros técnicos** tienen su origen en fuentes energéticas (electricidad, combustible, presión hidráulica, presión neumática y así sucesivamente) o en funciones críticas para la seguridad operacional (posibilidad de fallas de soporte físico, mal funcionamiento del soporte lógico, advertencias y así sucesivamente) necesarias para las operaciones relacionadas con la prestación de servicios. Los ejemplos de peligros técnicos comprenden deficiencias respecto de:

- a) aeronaves y componentes, sistemas, subsistemas y equipo conexo de aeronaves;
- b) instalaciones, herramientas y equipo conexo de la organización; o
- c) instalación de sistemas, subsistemas y equipo conexo externos a la organización.

4.3.8 Los **peligros económicos** son consecuencia del entorno sociopolítico en el que se realizan las operaciones relacionadas con la prestación de servicios. Los ejemplos del peligro económico comprenden:

- a) crecimiento;
- b) recesión; y
- c) costo de materiales y equipo.

4.3.9 Las actividades de gestión de la seguridad operacional dirigidas a controlar los riesgos de seguridad operacional tratarán principalmente, pero no necesariamente con carácter exclusivo, los peligros técnicos y naturales.

#### 4.4 SEGUNDO FUNDAMENTO — IDENTIFICACIÓN DE PELIGROS

4.4.1 Ya se ha señalado que los peligros son parte de la estructura de cualquier sistema sociotécnico de producción. Por consiguiente, el ámbito de los peligros en la aviación es amplio. El ámbito de factores y procesos que deberían examinarse al proceder a la identificación de peligros comprende:

- a) factores de diseño, incluyendo diseño de equipo y tareas;
- b) procedimientos y prácticas operacionales, incluyendo su documentación y listas de verificación y su validación en condiciones reales de funcionamiento;
- c) comunicaciones, incluyendo medios, terminología y lenguaje;
- d) factores de personal, como las políticas de la compañía para contratación, instrucción, remuneración y asignación de recursos;

- e) factores de organización, como la compatibilidad de los objetivos de producción de seguridad operacional, la asignación de recursos, las presiones operacionales y la cultura de seguridad operacional de la compañía;
- f) factores del entorno laboral, como ruido y vibraciones, temperatura e iluminación ambientes, y la disponibilidad de equipo y ropas de protección;
- g) factores de vigilancia normativa, incluyendo la aplicación e imposición de reglamentos; la certificación de equipo, personal y procedimientos y la adecuación de la vigilancia;
- h) defensas, incluyendo factores como el suministro de sistemas adecuados de detección y aviso, la tolerancia al error del equipo y la capacidad de recuperación del equipo frente a errores y fallas; y
- i) actuación humana, restringida a condiciones médicas y limitaciones físicas.

4.4.2 Según se vio en el Capítulo 3, los peligros pueden identificarse después de sucesos de seguridad reales (accidentes o incidentes), o pueden identificarse mediante procesos proactivos y predictivos dirigidos a identificar los peligros antes de que precipiten sucesos de seguridad operacional. Hay una variedad de fuentes para la identificación de peligros. Algunas son internas a la organización mientras que otras son externas.

4.4.3 Las fuentes internas de identificación de peligros de que dispone una organización comprenden:

- a) análisis de datos de vuelo;
- b) sistema de notificación voluntaria de la compañía;
- c) encuestas de seguridad operacional;
- d) auditorías de la seguridad operacional;
- e) planes de supervisión normal de operaciones;
- f) análisis de tendencias;
- g) información obtenida de la instrucción; y
- h) investigación y seguimiento de incidentes.

4.4.4 Las fuentes externas de identificación de peligros de que dispone una organización comprenden:

- a) informes de accidentes;
- b) sistema estatal de notificación obligatoria de sucesos;
- c) sistema estatal de notificación voluntaria;
- d) auditorías estatales de vigilancia; y
- e) sistemas de intercambio de información.

4.4.5 El punto fundamental en este análisis es que ninguna fuente o programa sustituye por completo a las otras, o hace que otras fuentes o programas sean redundantes o innecesarios. La identificación de peligros realizada en el marco de prácticas maduras de gestión de la seguridad operacional recurre a una combinación sensata de fuentes internas y externas, procesos reactivos, proactivos y predictivos y sus programas presentes.

4.4.6 Todo el personal de las organizaciones de aviación debería recibir la instrucción apropiada en gestión de la seguridad operacional, a un nivel conmensurable con sus responsabilidades, de modo que todos los miembros de la organización estén preparados y en condiciones de identificar y notificar peligros. Desde este punto de vista, la identificación y notificación de peligros son responsabilidad de todos. No obstante, las organizaciones deben contar con personal especializado con la función exclusiva de identificar y analizar los peligros. Normalmente se trataría del personal asignado a la oficina de servicios de seguridad operacional, que se analiza en el Capítulo 8. Por consiguiente, ampliando la perspectiva anterior, en las organizaciones de aviación la identificación de peligros es responsabilidad de todos, pero la responsabilidad de la identificación de los peligros recae en el personal de seguridad operacional especializado.

4.4.7 La forma en que se identifican los peligros dependerá de los recursos y limitaciones de cada organización particular. Algunas organizaciones aplicarán programas de identificación de peligros completos y con mucha tecnología. Otras organizaciones aplicarán programas más modestos de identificación de peligros mejor adecuados a su tamaño y a la complejidad de sus operaciones. No obstante, la identificación de los peligros, independientemente de la aplicación, complejidad y tamaño, debe ser un proceso formal claramente descrito en la documentación de seguridad operacional de la organización. La identificación ad hoc de peligros es una práctica de gestión de la seguridad operacional inaceptable.

4.4.8 En el marco de prácticas de gestión de la seguridad operacional maduras, la identificación de peligros es una actividad continua, permanente y diaria. Nunca se detiene ni descansa. Es parte integral de los procesos de la organización dirigidos a la prestación de servicios a la que se dedica la organización. No obstante, hay tres condiciones específicas en las cuales se justifica la atención especial a la identificación de peligros. Estas tres condiciones deberían dar origen a actividades de identificación de peligros más profundas y de mayor alcance, y comprenden:

- a) toda vez que la organización experimente un aumento no explicado de sucesos relacionados con la seguridad operacional o infracciones a los reglamentos;
- b) toda vez que se prevean cambios operacionales importantes, incluyendo cambios del personal clave u otro equipo o sistemas importantes; y
- c) antes y durante períodos de cambios importantes en la organización, incluyendo el rápido crecimiento o contracción, fusiones empresariales, adquisiciones o reducción de volumen.

## 4.5 TERCER FUNDAMENTO — ANÁLISIS DE PELIGROS

4.5.1 La identificación de peligros no tiene sentido a menos que de los datos recogidos se extraiga información de seguridad operacional. La primera etapa en el desarrollo de la información de seguridad operacional es el análisis de peligros.

4.5.2 En esencia, el análisis de peligros es un proceso en tres etapas:

- a) **Primera etapa.** Identificar el peligro genérico (también conocido como peligro de máximo nivel o TLH). El término peligro genérico se emplea en el contexto de este manual con la intención de proporcionar concentración y perspectiva en un problema de seguridad operacional, contribuyendo al mismo tiempo a simplificar el seguimiento y la clasificación de muchos peligros individuales dimanantes del peligro genérico.

- b) **Segunda etapa.** Desglose del peligro genérico en peligros o componentes específicos del peligro genérico. Cada peligro específico tendrá probablemente un conjunto distinto y único de factores causales, lo que hace que cada peligro específico tenga carácter diferente y único.
- c) **Tercera etapa.** Relacionar los peligros específicos con consecuencias específicas posibles, es decir sucesos o resultados específicos.

4.5.3 A continuación se proporciona un ejemplo para ilustrar las nociones de peligro genérico, peligro específico y consecuencias. Un aeropuerto internacional que tramita cien mil movimientos por año inicia un proyecto de construcción para ampliar y repavimentar una de dos pistas que se cruzan. El siguiente proceso de análisis de peligros en tres etapas aplicaría:

- a) **Etapa A.** Declarar el peligro genérico (declaración de peligro o TLH)
  - construcción en aeropuerto
- b) **Etapa B.** Identificar peligros específicos o componentes específicos del peligro genérico
  - equipo de construcción
  - calles de rodaje cerradas, etc.
- c) **Etapa C.** Relacionar peligros específicos con consecuencias específicas
  - colisión de aeronaves con equipo de construcción (equipo de construcción)
  - ingreso de aeronaves en despegue a la calle de rodaje equivocada (calle de rodaje cerrada), etc.

4.5.4 El ejemplo de construcción de pistas en 4.5.3 puede utilizarse para ampliar el análisis sobre el “dilema de las dos P” del Capítulo 3 al análisis de peligros: el suministro eficiente y seguro del servicio exige un equilibrio constante entre los objetivos de producción y los objetivos de seguridad operacional. En el caso del ejemplo de la construcción de pistas, existe claramente un objetivo de eficiencia (producción): mantener las operaciones ordinarias del aeródromo durante las obras de construcción de las pistas. Existe un objetivo de seguridad operacional (protección) igualmente claro: mantener los márgenes de seguridad existentes en las operaciones de aeródromo durante las actividades de construcción en la pista. Al realizar el análisis de peligros, deben considerarse en primer lugar dos premisas básicas de la gestión de la seguridad operacional:

- a) los peligros son vulnerabilidades posibles inherentes a los sistemas sociotécnicos de producción. Son una parte necesaria del sistema como resultado de las capacidades que proporcionan o pueden posiblemente proporcionar al sistema para la prestación de sus servicios. Por consiguiente, los lugares de trabajo de la aviación contienen peligro cuyo tratamiento puede no ser rentable cuando deben continuar las operaciones; y
- b) la identificación de peligros no tiene sentido si se limita a las consecuencias de sucesos poco frecuentes en los que se han producido lesiones graves o daños importantes. Esto se muestra gráficamente en la Figura 4-1, conectando la identificación de peligros con la deriva práctica analizada en el Capítulo 3.

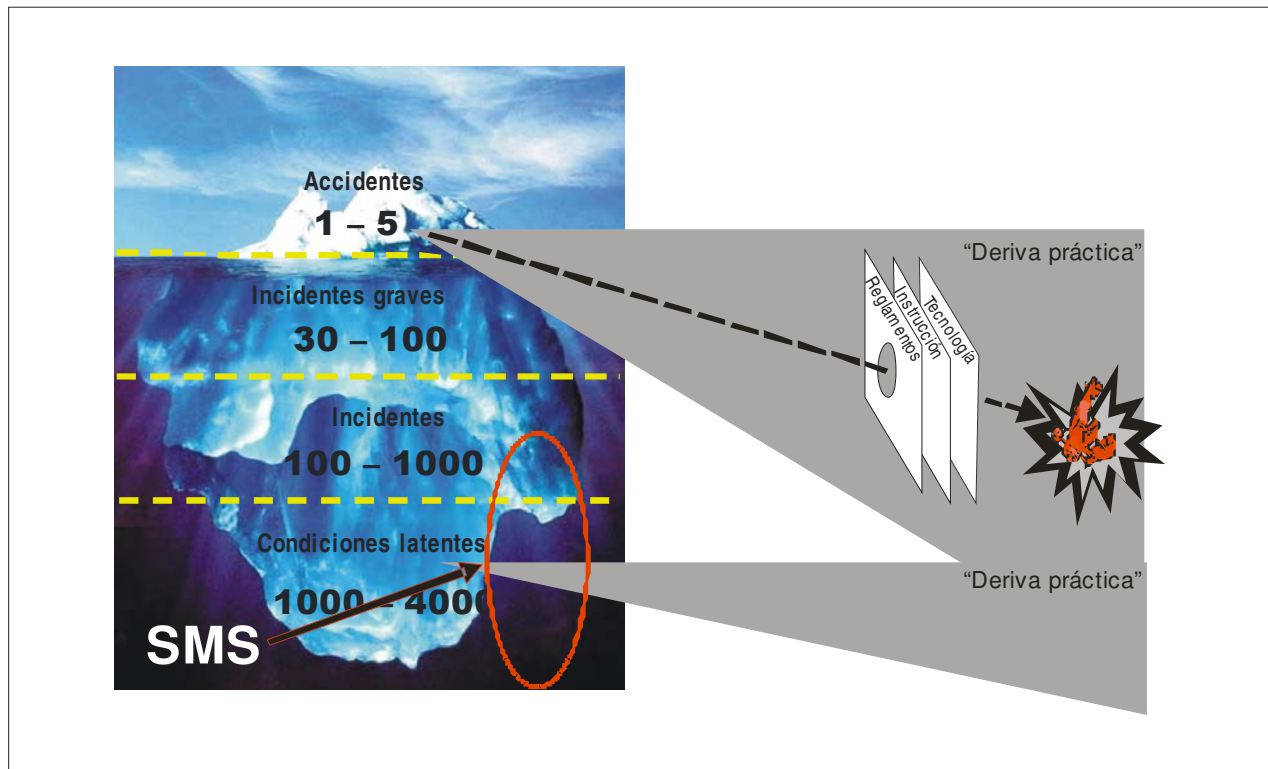


Figura 4-1. El foco de la identificación de peligros

#### 4.6 CUARTO FUNDAMENTO — DOCUMENTACIÓN DE LOS PELIGROS

4.6.1 Normalmente, los peligros se perpetúan en un sistema y desatan su potencial perjudicial principalmente debido a la ausencia o ineficacia de la identificación de peligros. La falta de identificación de peligros se debe a menudo a:

- a) no pensar sobre las condiciones operacionales con posibilidad de desatar el potencial perjudicial de los peligros;
- b) no conocer las condiciones operacionales con potencial de desencadenar el potencial perjudicial de los peligros;
- c) renuencia a considerar o investigar condiciones operacionales que pueden desencadenar el potencial perjudicial de los peligros; y
- d) renuencia a gastar dinero para investigar las condiciones operacionales que pueden desencadenar el potencial perjudicial de los peligros.

4.6.2 El desconocimiento y la renuencia solo pueden superarse mediante el conocimiento. Por lo tanto, la documentación oficial de los peligros es un requisito fundamental para la identificación de los peligros así como una característica de la gestión de la seguridad operacional madura. La información de seguridad operacional (es decir los datos brutos analizados) y la inteligencia de seguridad operacional (es decir, información de seguridad que ha sido



corroborada y analizada agregando contexto) se combinan para generar un conocimiento de la seguridad operacional que debe existir formalmente en la organización, y no en las mentes de miembros individuales de la misma. Un depósito oficial de conocimiento de seguridad operacional constituye una salvaguardia contra la volatilidad de la información. Además, una organización que tiene conocimiento histórico de la seguridad operacional adoptará las decisiones de seguridad operacional basándose en hechos y no en opiniones.

4.6.3 La gestión apropiada de la documentación respecto de la identificación de peligros es importante como procedimiento formal para traducir la información bruta de seguridad operacional en conocimiento relacionado con los peligros. La compilación y la gestión oficial continuas de este conocimiento relacionado con los peligros constituyen la “biblioteca de seguridad operacional” de una organización. Para elaborar conocimientos sobre peligros y construir así la “biblioteca de seguridad operacional”, debe recordarse que el seguimiento y el análisis de los peligros se facilita mediante la normalización de:

- a) definiciones de términos utilizados;
- b) comprensión de términos utilizados;
- c) validación de la información de seguridad operacional recogida;
- d) notificación (es decir lo que espera la organización);
- e) medición de la información de seguridad operacional recogida; y
- f) gestión de la información de seguridad operacional recogida.

4.6.4 En la Figura 4-2 se ilustra el proceso de documentación de peligros. Los peligros se identifican constantemente mediante fuentes reactivas, proactivas y predictivas y métodos subyacentes de recolección de información de seguridad. Después de la recolección e identificación, la información sobre peligros se evalúa en términos de consecuencias, y prioridades y responsabilidades respecto de respuestas y estrategias de mitigación. Toda esta información, incluyendo los peligros, consecuencias, prioridades, responsabilidades y estrategias, deben incorporarse a la “biblioteca de seguridad operacional” de la organización. El producto de la “biblioteca de seguridad operacional” no es solamente la conservación de la memoria de seguridad operacional de la empresa, sino que la biblioteca de seguridad operacional pasa a ser una fuente de conocimientos de seguridad para utilizar como referencia en la adopción de decisiones de seguridad operacional de la organización. El conocimiento de seguridad incorporado en la “biblioteca de seguridad operacional” proporciona información y referencias de control respecto de las cuales medir el análisis de peligros y la gestión de consecuencias, así como la eficiencia de las fuentes o métodos de recolección de información de seguridad operacional. También proporciona material para análisis de tendencia de seguridad operacional así como para fines de educación en seguridad (boletines, informes, seminarios de seguridad operacional y similares).

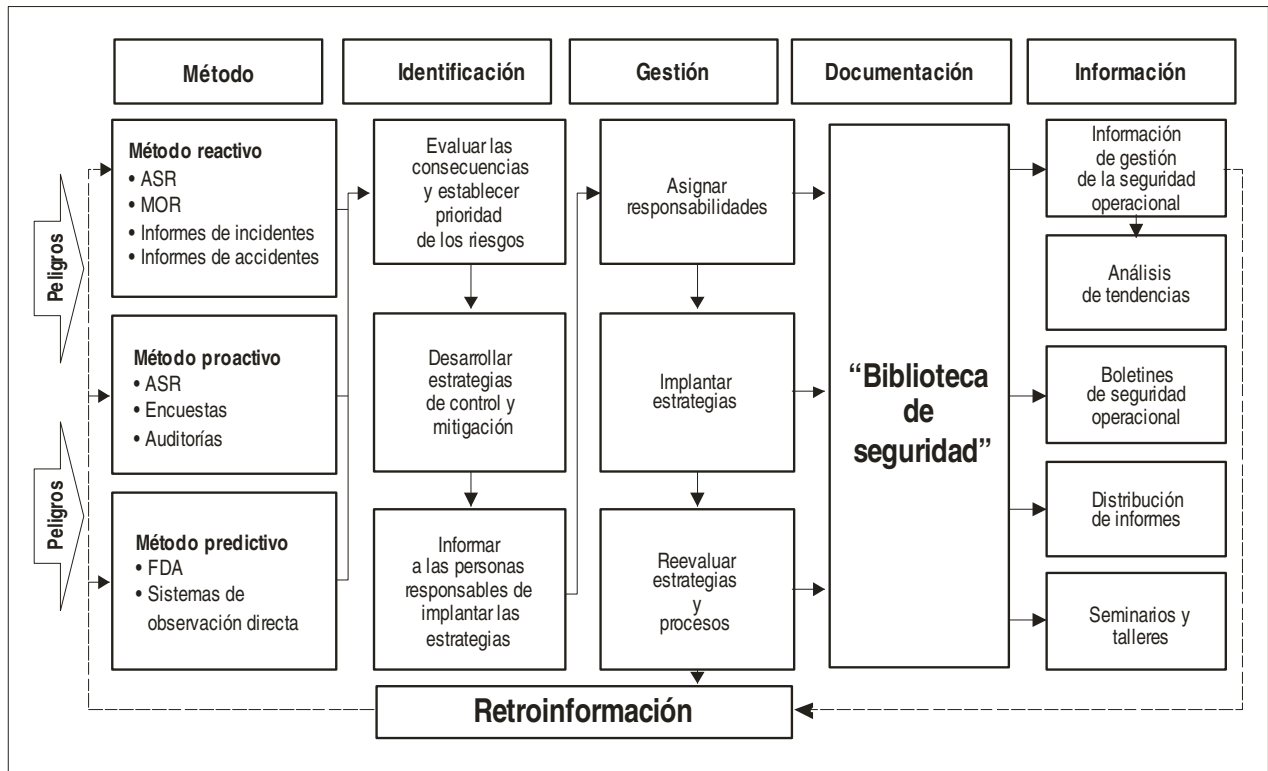


Figura 4-2. Documentación de los peligros

## Apéndice 1 del Capítulo 4

# ANÁLISIS DE LA INFORMACIÓN DE SEGURIDAD OPERACIONAL

1. Después de recoger y registrar la información de seguridad operacional a través de varias fuentes de identificación de peligros, las conclusiones significativas pueden alcanzarse solamente mediante el análisis de dicha información. La reducción de la información a simples estadísticas tiene poca utilidad si no se evalúa la importancia práctica de esas estadísticas para definir un problema que pueda resolverse.

2. Habiendo establecido bases de datos y sistemas de notificación de la seguridad operacional, las organizaciones deben analizar la información contenida en sus informes y bases de datos para determinar las medidas de seguridad operacional requeridas.

### ANÁLISIS DE LA INFORMACIÓN DE SEGURIDAD OPERACIONAL — ¿DE QUÉ SE TRATA?

3. El análisis es el proceso de organizar los hechos aplicando métodos, herramientas o técnicas específicos. Entre otros fines, puede utilizarse para:

- a) ayudar a decidir qué hechos adicionales se necesitan;
- b) determinar factores subyacentes en las deficiencias de seguridad operacional; y
- c) ayudar a alcanzar conclusiones válidas.

4. El análisis de la seguridad operacional se basa en información concreta originada en varias fuentes. Deben recogerse, clasificarse y almacenarse los datos pertinentes. Posteriormente, se seleccionan y aplican métodos y herramientas analíticos adecuados para el análisis. El análisis de seguridad operacional tiene con frecuencia carácter iterativo, y requiere múltiples ciclos. Puede ser cuantitativo o cualitativo. La ausencia de datos básicos cuantitativos puede llevar a basarse en métodos de análisis más cualitativos.

### OBJETIVIDAD Y PARCIALIDAD

5. Debe considerarse toda la información pertinente; no obstante, no toda la información de seguridad operacional es fiable. Las limitaciones de tiempo no siempre permiten recoger y evaluar suficiente información como para asegurar la objetividad. A veces pueden alcanzarse conclusiones intuitivas que no se corresponden con la objetividad requerida de los análisis de seguridad operacional creíbles.

6. Los seres humanos están sujetos a ciertos niveles de parcialidad en sus juicios. La experiencia anterior influirá a menudo en sus juicios, así como la creatividad, para establecer hipótesis. Una de las formas más frecuentes de error de juicio se conoce como “tendencia a la confirmación”, se trata de la tendencia a buscar y conservar información que confirme lo que uno ya cree que es cierto.

## MÉTODOS Y HERRAMIENTAS ANALÍTICOS

7. Existen distintos métodos aplicados en el análisis de la seguridad operacional. Algunos son automáticos y otros no lo son. Además, existen varias herramientas basadas en soporte lógico (que requieren diferentes niveles de conocimiento para su aplicación eficaz). A continuación se indican algunos métodos y herramientas analíticas disponibles:

- a) **Análisis estadístico.** Muchos de los métodos y herramientas analíticas aplicados en el análisis de seguridad operacional se basan en procedimientos y conceptos estadísticos; por ejemplo, el análisis de riesgos utiliza conceptos de probabilidad estadística. La estadística desempeña una función importante en el análisis de la seguridad operacional pues contribuye a cuantificar situaciones, proporcionando una comprensión clara mediante números. Esto genera resultados más creíbles para un argumento de seguridad operacional convincente.

El tipo de análisis de seguridad operacional realizado a nivel de las actividades de gestión de la seguridad operacional de una organización exige conocimientos básicos para analizar datos numéricos, identificar tendencias y efectuar cálculos estadísticos básicos como la media aritmética, percentiles y medianas. Los métodos estadísticos también son útiles para la presentación gráfica de los análisis.

Las computadoras pueden realizar la manipulación de grandes volúmenes de datos. La mayoría de los procedimientos de análisis estadístico están disponibles en paquetes de soporte lógico comerciales (p. ej., Microsoft Excel). Utilizando tales aplicaciones, pueden ingresarse los datos directamente en un procedimiento preprogramado. Si bien no es necesaria una comprensión detallada de la teoría estadística en que se basa la técnica, el analista debería comprender cómo funciona el procedimiento y cómo interpretar los resultados.

Si bien la estadística es una poderosa herramienta para los análisis de seguridad operacional, también puede utilizarse mal y, en consecuencia, puede conducir a conclusiones erróneas. Debe ejercerse cautela en la selección y utilización de los datos en los análisis estadísticos. Para asegurar la aplicación apropiada de los métodos más complejos, puede requerirse la asistencia de especialistas en análisis estadístico.

- b) **Análisis de tendencias.** Vigilando las tendencias en los datos de seguridad operacional, pueden realizarse predicciones sobre sucesos futuros. Las tendencias emergentes pueden indicar peligros en gestación. Los métodos estadísticos pueden utilizarse para evaluar la importancia de las tendencias percibidas. Pueden definirse los límites superior e inferior de actuación aceptable respecto de los cuales comparar la actuación actual. Puede utilizarse el análisis de tendencia para activar “alarmas” cuando la actuación está a punto de apartarse de los límites aceptados.
- c) **Comparaciones normativas.** Puede no disponerse de datos suficientes para proporcionar una base concreta respecto de la cual comparar las circunstancias del suceso o situación que se examina con la experiencia cotidiana. La ausencia de datos normativos creíbles compromete a menudo la utilidad de los análisis de seguridad operacional. En tales casos, puede ser necesario realizar un muestreo de experiencia en el mundo real en condiciones operacionales similares. Los programas de supervisión normal de las operaciones proporcionan datos normativos útiles para el análisis de las operaciones de aviación.
- d) **Simulación y ensayo.** En algunos casos, los peligros pueden hacerse evidentes mediante ensayos; por ejemplo, pueden requerirse ensayos en laboratorio para analizar defectos de materiales. Para procedimientos operacionales sospechosos, puede justificarse la simulación en el terreno en condiciones operacionales reales o en un simulador.

- e) **Grupos de expertos.** Dado el diverso carácter de los peligros y las diferentes perspectivas posibles en la evaluación de toda condición insegura particular, debería procurarse las opiniones de otros, incluyendo pares y especialistas. Un equipo multidisciplinario constituido para evaluar las pruebas de una condición insegura también puede ayudar a identificar y evaluar el mejor curso de acción correctiva.
  
  - f) **Análisis de costo-beneficios.** La aceptación de medidas de control del riesgo de seguridad operacional recomendadas puede depender de análisis de costo-beneficios creíbles. El costo de implantar las medidas propuestas se sopesa con respecto a los beneficios previstos con el tiempo. A veces, el análisis de costo-beneficios puede sugerir que la aceptación de las consecuencias del riesgo de seguridad es preferible al tiempo, esfuerzos y costos necesarios para implantar las medidas correctivas.
-



## **Apéndice 2 del Capítulo 4**

# **GESTIÓN DE LA INFORMACIÓN DE SEGURIDAD OPERACIONAL**

### **1. GENERALIDADES**

1.1 Los datos de seguridad operacional de calidad son el alma de la gestión de la seguridad operacional. La gestión efectiva de la seguridad operacional es “basada en datos”. La información recogida de informes de operaciones y mantenimiento, informes de seguridad operacional, auditorías, evaluaciones de prácticas laborales, etc., genera una enorme cantidad de datos — aunque no todos son pertinentes a la gestión de la seguridad operacional. Tanta información relacionada con la seguridad operacional se recoge y almacena que existe el riesgo de abrumar a los gestores responsables, comprometiendo con ello la utilidad de los datos. La buena gestión de las bases de datos de la organización es fundamental para las funciones de gestión efectiva de la seguridad operacional (como el monitoreo de tendencias, la evaluación de riesgos, los análisis de costo-beneficios y las investigaciones de sucesos).

1.2 El argumento necesario para el cambio en materia de seguridad operacional debe basarse en el análisis de datos consolidados y de seguridad operacional. El establecimiento y mantenimiento de una base de datos de seguridad operacional proporcionan una herramienta esencial para los administradores de la empresa, gestores de seguridad y autoridades normativas que monitorean aspectos de seguridad operacional en el sistema. Lamentablemente, muchas bases de datos carecen de la calidad de datos necesaria para proporcionar una base fiable a efectos de ajustar las prioridades de seguridad operacional, evaluar la eficacia de las medidas de mitigación de riesgo e iniciar investigaciones relacionadas con la seguridad operacional. Para alcanzar decisiones oportunas y válidas es necesario comprender los datos y las bases de datos y utilizar herramientas apropiadas.

1.3 Se está usando cada vez más soporte lógico de computadoras para facilitar el registro, almacenamiento, análisis y presentación de información de seguridad operacional. Ahora es posible realizar fácilmente complejos análisis de la información en la base de datos. Se dispone comercialmente de una amplia gama de bases de datos electrónicas de relativamente bajo costo para computadoras de mesa, capaces de apoyar los requisitos de la gestión de datos de la organización. Estos sistemas independientes tienen la ventaja de no utilizar el sistema de computadoras principal de la organización, mejorando así la protección de los datos.

### **2. REQUISITOS DEL SISTEMA DE INFORMACIÓN**

Dependiendo del volumen de sus organizaciones, los usuarios requieren un sistema con diversas capacidades y resultados para gestionar sus datos de seguridad operacional. En general, los usuarios necesitan:

- a) un sistema con capacidad de transformar grandes volúmenes de datos de seguridad operacional en información útil que apoye la toma de decisiones;
- b) un sistema que reduzca la carga de trabajo de los gestores y del personal de seguridad operacional;
- c) un sistema automático adaptable a su propia cultura; y
- d) un sistema que pueda funcionar a un costo relativamente bajo.

### 3. COMPRESIÓN DE LAS BASES DE DATOS

3.1 Para aprovechar las ventajas potenciales de las bases de datos de la seguridad operacional, se requiere una comprensión básica de su funcionamiento. ¿Qué es una base de datos? Cualquier información que se haya agrupado en forma organizada puede considerarse como una base de datos. Los registros en papel pueden mantenerse en un sistema de archivo sencillo (es decir una “base de datos” manual), pero dicho sistema alcanzará solamente para las explotaciones más pequeñas. El almacenamiento, registro, búsqueda y recuperación de los datos son tareas engorrosas. Es preferible almacenar los datos de seguridad operacional, cualquiera sea su origen, en una base de datos electrónica que facilite la recuperación de esa información en varios formatos.

3.2 La capacidad de manipular, analizar y recuperar información en diversas formas se conoce como gestión de base de datos. La mayoría de los paquetes de soporte lógico de gestión de bases de datos incorporan los siguientes elementos de organización para definir una base de datos:

- a) **Registro.** Un agrupamiento de elementos de información que van juntos como una unidad (como todos los datos relativos a un suceso);
- b) **Campo.** Cada elemento de información separado en un registro (como la fecha o la ubicación de un suceso); y
- c) **Fichero.** Un grupo de registros con la misma estructura e interrelacionados (tales como sucesos relacionados con motores para un año específico).

3.3 Las bases de datos se consideran “estructuradas” cuando cada campo de datos tiene una longitud fija y su formato está claramente definido por un número, fecha, respuesta “sí/no”, carácter o texto. A menudo el usuario sólo dispone de una selección fija de valores. Estos valores se almacenan en ficheros de referencia, a menudo conocidos como tablas de base o tablas de listas de valores, por ejemplo, una selección de marcas y modelos de aeronaves extraídas de una lista predeterminada. Para facilitar el análisis cuantitativo y la búsqueda sistemática, el texto libre ingresado en las bases de datos estructuradas se minimiza confinándolo a una longitud de campo fija. A menudo tal información se categoriza mediante un sistema de palabras clave.

3.4 Las bases de datos se consideran “basadas en texto” cuando los contenedores de información son principalmente documentos escritos (por ejemplo, resúmenes de accidentes e incidentes o correspondencia escrita). Los datos se indexan y almacenan en campos de texto de forma libre. Algunas bases de datos contienen grandes volúmenes de texto y datos estructurados; no obstante, las bases de datos modernas son mucho más que archivos electrónicos.

### 4. LIMITACIONES DE LAS BASES DE DATOS

Hay que considerar ciertas limitaciones al elaborar, mantener o utilizar bases de datos. Algunas de las limitaciones se relacionan directamente con el sistema de la base de datos, mientras que otros se relacionan con el uso de los datos. Si se quieren evitar conclusiones y decisiones sin apoyo, los usuarios de la base de datos deben comprender estas limitaciones. Los usuarios de la base de datos también deben conocer la finalidad para la cual se creó la base de datos y la credibilidad de la información ingresada por la organización que la creó y mantiene.

### 5. INTEGRIDAD DE LA BASE DE DATOS

5.1 Las bases de datos de seguridad operacional son un elemento estratégico de las actividades de gestión de la seguridad operacional de una organización. Los datos son susceptibles de corrupción de muchas fuentes y debe



ejercerse cautela para conservar la integridad de los datos. Muchos empleados pueden tener acceso a la base de datos para ingresar información. Otros requerirán acceso a los datos para la realización de sus tareas de seguridad operacional. El acceso desde múltiples sitios de un sistema en red puede aumentar la vulnerabilidad de la base de datos.

5.2 La utilidad de una base de datos se verá comprometida por la inadecuada atención al mantenimiento de los datos. Los datos ausentes, las demoras en ingresar datos actuales, y la imprecisión de los datos de ingreso, etc., corrompen la base de datos. Incluso la aplicación de las mejores herramientas analíticas no puede compensar la mala calidad de los datos.

## 6. GESTIÓN DE LA BASE DE DATOS

### Protección de los datos de seguridad operacional

Dado el potencial de uso incorrecto de los datos de seguridad operacional que se han reunido estrictamente para fines de mejorar la seguridad operacional en la aviación, la gestión de la base de datos debe comenzar con la protección de los mismos. Los administradores de la base de datos deben equilibrar la necesidad de protección de los datos con la de que dichos datos sean accesibles a quienes pueden mejorar la seguridad operacional de la aviación. Las consideraciones de protección comprenden:

- a) adecuación de las leyes de “acceso a la información” con respecto a los requisitos de gestión de la seguridad operacional;
- b) políticas de la organización sobre protección de datos de seguridad operacional;
- c) desidentificación, suprimiendo todos los detalles que pudieran llevar a terceros a deducir la identidad de individuos (por ejemplo, números de vuelo, fechas/horas, lugares y tipos de aeronaves);
- d) protección de los sistemas de información, almacenamiento de datos y redes de comunicaciones;
- e) limitación del acceso a las bases de datos a aquellos que “necesitan saber”; y
- f) prohibiciones del uso no autorizado de los datos.

## 7. CAPACIDADES DE LA BASE DE DATOS DE SEGURIDAD

La propiedad y atributos funcionales de diferentes sistemas de gestión de bases de datos varían, y cada una debería considerarse antes de decidir cuál es el sistema más adecuado para las necesidades de un explotador. La experiencia ha demostrado que la mejor manera de registrar y hacer el seguimiento de incidentes aéreos relacionados con la seguridad es el uso de una base de datos basada en computadora personal. El número de características disponible depende del tipo de sistema seleccionado. Las características básicas deberían permitir al usuario ejecutar las tareas siguientes:

- a) registrar los sucesos de seguridad operacional en varias categorías;
- b) relacionar los sucesos con documentos conexos (p. ej., informes y fotografías);
- c) monitorear las tendencias;
- d) recopilar análisis, cartas e informes;

- e) verificar historiales;
- f) compartir datos con otras organizaciones;
- g) monitorear las investigaciones de sucesos; y
- h) señalar medidas de respuesta postergadas.

## 8. CONSIDERACIONES DE SELECCIÓN DE BASE DE DATOS

8.1 La selección de sistemas de base de datos disponibles en el comercio dependerá de las expectativas del usuario, los datos requeridos, el sistema de computadora y la complejidad de las tareas que han de manejarse. Hay disponibles varios programas con diferentes capacidades y requisitos de idoneidad. La elección de qué tipo utilizar requiere un equilibrio de las consideraciones siguientes:

- a) **Facilidad para el usuario.** El sistema debería ser de fácil uso intuitivo. Algunos programas proporcionan una amplia gama de características pero exigen una considerable instrucción. Lamentablemente, hay a menudo compensaciones entre la facilidad para el usuario y la potencia de búsqueda; cuanto más fácil sea el manejo de la herramienta menos probable será que pueda tramitar interrogaciones complejas.
- b) **Acceso.** Aunque el acceso a todos los detalles almacenados en la base de datos sería ideal, no todos los usuarios necesitan tal acceso. La estructura y la complejidad de la base de datos influirá en la elección de cualquier herramienta de interrogación particular.
- c) **Performance.** La performance es una medida de la eficiencia en el funcionamiento del sistema. Depende de consideraciones como:
  - 1) cuán bien se captan, mantienen y vigilan los datos;
  - 2) si los datos se almacenan en formatos que faciliten el análisis de tendencias o de otro tipo;
  - 3) la complejidad de la estructura de la base de datos; y
  - 4) el diseño del sistema de computadora central (o red).
- d) **Flexibilidad.** La flexibilidad depende de la capacidad del sistema para:
  - 1) procesar una amplia gama de interrogaciones;
  - 2) filtrar y clasificar datos;
  - 3) usar lógica binaria (es decir el sistema puede manejar condiciones de tipo "Y/O" como "todos los pilotos que son comandantes y tienen 15 000 horas de experiencia", o "todos los pilotos que son comandantes o tienen 15 000 horas de experiencia");
  - 4) realizar análisis básicos (conteos y tabulaciones);
  - 5) producir resultados definidos por el usuario; y
  - 6) conectar con otras bases de datos para importar o exportar datos.

8.2 Los costos varían según los requisitos de cada organización. El precio cobrado por algunos vendedores de sistemas es una tarifa única, que permite múltiples usuarios en una licencia. Alternativamente, otros vendedores del sistema aumentan la tarifa dependiendo del número de usuarios autorizados. El comprador debe tener en cuenta factores relacionados con los costos como:

- a) costos de instalación;
  - b) costos de instrucción;
  - c) costos de perfeccionar el soporte lógico;
  - d) honorarios de mantenimiento y apoyo; y
  - e) otros derechos de licencia de soporte lógico que puedan ser necesarios.
-



# Capítulo 5

## RIESGOS DE SEGURIDAD OPERACIONAL

### 5.1 OBJETIVO Y CONTENIDO

En este capítulo se presentan los fundamentos de la gestión de los riesgos de seguridad operacional. El capítulo comprende los temas siguientes:

- a) Definición de los riesgos de seguridad operacional;
- b) Primer fundamento — Gestión de los riesgos de seguridad operacional;
- c) Segundo fundamento — Probabilidad de los riesgos de seguridad operacional;
- d) Tercer fundamento — Gravedad de los riesgos de seguridad operacional;
- e) Cuarto fundamento — Tolerabilidad de los riesgos de seguridad operacional;
- f) Quinto fundamento — Control/mitigación de los riesgos de seguridad operacional; y
- g) Los cinco fundamentos de la gestión de los riesgos de seguridad operacional — Resumen.

### 5.2 DEFINICIÓN DE RIESGO DE SEGURIDAD OPERACIONAL

5.2.1 En el Capítulo 2 de este manual se define la seguridad operacional como el resultado de la gestión de varios procesos de la organización. La gestión de estos procesos de organización tiene la finalidad de mantener los riesgos de seguridad operacional bajo control de la organización. Un aspecto clave de esta perspectiva es la noción de seguridad operacional como resultado, y de gestión de los riesgos de seguridad operacional como proceso.

5.2.2 En el Capítulo 4 de este manual se continúa analizando la identificación de los peligros como una de las dos actividades básicas que apoyan la gestión de la seguridad operacional. La identificación de peligros también contribuye a la solidez de otros procesos de organización indirectamente relacionados con la gestión de la seguridad operacional. Para proporcionar una adecuada identificación y análisis de los peligros, en el Capítulo 4 se establece una clara diferenciación entre peligros, como fuentes de posibles lesiones o daños, y sus consecuencias de seguridad operacional descritas en términos operacionales.

5.2.3 La gestión de los riesgos de seguridad operacional es la otra actividad básica que apoya la gestión de la seguridad operacional y contribuye a otros procesos de la organización indirectamente relacionados. El término gestión de la seguridad operacional, al contrario del término más genérico gestión de los riesgos, está dirigido a trasladar la noción de que la gestión de la seguridad operacional no apunta directamente a la gestión del riesgo financiero, el riesgo jurídico, el riesgo económico y así sucesivamente, sino que se limita principalmente a la gestión de los riesgos de seguridad operacional.

5.2.4 Es una carencia común que las actividades de gestión de la seguridad operacional a menudo no avanzan más allá de la identificación y análisis de peligros o, en otros casos, saltan directamente de la identificación de peligros a la aplicación de medidas de mitigación, ignorando la evaluación y las prioridades de los riesgos de seguridad operacional de

las consecuencias de los peligros. Después de todo, una vez identificada la fuente de peligro o daño y analizadas y convenidas sus consecuencias, las estrategias de mitigación para proteger contra las consecuencias pueden por cierto aplicarse. Esta adición sería correcta si aplicáramos la necesidad de “seguridad operacional como primera prioridad” y nos concentráramos en la prevención de malos resultados. No obstante, en el marco de la noción de gestión de la seguridad operacional, convenir en las consecuencias de peligros identificados y describirlos en términos operacionales no alcanza para aplicar medidas de mitigación. Es necesario evaluar la gravedad de las consecuencias, para definir prioridades en la asignación de recursos al proponer estrategias de mitigación.

5.2.5 Ya se ha propuesto que es un axioma básico de las actividades de gestión que no se puede gestionar lo que no se puede medir. Por consiguiente, es fundamental medir de alguna forma la gravedad de las consecuencias de los peligros. Esta es la contribución esencial de la gestión de los riesgos de seguridad operacional al proceso de gestión de la seguridad operacional. Mediante la “asignación de un número” a las consecuencias de los peligros, el proceso de gestión de la seguridad operacional proporciona a la organización una base de principios para la adopción de decisiones sobre los riesgos de seguridad operacional y la consiguiente asignación de recursos de la organización para contener el potencial perjudicial de los peligros. De esta forma, la gestión de los riesgos de seguridad operacional completa la trilogía básica de gestión de la seguridad operacional integrada por peligros-consecuencias-riesgos de seguridad operacional, y apoya directamente la resolución del “dilema de las dos P” analizado en el Capítulo 3.

5.2.6 El riesgo, en su sentido familiar y más amplio, ha sido objeto de muchos análisis, y la literatura en la materia es abundante. Existe una posibilidad de confusión que se debe parcialmente al uso familiar del término, que es demasiado frecuente, bastante amplio y generalmente vago. La primera medida para tratar la confusión es afinar el uso del término genérico “riesgo” al muy específico término “riesgo de seguridad operacional”. Más allá de esto, es esencial desde un principio establecer una clara definición de riesgo de seguridad operacional y relacionar dicha definición con los conceptos de peligro y consecuencias expresados en términos operacionales.

5.2.7 Aún después de afinar el uso del término genérico “riesgo” al término más específico “riesgo de seguridad operacional”, las confusiones pueden seguir existiendo. Esto se debe a que la noción de riesgo es artificial. Los riesgos de seguridad operacional no son componentes tangibles o visibles de ningún entorno físico o natural; es necesario pensar acerca de los riesgos de seguridad operacional para comprender o formarse una imagen de los mismos. Por el contrario, los peligros y las consecuencias son componentes tangibles o visibles de un entorno físico o natural y, por consiguiente, intuitivos en términos de comprensión y visualización. La noción de riesgo de seguridad operacional es lo que se conoce como una construcción, es decir, una convención artificial creada por los seres humanos. En términos sencillos, mientras que los peligros y las consecuencias son componentes físicos del mundo natural, los riesgos de seguridad operacional no existen realmente en el mundo natural. El riesgo de seguridad operacional es un producto de la mente humana dirigido a medir la gravedad o a “asignar un número” en las consecuencias de los peligros.

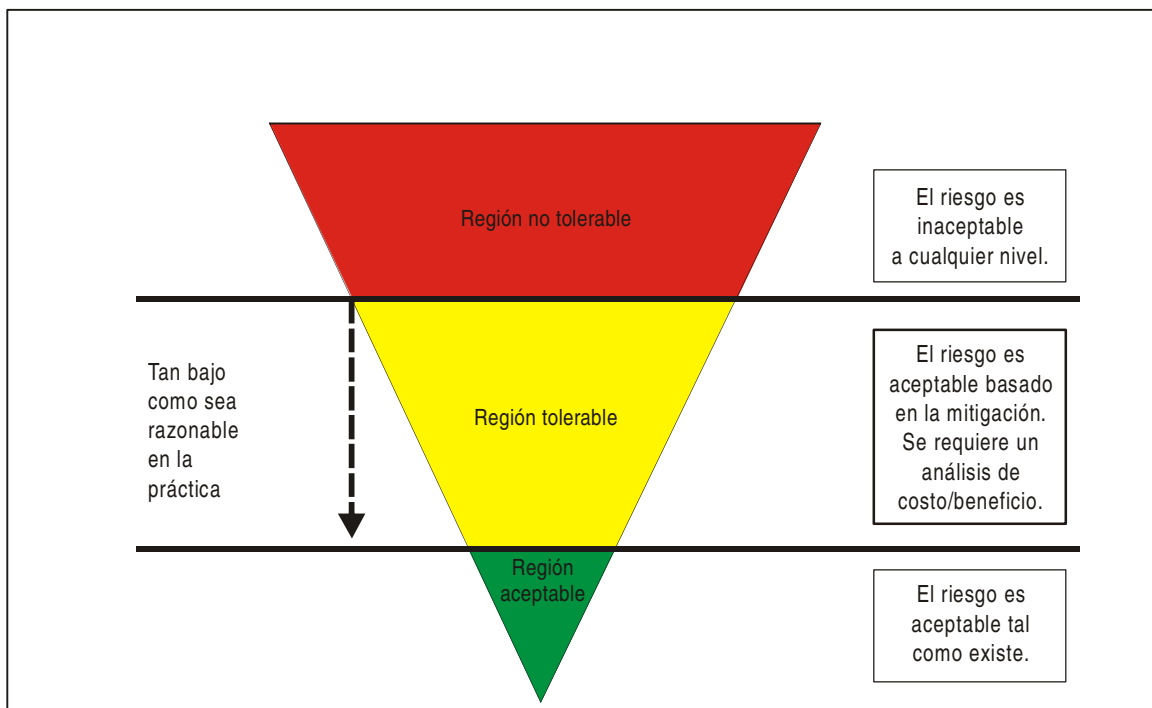
5.2.8 El riesgo de seguridad operacional se define como la evaluación, expresada en términos de probabilidad y gravedad previstas, de las consecuencias de un peligro, tomando como referencia la peor situación previsible. Normalmente, los riesgos de seguridad operacional se designan mediante una convención alfanumérica que permite su medición. Aplicando el ejemplo del viento transversal presentado en el Capítulo 4, puede verse que la definición propuesta de riesgo de seguridad operacional permite relacionar riesgos de seguridad operacional con peligros y consecuencias, cerrando así el bucle de la trilogía de peligro-consecuencia-riesgo de seguridad operacional:

- a) un viento de 15 nudos directamente perpendicular a la pista es un peligro;
- b) la posibilidad de excursión lateral de la pista porque un piloto puede no estar en condiciones de controlar la aeronave durante el despegue o el aterrizaje es una de las consecuencias del peligro; y
- c) la evaluación de las consecuencias de una excursión lateral de la pista, expresada en términos de probabilidad y gravedad como convención alfanumérica, constituye el riesgo de seguridad operacional.

**5.3 PRIMER FUNDAMENTO — GESTIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL**

5.3.1 La gestión de los riesgos de seguridad operacional es un término genérico que engloba la evaluación y mitigación de los riesgos de seguridad operacional como consecuencias de los peligros que amenazan las capacidades de una organización, a un nivel tan bajo como sea razonable en la práctica (ALARP). El objetivo de la gestión de los riesgos de seguridad operacional es proporcionar el fundamento para una equilibrada asignación de recursos entre todos los riesgos de seguridad operacional evaluados y aquellos para los cuales son viables el control y la mitigación. En otras palabras, la gestión de los riesgos de seguridad operacional ayuda a resolver el “dilema de las dos P”. La gestión de los riesgos de seguridad operacional es, por consiguiente, un componente fundamental del proceso de gestión de la seguridad operacional. No obstante, su valor agregado corresponde al hecho de que es un enfoque basado en datos para asignación de recursos, por lo tanto fácil de defender y de explicar.

5.3.2 En la Figura 5-1 se muestra una representación visual genérica ampliamente adoptada del proceso de gestión de los riesgos de seguridad operacional. El triángulo se presenta en posición invertida, lo que sugiere que la aviación (al igual que cualquier otro sistema de producción sociotécnico) está “recargada desde arriba” desde una perspectiva de riesgos de seguridad: la mayoría de los riesgos de seguridad operacional de las consecuencias de los peligros se evaluarán como que corresponden inicialmente a la región intolerable. Un número menor de riesgos de seguridad operacional de las consecuencias de los peligros será evaluado en forma tal que dicha evaluación caiga directamente en la región tolerable y un número aún menor se evaluará de forma que la evaluación caiga directamente en la región aceptable.



**Figura 5-1. Gestión de los riesgos de seguridad operacional**

5.3.3 Los riesgos de seguridad operacional evaluados como que corresponden inicialmente a la región intolerable son inaceptables en todas circunstancias. La probabilidad o gravedad de las consecuencias de los peligros son de tal magnitud, y el potencial perjudicial del peligro plantea una amenaza tal a la viabilidad de la organización, que se requieren medidas inmediatas de mitigación. En términos generales, la organización dispone de dos alternativas para llevar los riesgos de seguridad operacional a las regiones tolerable o aceptable:

- a) asignar recursos para reducir la exposición al potencial perjudicial de las consecuencias de los peligros o la magnitud de éste; o
- b) si la mitigación no es posible, cancelar la operación.

5.3.4 Los riesgos de seguridad operacional evaluados como que corresponden inicialmente a la región tolerable son aceptables siempre que las estrategias de mitigación ya existentes garanticen que, en la medida previsible, la probabilidad o gravedad de las consecuencias de los peligros se mantienen bajo control de la organización. Los mismos criterios de control se aplican a los riesgos que inicialmente corresponden a la región intolerable y son mitigados a la región tolerable. Un riesgo de seguridad operacional evaluado inicialmente como intolerable que se mitiga y se lleva a la región tolerable debe permanecer "protegido" mediante estrategias de mitigación que garanticen su control. En ambos casos, se requiere un análisis de costo-beneficios:

- a) ¿Existe un rendimiento económico de la inversión en que se base la asignación de recursos para llevar la probabilidad o gravedad de las consecuencias de los peligros bajo control de la organización? o
- b) ¿Se requiere una asignación de recursos de tal magnitud que plantee una mayor amenaza a la viabilidad de la organización que llevar la probabilidad o gravedad de la consecuencia de los peligros bajo control de la organización?

5.3.5 El acrónimo ALARP se utiliza para describir un riesgo de seguridad operacional que se ha reducido a un nivel tan bajo como sea razonable en la práctica. Para determinar lo que es "razonable en la práctica" en el contexto de la gestión de los riesgos de seguridad operacional, deben considerarse tanto la viabilidad técnica de continuar reduciendo el riesgo de seguridad operacional como el costo. Esto debe incluir un análisis de costo-beneficios. Si se indica que el riesgo de seguridad operacional en un sistema es ALARP, ello significa que toda ulterior reducción del riesgo es impracticable o está ampliamente superada por el costo. No obstante, debe tenerse en cuenta que cuando una organización "acepta" un riesgo de seguridad, ello no significa que el riesgo de seguridad haya sido eliminado. Permanece cierto nivel residual de riesgo de seguridad operacional; no obstante, la organización ha aceptado que dicho riesgo residual es suficientemente bajo como para ser superado por los beneficios.

5.3.6 Los riesgos de seguridad operacional evaluados como que corresponden inicialmente a la región aceptable son aceptables en su estado actual y no requieren medidas para llevar o mantener la probabilidad o la gravedad de las consecuencias de los peligros bajo control de la organización.

5.3.7 Los análisis de costo-beneficios están en el centro de la gestión de los riesgos de seguridad operacional. Hay dos costos claramente separados que deben considerarse en los análisis de costo-beneficios: los costos directos y los costos indirectos.

5.3.8 Los **costos directos** son los costos obvios y son relativamente fáciles de determinar. Se relacionan en su mayoría con los daños físicos y comprenden la rectificación, sustitución o indemnización por lesiones, o daños a la aeronave, al equipo u otros bienes materiales. Los elevados costos que entraña la pérdida de control por parte de la organización de ciertas consecuencias extremas de los peligros, tales como un accidente, pueden reducirse mediante cobertura de seguros. No obstante, se debe considerar que la compra de seguros no hace nada por llevar la probabilidad o gravedad de las consecuencias de los peligros bajo control de la organización; sólo transfiere el riesgo monetario de la organización al asegurador. El riesgo de seguridad operacional permanece sin tratarse. La simple



compra de seguros para transferir el riesgo monetario difícilmente puede considerarse como estrategia de gestión de la seguridad operacional.

5.3.9 Los **costos indirectos** comprenden todos los costos que no están directamente cubiertos por el seguro. Los costos indirectos pueden representar más que los costos directos resultantes de la pérdida de control por parte de la organización de ciertas consecuencias extremas de los peligros. A veces, estos costos no son obvios y a menudo se postergan. Algunos ejemplos de costos no asegurados que pueden deberse a la pérdida de control por la organización de consecuencias extremas de los peligros comprenden:

- a) **Pérdida de negocios y daños a la reputación de la organización.** Muchas organizaciones no permitirán que su personal vuele con una línea aérea que presente un registro de seguridad operacional cuestionable.
- b) **Pérdida del uso de equipo.** Esto equivale al lucro cesante. Puede tener que adquirirse o alquilarse equipo de remplazo. Las compañías que explotan aeronaves de un solo tipo pueden encontrar que sus inventarios de repuestos y las personas especialmente entrenadas para dichas aeronaves constituyen un excedente.
- c) **Pérdida de productividad del personal.** Si hay personas que resultan lesionadas en un suceso y no pueden trabajar, la legislación laboral puede exigir que continúen recibiendo algún tipo de compensación. Además, estas personas deberán remplazarse, por lo menos a corto plazo, y con ello la organización incurrirá en el costo de salarios, instrucción, horas extraordinarias y tendrá que imponer también una mayor carga de trabajo a los trabajadores experimentados.
- d) **Investigación y limpieza.** A menudo estos costos no están asegurados. Los explotadores pueden incurrir en costos debidos a las investigaciones que comprenden el costo de la participación de su personal en las mismas, así como el costo de ensayos y análisis, recuperación de restos y restauración del lugar del suceso.
- e) **Deducibles del seguro.** La obligación del titular de la póliza de cubrir la primera porción del costo de cualquier suceso debe pagarse. Una reclamación también llevará a una compañía a una más alta categoría de riesgos con fines de seguro y, por consiguiente, a aumentos en las primas. (Por el contrario, la implantación de intervenciones de mitigación de seguridad operacional podría contribuir a que la compañía negocie una prima más baja).
- f) **Acciones judiciales e indemnización por daños.** Los costos jurídicos pueden crecer rápidamente. Si bien es posible contratar seguros por responsabilidad pública y daños, es virtualmente imposible abarcar el costo del tiempo perdido al tramitar las acciones judiciales y los reclamos de indemnización por daños.
- g) **Multas y citaciones.** Las autoridades gubernamentales pueden imponer multas y citaciones y posiblemente clausurar las operaciones que no sean seguras.

5.3.10 Los análisis de costo-beneficios producen resultados que pueden ser numéricamente precisos y analíticamente exactos. No obstante, en los análisis de costo-beneficios hay menos factores numéricos exactos. Estos factores comprenden:

- a) **Administrativos.** ¿Es coherente el riesgo de seguridad operacional con la política y objetivos de la organización en la materia?
- b) **Jurídicos.** ¿Se ajusta el riesgo de seguridad operacional a las normas reglamentarias actuales y la capacidad de hacerlas cumplir?

- c) **Cultural.** ¿Cómo considerarán el personal de la organización y otras partes interesadas el riesgo de seguridad operacional?
- d) **Mercado.** ¿Se verán comprometidos por el riesgo de seguridad operacional la competitividad y el bienestar de la organización frente a otras organizaciones?
- e) **Político.** ¿Habrá un precio político a pagar por no tratar el riesgo de seguridad operacional?
- f) **Público.** ¿Cuán influyentes serán los medios masivos de comunicación o los grupos de intereses especiales en afectar la opinión pública respecto del riesgo de seguridad operacional?

#### 5.4 SEGUNDO FUNDAMENTO — PROBABILIDAD DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

5.4.1 El proceso de llevar los riesgos de seguridad operacional de las consecuencias de los peligros bajo control de la organización se inicia evaluando la probabilidad de que las consecuencias de los peligros se materialicen durante las operaciones dirigidas a la prestación de servicios. Esto se conoce como evaluación de la probabilidad de los riesgos de seguridad operacional.

5.4.2 La probabilidad de los riesgos de seguridad operacional se define como la probabilidad de que pueda ocurrir un suceso o condición insegura. Las siguientes preguntas pueden ayudar a definir dicha probabilidad:

- a) ¿Existe un historial de sucesos similares al que se está considerando, o se trata de un suceso aislado?
- b) ¿Qué otro equipo o componentes del mismo tipo pueden tener efectos similares?
- c) ¿Cuántas personas están siguiendo los procedimientos en cuestión o están sujetas a éstos?
- d) ¿Qué porcentaje del tiempo se utiliza el equipo problemático o el procedimiento cuestionable?
- e) ¿En qué medida existen consecuencias de organización, gestión o normativas que puedan reflejar mayores amenazas a la seguridad pública?

5.4.3 Cualquiera de los factores subyacentes en estas preguntas, o todos ellos, pueden ser válidos, y subrayan la importancia de considerar las causas múltiples. Al evaluar la probabilidad de que pueda ocurrir un suceso o condición insegura, deben evaluarse todas las perspectivas potencialmente válidas.

5.4.4 Para evaluar la probabilidad de que pueda ocurrir un suceso o condición insegura, referirse a los datos históricos contenidos en la “biblioteca de seguridad operacional” de la organización es fundamental a efectos de tomar decisiones informadas. De esto sigue que una organización que no cuente con una “biblioteca de seguridad operacional” sólo puede realizar evaluaciones de probabilidad basadas, como mucho, en tendencias de la industria y como mínimo en opiniones.

5.4.5 Sobre la base de las consideraciones que surjan de las respuestas a preguntas como las indicadas en 5.4.2, puede establecerse la probabilidad de que pueda ocurrir un suceso o condición inseguro y evaluarse su importancia aplicando una tabla de probabilidad de riesgos de seguridad operacional.

5.4.6 En la Figura 5-2 se presenta una tabla típica de probabilidad de los riesgos de seguridad operacional, en este caso, con una escala de cinco puntos. La tabla comprende cinco categorías para indicar la probabilidad de ocurrencia de una condición o proceso inseguro, el significado de cada categoría y una asignación de valor a cada

categoría. Debe subrayarse que este es un ejemplo presentado solamente con fines didácticos. Aunque esta tabla, así como la tabla de gravedad y las matrices de evaluación de los riesgos y tolerancia que se analizarán en los párrafos siguientes son, desde el punto de vista conceptual, normas industriales, el nivel de detalle y complejidad de las tablas y matrices puede adaptarse y hacerse corresponder con las necesidades particulares y complejidades de diferentes organizaciones. Hay organizaciones que incluyen definiciones cualitativas y cuantitativas. Análogamente, algunas tablas se extienden hasta quince puntos. Las tablas de cinco puntos y las matrices de cinco por cinco no constituyen de modo alguno una norma. Sólo se consideran como que tienen una complejidad adecuada a los fines didácticos así como a las necesidades del presente manual.

## 5.5 TERCER FUNDAMENTO — GRAVEDAD DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

5.5.1 Una vez evaluados en términos de probabilidad los riesgos de seguridad de un suceso o condición inseguro, la segunda etapa del proceso de llevar bajo control de la organización a los riesgos de seguridad de las consecuencias de los peligros es la evaluación de la gravedad de las consecuencias del peligro si su potencial perjudicial se materializa durante operaciones dirigidas a la prestación de servicios. Esto se conoce como evaluación de la gravedad de los riesgos de seguridad operacional.

5.5.2 La gravedad de los riesgos de seguridad operacional se define como la posible consecuencia de un suceso o condición inseguro, tomando como referencia la peor situación previsible. La evaluación de la gravedad de las consecuencias del peligro si se materializa su potencial perjudicial durante operaciones dirigidas a la prestación de servicios puede ayudarse mediante preguntas como:

- a) ¿Cuántas vidas pueden perderse (empleados, pasajeros, circunstantes y público en general)?
- b) ¿Cuál es la probable extensión de los daños materiales o financieros (pérdida directa de bienes del explotador, daños a la infraestructura aeronáutica, daños colaterales a terceros, consecuencias financieras y económicas para el Estado)?
- c) ¿Cuál es la probabilidad de consecuencias para el medio ambiente (derrame de combustible u otros productos peligrosos y perturbación física del hábitat natural)?
- d) ¿Cuáles son las posibles consecuencias políticas o el interés de los medios de comunicación?

	<b>Significado</b>	<b>Valor</b>
<b>Frecuente</b>	Probable que ocurra muchas veces (ha ocurrido con frecuencia)	<b>5</b>
<b>Ocasional</b>	Probable que ocurra algunas veces (ha ocurrido infrecuentemente)	<b>4</b>
<b>Remoto</b>	Improbable, pero posible que ocurra (ha ocurrido raramente)	<b>3</b>
<b>Improbable</b>	Muy improbable que ocurra (no se sabe que haya ocurrido)	<b>2</b>
<b>Extremadamente Improbable</b>	Casi inconcebible que el suceso ocurra	<b>1</b>

Figura 5-2. Tabla de probabilidad de los riesgos de seguridad operacional

5.5.3 Sobre la base de las consideraciones que surjan de las respuestas a preguntas como las indicadas en 5.5.2, la gravedad de las posibles consecuencias de un suceso o condición inseguro, tomando como referencia la peor situación previsible, puede evaluarse utilizando una tabla de gravedad de los riesgos de seguridad operacional.

5.5.4 La Figura 5-3 presenta una tabla típica de gravedad de los riesgos de seguridad operacional, también de cinco puntos. Comprende cinco categorías para indicar el nivel de gravedad de la ocurrencia de un suceso o condición inseguro, el significado de cada categoría y la asignación de un valor a cada categoría. Al igual que con la tabla de probabilidad de los riesgos de seguridad operacional, esta tabla constituye un ejemplo presentado solamente con fines didácticos, y se aplican los mismos comentarios expresados en 5.4.6.

## 5.6 CUARTO FUNDAMENTO — TOLERABILIDAD DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

5.6.1 Una vez evaluados los riesgos de seguridad operacional de las consecuencias de un suceso o condición inseguro en términos de probabilidad y gravedad, la tercera etapa del proceso de llevar bajo control de la organización a los riesgos de seguridad operacional de las consecuencias del suceso o condición inseguro es la evaluación de la tolerabilidad de las consecuencias del peligro si su potencial perjudicial se materializa durante operaciones dirigidas a la prestación de servicios. Esto se conoce como evaluación de la tolerabilidad de los riesgos de seguridad operacional. Se trata de un proceso en dos etapas.

<b>Gravedad del suceso</b>	<b>Significado</b>	<b>Valor</b>
<b>Catastrófico</b>	<ul style="list-style-type: none"> <li>— Destrucción de equipo</li> <li>— Muertes múltiples</li> </ul>	<b>A</b>
<b>Peligroso</b>	<ul style="list-style-type: none"> <li>— Reducción importante de los márgenes de seguridad, daño físico o una carga de trabajo tal que los operarios no pueden desempeñar sus tareas en forma precisa y completa</li> <li>— Lesiones graves</li> <li>— Daños mayores al equipo</li> </ul>	<b>B</b>
<b>Mayor</b>	<ul style="list-style-type: none"> <li>— Reducción significativa de los márgenes de seguridad, reducción en la habilidad del operador en responder a condiciones operacionales adversas como resultado del incremento de la carga de trabajo, o como resultado de condiciones que impiden su eficiencia</li> <li>— Incidente grave</li> <li>— Lesiones a las personas</li> </ul>	<b>C</b>
<b>Menor</b>	<ul style="list-style-type: none"> <li>— Interferencia</li> <li>— Limitaciones operacionales</li> <li>— Uso de procedimientos de emergencia</li> <li>— Incidentes menores</li> </ul>	<b>D</b>
<b>Insignificante</b>	<ul style="list-style-type: none"> <li>— Consecuencias leves</li> </ul>	<b>E</b>

Figura 5-3. Tabla de gravedad de los riesgos de seguridad operacional

5.6.2 En primer término, es necesario obtener una evaluación general de los riesgos de seguridad operacional. Esto se logra combinando las tablas de probabilidad de los riesgos de seguridad operacional y de gravedad de los riesgos de seguridad operacional en una matriz de evaluación de los riesgos de seguridad operacional, de la cual se muestra un ejemplo en la Figura 5-4. Por ejemplo, se ha evaluado la probabilidad de los riesgos de seguridad operacional como ocasional (4). La gravedad de los riesgos de seguridad operacional se ha evaluado como peligrosa (B). La unión de la probabilidad y la gravedad (4B) constituye el riesgo de seguridad operacional de las consecuencias del peligro que se considera. Ampliando el análisis de 5.2, puede verse, mediante este ejemplo, que un riesgo de seguridad operacional es solamente un número o una combinación alfanumérica y no un componente visible o tangible del mundo natural. La codificación en colores de la matriz de la Figura 5-4 refleja las regiones de tolerabilidad del triángulo invertido de la Figura 5-1.

5.6.3 En segundo lugar, el índice de riesgo de seguridad operacional obtenido de la matriz de evaluación de los riesgos de seguridad operacional debe exportarse a una matriz de tolerabilidad de los riesgos de seguridad que describe los criterios de tolerabilidad. El criterio para un riesgo de seguridad operacional evaluado como 4B es, con arreglo a la tabla de tolerabilidad de la Figura 5-5, “inaceptable en las circunstancias actuales”. En este caso, el riesgo de seguridad operacional cae en la región intolerable del triángulo invertido. El riesgo de seguridad operacional de las consecuencias del peligro es inaceptable. La organización debe:

- a) asignar recursos para reducir la exposición a las consecuencias de los peligros;
- b) asignar recursos para reducir la magnitud o el potencial perjudicial de las consecuencias de los peligros; o
- c) cancelar la operación, si la mitigación no es posible.

## 5.7 QUINTO FUNDAMENTO —CONTROL/MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

5.7.1 En la cuarta y última etapa del proceso de llevar bajo control de la organización los riesgos de seguridad operacional de las consecuencias de un suceso o condición inseguro, deben aplicarse estrategias de control/mitigación. En términos generales, control y mitigación son términos que pueden usarse indistintamente. Ambos tienen el significado de designar medidas para enfrentar el peligro y llevar bajo control de la organización la probabilidad de los riesgos de seguridad operacional y la gravedad de las consecuencias del peligro.

5.7.2 Continuando con el ejemplo presentado en 5.6, el riesgo de seguridad operacional de las consecuencias del peligro que se está analizando se ha evaluado como 4B (“inaceptable en las circunstancias actuales”). Entonces deben asignarse recursos para llevarlo hacia abajo en el triángulo, a la región tolerable, donde los riesgos de seguridad operacional son ALARP. Si esto no puede hacerse, entonces debe cancelarse la operación dirigida a la prestación de servicios que expone a la organización a las consecuencias de los peligros en cuestión. En la Figura 5-6 se presenta el proceso de gestión de los riesgos de seguridad operacional en forma gráfica.

5.7.3 Hay tres estrategias genéricas para el control/mitigación de los riesgos de seguridad operacional:

- a) **Evitar.** Se cancela la operación o actividad debido a que los riesgos de seguridad operacional exceden los beneficios de continuar la operación o actividad. Las estrategias para evitar la exposición comprenden:
  - 1) se cancelan las operaciones hacia aeródromos rodeados por geografía compleja y sin las ayudas necesarias;
  - 2) se cancelan las operaciones en el espacio aéreo RVSM para aeronaves no equipadas con RVSM.

Probabilidad del riesgo	Gravedad del riesgo				
	Catastrófico A	Peligroso B	Mayor C	Menor D	Insignificante E
Frecuente 5	<b>5A</b>	<b>5B</b>	<b>5C</b>	<b>5D</b>	<b>5E</b>
Ocasional 4	<b>4A</b>	<b>4B</b>	<b>4C</b>	<b>4D</b>	<b>4E</b>
Remoto 3	<b>3A</b>	<b>3B</b>	<b>3C</b>	<b>3D</b>	<b>3E</b>
Improbable 2	<b>2A</b>	<b>2B</b>	<b>2C</b>	<b>2D</b>	<b>2E</b>
Extremadamente improbable 1	<b>1A</b>	<b>1B</b>	<b>1C</b>	<b>1D</b>	<b>1E</b>

Figura 5-4. Matriz de evaluación de los riesgos de seguridad operacional

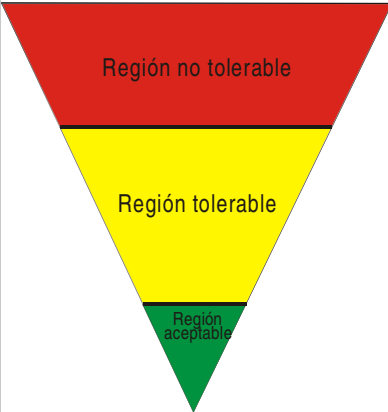
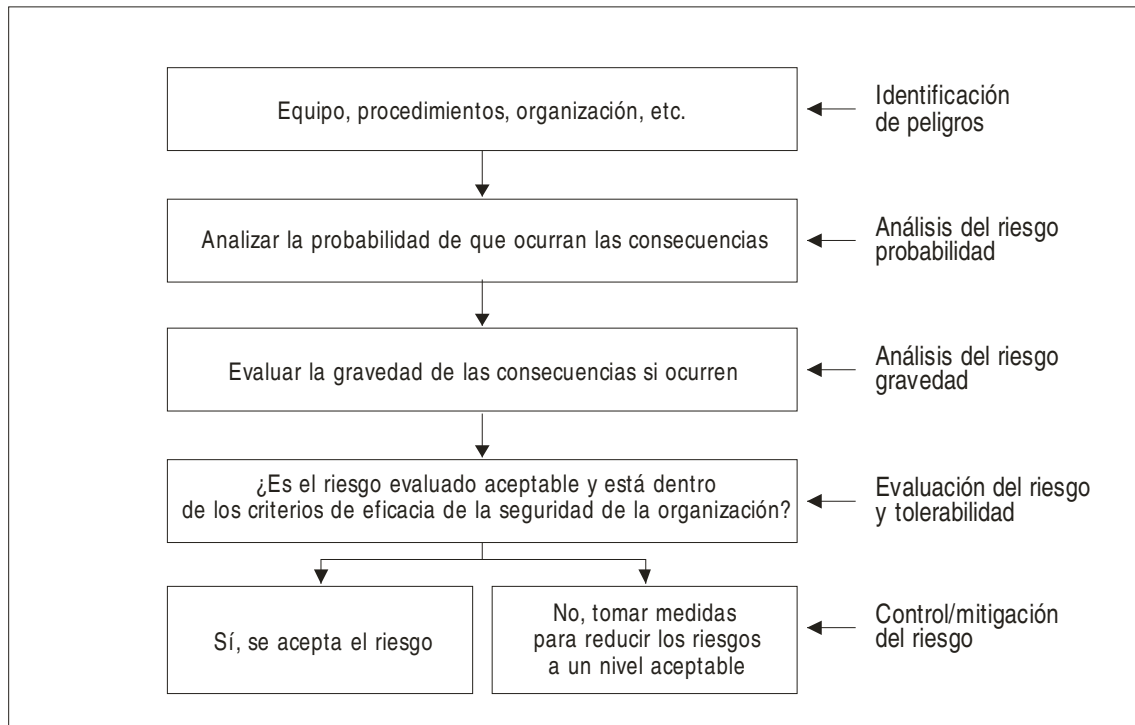
Criterios sugeridos	Índice de evaluación del riesgo	Criterios sugeridos
	<b>5A, 5B, 5C, 4A, 4B, 3A</b>	Inaceptable bajo las circunstancias existentes
	<b>5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C</b>	Aceptable en base a mitigación del riesgo. Puede requerir una decisión de la dirección.
	<b>3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E</b>	Aceptable

Figura 5-5. Matriz de tolerabilidad de los riesgos de seguridad operacional



**Figura 5-6. Proceso de gestión de los riesgos de seguridad operacional**

- b) **Reducir.** Se reduce la frecuencia de la operación o actividad, o se adoptan medidas para reducir la magnitud de las consecuencias de los riesgos aceptados. Las estrategias para reducir comprenden:
- 1) se limitan a condiciones diurnas y de vuelo visual las operaciones en un aeródromo rodeado por geografía compleja y sin las ayudas necesarias;
  - 2) las operaciones de aeronaves no equipadas con RVSM se realizan por encima o por debajo del espacio aéreo RVSM.
- c) **Separar la exposición.** Se adoptan medidas para aislar los efectos de las consecuencias de los peligros o crear redundancia para protegerse de los mismos. Las estrategias basadas en la segregación a la exposición comprenden:
- 1) las operaciones hacia un aeródromo rodeado de geografía compleja y sin las ayudas necesarias se limitan a aeronaves con capacidades específicas de performance de navegación;
  - 2) no se permite que las aeronaves no equipadas con RVSM vuelen en el espacio aéreo RVSM.

5.7.4 Cuando se evalúan las opciones específicas para mitigar los riesgos de seguridad operacional, debe tenerse en cuenta que no todas ofrecen el mismo potencial de reducción de los riesgos. Es necesario evaluar la eficacia de cada opción antes de adoptar una decisión. Es importante considerar toda la gama de posibles medidas de control y también considerar la compensación entre las diversas medidas para encontrar una solución óptima. Cada opción propuesta para mitigar los riesgos debería ser examinada desde perspectivas como las que siguen:

- a) **Eficacia.** ¿Reducirá o eliminará los riesgos de seguridad operacional de las consecuencias del suceso o condición inseguro? ¿En qué medida las alternativas mitigan tales riesgos de seguridad operacional? La eficacia puede considerarse como una continuidad, como sigue:
- 1) **Mitigaciones de ingeniería.** Esta mitigación elimina los riesgos de seguridad operacional de las consecuencias del suceso o condición insegura, por ejemplo, previendo interruptores de seguridad para impedir la activación del inversor de empuje durante el vuelo.
  - 2) **Mitigaciones de control.** Esta mitigación acepta los riesgos de seguridad operacional de las consecuencias del suceso o condición insegura pero ajusta el sistema para mitigar dichos riesgos reduciéndolos a un nivel manejable, por ejemplo, imponiendo condiciones de utilización más restrictivas. Ambas mitigaciones, ingeniería y control, se consideran mitigaciones “duras” dado que no confían en una actuación humana impecable.
  - 3) **Mitigaciones de personal.** Esta mitigación acepta que las mitigaciones de ingeniería o control pueden no ser eficientes o efectivas, de modo que el personal debe aprender a enfrentar los riesgos de seguridad operacional de las consecuencias del peligro, por ejemplo, agregando advertencias, listas de verificación revisadas, SOP o instrucción adicional. Las mitigaciones de personal son consideradas “medidas blandas”, dado que confían en una actuación humana impecable.
- b) **Costo-beneficio.** ¿Superan los costos los beneficios percibidos? ¿Las ganancias potenciales serán proporcionales a las repercusiones del cambio necesario?
- c) **Práctica.** ¿Es factible y apropiada la mitigación en términos de tecnología disponible, factibilidad financiera y administrativa, legislación y reglamentos, voluntad política, etc.?
- d) **Reto.** ¿Puede la medida de mitigación resistir el análisis crítico de todos los interesados (empleados, personal directivo, partes interesadas y administraciones de los Estados, etc.)?
- e) **Aceptación de cada interesado.** ¿Cuánta aceptación (o resistencia) puede esperarse de las partes interesadas? (Las conversaciones con los interesados durante la fase de evaluación de los riesgos de seguridad operacional pueden indicar cuál es la opción que prefieren para mitigar los riesgos).
- f) **Cumplimiento obligatorio.** Si se ponen en vigor nuevas reglas (SOP, reglamentos, etc.) ¿pueden hacerse cumplir?
- g) **Duración.** ¿Resistirá la medida la prueba del tiempo? ¿Será de beneficio temporario o será útil a largo plazo?
- h) **Riesgos de seguridad operacional residuales.** Una vez implantada la mitigación, ¿cuáles serán los riesgos residuales con relación al peligro original? ¿Cuál es la capacidad para mitigar los riesgos residuales?
- i) **Nuevos problemas.** ¿Qué nuevos problemas, o nuevos (quizás peores) riesgos de seguridad operacional introducirá el cambio propuesto?

5.7.5 Las medidas de mitigación más efectivas son las mitigaciones duras. Debido a que estas son a menudo onerosas, las organizaciones recurren con frecuencia a las medidas de mitigación blandas (como la instrucción). En tales casos, la organización delega muy frecuentemente en los subordinados la responsabilidad de la gestión de los riesgos de seguridad operacional.



5.7.6 En resumen, las estrategias de control/mitigación de los riesgos de seguridad operacional se basan principalmente en la introducción de defensas de seguridad adicionales o en el reforzamiento de las existentes. Las defensas se analizaron en el Capítulo 2 y se recuerda que en el sistema aeronáutico estas pueden agruparse en tres categorías generales:

- a) tecnología;
- b) instrucción; y
- c) reglamentos.

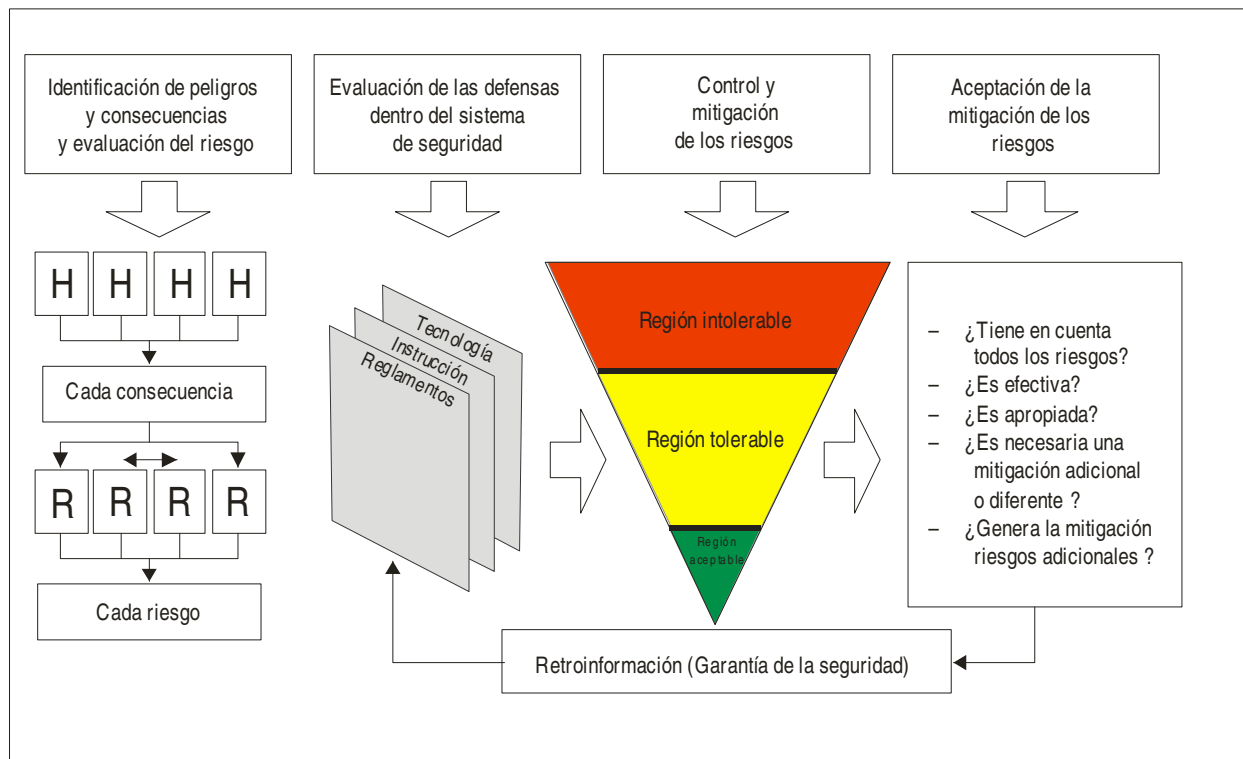
5.7.7 Como parte del control/mitigación de los riesgos de seguridad operacional, es importante determinar por qué se necesitan nuevas defensas o por qué deben reforzarse las existentes. Las preguntas siguientes pueden contribuir a dicha determinación:

- a) ¿existen defensas para protegerse contra los riesgos de seguridad operacional de las consecuencias de los peligros?
- b) ¿funcionan las defensas como estaba previsto?
- c) ¿son prácticas las defensas para usarlas en condiciones de trabajo reales?
- d) ¿conoce el personal afectado los riesgos de seguridad operacional de las consecuencias de los peligros y las defensas existentes?
- e) ¿son necesarias medidas adicionales de mitigación/control de los riesgos de seguridad operacional?

5.7.8 En la Figura 5-7 se presenta en forma gráfica el proceso completo de mitigación de los riesgos de seguridad operacional. Los peligros son posibles vulnerabilidades de seguridad operacional inherentes al sistema de aviación. Tales vulnerabilidades se manifiestan como un conjunto de consecuencias. Para gestionar la seguridad operacional, es necesario evaluar los riesgos de seguridad operacional de las consecuencias de los peligros, asignando un índice a cada riesgo de seguridad. Cada peligro puede generar una o más consecuencias, y cada consecuencia puede evaluarse como uno o varios riesgos de seguridad operacional. La primera etapa en el proceso de mitigación/control de los riesgos de seguridad operacional es, por lo tanto, la identificación de peligros y consecuencias y la evaluación de los riesgos de seguridad operacional.

5.7.9 Una vez identificados los peligros y consecuencias y evaluados los riesgos de seguridad operacional, debe evaluarse la eficacia y la eficiencia de las defensas existentes en el sistema aeronáutico (tecnología, instrucción y reglamentos) relativas a los peligros y consecuencias en cuestión. Como consecuencia de esta evaluación, se reforzarán las defensas existentes, se introducirán defensas nuevas o ambas cosas. La segunda etapa en el proceso de mitigación/control de los riesgos de seguridad operacional es, por consiguiente, la evaluación de la eficacia de las defensas existentes dentro del sistema de aviación.

5.7.10 Sobre la base del reforzamiento de las defensas existentes o la introducción de nuevas, los riesgos de seguridad operacional iniciales se vuelven a evaluar para determinar si ahora son ALARP. La tercera etapa del proceso de mitigación/control de los riesgos de seguridad operacional es, por lo tanto, la aplicación de medidas de control o mitigación.



**Figura 5-7. El proceso de mitigación de los riesgos de seguridad operacional**

5.7.11 Continuando con la reevaluación de los riesgos de seguridad operacional, deben confirmarse la eficacia y eficiencia de las estrategias de mitigación/control. La cuarta etapa del proceso de mitigación/control de los riesgos de seguridad operacional es aceptar la mitigación de los riesgos de seguridad operacional. Corresponde plantear las preguntas siguientes:

- ¿Trata la mitigación los riesgos de seguridad operacional?
- ¿Es la mitigación efectiva?
- ¿Es la mitigación apropiada?
- ¿Se necesita una mitigación adicional o diferente?
- ¿Generan las estrategias de mitigación riesgos adicionales?

5.7.12 Una vez aceptada la mitigación, las estrategias elaboradas y aplicadas deben, como parte del proceso de garantía de seguridad operacional, reintroducirse en las defensas de la organización, en las cuales se basan las estrategias de mitigación, para asegurar la integridad, eficiencia y eficacia de tales defensas en las nuevas condiciones operacionales.

## 5.8 LOS CINCO FUNDAMENTOS DE LA GESTIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL — RESUMEN

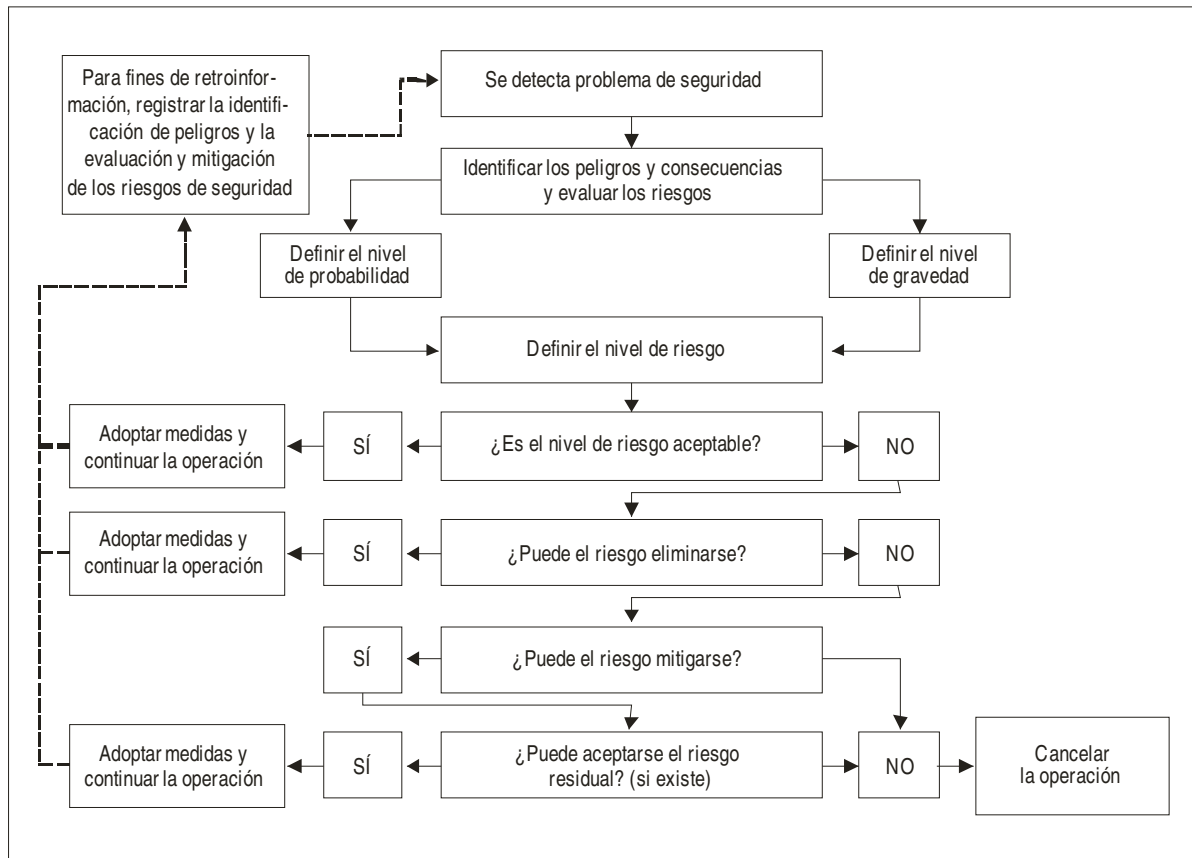
5.8.1 Los conceptos importantes con respecto a la gestión de los riesgos de seguridad operacional analizada en todo este capítulo pueden resumirse como siguen:

- a) No existe la seguridad operacional absoluta — en la aviación no es posible eliminar todos los riesgos de seguridad operacional.
- b) Los riesgos de seguridad operacional deben gestionarse para llevarlos a un nivel “tan bajo como sea razonable en la práctica” (ALARP).
- c) La mitigación de los riesgos de seguridad operacional debe balancearse con respecto a:
  - 1) el tiempo;
  - 2) los costos; y
  - 3) la dificultad de adoptar medidas para reducir o eliminar el riesgo de seguridad operacional (es decir gestionado).
- d) La gestión efectiva de los riesgos de seguridad operacional procura maximizar los beneficios de aceptar un riesgo de seguridad (más frecuentemente, una reducción ya sea en el tiempo o en los costos de la prestación del servicio) minimizando al mismo tiempo el propio riesgo de seguridad operacional.
- e) El fundamento de las decisiones en materia de riesgos de seguridad operacional deben comunicarse a los interesados afectados por las mismas, para obtener su aceptación.

5.8.2 En la Figura 5-8 se presenta en su totalidad el proceso de gestión de los riesgos de seguridad operacional. Después de haberse percibido un problema de seguridad operacional, se identifican los peligros subyacentes en el mismo y las posibles consecuencias de dichos peligros, y se evalúan los riesgos de seguridad operacional de las consecuencias en términos de probabilidad y gravedad para definir el nivel de riesgo de seguridad operacional (índice de riesgo de seguridad operacional). Si los riesgos de seguridad operacional se consideran aceptables, se adoptan las medidas apropiadas y la operación continúa. Para fines de información (biblioteca de seguridad operacional), la identificación de los peligros y la evaluación y mitigación de los riesgos de seguridad operacional se registran.

5.8.3 Si los riesgos de seguridad operacional se consideran inaceptables, corresponde formular las preguntas siguientes:

- a) **¿Pueden eliminarse los riesgos de seguridad operacional?** Si la respuesta es sí, entonces se adoptan las medidas apropiadas y se traslada la información a la biblioteca de seguridad operacional establecida. Si la respuesta es no, se plantea la próxima pregunta:
- b) **¿Pueden mitigarse los riesgos de seguridad operacional?** Si la respuesta es no, la operación debe cancelarse. Si la respuesta es sí, se adoptan las medidas de mitigación apropiadas y se plantea la próxima pregunta:
- c) **¿Pueden aceptarse los riesgos de seguridad operacional residual?** Si la respuesta es sí, entonces se adoptan medidas (si es necesario) y se traslada la información a la biblioteca de seguridad operacional establecida. Si la respuesta es no, debe cancelarse la operación.



**Figura 5-8. El proceso de gestión de los riesgos de seguridad operacional**

5.8.4 La pregunta 5.8.3 c) refleja el hecho de que las estrategias de mitigación nunca pueden mitigar completamente los riesgos de seguridad operacional. Debe aceptarse que siempre existirá un riesgo de seguridad operacional residual y la organización debe asegurar que los riesgos de seguridad operacional residuales también están bajo control.

5.8.5 Para proporcionar una ilustración práctica del proceso de gestión de los riesgos de seguridad operacional, se presentan en los apéndices de este capítulo tres escenarios diferentes de gestión de los riesgos de seguridad operacional. El Apéndice 1 comprende un ejemplo de ejercicio de gestión de los riesgos de seguridad operacional en un aeródromo. El Apéndice 2 comprende un ejemplo de un ejercicio de gestión de los riesgos de seguridad operacional por parte de un proveedor de servicios de tránsito aéreo. El Apéndice 3 comprende un ejemplo de ejercicio de gestión de los riesgos de seguridad operacional en una línea aérea.

## **Apéndice 1 del Capítulo 5**

# **PLAN DE CONSTRUCCIÓN EN EL AEROPUERTO INTERNACIONAL DE ACULLÁ**

### **1. ESCENARIO**

1.1 El Aeropuerto internacional de Acullá (AIA) tiene dos pistas paralelas, una principal y una secundaria, y prevé instalar un sistema de drenaje cerca del extremo de aproximación de la pista secundaria. Los vehículos de construcción deben cruzar la pista principal para llegar al sitio de construcción. Debido a que durante el día se registran muchas operaciones, se decide trabajar por la noche, en condiciones de tránsito más ligeras, para evitar la interrupción de las operaciones diurnas. El gerente de seguridad operacional de AIA debe evaluar las consecuencias para la seguridad operacional del plan de construcción nocturna del sistema de drenaje.

1.2 Se ha encargado al Grupo de acción de seguridad operacional (SAG) de AIA que apoye al gerente de seguridad operacional de AIA en la evaluación de las consecuencias de seguridad del plan de construcción. Un sector de preocupación genérico, inmediato y obvio, es el movimiento de vehículos de construcción hacia y desde el lugar de trabajo, que podría llevar a incursiones en las pistas. El SAG aplica un proceso de gestión de los riesgos de seguridad operacional para evaluar las consecuencias del plan de construcción sobre la seguridad operacional.

### **2. DESCRIPCIÓN DEL SISTEMA**

Una de las primeras tareas del SAG es describir el sistema modificado en cuyo marco el aeropuerto continuará sus operaciones mientras se realizan las obras de construcción, como sigue:

- a) el entorno de la pista durante las obras nocturnas, incluyendo un elevado volumen de tránsito de vehículos de construcción entre la rampa y el lugar de la obra;
- b) el programa de instrucción de conductores existente y el uso de escoltas para los vehículos de construcción;
- c) la torre de control de tránsito aéreo y el hecho de que no existen radiocomunicaciones con los vehículos de construcción que no están equipados para ello; y
- d) carteles, señales e iluminación para las calles de rodaje, pistas y zona de obras.

### **3. PROCESO DE IDENTIFICACIÓN DE PELIGROS**

La segunda tarea del SAG es identificar los peligros y sus posibles consecuencias que puedan afectar la operación del aeródromo durante la construcción, como sigue:

- a) Declarar el peligro genérico
  - 1) Obras de construcción en el aeropuerto.

- b) Declarar el componente específico del peligro
  - 1) Vehículos de construcción que cruzan la pista principal.
- c) Evaluar las consecuencias de los componentes específicos del peligro genérico
  - 1) Los vehículos de construcción pueden desviarse de los procedimientos prescritos y cruzar la pista principal sin escolta.
  - 2) Las aeronaves pueden entrar en conflicto con un vehículo que cruza.

#### **4. PROCESO DE EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL**

La tercera tarea del SAG consiste en identificar y evaluar los riesgos de seguridad operacional de las consecuencias de los peligros, y las defensas existentes, como sigue:

- a) La evaluación del SAG conduce a la conclusión de que existe una probabilidad remota de que un vehículo de construcción se desvíe de los procedimientos prescritos y cruce la pista principal sin escolta.
- b) Pueden haber operaciones de transporte aéreo nocturnas en el aeropuerto, de modo que existe una probabilidad remota de que una aeronave pueda entrar en conflicto con un vehículo que cruza.
- c) Si bien la probabilidad de conflicto entre una aeronave y un vehículo de construcción es remota, el SAG evalúa que, en caso de ocurrir dicho conflicto, la gravedad del suceso podría ser catastrófica.
- d) El SAG evalúa las defensas existentes (programa de instrucción de conductores, uso de escoltas para vehículos de construcción, carteles, señales e iluminación).
- e) Aplicando la matriz de evaluación de los riesgos de seguridad operacional (Capítulo 5, Figura 5-4) y la matriz de tolerabilidad de los riesgos de seguridad operacional (Capítulo 5, Figura 5-5), el SAG evalúa el índice de riesgo de seguridad operacional como 3A (inaceptable en las circunstancias actuales).
- f) El SAG llega a la conclusión de que el riesgo de seguridad operacional de las consecuencias del peligro generado por el movimiento de vehículos de construcción hacia el lugar de la obra es, en las condiciones actuales, inaceptable y que es necesario aplicar medidas de control/mitigación.

#### **5. PROCESO DE CONTROL/MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL**

La cuarta y última tarea del SAG es mitigar los riesgos de seguridad operacional de las consecuencias de los peligros, como sigue:

- a) El SAG decide controlar los riesgos de seguridad operacional de las consecuencias del peligro utilizando un camino perimetral del aeródromo existente para acceder al sitio de la obra. Todos los vehículos de construcción serán escoltados por el camino perimetral.

- b) Con esta mitigación, el SAG reevalúa la probabilidad de que los vehículos de construcción atraviesen la pista principal sin escolta, o que las aeronaves puedan entrar en conflicto con un vehículo que cruza, como de carácter extremadamente improbable. No obstante, si ocurriera un conflicto entre aeronaves y vehículos de construcción, la gravedad de tal suceso continuaría siendo catastrófica.
- c) El uso del camino perimetral como mitigación podría conducir a demoras en los vehículos de construcción debidas a la distancia adicional que deben recorrer, pero en la evaluación del SAG:
  - 1) Si bien no elimina enteramente la posibilidad de que ocurran las consecuencias del peligro (los vehículos de construcción todavía pueden atravesar la pista principal debido a varias circunstancias), no obstante lleva los riesgos de seguridad operacional de las consecuencias (vehículos de construcción que se desvían de procedimientos prescritos y atraviesan la pista principal sin escolta, y aeronaves en conflicto con un vehículo que cruza) a un nivel tan bajo como sea razonable en la práctica (ALARP).
- d) Aplicando la matriz de evaluación de los riesgos de seguridad operacional (Capítulo 5, Figura 5-4) y la matriz de tolerabilidad de los riesgos de seguridad operacional (Capítulo 5, Figura 5-5), el SAG reevalúa el índice de riesgo de seguridad operacional como 1A (aceptable);
- e) El SAG documenta este proceso de decisión para seguimiento futuro y lo presenta al gerente de seguridad operacional del Aeropuerto internacional de Acullá.

## **6. REGISTRO DE IDENTIFICACIÓN DE PELIGROS Y GESTIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL**

6.1 El registro de identificación de peligros y gestión de los riesgos de seguridad operacional que figura en la Tabla 5-Ap 1-1 se utiliza para dejar constancia de los riesgos de seguridad operacional identificados y las medidas adoptadas por las personas designadas. El registro debería conservarse permanentemente en la “biblioteca de seguridad operacional” para proporcionar evidencia de la gestión de los riesgos de seguridad operacional así como una referencia para futuras evaluaciones de los riesgos de seguridad operacional.

6.2 Habiendo identificado y jerarquizado los riesgos de seguridad operacional, deberían identificarse las defensas existentes contra los mismos. Estas defensas deben evaluarse posteriormente en cuanto a su adecuación. Si se encuentra que son menos que adecuadas, entonces deberán prescribirse medidas adicionales. Todas las medidas debe dirigirlas un individuo especificado (normalmente el gerente de línea responsable), y debe establecerse un plazo para completarlas. El registro de identificación de peligros y gestión de los riesgos de seguridad operacional no se autorizará hasta que estas medidas se hayan completado.

Tabla 5-Ap 1-1. Identificación de peligros y gestión de los riesgos de seguridad operacional

Tipo de operación o actividad	Peligro genérico	Componentes específicos del peligro	Consecuencias relacionadas con el peligro	Defensas existentes para controlar los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional	Nuevas medidas para reducir los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional resultante
Operaciones de aeropuerto	Construcción en el aeropuerto	Vehículos de construcción que cruzan la pista principal	<p>a) Los vehículos de construcción pueden desviarse de los procedimientos prescritos y cruzar la pista principal sin escolta.</p> <p>b) Las aeronaves pueden entrar en conflicto con un vehículo que cruza.</p>	<p>a) La evaluación del SAG lleva a la conclusión de que existe una probabilidad remota de que un vehículo de construcción se desvíe de los procedimientos prescritos y cruce la pista principal sin escolta.</p> <p>b) Hay operaciones nocturnas de transportistas aéreos en el aeropuerto, de modo que existe una probabilidad remota de que una aeronave pueda entrar en conflicto con un vehículo que cruza.</p> <p>c) Si bien la probabilidad de conflicto entre aeronave y vehículo de construcciones es remota, el SAG evalúa que, en caso de ocurrir, la gravedad del suceso sería catastrófica.</p> <p>d) El SAG evalúa las defensas existentes (programa de instrucción de conductores, uso de escoltas para vehículos de construcción, carteles, señales e iluminación).</p> <p>e) Aplicando la matriz de evaluación de los riesgos de seguridad operacional (Capítulo 5, Figura 5-4) y la matriz de tolerabilidad de los riesgos de seguridad operacional (Capítulo 5, Figura 5-5), el SAG evalúa: Índice de riesgo de seguridad operacional: 3A Tolerabilidad de los riesgos de seguridad operacional: inaceptable en las circunstancias actuales.</p>	<p>a) El SAG decide controlar los riesgos de seguridad operacional utilizando un camino perimetral del aeródromo existente para llegar al sitio de construcción. Todos los vehículos de construcción serán escoltados por el camino perimetral.</p> <p>b) Con esta mitigación, el SAG reevalúa la probabilidad de que los vehículos de construcción crucen la pista principal sin escolta, o que las aeronaves puedan entrar en conflicto con un vehículo que cruza, como de carácter extremadamente improbable. No obstante, si ocurriera un conflicto entre aeronaves y vehículos, la gravedad de tal suceso seguiría siendo catastrófica.</p> <p>c) El uso del camino perimetral como mitigación puede introducir demoras en los vehículos de construcción debidas a la distancia adicional que ha de recorrerse, pero en la evaluación del SAG:</p> <p>1) si bien no elimina enteramente la posibilidad de que ocurran las consecuencias del peligro (los vehículos de construcción pueden todavía cruzar la pista principal debido a varias circunstancias), no obstante lleva los riesgos de seguridad de las consecuencias (vehículo de construcción que se desvíe de los procedimientos prescritos y cruce la pista principal sin escolta, y aeronaves en conflicto con vehículos que cruzan) a un nivel aceptable.</p> <p>d) Aplicando la matriz de evaluación de los riesgos de seguridad operacional (Capítulo 5, Figura 5-4) y la matriz de tolerabilidad de los riesgos de seguridad operacional (Capítulo 5, Figura 5-5), el SAG reevalúa: Índice de riesgo de seguridad operacional: 1A Tolerabilidad de los riesgos de seguridad operacional: aceptable.</p> <p>e) El SAG documenta el proceso de decisión para futuro seguimiento y lo presenta al gerente de seguridad del Aeropuerto internacional de Acullá.</p>



## Apéndice 2 del Capítulo 5

# OPERACIONES EN PISTAS CONVERGENTES

### 1. ESCENARIO

1.1 Un proveedor de servicios de tránsito aéreo ha recibido información de usuarios de un aeropuerto expresando preocupaciones de seguridad operacional con respecto a las operaciones en pistas convergentes en el Aeropuerto internacional XYZ. El Aeropuerto internacional XYZ tiene tres pistas, 08L/26R, 08R/26L, y 12/30 (véase la Figura 5-Ap 2-1). Ocasionalmente se realizan operaciones en pistas convergentes en las pistas 26R y 12. El proveedor de servicios de tránsito aéreo ha pedido a su gerente de seguridad operacional que reevalúe la seguridad operacional de los procedimientos para operaciones en pistas convergentes para las pistas 26R y 12 en el Aeropuerto internacional XYZ a la luz de las preocupaciones expresadas por los usuarios.

1.2 Se encargó al Grupo de acción de seguridad operacional (SAG) que ayude al gerente de seguridad operacional del proveedor de servicios ATS en la reevaluación de la seguridad operacional de los procedimientos de operaciones en pistas convergentes en el Aeropuerto internacional XYZ. El SAG está integrado por representantes del proveedor de servicios ATS, líneas aéreas que operan en el Aeropuerto internacional XYZ y su asociación de pilotos, representantes del aeropuerto así como representantes de la autoridad de vigilancia del Estado. La preocupación genérica de seguridad operacional es la convergencia de las trayectorias de vuelo de las aeronaves que salen y llegan al Aeropuerto internacional XYZ. El SAG aplica un proceso de gestión de los riesgos de seguridad operacional para reevaluar la seguridad de las operaciones en pistas convergentes.

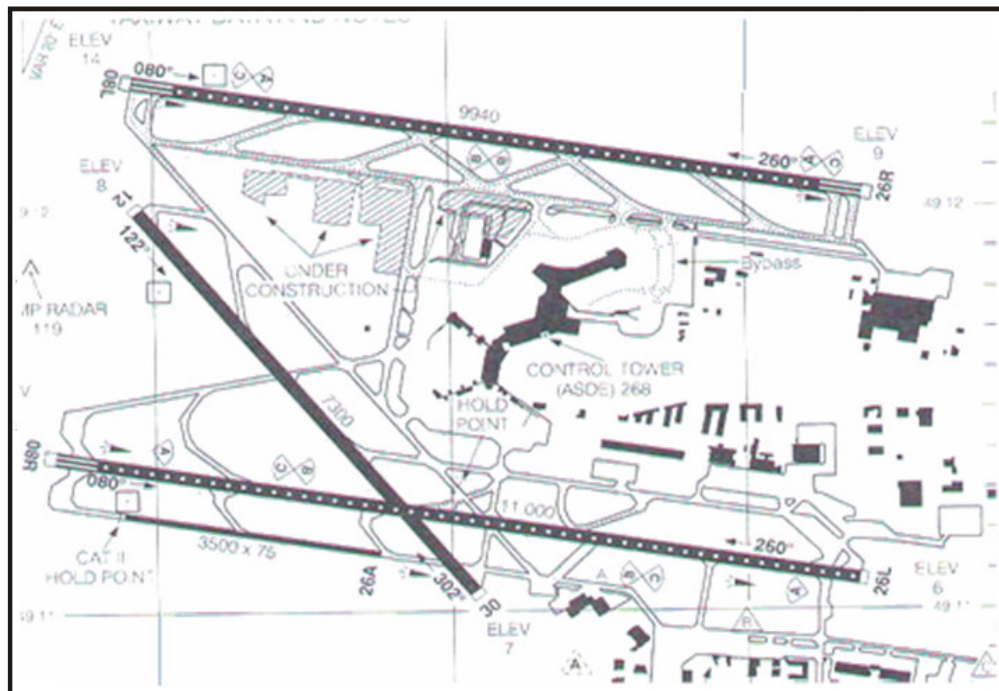


Figura 5-Ap 2-1. Aeropuerto internacional XYZ

## 2. DESCRIPCIÓN DEL SISTEMA

Una de las primeras tareas del SAG consiste en describir el sistema en el que se realizan las operaciones, como sigue:

- a) El Aeropuerto internacional XYZ tiene tres pistas principales y una pequeña pista secundaria.
- b) El aeropuerto tramita unos 325 000 movimientos anuales.
- c) La pista 26L-08R tiene 11 000 pies de longitud y se utiliza para salidas oeste y este y llegadas oeste y este. La pista 12-30 tiene 7 300 pies de longitud. La pista 12 se utiliza principalmente para llegadas. La pista 30 se utiliza a veces para salidas y rara vez para llegadas. La pista 12 atraviesa físicamente la pista 08R-26L y se considera como pista de "intersección". La pista 08L-26R tiene 9 940 pies de longitud y se usa principalmente para el tránsito de llegada y ocasionalmente para el de salida. La pista 08L se utiliza solamente para llegadas debido a que no se han establecido todavía procedimientos de salida.
- d) Las señales, carteles e iluminación del aeropuerto cumplen las normas de las autoridades de vigilancia y de la OACI.
- e) Existen dos frecuencias de control utilizadas para control desde la torre. Una frecuencia abarca la pista sur (26L-08R) y la pista oeste (12-30). La segunda frecuencia abarca la pista norte (26R-08L).
- f) Las pistas sur (26L-08R) tienen aproximaciones a pistas convergentes publicadas para evitar conflictos con el tránsito en la pista 12. No hay aproximaciones convergentes publicadas para las pistas norte (26R-08L), dado que, técnicamente, no se consideran de intersección debido a que no se cortan físicamente. Si bien la pista 12 tiene una aproximación ILS, es en general una pista VFR y la mayoría de los aterrizajes se hacen a partir de aproximaciones visuales.
- g) La información de tránsito en la pista 12 se transmite actualmente al tránsito en la pista 08R-26L porque se considera que las pistas se cruzan. El tránsito en ambas pistas se controla en la misma frecuencia. No obstante, debido a que las pistas 08L-26R y 12 no se cortan físicamente, el tránsito en ellas se controla en frecuencias diferentes. Como resultado, no se comparte la información de tránsito.
- h) Si bien se proporciona separación de tránsito IFR al tránsito IFR en la pista 26R, se proporciona servicio de control de aeropuerto a las aproximaciones VFR y visuales de aeronaves en la pista 12. No obstante, los controladores de tránsito aéreo actuarán inmediatamente para resolver cualquier conflicto de tránsito conocido. El procedimiento normalizado es dar prioridad al tránsito en las pistas 26R-08L y desviar el tránsito en la pista 12.

## 3. PROCESO DE IDENTIFICACIÓN DE PELIGROS

La segunda tarea del SAG es identificar los peligros y sus consecuencias que afectarán a las operaciones de aeródromo, como sigue:

- a) Declarar el peligro genérico
  - 1) Trayectorias de vuelo convergentes en las pistas 26R-08L y 12, independientemente de si las aeronaves están en aproximación o salida.
- b) Declarar los componentes específicos del peligro

- 1) La aeronave rechaza aterrizar en la pista 26R contra el tránsito que aterriza en la pista 12.
  - 2) La aeronave despegue en la pista 26R contra el tránsito que aterriza en la pista 12.
  - 3) La aeronave se aproxima a la pista 08L contra el tránsito que aterriza en la pista 12.
  - 4) La aeronave da un "paso lateral" desde una aproximación sobre la pista 08L a la pista 08R o desde la pista 08R a la pista 08L contra el tránsito que aterriza en la pista 12.
- c) Evaluar las consecuencias de los componentes específicos del peligro genérico
- 1) Encuentro con estela turbulenta.
  - 2) Acción evasiva para evitar otro tránsito.
  - 3) Pérdida de control después de la maniobra para evitar otro tránsito.
  - 4) Rebase de la pista después de una aproximación inestable.
  - 5) Colisión en vuelo en el extremo de salida de la pista 26R entre una aeronave que se aproxima a la pista 12 y una aeronave que se aproxima a la pista 08L o que sale de la pista 26R (peor consecuencia posible).

#### 4. PROCESO DE EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

4.1 El SAG identifica las defensas que apoyan las operaciones en pistas convergentes para las pistas 26R-08L y 12 en el Aeropuerto internacional XYZ. Tales defensas tienen carácter de tecnología, programas y procedimientos dirigidos a reducir los riesgos de seguridad operacional de las consecuencias de las trayectorias de vuelo convergentes para las pistas 26R-08L y 12.

4.2 Las defensas comprenden:

- a) procedimientos de coordinación por el controlador;
- b) mayor espaciado para proteger el espacio aéreo para aproximaciones frustradas mediante condiciones meteorológicas adversas;
- c) restricciones a las llegadas a la pista 12 cuando la pista 26R se utiliza para salidas;
- d) equipo de detección en la superficie del aeródromo (ASDE);
- e) programa de prevención de incursiones en las pistas y programa de control de la fauna silvestre;
- f) instrucción inicial y de repaso para conductores en la parte aeronáutica y exámenes correspondientes;
- g) vigilancia continua y seguimiento estadístico de los límites de vientos transversales;
- h) disponibilidad y uso del radar de aproximación;
- i) normas para tiempo de ocupación de pista;

- j) frecuencias de torre separadas; y
- k) señales y carteles.

4.3 Sobre la base de estas defensas existentes, el SAG, utilizando la matriz de evaluación de los riesgos de seguridad operacional (Capítulo 5, Figura 5-4) y la matriz de tolerabilidad de los riesgos de seguridad operacional (Capítulo 5, Figura 5-5), evalúa los riesgos de seguridad operacional de las consecuencias de las trayectorias de vuelo convergentes para las pistas 26R-08L y 12 como sigue:

- a) Encuentro con estela turbulenta: probabilidad remota, gravedad mayor. Tolerabilidad de los riesgos de seguridad operacional: 3C (aceptable basada en mitigación de los riesgos).
- b) Acción evasiva para evitar otro tránsito: probabilidad remota, gravedad mayor. Tolerabilidad de los riesgos de seguridad operacional: 3C (aceptable basada en mitigación de los riesgos).
- c) Pérdida de control después de una maniobra para evitar otro tránsito: probabilidad remota, gravedad peligrosa. Tolerabilidad de los riesgos de seguridad operacional: 3B (aceptable basada en mitigación de los riesgos).
- d) Rebase de la pista después de una aproximación inestable: probabilidad remota, gravedad peligrosa. Tolerabilidad de los riesgos de seguridad operacional: 3B (aceptable basada en mitigación de los riesgos).
- e) Colisión en el aire en el extremo de salida de la pista 26R entre una aeronave que se aproxima a la pista 12 y una aeronave que se aproxima a la pista 08L o que sale de la pista 26R: probabilidad improbable, gravedad catastrófica. Tolerabilidad de los riesgos de seguridad operacional: 2A (aceptable basada en mitigación de los riesgos).

## 5. PROCESO DE CONTROL/MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

5.1 El SAG reconoce que la prohibición de operaciones en pistas convergentes eliminaría efectivamente las peores consecuencias posibles de las trayectorias de vuelo convergentes para las pistas 26R-08L y 12, es decir una colisión en vuelo en el extremo de salida de la pista 26R. No obstante, las medidas de gestión de la seguridad operacional deben ser eficientes y no solo efectivas. Prohibir el uso de pistas convergentes sería ineficiente.

5.2 El SAG llega a la conclusión de que no hay problemas reales de seguridad operacional en el Aeropuerto internacional XYZ con respecto a las operaciones en pistas convergentes para las pistas 26R y 12 que requieran medidas urgentes e inmediatas. Las defensas existentes para los riesgos de seguridad operacional de las consecuencias de las trayectorias de vuelo convergentes para las pistas 26R-08L y 12 en el Aeropuerto internacional XYZ, incluyendo el peor escenario posible (una colisión en vuelo) son controles efectivos para mantener los riesgos de seguridad operacional ALARP (tan bajo como sea razonable en la práctica). No obstante, se formulan recomendaciones para reforzar la seguridad de las operaciones en el Aeropuerto internacional XYZ. Si bien no tiene carácter urgente, la aplicación de estas recomendaciones proporcionaría un mayor margen de seguridad operacional.

5.3 Las recomendaciones comprenden:

- a) Iniciar una campaña continua para alentar a las tripulaciones de vuelo a que transmitan los informes de piloto (PIREP) a las dependencias de control de tránsito aéreo cuando las condiciones meteorológicas difieren de las pronosticadas o previstas.
- b) Estudiar la adecuación y eficacia de la implantación de una presentación visual de pistas convergentes (CRDA) como un dispositivo esencial de mejoramiento de la seguridad operacional y la capacidad en el Aeropuerto internacional XYZ.

- c) Si no se implanta una CRDA en el Aeropuerto internacional XYZ, establecer criterios y procedimientos de separación para ajustar el espaciado de las aeronaves que aterrizan de modo que una aeronave que pueda rechazar un aterrizaje en la pista 26R cuente con espacio aéreo protegido respecto de aeronaves que puedan estar aproximándose a la pista 12.
- d) Mostrar una gama de limitaciones a la velocidad de aproximación en las cartas de tipo llegada; y modificar los procedimientos de comunicaciones del controlador de tránsito aéreo de modo que se mantenga informado al tránsito sobre la pista 08L-26R respecto del tránsito que está cruzando en la pista 12.
- e) Instalar un dispositivo anulador de frecuencias de emergencia de modo que un controlador pueda conmutar a la frecuencia de otro controlador para expedir instrucciones de emergencia.

5.4 El SAG documenta este proceso de decisión para seguimiento futuro y lo presenta al gerente de seguridad operacional del servicio de tránsito aéreo.

## **6. REGISTRO DE IDENTIFICACIÓN DE PELIGROS Y GESTIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL**

6.1 El registro de identificación de peligros y gestión de los riesgos de seguridad operacional que figura en la Tabla 5-Ap 2-1 se utiliza para dejar constancia de los riesgos identificados y las medidas adoptadas por las personas designadas. El registro debería conservarse permanentemente en la "biblioteca de seguridad operacional" para proporcionar evidencia de la gestión de los riesgos de seguridad operacional así como una referencia para futuras evaluaciones de los riesgos.

6.2 Habiendo identificado y calificado los riesgos de seguridad operacional, deberían identificarse las defensas existentes contra los mismos. Estas defensas deben evaluarse posteriormente en cuanto a su adecuación. Si se encuentra que son menos que adecuadas, entonces deberán prescribirse medidas adicionales. Todas las medidas debe dirigirlas un individuo específico (normalmente el gerente de línea responsable), y debe establecerse un plazo para completarlas. El registro de identificación de peligros y gestión de los riesgos de seguridad operacional no se autorizará hasta que estas medidas se hayan completado.

Tabla 5-AP 2-1. Identificación de peligros y gestión de los riesgos de seguridad operacional

Tipo de operación o actividad	Peligro genérico	Componentes específicos del peligro	Consecuencias relacionadas con el peligro	Defensas existentes para controlar los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional	Otras medidas para reducir los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional resultante
Actividades de control de tránsito aéreo	Trayectoria de vuelos convergentes en pistas 26R-08L y 12, independientemente de que la aeronave esté en aproximación o salida	<p>a) La aeronave rechaza el aterrizaje en la pista 26R contra tránsito que aterriza en pista 12.</p> <p>b) La aeronave despegue en pista 26R contra tránsito que aterriza en pista 12.</p> <p>c) La aeronave se aproxima a pista 08L contra tránsito que aterriza en pista 12.</p> <p>d) Una aeronave da un "paso lateral" desde una aproximación sobre pista 08L a pista 08R o de pista 08R a pista 08L contra tránsito que aterriza en pista 12.</p>	<p>a) Encuentro con estela turbulenta.</p> <p>b) Acción evasiva para evitar otro tránsito.</p> <p>c) Pérdida de control después de maniobra para evitar otro tránsito.</p> <p>d) Rebaje de pista después de aproximación inestable.</p> <p>e) Colisión en vuelo en el extremo de salida de la pista 26R entre una aeronave que se aproxima a pista 12 y una aeronave que se aproxima a pista 08L o que sale de pista 26R (peor consecuencia posible).</p>	<ul style="list-style-type: none"> <li>• Procedimientos de coordinación del controlador;</li> <li>• mayor espaciado para proteger el espacio aéreo para aproximaciones frustradas durante condiciones meteorológicas adversas;</li> <li>• restricciones a las llegadas en pista 12 cuando la pista 26R se utiliza para salidas;</li> <li>• equipo de detección en la superficie del aeródromo (ASDE);</li> <li>• programa de prevención de incursiones en las pistas y programa de control de fauna silvestre;</li> <li>• instrucción inicial y de repaso de conductores de la parte aeronáutica y exámenes correspondientes;</li> <li>• vigilancia continua y seguimiento estadístico de los límites de vientos transversales;</li> <li>• disponibilidad y uso del radar de aproximación;</li> <li>• normas para el tiempo de ocupación de pista;</li> <li>• frecuencias de torre separadas; y</li> <li>• señales y carteles.</li> </ul> <p>a) Encuentro con estela turbulenta: Índice de riesgo de seguridad operacional: 3C Tolerabilidad de los riesgos de seguridad operacional: aceptable basado en mitigación de los riesgos.</p> <p>b) Acción evasiva para evitar otro tránsito: Índice de riesgo de seguridad operacional: 3C Tolerabilidad de los riesgos de seguridad operacional: aceptable basado en mitigación de los riesgos.</p> <p>c) Pérdida de control después de maniobra para evitar otro tránsito: Índice de riesgo de seguridad operacional: 3B Tolerabilidad de los riesgos de seguridad operacional: aceptable basado en mitigación de los riesgos.</p> <p>d) Rebaje de pista después de aproximación inestable: Índice de riesgo de seguridad operacional: 3B Tolerabilidad de los riesgos de seguridad operacional: aceptable basado en mitigación de los riesgos.</p> <p>e) Colisión en vuelo en el extremo de salida de la pista 26R entre una aeronave que se aproxima a la pista 12 y una aeronave que se aproxima a la pista 08L o que sale de la pista 26R: Índice de riesgo de seguridad operacional: 2A Tolerabilidad de los riesgos de seguridad operacional: aceptable basada en mitigación de los riesgos.</p>	<p>a) Iniciar una campaña continua para alentar a las tripulaciones de vuelo a que transmitan PIREP a las dependencias de control de tránsito aéreo cuando las condiciones meteorológicas difieren de las pronosticadas o previstas;</p> <p>b) estudiar la adecuación y eficacia de la implantación de una presentación visual de pistas convergentes (CRDA) como un dispositivo esencial para mejorar la seguridad operacional y la capacidad en el Aeropuerto internacional XYZ;</p> <p>c) si no se implanta CRDA en el Aeropuerto internacional XYZ, establecer criterios y procedimientos de separación para ajustar el espaciado de las aeronaves que aterrizan de modo que una aeronave que pueda rechazar un aterrizaje en pista 26R cuente con espacio aéreo protegido respecto de las aeronaves que pueden estar aproximándose a la pista 12;</p> <p>d) mostrar una gama de limitaciones a la velocidad de aproximación en cartas de tipo llegada; y modificar los procedimientos de comunicación del controlador de tránsito aéreo para que se informe al tránsito en la pista 08L-26R respecto del tránsito que cruza en la pista 12;</p> <p>e) instalar un sistema de anulación de frecuencia de emergencia de modo que un controlador pueda conmutar a la frecuencia de otro controlador para expedir instrucciones de emergencia.</p>

## Apéndice 3 del Capítulo 5

# OPERACIONES COMERCIALES EN EL AEROPUERTO INTERNACIONAL DE CIUDAD ANDES

### 1. ESCENARIO

1.1 Aerolíneas Seguras es un explotador de servicios aéreos de tamaño mediano con una flota de quince birreactores de moderna tecnología. La línea aérea está planeando iniciar operaciones comerciales hacia Ciudad Andes, un centro turístico emplazado en lo alto de las montañas rodeado por hermosos paisajes y que guarda vestigios de una antigua civilización. El transporte terrestre puede llevar más de dos días por caminos peligrosos y, por consiguiente, el transporte aéreo es el medio de transporte más adecuado.

1.2 Ciudad Andes cuenta con un aeródromo muy elevado rodeado de una geografía compleja y sin ayudas para la navegación en aproximación, lo que hace que los vuelos se limiten a las condiciones diurnas y visuales. La administración superior de Aerolíneas Seguras pide al director de operaciones de vuelo que implante esa operación con arreglo a todos los requisitos de seguridad operacional y, al mismo tiempo, garantice la máxima carga de pago comercial, con debida consideración a la performance y las limitaciones de las aeronaves. La operación prevista involucraría un vuelo a temprana hora de la tarde hacia Ciudad Andes, con un rápido regreso a la base principal, a unos noventa minutos de allí.

1.3 El director de operaciones de vuelo pide al gerente de seguridad operacional que, con apoyo del Grupo de acción de seguridad operacional (SAG), evalúe las consecuencias para la seguridad operacional de la operación en el Aeropuerto internacional de Ciudad Andes. Una preocupación inmediata y obvia de carácter genérico es la operación en un aeródromo muy elevado rodeado de geografía compleja y sin ayudas para la navegación en aproximación. El SAG aplica un proceso de gestión de los riesgos de seguridad operacional para evaluar las consecuencias para la seguridad operacional de la operación en el Aeropuerto internacional de Ciudad Andes.

### 2. DESCRIPCIÓN DEL SISTEMA

Una de las primeras tareas del SAG es describir el sistema en el cual se realizará la operación, como sigue:

- a) El Aeropuerto internacional de Ciudad Andes está ubicado en un valle a una elevación de 3 360 m (11 000 ft) rodeado de montañas de más de 4 900 m (16 000 ft) de altura.
- b) El aeródromo cuenta con solamente una pista de 3 400 m (11 155 ft) de longitud, orientada de este a oeste (pista 09-27).
- c) Debido a la topografía del lugar, la pista 09 se utiliza exclusivamente para aterrizajes y la pista 27 exclusivamente para despegues.
- d) Se utiliza un VOR para aproximaciones por instrumentos. El radiofaro está emplazado en el valle 30 km al este del aeródromo.

- e) No se dispone de ILS para aproximaciones.
- f) No se permiten aproximaciones que no sean visuales una vez que una aeronave en salida haya sido autorizada a despegar hasta que dicha aeronave haya notificado su ascenso hasta una altitud en ruta libre de todo obstáculo.
- g) La aproximación visual en VMC al Aeropuerto internacional de Ciudad Andes comienza a 18 000 pies por encima del VOR. Si no se establece contacto con tierra a 18 000 ft, el ATC no autoriza las aproximaciones VMC.
- h) No se dispone de ayudas visuales para el aterrizaje.
- i) No se permiten despegues hasta que una aeronave autorizada por el ATC para iniciar la aproximación visual al Aeropuerto internacional de Ciudad Andes haya aterrizado y anunciado que ha abandonado la pista después del aterrizaje.
- j) El tiempo en el Aeropuerto internacional de Ciudad Andes es variable, y está caracterizado a menudo por una alta capa de nubes con base alrededor de los 19 000 a 21 000 pies.
- k) La temperatura exterior es elevada entre las 10:00 y las 14:00 horas, lo que afecta la performance de las aeronaves.
- l) Los vientos catabáticos pueden imponer la necesidad de despegues con viento de cola desde la pista 27 después de las 16:00 horas aproximadamente todos los días.
- m) En caso de incendio de motor, apagado de motor o cualquier condición de emergencia, el regreso al aeropuerto es obligatorio, dado que las limitaciones de peso y performance harían improbable ajustarse a los procedimientos de franqueamiento de obstáculos y a la trayectoria neta.
- n) La Administración de aviación civil (AAC) nacional exige que la línea aérea demuestre que las aeronaves pueden cumplir con la trayectoria neta y el franqueamiento de obstáculos durante las fases de aproximación, aterrizaje, despegue, ascenso y en ruta, y que pueden maniobrar dentro de la topografía compleja, con los márgenes de seguridad operacional y limitaciones de las aeronaves, para obtener la autorización especial de explotación como parte de su certificado de explotador de servicios aéreos.
- o) La AAC exige un ensayo de vuelo cuando la operación esté lista para iniciarse, después de haberse examinado y aprobado la documentación, y que la tripulación de vuelo y de cabina haya recibido instrucción especial para la operación en el Aeropuerto internacional de Ciudad Andes.

### 3. PROCESO DE IDENTIFICACIÓN DE PELIGROS

La segunda tarea del SAG es identificar los peligros que afectarán a la operación en el Aeropuerto internacional de Ciudad Andes, y sus consecuencias, como sigue:

- a) Declarar el peligro genérico
  - 1) Operación en un aeropuerto muy elevado rodeado de geografía compleja.



- b) Declarar los componentes específicos del peligro
  - 1) Montañas circundantes.
  - 2) Aeródromo muy elevado.
  - 3) Ausencia de ayudas para la navegación en aproximación y aterrizaje.
  - 4) Ausencia de ayudas visuales para aterrizaje.
  - 5) Tránsito conflictivo.
  - 6) Pista resbalosa cuando está mojada.
  - 7) Fauna silvestre.
- c) Evaluar las consecuencias de los componentes específicos del peligro genérico
  - 1) Impacto contra el suelo sin pérdida de control (CFIT) debido a:
    - i) pérdida de motor crítico durante aproximación y aterrizaje;
    - ii) pérdida de motor crítico durante despegue después de  $V_1$ ;
    - iii) pérdida de motor crítico durante ascenso en ruta.
  - 2) Colisión en vuelo.
  - 3) Rebase de pista después de aterrizaje.
  - 4) Rebase de pista en aterrizaje después de despegue interrumpido.
  - 5) Choques con aves.

#### 4. PROCESO DE EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

*Nota.— El impacto contra el suelo sin pérdida de control debido a pérdida de motor crítico durante el despegue después de  $V_1$  es la única consecuencia que se analiza en este ejercicio. En una evaluación real de los riesgos de seguridad operacional todas las consecuencias deben analizarse y todos los riesgos de seguridad operacional deben evaluarse y mitigarse.*

4.1 La tercera tarea del SAG es evaluar la eficacia de las defensas existentes para enfrentar los riesgos de seguridad operacional de las consecuencias de los peligros.

4.2 El SAG examina las defensas existentes de seguridad operacional que pueden verse afectadas o están ausentes en relación con esta operación. Estas defensas se relacionan principalmente con la instrucción de la tripulación de vuelo y los procedimientos y limitaciones en el manual de operaciones de la compañía con respecto a operaciones similares.

4.3 Las defensas existentes identificadas durante la evaluación son las siguientes:

- a) operación de las aeronaves en VMC y condiciones diurnas;
- b) plano del aeródromo disponible en la AIP nacional;
- c) procedimientos ATC aplicados en el aeródromo;
- d) manual de operaciones de la compañía;
- e) manual de actuación de despacho;
- f) manual de operación de la aeronave;
- g) instrucción periódica sobre fallas de motor antes y después de  $V_1$  y procedimientos de aproximación frustrada;
- h) instrucción en CRM.

4.4 El SAG considera que las defensas existentes son inadecuadas, principalmente porque no encaran la operación específica en un aeródromo muy elevado rodeado de geografía compleja.

4.5 Se examina la documentación operacional así como los procedimientos ATC actuales en el Aeropuerto internacional de Ciudad Andes.

4.6 Utilizando la matriz de evaluación de los riesgos de seguridad operacional (Capítulo 5, Figura 5-4) y la matriz de tolerabilidad de los riesgos de seguridad operacional (Capítulo 5, Figura 5-5), el SAG evalúa el índice de riesgo de seguridad operacional como 3A (inaceptable en las circunstancias actuales).

## 5. PROCESO DE CONTROL/MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

5.1 La cuarta y última tarea del SAG es controlar y mitigar los riesgos de seguridad operacional identificados de las consecuencias del CFIT debido a la pérdida de un motor crítico durante el despegue después de  $V_1$ . Después de varias reuniones, el SAG propone varias mitigaciones. Las mitigaciones propuestas se dirigen a reforzar las defensas y disminuir los riesgos de seguridad operacional a un nivel “tan bajo como sea razonable en la práctica” (ALARP). Las mitigaciones comprenden:

- a) Elaborar procedimientos de despegue y ascenso en caso de pérdida de un motor crítico después de  $V_1$ , considerando la posibilidad de un regreso a tierra.
- b) Elaborar y brindar instrucción en los procedimientos mencionados (simulador de vuelo completo y mantener la calificación cada seis meses).
- c) Considerar que el Aeropuerto internacional de Ciudad Andes es una “operación de aeródromo especial” que exige calificación especial de la tripulación, válida por solamente un año a menos que se renueve.
- d) Proporcionar instrucción apropiada para “operación de aeródromo especial” a las tripulaciones de cabina. (Esta mitigación no se refiere a la probabilidad sino a la gravedad — evacuación de emergencia — de una consecuencia de los riesgos de seguridad operacional).

- e) Proporcionar información meteorológica precisa, en particular vientos en la superficie después de las 16:00 horas.
- f) Elaborar documentación operacional e incluirla en el manual de operaciones de la compañía y en el manual de despacho, para aprobación por la AAC.
- g) Prohibir una política abierta de artículos críticos en la lista de equipo mínimo (MEL).
- h) En el marco del programa de fiabilidad de mantenimiento, el departamento de mantenimiento debe examinar los motores de las aeronaves asignadas a la operación.
- i) Efectuar el seguimiento de las medidas de seguridad operacional e implantar nuevas defensas para el control y mitigación de los riesgos de seguridad operacional relacionados a la operación en el Aeropuerto internacional de Ciudad Andes. Se prevé realizar exámenes de la eficacia de las defensas para seis meses y doce meses después de haberse implantado los cambios y de que la AAC haya otorgado la autorización correspondiente.

5.2 Teniendo en cuenta las nuevas defensas introducidas para esta operación especial, los riesgos de seguridad operacional de un CFIT debido a la pérdida de un motor crítico durante el despegue después de  $V_1$  se evalúa ahora como improbable (2 — muy probablemente no ocurra) aunque la gravedad de un CFIT sigue siendo catastrófica (A — equipo destruido — múltiples muertes).

5.3 La operación cae ahora en la región tolerable y el índice de riesgo resultante es 2A (aceptable basada en la mitigación de los riesgos). Puede exigir una decisión de la administración (véase el Capítulo 5, Figura 5-8). Los datos de seguridad operacional y documentación resultante de los procesos de identificación de peligros y de gestión de los riesgos se incorporan en la “biblioteca de seguridad operacional” de la compañía.

## **6. RESPONSABILIDADES INDIVIDUALES PARA IMPLANTAR LAS MEDIDAS DE MITIGACIÓN**

Las responsabilidades individuales para implantar las medidas de mitigación propuestas son las siguientes:

- a) Medidas de mitigación a), f) e i) — director de operaciones de vuelo;
- b) Medidas de mitigación b), c) y d) —director de instrucción de vuelo;
- c) Medida de mitigación e) —director de despacho;
- d) Medidas de mitigación g) y h) — director de mantenimiento.

## **7. REGISTRO DE IDENTIFICACIÓN DE PELIGROS Y GESTIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL**

7.1 El registro de identificación de peligros y de gestión de los riesgos de seguridad operacional que figura en la Tabla 5-Ap 3-1 se utiliza para dejar constancia de los riesgos de seguridad operacional identificados y de las medidas adoptadas por las personas designadas. El registro debería conservarse permanentemente en la “biblioteca de seguridad operacional” para proporcionar evidencia de la gestión de los riesgos de seguridad operacional así como una referencia para futuras evaluaciones de los riesgos.

7.2 Habiendo identificado y calificado los riesgos de seguridad operacional, deberían identificarse las defensas existentes contra los mismos. Estas defensas deben evaluarse posteriormente en cuanto a su adecuación. Si se encuentra que son menos que adecuadas, entonces deberán prescribirse medidas adicionales. Todas las medidas debe dirigirlas un individuo específico (normalmente el gerente de línea responsable), y debe establecerse un plazo para completarlas. El registro de identificación de peligros y gestión de los riesgos de seguridad operacional no se autorizará hasta que estas medidas se hayan completado.

**Tabla 5-AP 3-1. Identificación de peligros y gestión de los riesgos**

Tipo de operación o actividad	Peligro genérico	Componentes específicos del peligro	Consecuencias relacionadas con el peligro	Defensas existentes para controlar los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional	Otras medidas para reducir los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional resultante	Persona responsable
Operaciones de vuelo	Operación en un aeropuerto muy elevado rodeado de geografía compleja	<ul style="list-style-type: none"> <li>a) Montañas circundantes.</li> <li>b) Aeródromo muy elevado.</li> <li>c) Ausencia de ayudas para la navegación en aproximación y aterrizaje.</li> <li>d) Ausencia de ayudas visuales de aterrizaje.</li> <li>e) Tránsito conflictivo.</li> <li>f) Pista resbaladiza cuando húmeda.</li> <li>g) Fauna silvestre.</li> </ul>	<ul style="list-style-type: none"> <li>a) Impacto contra el suelo sin pérdida de control (CFIT) debido a:               <ul style="list-style-type: none"> <li>1) pérdida de motor crítico durante aproximación y aterrizaje;</li> <li>2) pérdida de motor crítico durante despegue después de <math>V_1</math>;</li> <li>3) pérdida de motor crítico durante ascenso en ruta.</li> </ul> </li> <li>b) Colisión en vuelo.</li> <li>c) Rebase de pista después de aterrizaje.</li> <li>d) Rebase de pista en aterrizaje después de despegue interrumpido.</li> <li>e) Choques con aves.</li> </ul> <p><i>Nota.— El impacto contra el suelo sin pérdida de control debido a pérdida de un motor crítico durante el despegue después de <math>V_1</math> es la única consecuencia que se analiza en este ejercicio. En una evaluación real, todas las consecuencias deben analizarse y todos los riesgos de seguridad operacional evaluarse y mitigarse.</i></p>	<ul style="list-style-type: none"> <li>a) Operación de aeronaves en VMC y condiciones diurnas.</li> <li>b) Plano de aeródromo disponible en la AIP nacional.</li> <li>c) Procedimientos ATC aplicados en el aeródromo.</li> <li>d) Manual de operaciones de la compañía.</li> <li>e) Manual de actuación de despacho.</li> <li>f) Manual de operación de la aeronave.</li> <li>g) Instrucción periódica sobre fallas de motor antes y después de <math>V_1</math> y procedimientos de aproximación frustrada.</li> <li>h) Instrucción en CRM.</li> </ul> <p>Índice de riesgo de seguridad operacional: 3A Tolerabilidad de los riesgos de seguridad operacional: inaceptable en las circunstancias actuales.</p>	<ul style="list-style-type: none"> <li>a) Elaborar procedimientos de despegue y ascenso en caso de pérdida de un motor crítico después de <math>V_1</math>, considerando la posibilidad de un regreso a tierra.</li> <li>b) Elaborar y brindar instrucción en los procedimientos mencionados (simulador de vuelo completo y mantener calificación cada seis meses).</li> <li>c) Considerar que el Aeropuerto internacional de Ciudad Andes es una "operación de aeródromo especial" que requiere calificación especial de la tripulación, válida por solo un año a menos que se renueve.</li> <li>d) Proporcionar instrucción apropiada en "operación de aeródromo especial" a las tripulaciones de cabina. (Esta mitigación no trata la probabilidad sino la gravedad — evacuación de emergencia — de los riesgos de seguridad operacional).</li> <li>e) Proporcionar información meteorológica precisa, en particular vientos en la superficie después de las 16:00 horas.</li> <li>f) Elaborar documentación operacional e incluirla en el manual de operaciones de la compañía y en el manual de despacho, para aprobación por la AAC.</li> <li>g) Prohibir una política abierta de artículos críticos en la lista de equipo mínimo (MEL).</li> </ul>	<ul style="list-style-type: none"> <li>Director de operaciones</li> <li>Director de instrucción</li> <li>Director de instrucción</li> <li>Director de instrucción</li> <li>Director de despacho</li> <li>Director de operaciones</li> <li>Director de mantenimiento</li> </ul>

Tipo de operación o actividad	Peligro genérico	Componentes específicos del peligro	Consecuencias relacionadas con el peligro	Defensas existentes para controlar los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional	Otras medidas para reducir los riesgos de seguridad operacional e índice de los riesgos de seguridad operacional resultante	Persona responsable
					<p>h) En el marco del programa de fiabilidad de mantenimiento, el departamento de mantenimiento debe examinar los motores de las aeronaves asignadas a la operación.</p> <p>i) Realizar seguimientos de las medidas de seguridad operacional e implantación de nuevas defensas para el control y mitigación de los riesgos de seguridad operacional relacionados con la operación en el Aeropuerto internacional de Ciudad Andes. Se prevé un examen de la eficacia de las defensas para seis meses y seis meses después de haberse implantado los cambios y de que la AAC haya otorgado la autorización correspondiente.</p> <p>Índice de riesgo de seguridad operacional: 2A                      Tolerabilidad de los riesgos de seguridad operacional: aceptable basada en la mitigación de los riesgos. Podría exigir decisión de la administración.</p>	<p>Director de mantenimiento</p> <p>Director de operaciones</p>



## Capítulo 6

# REQUISITOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL DE LA OACI

### 6.1 OBJETIVO Y CONTENIDO

En este capítulo se presentan los SARPS de la OACI sobre gestión de la seguridad operacional que figuran en el Anexo 1 — *Licencias al personal*, Anexo 6 — *Operación de aeronaves*, Anexo 8 — *Aeronavegabilidad*, Anexo 11 — *Servicios de tránsito aéreo*, Anexo 13 — *Investigación de accidentes e incidentes de aviación* y Anexo 14 — *Aeródromos*. También se presentan la relación entre el programa estatal de seguridad operacional (SSP) y el sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios. Este capítulo comprende los temas siguientes:

- a) SARPS de la OACI sobre gestión de la seguridad operacional — Generalidades;
- b) Programa estatal de seguridad operacional (SSP);
- c) Nivel aceptable de seguridad operacional (ALoS);
- d) Sistema de gestión de la seguridad operacional (SMS);
- e) Eficacia de la seguridad operacional del SMS;
- f) Responsabilidad y rendición de cuentas de la administración;
- g) Relación entre un SSP y un SMS; y
- h) Cumplimiento y eficacia.

### 6.2 SARPS DE LA OACI SOBRE GESTIÓN DE LA SEGURIDAD OPERACIONAL — GENERALIDADES

6.2.1 Los SARPS de la OACI sobre gestión de la seguridad operacional figuran en los Anexos 1; 6, Partes I y III; 8; 11; 13 y 14. Estos Anexos tratan de las actividades de las organizaciones de instrucción reconocidas, los explotadores de aeronaves internacionales, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados. En el caso del Anexo 1, los SARPS sobre gestión de la seguridad operacional se limitan exclusivamente a las organizaciones de instrucción reconocidas que están expuestas a los riesgos de seguridad operacional durante la prestación de sus servicios.

6.2.2 Los SARPS sobre gestión de seguridad operacional se dirigen a dos grupos específicos: los Estados y los proveedores de servicios. En el contexto de este manual, el término “proveedor de servicios” se refiere a toda organización que proporciona un servicio de aviación. El término incluye las organizaciones de instrucción reconocidas que están expuestas a los riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados, según corresponda.

6.2.3 Los SARPS de la OACI sobre gestión de la seguridad operacional se refieren a tres tipos de requisitos bien definidos:

- a) requisitos relativos al programa estatal de seguridad operacional (SSP), incluyendo el nivel aceptable de seguridad operacional (ALoS) de un SSP;
- b) requisitos relativos a los sistemas de gestión de la seguridad operacional (SMS), incluyendo la eficacia de la seguridad operacional de un SMS; y
- c) requisitos relativos a la responsabilidad y rendición de cuentas de la administración con respecto a la gestión de la seguridad operacional durante el suministro de servicios.

6.2.4 Los SARPS de la OACI sobre gestión de la seguridad operacional introducen la noción de nivel aceptable de seguridad operacional (ALoS) como forma de expresar el grado mínimo de seguridad operacional que ha sido establecido por el Estado y debe ser asegurado por un SSP, y la noción de eficacia de seguridad operacional como forma de medir la eficacia de la seguridad operacional de un proveedor de servicios y su SMS.

### **6.3 PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)**

6.3.1 En los Anexos 1, 6, 8, 11, 13 y 14 se incluye el requisito de que los Estados establezcan un programa estatal de seguridad operacional (SSP), para lograr un nivel aceptable de seguridad operacional en la aviación civil. Un SSP es un sistema de gestión para la gestión de la seguridad operacional por el Estado.

6.3.2 Un SSP se define como un conjunto integrado de reglamentación y actividades destinadas a mejorar la seguridad operacional. Comprende actividades específicas de seguridad operacional que debe realizar el Estado y reglamentos y directrices promulgados por el Estado para apoyar el cumplimiento de sus responsabilidades con respecto a la realización segura y eficiente de las actividades de aviación en el Estado.

6.3.3 Para ayudar a los Estados a establecer su SSP, la OACI ha elaborado un marco que comprende los componentes y los elementos de un SSP. El marco consta de cuatro componentes y once elementos y se presenta en su totalidad en el Capítulo 11. Las responsabilidades abarcadas por el SSP no son nuevas. Se supone razonablemente que la mayoría de los Estados ya están cumpliendo la mayoría de estas responsabilidades. Lo nuevo es la noción de SSP en sí misma, proponiendo una forma de organizar las responsabilidades y rendición de cuentas en materia de seguridad operacional de un Estado en una forma estructurada y con arreglo a principios, y midiendo la eficacia con la cual se cumplen dichas responsabilidades de seguridad operacional y se lleva a cabo la rendición de cuentas de seguridad operacional en el Estado. La organización de las responsabilidades y la rendición de cuentas en materia de seguridad operacional en un Estado que observe ciertos principios y adopte una estructura normalizada permiten que los reglamentos y actividades dirigidos a mejorar la seguridad operacional sean documentados, explícitos e identificables. Si bien el objetivo estratégico a largo plazo de un SSP es el mejoramiento de la seguridad operacional en el Estado, la organización de un SSP apunta a dos objetivos tácticos a corto plazo: el cumplimiento eficiente y efectivo de las responsabilidades y rendición de cuentas en materia de seguridad operacional por parte del Estado, y la auditoría eficiente de dichas responsabilidades y rendición de cuentas por el Estado.

6.3.4 La importancia del segundo objetivo, la auditoría eficiente de las responsabilidades y rendición de cuentas en materia de seguridad operacional por el Estado, no debería subestimarse. Actualmente, el Programa universal OACI de auditoría de la vigilancia de la seguridad operacional (USOAP) realiza auditorías de las responsabilidades de seguridad operacional de los Estados en forma completa, aunque aplica una arquitectura básica propuesta por los Anexos al Convenio sobre Aviación Civil Internacional. Los elementos críticos que debe vigilar la función de vigilancia de la seguridad operacional del Estado han sido definidos, y las auditorías del USOAP verifican el Estado de aplicación de elementos y funciones, con un criterio de cumplimiento/incumplimiento. Se prevé que una vez que la noción de SSP



haya alcanzado la madurez y se aplique en los Estados, el USOAP auditará el SSP en forma integral en vez de los elementos de la función de vigilancia de la seguridad operacional, mediante un enfoque basado en el concepto de supervisión continua.

6.3.5 La noción de SSP también se dirige a un tercer objetivo, que es a mediano plazo: la transición desde un entorno normativo predominantemente prescriptivo a un entorno normativo integrado que combina enfoques normativos prescriptivos y basados en la eficacia. En esta transición, la noción de ALoS de un SSP y la de eficacia de seguridad operacional de un SMS, basándose en el componente de garantía de la seguridad operacional del SSP y del SSM, que se analizarán posteriormente en este capítulo, resultan fundamentales. No obstante, esta transición debe comenzar estableciendo con claridad el papel de la función de vigilancia de la seguridad operacional del Estado dentro del SSP y sus relaciones mutuas. A continuación se presenta un breve análisis.

6.3.6 La función de vigilancia de la seguridad operacional del Estado es parte del SSP y componente fundamental de su componente de garantía de la seguridad operacional. Los objetivos de la función de vigilancia de la seguridad operacional del Estado, como se la practica tradicionalmente, se satisfacen mediante controles administrativos (inspecciones, auditorías y encuestas) llevados a cabo regularmente por las autoridades de aviación civil, y no constituyen necesariamente controles de los riesgos de seguridad operacional, según lo analizado en el Capítulo 5 y en la Sección 6.8. El SSP es necesario para transformar los resultados de la vigilancia de la seguridad operacional en controles de los riesgos de seguridad operacional. Por ejemplo, la función de vigilancia de la seguridad operacional de un Estado verifica actualmente que el Estado cuenta con un sistema de reglamentos, pero no requiere un análisis de los riesgos de seguridad operacional para producir tales reglamentos, ni verifica la eficacia de los reglamentos como controles de los riesgos de seguridad operacional. Por otra parte, el SSP considera los reglamentos como controles de los riesgos de seguridad operacional y requiere, mediante su componente de gestión de los riesgos de seguridad operacional, que el proceso de establecimiento de las reglas aplique principios de gestión de los riesgos de seguridad operacional (identificar peligros, evaluar los riesgos de seguridad de las consecuencias de los peligros, y elaborar reglamentos que proporcionen una mitigación o un control aceptables de las consecuencias de los peligros). En una segunda etapa, el SSP verifica, mediante su componente de garantía de la seguridad operacional, la eficacia y la eficiencia de los reglamentos en cuanto a controles de los riesgos de seguridad operacional.

6.3.7 La clara articulación de la diferencia entre reglamentos como controles administrativos y reglamentos como controles de los riesgos de seguridad operacional constituye el fundamento del cambio desde una reglamentación prescriptiva a una reglamentación basada en la eficacia. El SSP, según se propone en el marco que se analizará en el Capítulo 11, es un primer paso que permite dicho cambio. Además, la integración en el SSP, según corresponda, de los principios en que se basa la actuación de los elementos críticos de una función de vigilancia de la seguridad operacional del Estado producirá un SSP más robusto y efectivo.

## **6.4 NIVEL ACEPTABLE DE SEGURIDAD OPERACIONAL (ALoS)**

6.4.1 Los Anexos 1, 6, 8, 11, 13 y 14 requieren que el nivel aceptable de seguridad operacional (ALoS) que ha de alcanzarse (con un SSP) sea establecido por el Estado.

6.4.2 La noción de ALoS es un ingrediente esencial para el funcionamiento efectivo de un SSP. A menos que la noción de ALoS sea comprendida y adecuadamente desarrollada e implantada, será difícil avanzar hacia un entorno normativo basado en la eficacia y verificar la eficacia real de un SSP. Entonces el funcionamiento de un SSP puede reducirse al simple proceso de “marcar la casilla adecuada” en una falsa impresión de estar gestionando la seguridad operacional.

6.4.3 El axioma básico de la gestión, de que “no se puede gestionar lo que no se puede medir”, se analiza en otras partes de este manual. En todo sistema, es necesario definir un conjunto de resultados de eficacia medibles para poder determinar si el sistema funciona verdaderamente con arreglo a las previsiones del diseño, y que no está simplemente satisfaciendo requisitos normativos. La definición de un conjunto de resultados de eficacia medibles

también permite identificar dónde pueden necesitarse medidas para llevar la eficacia operacional del sistema al nivel de las previsiones de diseño. Así pues, los resultados de eficacia medibles permiten evaluar la eficacia real de las actividades críticas para la seguridad operacional con respecto a los controles de organización existentes, de modo que los riesgos para la seguridad operacional puedan mantenerse en un nivel ALARP y adoptarse las medidas correctivas necesarias. Esta noción se aplica tanto al SSP como al SMS, aunque con ciertas consideraciones relativas a las especificidades de cada uno, que se destacan en esta sección y en la Sección 6.6.

6.4.4 La introducción de la noción de ALoS también responde a la necesidad de complementar el enfoque tradicional de la gestión de la seguridad operacional basada en el cumplimiento de los reglamentos, con un enfoque basado en la eficacia. Un enfoque basado en la eficacia evaluará la eficacia real de las actividades críticas para la seguridad operacional con respecto a los controles de organización existentes. Sólo mediante la garantía de eficaz implantación del SSP puede alcanzarse el objetivo de mejoramiento continuo de la seguridad operacional en que se basa la gestión de esta seguridad.

6.4.5 La elaboración e implantación de ALoS se basa en ciertos conceptos fundamentales de la teoría de sistemas. A continuación se presenta un breve análisis.

6.4.6 Existe una jerarquía inherente a los conceptos básicos de la teoría de sistemas subyacentes en el ALoS y la forma en que estos conceptos deben ordenarse en progresión cuando se elabore el ALoS. La comprensión de los conceptos y su jerarquía inherente es un fundamento esencial para la elaboración de un ALoS respecto de un SSP. Los conceptos involucrados, y sus jerarquías correspondientes, son los siguientes:

- a) la **seguridad operacional** (según se define en el Capítulo 2);
- b) el **nivel de seguridad operacional** es el grado de seguridad operacional de un sistema. Es una propiedad emergente en el sistema, que representa la calidad del mismo con respecto a la seguridad operacional. Se expresa mediante indicadores de seguridad operacional;
- c) los **indicadores de seguridad operacional** son los parámetros que caracterizan o tipifican el nivel de seguridad operacional de un sistema;
- d) los **objetivos de seguridad operacional** son los objetivos concretos del nivel de seguridad operacional;
- e) el **nivel aceptable de seguridad operacional** es el grado mínimo de seguridad operacional que debe ser garantizado por un sistema en la práctica real;
- f) el **valor del indicador de seguridad operacional** es la cuantificación de un indicador de seguridad operacional; y
- g) el **valor del objetivo de seguridad operacional** es la cuantificación de un objetivo de seguridad operacional.

6.4.7 La selección de indicadores de seguridad operacional apropiados es fundamental para el desarrollo de un ALoS. Dicha selección debería ser función del detalle con el cual se prevea representar el nivel de seguridad operacional del sistema. Si el nivel de seguridad operacional se representa en términos amplios y genéricos, la selección de indicadores de seguridad operacional que representen resultados del sistema de alto nivel/grandes consecuencias (cuantitativos) o funciones del sistema de alto nivel (cualitativo) resulta apropiada. Si el nivel de seguridad operacional del sistema se representa en términos específicos y más estrechos, entonces se requiere la selección de indicadores que representen resultados del sistema de bajo nivel o pocas consecuencias y funciones del sistema de menor nivel. En ambos casos, los indicadores de seguridad operacional significativos deben ser representativos de los resultados, procesos y funciones que caracterizan la seguridad operacional del sistema.

6.4.8 Los ejemplos típicos de indicadores de seguridad operacional en el sistema de aviación comprenden, entre otros:

- a) accidentes de línea aérea mortales;
- b) incidentes graves;
- c) sucesos de excursión de la pista;
- d) sucesos de colisión en tierra;
- e) desarrollo/ausencia de legislación aeronáutica básica;
- f) desarrollo/ausencia de reglamentos de operación; y
- g) nivel de cumplimiento de los reglamentos.

6.4.9 Los ejemplos típicos de objetivos de seguridad operacional en el sistema de aviación comprenden, entre otros:

- a) reducción de los accidentes de línea aérea mortales;
- b) reducción de los incidentes graves;
- c) reducción de los sucesos de excursión de la pista;
- d) reducción de los sucesos de colisión en tierra; y
- e) el número de inspecciones que se completan trimestralmente.

6.4.10 La primera etapa en elaboración de un ALoS relativo a un SSP es, por consiguiente, decidir con respecto al detalle con el cual se pretende representar el nivel de seguridad operacional del sistema de aviación de un Estado en particular, y luego seleccionar indicadores de seguridad operacional significativos que caractericen o tipifiquen el nivel de seguridad operacional del sistema aeronáutico del Estado. La disponibilidad de datos de seguridad operacional para el Estado es un factor determinante en la decisión con respecto al detalle de la representación, así como en la selección de indicadores de seguridad operacional cuantitativos o cualitativos. Los Estados que han desarrollado capacidades de recolección y análisis de datos de seguridad operacional estarían en condiciones de representar el nivel de seguridad operacional con mayor detalle que los Estados que no lo han hecho. Los Estados del primer grupo deberían poder definir indicadores de seguridad operacional cuantitativos, mientras que los Estados del segundo grupo pueden optar por aplicar inicialmente indicadores de seguridad operacional cualitativos mientras desarrollan sus capacidades de recolección y análisis de datos de seguridad operacional. Una vez definidos los indicadores de seguridad operacional, la etapa siguiente es definir los objetivos de seguridad operacional conexos, que pueden considerarse como objetivos del mejoramiento.

6.4.11 Una vez seleccionados los indicadores y los objetivos de seguridad operacional, puede establecerse el nivel de seguridad operacional que representa el sistema aeronáutico del Estado en particular. En ese punto, el Estado debería estar en condiciones de avanzar en la elaboración del ALoS, el grado *mínimo* de seguridad operacional en la aviación civil que debe garantizarse con el SSP en la práctica real. Para elaborar el ALoS, deben asignarse valores a los indicadores de seguridad operacional, y los objetivos de mejoramiento o mantenimiento de tales valores deben asignarse a los objetivos de seguridad operacional. Si bien se acepta en general que el ALoS relativo a un SSP se exprese mediante valores de los indicadores de seguridad operacional y valores de los objetivos de seguridad operacional, en términos estrictos son los valores de los objetivos de seguridad operacional los que representan la

verdadera expresión de un ALoS. En la Figura 6-1 se incluye un ejemplo de valores de indicadores de seguridad operacional y valores de objetivos de seguridad operacional. Al establecer un ALoS debe también considerarse lo siguiente:

- a) el nivel de riesgo de seguridad operacional que se aplica;
- b) la tolerancia a los riesgos de seguridad operacional;
- c) los costos/beneficios de las mejoras al sistema de aviación; y
- d) las expectativas del público con respecto al sistema de aviación civil.

6.4.12 Para elaborar adecuadamente el ALoS con respecto a un SSP, también es fundamental comprender la diferencia entre dos conceptos estrechamente interrelacionados — y que por consiguiente a veces causan confusión — aunque bien distintos: la medición de la seguridad operacional y la medición de la eficacia de la seguridad operacional.

Valor del indicador de seguridad operacional	Valor del objetivo de seguridad operacional
1. <i>[Proporción/número]</i> accidentes mortales de línea aérea por <i>[número]</i> operaciones	→ 1. Reducir en <i>[número]</i> el número de/ Máximo de <i>[número]</i> accidentes mortales de línea aérea por <i>[número]</i> operaciones
2. <i>[Proporción/número]</i> sucesos de excursión de la pista por <i>[número]</i> operaciones	→ 2. Reducir en <i>[número]</i> el número de/ Máximo de <i>[número]</i> sucesos de excursión de la pista por <i>[número]</i> operaciones
3. <i>[Proporción/número]</i> sucesos de colisión en tierra por <i>[número]</i> operaciones	→ 3. Reducir en <i>[número]</i> el número de/ Máximo de <i>[número]</i> sucesos de colisión en tierra por <i>[número]</i> operaciones
4. <i>[Número]</i> inspecciones de explotadores completadas en <i>[lapso de tiempo]</i>	→ 4. Mínimo de <i>[número]</i> inspecciones de explotadores completadas en <i>[lapso de tiempo]</i>

**Figura 6-1. Ejemplo de valores de indicadores de seguridad operacional y valores de objetivos de seguridad operacional**

6.4.13 La **medición de la seguridad operacional** se refiere a la cuantificación de los resultados de sucesos seleccionados de alto nivel y consecuencias graves, como las proporciones de accidentes e incidentes graves. La medición de la seguridad operacional también puede aplicarse para reflejar la cuantificación de funciones estatales seleccionadas de alto nivel, como la condición de desarrollo/implantación de legislación de seguridad operacional aeronáutica básica o la ausencia de la misma, la situación de la elaboración/implantación de reglamentos de operación específicos o la ausencia de los mismos y el nivel de cumplimiento de los reglamentos dentro del Estado. La medición de la seguridad operacional no es un proceso continuo sino más bien una verificación puntual, normalmente realizada con arreglo a calendarios preespecificados, por ejemplo, anualmente, semestralmente o trimestralmente. La medición de la seguridad operacional se relaciona con el SSP y refleja la medida en la cual se han logrado los objetivos de seguridad operacional de alto nivel de las intervenciones de seguridad operacional o de las estrategias de mitigación.

6.4.14 La **medición de la eficacia de la seguridad operacional** se refiere a la cuantificación de los resultados de procesos seleccionados de bajo nivel y pocas consecuencias, como el número de desechos u objetos extraños (FOD) por número específico de operaciones en rampa, o el número de sucesos de vehículos terrestres no autorizados en las calles de rodaje por número específico de operaciones de aeropuerto o durante un período de tiempo especificado. La medición de la eficacia de la seguridad operacional es una actividad permanente, que involucra supervisión y medición continuas, por una organización, de determinadas actividades operacionales que son necesarias para prestar los servicios para los cuales se creó la organización (suministro de servicios de aeródromo, control de tránsito aéreo, instrucción, etc.). La medición de la eficacia de la seguridad operacional está relacionada principal pero no exclusivamente, con un SMS y proporciona una medida de la eficacia operacional real de un sistema de gestión como un SSP, un SMS, más allá de las medidas absolutas obtenidas con una medición de seguridad operacional (incluyendo el cumplimiento de las normas). También se aplica a las intervenciones de seguridad operacional y a las estrategias de mitigación establecidas como parte de un SSP, según corresponda.

6.4.15 El ALoS relacionado con un SSP debe elaborarse sobre la base de una sensata combinación de medición de la seguridad operacional y medición de la eficacia de la seguridad operacional. La medida en la cual el ALoS representa la medición de la seguridad operacional o la medición de la eficacia de la seguridad operacional depende del grado de maduración del SSP. Inicialmente, inmediatamente después de la elaboración e implantación de un SSP, los valores de indicadores de seguridad operacional y los valores de objetivos de seguridad operacional relacionados con el ALoS se expresarán probablemente mediante declaraciones de medidas cuantitativas sobre resultados seleccionados de alto nivel/consecuencias graves (medición de la seguridad operacional). En la Figura 6-2 se muestra un ejemplo de valores de indicadores de seguridad operacional y valores de objetivos de seguridad operacional basados en mediciones de la seguridad operacional.

6.4.16 A medida que el SSP madura y que se desarrollan capacidades de recolección y análisis de datos de seguridad operacional mediante el componente de garantía de la seguridad operacional del SSP, los valores de indicadores de seguridad operacional y de objetivos de seguridad operacional relacionados con el ALoS pueden modificarse y expresarse mediante una combinación de declaraciones de medidas cuantitativas sobre sucesos seleccionados de alto nivel/consecuencias graves (medición de la seguridad operacional) y declaraciones de medidas cuantitativas con respecto a resultados seleccionados de bajo nivel/consecuencias leves (medición de la eficacia de la seguridad operacional). Cuando el SSP alcanza la madurez, los valores de indicadores de seguridad operacional y de objetivos de seguridad operacional relacionados con el ALoS se expresarán mediante declaraciones de medidas cuantitativas sobre resultados seleccionados de bajo nivel/consecuencias leves (medición de la eficacia de la seguridad operacional). En la Figura 6-3 se muestra un ejemplo de valores de indicadores de seguridad operacional y de valores de objetivos de seguridad operacional basados en la medición de la eficacia de la seguridad operacional.

Valor del indicador de seguridad operacional	Valor del objetivo de seguridad operacional
1. [Número] accidentes CFIT en aproximación y aterrizaje por [número] salidas	1. Reducir en [número] el número de/Máximo de [número] accidentes CFIT en aproximación y aterrizaje por [número] operaciones
2. [Número] excursiones de pista por [número] operaciones	2. Reducir en [número] el número de/Máximo de [número] excursiones de pista por [número] operaciones
3. [Número] accidentes de colisión en tierra por año en un promedio de recorridos de [x-años]	3. Reducir en [número] el número de/Máximo de [número] accidentes de colisión en tierra por año en un promedio de recorrido de [x-años]
4. [Número] sucesos de mucha gravedad captados anualmente mediante el MOR del Estado	4. Mínimo de [número] sucesos de mucha gravedad captados anualmente mediante el MOR del Estado
5. [Número] inspecciones de explotadores completadas por trimestre	5. Mínimo de [número] inspecciones de explotadores completadas por trimestre
6. [Número] instalaciones AIS con QMS implantado	6. [Número] instalaciones AIS con QMS implantado para [fecha]
7. Presentación electrónica de diferencias completada dentro de [número] meses/semanas	7. Presentación electrónica de diferencias completada dentro de [número revisado] meses/semanas

**Figura 6-2. Ejemplo de valores de indicadores de seguridad operacional y valores de objetivos de seguridad operacional basados en mediciones de la seguridad operacional**

Valor del indicador de seguridad operacional	Valor del objetivo de seguridad operacional
1. [Número] desviaciones de la altitud por [número] operaciones	1. Reducir en [número] el número de/Máximo de [número] desviaciones de la altitud por [número] operaciones para [fecha]
2. [Número] incursiones en pistas de Cat B y C en 5 aeropuertos internacionales de [Estado] por [número] operaciones	2. Reducir en [número] el número de/Máximo de [número] incursiones en las pistas de Cat B y C en 5 aeropuertos internacionales de [Estado] para [fecha]
3. [Número] sucesos TCAS/airprox por [número] operaciones	3. Reducir en [número] el número de/Máximo de [número] sucesos TCAS/airprox por [número] operaciones para [fecha]
4. [Número] aproximaciones no conformes (NCA) en 5 aeropuertos internacionales de [Estado] por [número] operaciones	4. Reducir en [número] el número de/Máximo de [número] aproximaciones no conformes (NCA) en 5 aeropuertos internacionales de [Estado] para [fecha]
5. [Número] sucesos FOD en plataforma en 5 aeropuertos internacionales de [Estado] por [número] operaciones	5. Reducir en [número] el número de/Máximo de [número] sucesos FOD en plataforma en 5 aeropuertos internacionales de [Estado] para [fecha]

**Figura 6-3. Ejemplo de valores de indicadores de seguridad operacional y valores de objetivos de seguridad operacional basados en mediciones de la eficacia de seguridad operacional**

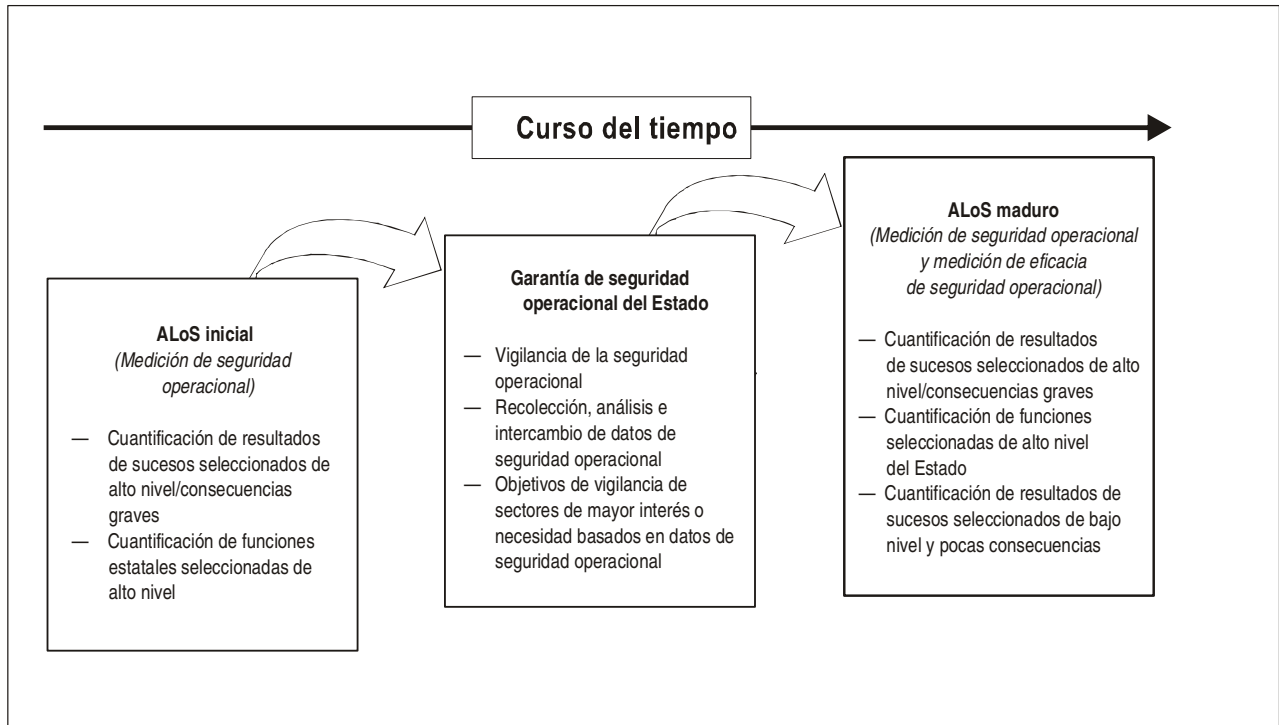
6.4.17 Dos aspectos genéricos deben considerarse cuando se evalúe si los valores específicos de objetivos de seguridad operacional del ALoS deberían representar mejoras con respecto a los valores de indicadores de seguridad operacional conexos o más bien el mantenimiento de los mismos. En primer lugar, debe considerarse la disponibilidad de recursos dentro del Estado para lograr la mejora considerada. En segundo lugar, debe considerarse cuán onerosos son los planes de acción que se estiman necesarios para lograr la mejora. Una tercera consideración, aplicable solamente a los valores de objetivos de seguridad operacional basados en mediciones de la eficacia de la seguridad operacional, es establecer si la evaluación de los riesgos de seguridad operacional de las consecuencias de los peligros que se tratan mediante la mejora se ubica en la región tolerable del proceso de gestión de los riesgos de la seguridad operacional analizado en el Capítulo 5. El valor del objetivo de seguridad operacional puede en determinado momento reflejar una evaluación de los riesgos de seguridad operacional que cae en la región tolerable en las circunstancias prevalecientes. No obstante, cambios en el sistema, crecimiento, etc., pueden quitarle validez a dicha evaluación de los riesgos de seguridad operacional. El valor del objetivo de seguridad operacional, en este caso, debe reflejar una mejora con respecto a su valor de indicador de seguridad operacional conexo para que resulte válido en el entorno modificado.

6.4.18 El ALoS se obtiene mediante planes de acción. Estos son las herramientas y medios necesarios para lograr los valores de objetivos de seguridad operacional del ALoS relacionado con un SSP. Los planes de acción comprenden los procedimientos operacionales, tecnología, sistemas y programas respecto de los cuales pueden especificarse mediciones de fiabilidad, disponibilidad, eficacia y/o exactitud. Un ejemplo de plan de acción para un objetivo de seguridad operacional relacionado con la reducción de los accidentes de impacto contra el suelo sin pérdida de control (CFIT) sería la implantación de procedimientos de llegada en descenso constante, y cartas de procedimientos de llegada designados para aproximaciones estabilizadas. Un ejemplo de plan de acción para un objetivo de seguridad operacional relacionado con la reducción de sucesos de incursiones en las pistas sería la instalación de un sistema radar con una disponibilidad de equipo crítico prevista del 98%.

6.4.19 Debe afirmarse enfáticamente que la noción de ALoS se refiere a objetivos nacionales o a nivel estatal, que han de lograrse mediante el SSP, como medio para verificar la implantación satisfactoria del SSP. Por consiguiente, siempre debe hacerse referencia al nivel aceptable de seguridad operacional relacionado con un SSP. Los valores de indicadores de seguridad operacional y de objetivos de seguridad operacional de un ALoS proporcionan una forma medible de asegurar y demostrar la eficacia de un SSP, más allá del cumplimiento de los reglamentos. Un SSP debería cumplir todos los requisitos normativos establecidos por los reglamentos internacionales y nacionales. El cumplimiento de los reglamentos todavía sigue siendo la base de la gestión de la seguridad operacional. Seleccionando una combinación de resultados de eficacia operacional medibles, que son específicos a cada Estado y que se basan en los fundamentos proporcionados por el cumplimiento de los reglamentos, puede asegurarse la eficacia y la eficiencia reales de los procesos de gestión de la seguridad operacional en que se basa un SSP.

6.4.20 La implantación de un ALoS va mucho más allá del cumplimiento normativo de los requisitos nacionales e internacionales. El establecimiento de un ALoS para un SSP no sustituye los requisitos jurídicos, normativos o de otro tipo establecidos, ni releva a los Estados de sus obligaciones con respecto al *Convenio sobre Aviación Civil Internacional* (Doc 7300 de la OACI) y sus disposiciones conexas contenidas en los Anexos al Convenio.

6.4.21 Como conclusión del análisis sobre ALoS, en las Figuras 6-4, 6-5 y 6-6 se resumen, en forma gráfica, la transición desde la etapa inicial a la madurez de un ALoS relacionado con un SSP, un ALoS que refleja la medición de la seguridad operacional y un ALoS que refleja la medición de la eficacia de seguridad operacional del SMS conexo, según se analizó en esta sección.



**Figura 6-4. Transición desde la etapa inicial a la maduración de un ALoS relacionado con un SSP**

Valores de objetivos de seguridad operacional	<ol style="list-style-type: none"> <li>1. Reducir en [número] el número de/Máximo de [número] accidentes CFIT en aproximación y aterrizaje por [número] salidas.</li> <li>2. Mínimo de [número] inspecciones de explotadores completadas cada trimestre.</li> <li>3. ...</li> </ol>
Planes de acción	<ol style="list-style-type: none"> <li>1. Paquete de instrucción CFIT distribuido a la industria y apoyado por cursos de instrucción.</li> <li>2. Revisión y, si es necesario, actualización de la política de contratación. Actualización del manual de inspección.</li> <li>3. ...</li> </ol>
Valores de indicador de la seguridad operacional	<ol style="list-style-type: none"> <li>1. [Número] accidentes CFIT y de aproximación y aterrizaje por [número] de salidas.</li> <li>2. [Número] inspecciones de explotadores completadas cada trimestre.</li> <li>3. ...</li> </ol>
Estado	Cumplirá todas las normas internacionales aplicables.

**Figura 6-5. ALoS que refleja la medición de la seguridad operacional**



Valores de objetivos de seguridad operacional	<ol style="list-style-type: none"> <li>1. Reducir en [número] el número de/Máximo de [número] aproximaciones no conformes (NCA) en 5 aeropuertos internacionales por [número] llegadas para [fecha].</li> <li>2. Reducir en [número] el número de/Máximo de [número] incursiones en las pistas de Cat B y C en 5 aeropuertos internacionales de [Estado] por [número] operaciones para [fecha].</li> <li>3. ...</li> </ol>
Planes de acción	<ol style="list-style-type: none"> <li>1. Implantación de procedimientos de llegada en descenso constante (CDA). Cartas de procedimientos de llegada diseñadas para aproximaciones estabilizadas.</li> <li>2. Instalación de ASDE/X en 5 aeropuertos internacionales de [Estado].</li> <li>3. ...</li> </ol>
Valores de indicador de la seguridad operacional	<ol style="list-style-type: none"> <li>1. [Número] aproximaciones no conformes (NCA) en 5 aeropuertos internacionales por [número] operaciones.</li> <li>2. [Número] incursiones en pistas de Cat B y C en 5 aeropuertos internacionales de [Estado] por [número] operaciones.</li> <li>3. ...</li> </ol>
Estado	Cumplirá todas las normas internacionales aplicables.

**Figura 6-6. ALoS que refleja la medición de la eficacia de la seguridad operacional**

## 6.5 SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

6.5.1 En los Anexos 1, 6, 8, 11, 13 y 14 se establece que los Estados, como parte de su SSP, exigirán que las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicio de tránsito aéreo y los aeródromos certificados implanten un sistema de gestión de la seguridad operacional (SMS). Un SMS es una herramienta de gestión para la gestión de la seguridad operacional por una organización. En los Anexos también se establece que los SMS deben ser aceptables para el Estado y que, como mínimo:

- a) identificarán peligros para la seguridad operacional;
- b) garantizarán la aplicación de las medidas correctivas necesarias para mantener la eficacia convenida respecto de la seguridad operacional;
- c) proporcionarán supervisión continua y evaluación periódica de la eficacia de seguridad operacional; y
- d) tendrán como objetivo el mejoramiento continuo de la actuación global del sistema de gestión de la seguridad operacional.

6.5.2 Los cuatro procesos genéricos incluidos en el requisito SMS de la OACI mencionado (identificación de peligros, implantación de medidas correctivas para encarar los riesgos de seguridad operacional de las consecuencias de los peligros, supervisión continua y mejoramiento continuo) engloban las cuatro actividades básicas para resolver problemas de seguridad operacional que apoyan la prestación de servicios para una organización:

- a) encontrar lo que está mal (identificación de peligro);

- b) proponer e implantar reparaciones (medidas correctivas);
- c) asegurarse de que las reparaciones propuestas funcionan según lo previsto (supervisión continua); y
- d) mejorar constantemente el sistema de gestión para asegurar la eficacia y la eficiencia de la prestación de servicios (mejoramiento continuo del SMS).

6.5.3 Un SMS se define como un enfoque sistemático de la gestión de la seguridad operacional, incluyendo las estructuras de organización, responsabilidades, políticas y procedimientos necesarios. Los fundamentos del SMS se analizan en el Capítulo 7. Al igual que con el SSP, la OACI ha elaborado un marco de SMS para ayudar a los proveedores de servicios en la implantación de su SMS. El marco está integrado por cuatro componentes y doce elementos y se presenta en su totalidad en los Capítulos 8 y 9.

## 6.6 EFICACIA DE LA SEGURIDAD OPERACIONAL DEL SMS

6.6.1 En los Anexos 1, 6, 8, 11 y 14 se establece que el SMS de un proveedor de servicios garantizará la aplicación de medidas correctivas para mantener la eficacia de la seguridad operacional y supervisará continuamente y evaluará periódicamente dicha eficacia de la seguridad operacional.

6.6.2 La noción de eficacia de la seguridad operacional es un ingrediente esencial para el funcionamiento efectivo de un SMS así como el avance hacia un entorno normativo basado en la eficacia. Ayuda a vigilar la eficacia real del SMS y a evitar que sencillamente se “marquen las casillas apropiadas”. Es necesario que el SMS defina un conjunto de resultados de eficacia medibles para determinar si el sistema funciona verdaderamente con arreglo a lo previsto en el diseño — no solamente satisfaciendo requisitos normativos — e identificar si pueden necesitarse medidas para llevar la eficacia del SMS al nivel de lo previsto en el diseño. Estos resultados de eficacia medibles permiten evaluar la eficacia real de las actividades críticas para la seguridad operacional con respecto a los controles de organización existentes de modo que se adopten las necesarias medidas correctivas y puedan mantenerse ALARP los riesgos de seguridad operacional.

6.6.3 Un enfoque normativo basado en la eficacia evaluará la eficacia real de las actividades críticas para la seguridad operacional con respecto a los controles de organización existentes. Además, sólo mediante la garantía de la eficacia de la seguridad operacional efectiva del SMS — mediante el establecimiento y medición de resultados específicos de la eficacia de seguridad operacional — puede alcanzarse el objetivo de un mejoramiento continuo de la seguridad operacional, que constituye la base de la gestión de la seguridad operacional.

6.6.4 La eficacia de la seguridad operacional de un SMS no se relaciona con la cuantificación de los resultados de consecuencias graves (medición de la seguridad operacional) sino más bien con la cuantificación de los procesos de consecuencias leves (medición de la eficacia de la seguridad operacional). La eficacia de la seguridad operacional de un SMS representa exclusivamente la medición de la eficacia de la seguridad operacional. La eficacia de la seguridad operacional expresa los objetivos de seguridad operacional de un proveedor de servicios en forma de resultados medibles de seguridad operacional de procesos especificados de bajo nivel del SMS. Desde la perspectiva de la relación entre el Estado y los proveedores de servicios, la eficacia de la seguridad operacional proporciona evidencia objetiva para que el Estado pueda medir la efectividad y eficiencia que el SMS de los proveedores de servicios debería lograr cuando los proveedores de servicios realizan sus funciones comerciales básicas. Dicha eficacia de la seguridad operacional debe acordarse entre el Estado y los proveedores de servicios, como el mínimo aceptable que el proveedor de servicios debe alcanzar durante la prestación de sus servicios. La eficacia de la seguridad operacional de un SMS es entonces una referencia con respecto a la cual el Estado puede medir la eficacia de la seguridad operacional del SMS, es decir, que el SMS funciona mucho más allá del mero cumplimiento de los reglamentos. Al acordar la eficacia de seguridad operacional de un SMS, es necesario considerar factores tales como el nivel de riesgo de seguridad operacional que se aplica, los costos y beneficios de las mejoras al sistema y las expectativas públicas respecto de la seguridad operacional de la industria de la aviación.

6.6.5 Dentro de cada Estado, la eficacia de la seguridad operacional de cada SMS será acordada por separado entre el Estado y cada organización de aviación. La eficacia de seguridad operacional acordada debería ser conmensurable con la complejidad de los contextos operacionales específicos de cada organización de aviación y la disponibilidad de los recursos de dicha organización para encararlos. En la práctica, la eficacia de la seguridad operacional de un SMS se expresa mediante valores de indicador de eficacia de la seguridad operacional y valores de objetivos de eficacia de seguridad operacional y se implanta mediante planes de acción.

6.6.6 Los valores de indicador de eficacia de la seguridad operacional son objetivos medibles a corto plazo que reflejan la eficacia de la seguridad operacional de un SMS. Se expresan en términos numéricos y deberían ser obvios, medibles y relacionados con los intereses de seguridad operacional de un SMS. Los valores de indicador de eficacia de la seguridad operacional reflejan exclusivamente la medición de la eficacia de la seguridad operacional. Los valores de indicador de eficacia de la seguridad operacional de un SMS no deberían reflejar la medición de la seguridad operacional. Dado que la eficacia de seguridad operacional de cada SMS será acordada por separado entre el Estado y cada organización de aviación, los valores de indicador de eficacia de la seguridad operacional serán por consiguiente distintos entre sectores de la industria de la aviación, como explotadores de aeronaves, explotadores de aeródromos certificados y proveedores de ATS. A continuación se brinda un ejemplo.

6.6.7 Mediante su SMS, un explotador de aeródromo certificado ha identificado problemas de seguridad operacional con respecto a restos de objetos extraños (FOD) en las operaciones de rampa. También ha determinado problemas de seguridad operacional con respecto al tránsito de vehículos no autorizados en las calles de rodaje. Por consiguiente, define los siguientes valores de indicador de la eficacia de la seguridad operacional, después de convenir con la autoridad de supervisión de la aviación civil del Estado: 15 sucesos FOD en plataforma por 10 000 operaciones, y 20 sucesos de vehículos no autorizados en las calles de rodaje por 10 000 operaciones. Estos valores de indicador de la eficacia de la seguridad operacional cumplen las condiciones analizadas en 6.6.6: se expresan en términos numéricos, son obvios, medibles y relacionados con los problemas de seguridad operacional del SMS del aeródromo. Además, ambos indicadores de eficacia de la seguridad operacional reflejan la medición de la eficacia de la seguridad operacional.

6.6.8 Los valores de objetivos de eficacia de la seguridad operacional son objetivos medibles a largo plazo que reflejan la eficacia de la seguridad operacional de un SMS. Los valores de objetivos de eficacia de la seguridad operacional se expresan en términos numéricos; deberían ser obvios, medibles, aceptables para los interesados y relacionados con el indicador de eficacia de la seguridad operacional (objetivo a corto plazo) del SMS.

6.6.9 Continuando con el ejemplo presentado en 6.6.7, el aeródromo define los siguientes valores y objetivos de eficacia de seguridad operacional, después de concertar acuerdo con la autoridad de supervisión de aviación civil del Estado: para enero de 2009, reducir los sucesos FOD en la plataforma a 8 por 10 000 operaciones, y mantener 20 sucesos de vehículos no autorizados en las calles de rodaje por 10 000 operaciones. Estos valores de objetivos de eficacia de la seguridad operacional cumplen las condiciones analizadas en 6.6.6: se expresan en términos numéricos, son obvios, medibles y relacionados con los indicadores de eficacia de la seguridad operacional del SMS del aeródromo. Además, ambos valores de objetivos de eficacia de la seguridad operacional reflejan la medición de la eficacia de la seguridad operacional.

6.6.10 Los planes de acción son las herramientas y los medios necesarios para lograr los valores de indicador de eficacia de la seguridad operacional y los valores de objetivos de eficacia de la seguridad operacional de un SMS. Comprenden los procedimientos operacionales, tecnología, sistemas y programas con respecto a los cuales pueden especificarse mediciones de fiabilidad, disponibilidad, eficacia o exactitud. Un ejemplo de plan de acción para lograr los valores de indicador de eficacia de la seguridad operacional y de objetivo de eficacia de la seguridad operacional de un SMS, como se mencionó anteriormente, sería el siguiente: implantar un programa de inspección ambulante en rampa tres veces por día, elaborar e implantar un curso de instrucción para conductores e instalar carteles en calles de rodaje (específicos del aeródromo).

6.6.11 Los valores de indicador de la eficacia de seguridad operacional y de objetivos de eficacia de la seguridad operacional respecto de la eficacia de la seguridad operacional de un SMS pueden ser diferentes, o pueden ser el mismo. Tres aspectos deben considerarse cuando se evalúe si valores de indicador de eficacia de la seguridad

operacional y valores de objetivo de eficacia en seguridad operacional específicos respecto de la eficacia de la seguridad operacional de un SMS son diferentes o el mismo. En primer lugar, debe considerarse la disponibilidad de recursos del proveedor de servicios para transformar el valor de indicador de eficacia de la seguridad operacional en un valor de objetivo de eficacia de la seguridad operacional más exigente. En segundo lugar, debe considerarse cuán onerosos son los planes de acción que se estiman necesarios para cambiar el valor del indicador de eficacia de seguridad operacional en un valor más exigente de objetivo de eficacia de la seguridad operacional. En tercer lugar, y de mayor importancia, debe considerarse si la evaluación de los riesgos de seguridad operacional de las consecuencias del peligro encarado por el indicador de eficacia de la seguridad operacional y el objetivo de eficacia de la seguridad operacional cae en la región tolerable del proceso de gestión de los riesgos de seguridad operacional analizado en el Capítulo 5, si el valor del indicador de eficacia de la seguridad operacional y el valor de objetivo de eficacia de la seguridad operacional siguen siendo el mismo. El valor de indicador de eficacia de la seguridad operacional puede reflejar una evaluación de los riesgos de seguridad operacional que cae en la región tolerable en las circunstancias prevalecientes. No obstante, cambios en el sistema, crecimiento, etc., pueden restar validez a tal evaluación de los riesgos de seguridad operacional. El valor de indicador de eficacia de la seguridad operacional debe, en este caso, transformarse en un valor de objetivo más exigente que sea válido en el entorno modificado.

6.6.12 Una gama de diferentes indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional proporcionará una mejor visión de la eficacia de la seguridad operacional del SMS de una organización aeronáutica que el uso de un solo indicador u objetivo. En otras palabras, la eficacia de la seguridad operacional de un SMS se expresará siempre mediante varios indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional y nunca mediante uno solo. A continuación se brindan más ejemplos.

6.6.13 Un explotador de aeronaves ha identificado las fases de vuelo de aproximación y aterrizaje como un importante problema de seguridad operacional que ha de tratar con su SMS. También identificó, mediante el componente de gestión de los riesgos de seguridad operacional de su SMS, un problema de seguridad con respecto a las aproximaciones no estabilizadas (o no conformes) a los aeródromos de la red servidos por aproximaciones que no son de precisión. Por consiguiente, define el siguiente valor de indicador de eficacia de la seguridad operacional, después de acuerdo con la autoridad supervisora de la aviación civil del Estado: 10 aproximaciones inestables (o no conformes) por 1 000 aterrizajes en aeródromos de la red servidos por aproximaciones que no son de precisión. Posteriormente, el explotador de aeronaves define el siguiente valor de objetivo de eficacia de la seguridad operacional, después de acuerdo con la autoridad supervisora de aviación civil del Estado: dentro de los tres próximos años, reducir en 50% el número de aproximaciones inestables (o no conformes) por 1 000 aterrizajes en aeródromos de la red servidos por aproximaciones que no son de precisión. El plan de acción para lograr el valor del indicador de eficacia de la seguridad operacional y el valor del objetivo de eficacia de la seguridad operacional mencionados anteriormente sería el siguiente: elaboración de aproximaciones GPS con ángulo de descenso constante (CDA) en los aeródromos de la red servidos por aproximaciones que no son de precisión.

6.6.14 Un proveedor ATS ha identificado la seguridad operacional del aeropuerto como un importante problema de seguridad que ha de tratar en su SMS. Ha identificado, mediante el componente de gestión de los riesgos de seguridad operacional de su SMS, un problema respecto de las incursiones en las pistas y ha definido el siguiente valor del indicador de eficacia de la seguridad operacional: 0,8 incursiones en las pistas de Cat A y B (las más graves) por millón de operaciones en todo 2009. Posteriormente, el proveedor ATS define el siguiente valor de objetivo de eficacia de la seguridad operacional: para 2010 reducir las incursiones en las pistas de Cat A y B (más graves) a un valor no mayor de 0,5 por millón de operaciones.

6.6.15 La eficacia de la seguridad operacional de un SMS debería definirse, en la medida posible, mediante indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional cuantitativos. No obstante, se reconoce que en muchos Estados las capacidades de recolección y análisis de datos de seguridad operacional de los proveedores de servicios pueden no estar plenamente desarrolladas. Por consiguiente, hasta que se desarrollen esas capacidades, la eficacia de la seguridad operacional de un SMS puede definirse mediante una combinación de indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional cuantitativos y cualitativos. No obstante, el objetivo debería seguir siendo la definición de eficacia de la seguridad operacional de un SMS mediante medidas cuantitativas solamente.

6.6.16 La definición de la eficacia de la seguridad operacional de un SMS es un requisito que va mucho más allá del cumplimiento normativo de los requisitos nacionales e internacionales. El establecimiento de la eficacia de la seguridad operacional para un SMS no sustituye los requisitos jurídicos, normativos o de otro tipo establecidos, ni releva a los proveedores de servicios de sus obligaciones en el marco de los reglamentos nacionales pertinentes, y de las que surgen del *Convenio sobre Aviación Civil Internacional* (Doc 7300 de la OACI) y sus disposiciones conexas contenidas en los Anexos al Convenio.

## 6.7 RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DE LA ADMINISTRACIÓN

6.7.1 El tercer y último grupo de los SARPS sobre gestión de la seguridad operacional de la OACI que figuran en los Anexos 1, 6, 8, 11, 13 y 14 es la responsabilidad y rendición de cuentas de la administración con respecto a la gestión de la seguridad operacional durante la prestación de los servicios. Los SARPS de la OACI establecen que en un sistema de gestión de la seguridad operacional aceptado se definirán claramente las jerarquías de responsabilidades en cuanto a la seguridad operacional en todas las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados, incluyendo la responsabilidad directa de la administración superior respecto de la seguridad operacional.

6.7.2 La contribución de la administración a la gestión de la seguridad operacional se analiza en los Capítulos 3 y 8, y no se considera necesario un mayor análisis. No obstante, cabe mencionar un aspecto lingüístico: el uso del término “responsabilidad” en los requisitos de gestión de la seguridad operacional de la OACI. Existen dos palabras en inglés “accountabilities” y “responsibilities”, para el término español “responsabilidad”. “Responsibilities” se refiere a la situación en que una persona debe ejecutar medidas específicas, mientras que “accountabilities” extiende la idea a la obligación o disposición de asumir responsabilidad por la ejecución de tales acciones. En términos de gestión de la seguridad operacional, las responsabilidades (responsibilities) de seguridad operacional describen la finalidad de seguridad operacional de las tareas que un individuo debe realizar. Las “accountabilities” son declaraciones de lo que el individuo debe realizar, ya sea directamente o mediante la supervisión y gestión de otros, incluyendo aquellos en quienes el individuo ha delegado responsabilidad. Existe claramente una diferencia importante entre ambos términos. No obstante, esta diferencia existe solamente en el idioma inglés. Por lo tanto, el término “responsabilidad”, con respecto a la gestión en los requisitos de gestión de la seguridad operacional de la OACI como figuran en las versiones de los Anexos 1, 6, 8, 11, 13 y 14 en idiomas distintos del inglés, debe entenderse en el sentido del término inglés “accountabilities”, que incluiría la rendición de cuentas.

6.7.3 La exitosa gestión de la seguridad operacional exige la activa participación de todos los niveles de administración y supervisión. Esto debería reflejarse en la estructura de la organización y en las rendiciones de cuentas de seguridad operacional publicadas. La organización debería definir, documentar y comunicar – con ayuda de diagramas o cartas de organización – las responsabilidades, líneas de rendición de cuentas y facultades. La rendición de cuentas de la administración superior y sus responsabilidades funcionales se presentan con más detalle en el Capítulo 8.

## 6.8 RELACIÓN ENTRE UN SSP Y UN SMS

6.8.1 Una clara comprensión de la relación entre un SSP y un SMS es esencial para las actividades concertadas de gestión de la seguridad operacional en los Estados. Esta relación puede expresarse en términos sencillos como sigue: los Estados son responsables de elaborar y establecer un SSP; los proveedores de servicios son responsables de elaborar y establecer un SMS. Este es un punto muy importante: no se espera que los Estados elaboren un SMS; el SSP cumple una función equivalente. No obstante, los Estados son responsables, como parte de

las actividades de su SSP, de aceptar y supervisar la elaboración, implantación y eficacia operacional del SMS del proveedor de servicio. En la supervisión de la eficacia de la seguridad operacional del SSM de un proveedor de servicios, la noción de ALoS de un SSP, analizada en 6.4, desempeña una función fundamental en la relación entre un SSP y un SMS. La relación entre el SSP y el SMS se ilustra en la Figura 6-7 y se analiza con más detalle en el Capítulo 11.

6.8.2 En el Capítulo 3 se presenta un posible dilema administrativo que puede surgir de la perspectiva que considera la administración de la seguridad operacional como un proceso de la organización y la gestión de la seguridad operacional como una función empresarial básica. Dicho dilema potencial, presentado como “dilema de las dos P” proporciona un fondo adecuado para explicar la relación entre un SSP y un SMS.

6.8.3 En la Figura 6-7, el SSP está ubicado en el lado “protección” de la balanza cuyos platillos son “protección” y “producción”. El SSP se dirige a garantizar la seguridad pública controlando los riesgos de seguridad operacional a nivel del Estado. El SSP no tiene objetivos de producción como tales. Aunque se espera eficiencia de las organizaciones de aviación del Estado, no tienen objetivos específicos en términos de entrega de productos o prestación de servicios dirigidos a obtener ganancias. El objetivo básico de un Estado, a través de su SSP, es garantizar en la medida posible la seguridad pública durante la prestación de servicios por los proveedores de éstos. Este objetivo se logra definiendo el ALoS para el SSP, y mediante el control de los riesgos de seguridad operacional dentro del Estado por los dos “componentes operacionales” del SSP: gestión de los riesgos de seguridad operacional y garantía de la seguridad operacional.

6.8.4 El SMS del proveedor de servicios está solo parcialmente situado sobre el platillo “protección” de la balanza. A diferencia del Estado, un proveedor de servicios tiene objetivos específicos en términos de entrega de productos o prestación de servicios dirigidos a obtener ganancias. El objetivo del SMS del proveedor de servicios es, en términos de protección, el control de los riesgos de seguridad que son consecuencia de actividades y procesos relacionados con la entrega de los productos o prestación de servicios en que se especializa la organización. El proveedor de servicios logra el control de los riesgos de seguridad operacional durante la prestación de los servicios principalmente mediante los dos “componentes operacionales” del SMS: gestión de los riesgos de seguridad operacional y garantía de la seguridad operacional, y donde la política y objetivos de seguridad operacional y la promoción de la seguridad operacional desempeñan una función de apoyo aunque importante.

6.8.5 El Estado, como parte de su SSP, acepta inicialmente el SMS de un proveedor de servicios. Esta aceptación es principalmente prescriptiva: el Estado, muy probablemente mediante su autoridad supervisora de la aviación civil, verificará que los componentes y elementos propuestos por el SMS del proveedor de servicios se ajustan a los reglamentos y directivas existentes promulgados por el Estado. Es importante señalar que la aceptación es principalmente un proceso administrativo: el Estado aprueba un plan de sistema de gestión y un plan de acción para su elaboración e implantación. En términos sencillos, la aceptación significa principalmente “marcar las casillas apropiadas”. Pero la aceptación, si bien asegura el cumplimiento de los reglamentos, no garantiza una eficacia apropiada del SSM. La aceptación y la vigilancia del cumplimiento se indican mediante la flecha vertical que une el SSP y el SMS en la Figura 6-7. La forma en que el Estado asegura la eficacia apropiada del SMS (es decir, que el SMS realmente funciona) es la supervisión del mismo durante la ejecución real de las actividades dirigidas a la prestación de servicios.

6.8.6 Para verificar la eficacia del SMS, la autoridad de vigilancia de la aviación civil del Estado debe vigilar su funcionamiento con carácter periódico, durante el curso de las actividades dirigidas a la prestación de servicios. Esto sería difícil, si no imposible, en la práctica, de ahí el motivo de introducir indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional en un SMS. Si bien la aceptación y la vigilancia en el cumplimiento, señaladas en 6.8.5, tienen carácter prescriptivo, la vigilancia de los indicadores y objetivos de eficacia de la seguridad operacional se basan en la eficacia. La noción de eficacia de la seguridad operacional presentada en la sección 6.6 extiende, así, al SMS del proveedor de servicios la noción de ALoS de un SSP presentada en la sección 6.4. La eficacia de la seguridad operacional es al SMS como el ALoS es al SSP.

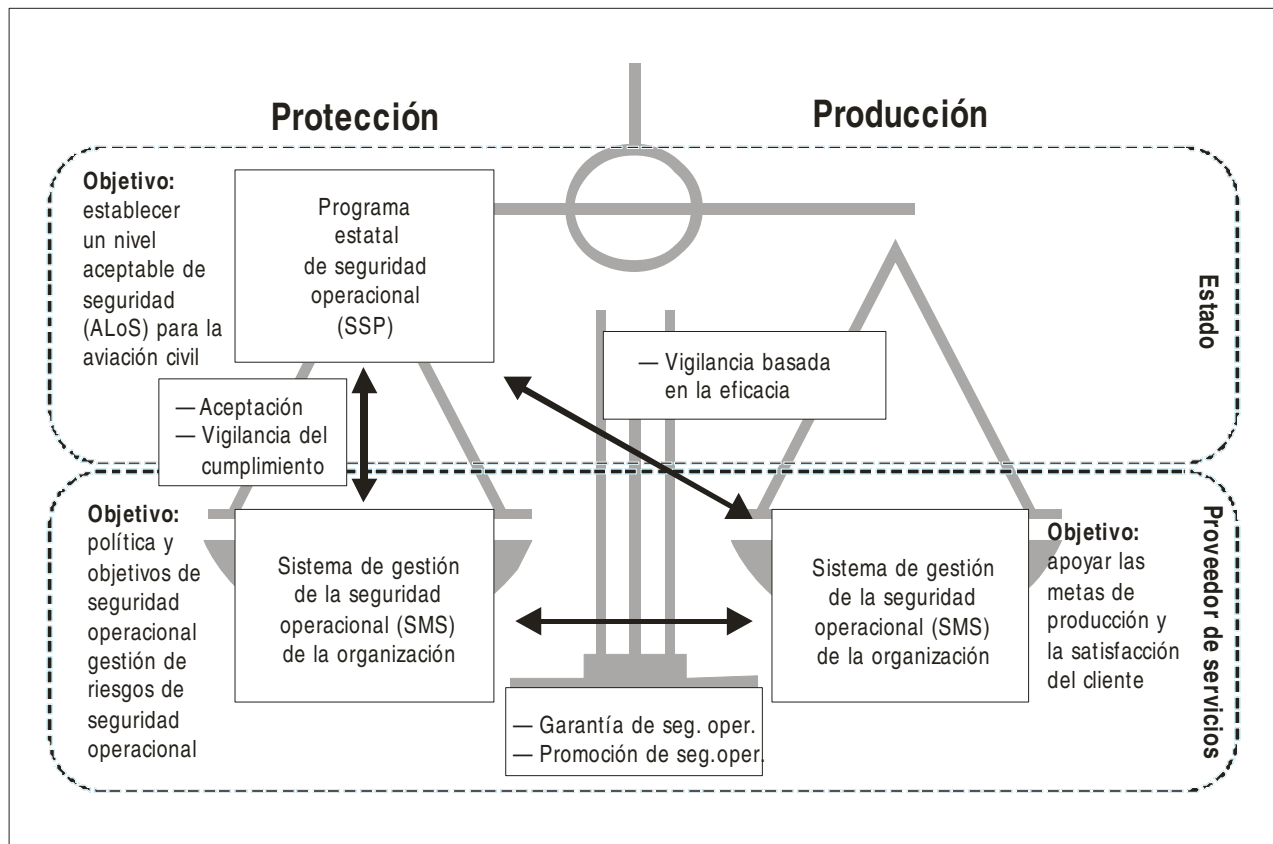


Figura 6-7. Relación entre un SSP y un SMS

6.8.7 La medición de la eficacia de la seguridad operacional de un SMS comprende la definición de indicadores de eficacia de la seguridad operacional, objetivos de eficacia de la seguridad operacional y planes de acción. Estos indicadores y objetivos fundamentales y convenidos son representativos de los peligros genéricos en el contexto operacional en el que el proveedor de servicios realiza actividades relacionadas con la prestación de sus servicios y proporcionan un proceso de vigilancia basado en la eficacia con un panorama justo de la eficacia del SMS. Mediante la definición de un conjunto jerarquizado de objetivos de seguridad operacional a corto y mediano plazo específicos de la actividad particular del proveedor de servicios, mediante la implantación de estrategias de mitigación frente a los riesgos de seguridad operacional de las consecuencias de los peligros subyacentes en los objetivos de seguridad operacional específicos y mediante el establecimiento de métricas y cronogramas que permiten la medición de la efectividad de las estrategias de mitigación, el proveedor de servicios proporciona a la autoridad de supervisión medios medibles de verificar la eficacia de seguridad operacional del SMS, o ausencia de la misma, más allá del cumplimiento de los reglamentos.

6.8.8 Consideremos ahora el platillo “producción” de la balanza en la Figura 6-7, como ya se señaló, un SSP no tiene objetivos de producción como tales, pero evidentemente un proveedor de servicios los tiene. El objetivo de las actividades de producción de un proveedor de servicios es lograr sus metas comerciales y obtener satisfacción del cliente. El SMS es el medio que utiliza el proveedor de servicios para asegurar que los riesgos de seguridad operacional de las consecuencias de los peligros que debe enfrentar en el logro de sus objetivos de producción permanecen bajo control de la organización. El SMS del proveedor de servicios identifica los riesgos de seguridad operacional y las medidas de mitigación necesarias para mantenerlos bajo control de la organización mediante la gestión de los riesgos de seguridad

operacional inicialmente. Una vez iniciadas las operaciones, el control de los riesgos de seguridad operacional y la vigilancia de las medidas de mitigación se logran mediante el proceso continuo de garantía de seguridad operacional, apoyado por la promoción de la seguridad operacional. La gestión de los riesgos de seguridad operacional, la garantía de la seguridad operacional y la promoción de la seguridad operacional proporcionan, así, los medios con que una organización mantiene el equilibrio entre producción y protección.

6.8.9 Aunque la función tradicional del Estado, por lo que hace a la aceptación del SMS y su vigilancia administrativa en términos de cumplimiento de las normas, está representada en el platillo “protección”, en un SSP hay lugar para la función de vigilancia también en el platillo “producción”. Las deficiencias en la identificación de peligros y la gestión de los riesgos de seguridad operacional, así como la elaboración de estrategias de mitigación, se relacionan a menudo con la asignación de recursos. Esto sucede normalmente cuando la asignación de recursos se inclina más hacia las actividades de producción. Las deficiencias en la identificación de peligros y en la gestión de los riesgos de seguridad operacional, así como la elaboración de estrategias de mitigación, también se harán más evidentes por la incapacidad de satisfacer la eficacia de seguridad operacional convenida del SMS del proveedor de servicios, debido a una asignación desequilibrada de los recursos entre la producción y la protección. Por consiguiente, al ejercer la vigilancia basada en la eficacia que se describe en 6.8.7, en la supervisión de la eficacia operacional del SMS con respecto a la eficacia de seguridad operacional acordada específica del proveedor de servicios, se harán evidentes las tendencias o preferencias en la asignación de recursos, así como la eficacia de la seguridad operacional del SMS en su totalidad: la falta de recursos conducirá a la no identificación de peligros de seguridad operacional o a una defectuosa gestión de los riesgos de seguridad operacional y, en consecuencia, a una baja eficacia de seguridad operacional del SMS. En tal caso, aunque quizás cumpla con los reglamentos, el SMS del proveedor de servicios no será efectivo. En la Figura 6-7, la aceptación y la vigilancia basadas en la eficacia están representadas por la flecha diagonal que une el SSP con los procesos de producción de la organización.

## 6.9 CUMPLIMIENTO Y EFICACIA

6.9.1 Existe la creciente convicción en el entorno aeronáutico sobre la necesidad de complementar el enfoque existente de la seguridad operacional basado en el cumplimiento con un enfoque basado en la eficacia, con miras a lograr una implantación realista de prácticas de gestión de la seguridad operacional mediante el SSP y el SMS. El tema ya se ha analizado en este capítulo con respecto al SSP y su ALoS conexo. En esta sección se presenta una conclusión resumida, subrayando los puntos importantes.

6.9.2 La búsqueda de la gestión de la seguridad operacional y de un enfoque basado en la eficacia se basa en la introducción y utilización efectiva de controles de los riesgos de seguridad operacional. Desde el punto de vista del Estado, los controles de los riesgos de seguridad operacional más efectivos a su disposición son los reglamentos de seguridad operacional.

6.9.3 En un entorno de seguridad operacional basada en el cumplimiento, el enfoque de la gestión de la seguridad operacional es rígido y prescriptivo, según se vio en el Capítulo 3 y en este capítulo. En un entorno de seguridad operacional basado en el cumplimiento, los reglamentos de seguridad operacional se emplean como controles administrativos. Un marco reglamentario estricto se apoya en inspecciones y auditorías con el objetivo exclusivo del cumplimiento de los reglamentos.

6.9.4 En un entorno de seguridad operacional basado en la eficacia, el enfoque es flexible y dinámico. En dicho entorno, los reglamentos de seguridad operacional se emplean como controles de los riesgos de seguridad operacional. Se implanta un marco normativo en el cual los reglamentos se elaboran para responder a los riesgos de seguridad operacional y controlarlos, y la vigilancia del cumplimiento del marco normativo se apoya mediante la identificación y jerarquización de los riesgos de seguridad operacional basadas en datos, con dos objetivos: cumplimiento de los reglamentos, pero más importante, verificación de la eficacia de la seguridad operacional efectiva.



6.9.5 En un entorno de seguridad operacional basado en la eficacia, es necesario definir un conjunto de objetivos medibles para el SSP y objetivos de eficacia medibles para el SMS a efectos de determinar si el SSP y el SMS están funcionando con arreglo a lo previsto en el diseño, más allá del cumplimiento de los reglamentos. Los objetivos medibles y los objetivos de eficacia permiten evaluar la eficacia real de las actividades críticas para la seguridad operacional con respecto a los controles existentes en la organización para poder adoptar las medidas correctivas o preventivas necesarias y mantener los riesgos de seguridad operacional en el nivel más bajo que sea razonable en la práctica (ALARP).

6.9.6 Las nociones de un ALoS relacionado con un SSP y de eficacia de la seguridad operacional para un SMS son ingredientes esenciales para el efectivo funcionamiento del SSP y del SMS. Proporcionan el fundamento para un entorno normativo basado en la eficacia, a efectos de supervisar la implantación real de un SSP y la eficacia real del SMS, más allá del cumplimiento de los reglamentos. Sólo mediante el establecimiento y medición de objetivos de seguridad operacional y objetivos de eficacia de la seguridad operacional específicos — mediante garantía de la implantación efectiva de un SSP y la eficacia de seguridad operacional efectiva de un SMS — puede lograrse el objetivo de mejora continua de la eficacia de la seguridad operacional en que se basan el SSP y el SMS.

6.9.7 Los indicadores de la seguridad operacional y los objetivos de seguridad operacional así como los indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional proporcionan una forma medible de asegurar y demostrar la eficacia de un SSP y un SMS respectivamente, más allá del cumplimiento de los reglamentos. El cumplimiento de los reglamentos todavía constituye uno de los fundamentos de la gestión de la seguridad operacional para el Estado así como para los proveedores de servicios. Las Figuras 6-8 y 6-9 amplían los ejemplos de indicadores de la seguridad operacional y objetivos de la seguridad operacional, indicadores de eficacia de la seguridad operacional, objetivos de eficacia de la seguridad operacional y planes de acción para un SSP y un SMS respectivamente, que ya se abarcaron en este capítulo, a efectos de ilustrar dónde y cómo encajan la prescripción y la eficacia dentro de un SSP y un SMS.

6.9.8 En resumen, con arreglo a los SARPS sobre gestión de la seguridad operacional armonizados de la OACI:

- a) Los Estados establecerán un programa estatal de seguridad operacional (SSP), para lograr un nivel aceptable de seguridad (ALoS) en la aviación civil.
- b) El nivel aceptable de seguridad operacional (ALoS) que ha de alcanzarse será establecido por el Estado.
- c) Los proveedores de servicios implantarán un sistema de gestión de la seguridad operacional (SMS) que:
  - 1) identifique los peligros para la seguridad operacional;
  - 2) garantice la aplicación de las medidas correctivas necesarias para mantener la eficacia de la seguridad operacional;
  - 3) proporcione supervisión continua y evaluación periódica de la eficacia de la seguridad operacional; y
  - 4) tenga como objetivo el mejoramiento continuo de la actuación global del SMS.

## **Eficacia**

Valores de objetivos de seguridad operacional	<ol style="list-style-type: none"> <li>1. Reducir en [número] el número de/Máximo de [número] aproximaciones no conformes (NCA) en 5 aeropuertos internacionales por [número] llegadas para [fecha].</li> <li>2. Reducir en [número] el número de/Máximo de [número] incursiones en la pista de Cat B y C en 5 aeropuertos internacionales de [Estado] por [número] operaciones para [fecha].</li> <li>3. ...</li> </ol>
Planes de acción	<ol style="list-style-type: none"> <li>1. Implantación de procedimientos de llegada en descenso continuo (CDA). Diseño de cartas de procedimientos de llegada para aproximaciones estabilizadas.</li> <li>2. Instalación de ASDE/X en 5 aeropuertos internacionales de [Estado].</li> <li>3. ...</li> </ol>
Valores de indicador de la seguridad operacional	<ol style="list-style-type: none"> <li>1. [Número] aproximaciones no conformes (NCA) en 5 aeropuertos internacionales por [número] operaciones.</li> <li>2. [Número] incursiones en la pista de Cat B y C en 5 aeropuertos internacionales de [Estado] por [número] operaciones.</li> <li>3. ...</li> </ol>

## **Prescripción**

Estado	Cumplirá todas las normas internacionales aplicables.
--------	---

**Figura 6-8. SSP — Prescripción combinada con eficacia**

## **Eficacia**

Valores de objetivos de la seguridad operacional	<ol style="list-style-type: none"> <li>1. [Número] sucesos de vehículos no autorizados en las calles de rodaje por [número] operaciones en 5 aeropuertos internacionales de [Estado] para [fecha].</li> <li>2. [Número] sucesos FOD en la plataforma por [número] operaciones.</li> <li>3. ...</li> </ol>
Planes de acción	<ol style="list-style-type: none"> <li>1. Curso de instrucción para conductores/instalación de carteles específicos.</li> <li>2. Programa de inspección ambulante en la rampa tres veces por día.</li> <li>3. ...</li> </ol>
Valores de indicador de la seguridad operacional	<ol style="list-style-type: none"> <li>1. [Número] sucesos de vehículos no autorizados en las calles de rodaje en 5 aeropuertos internacionales de [Estado].</li> <li>2. [Número] sucesos FOD en la plataforma en 5 aeropuertos internacionales de [Estado].</li> <li>3. ...</li> </ol>

## **Prescripción**

Estado	Cumplirá todas las normas internacionales aplicables.
--------	---

**Figura 6-9. SMS — Prescripción combinada con eficacia**





## Capítulo 7

# INTRODUCCIÓN A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

### 7.1 OBJETIVO Y CONTENIDO

En el presente capítulo se describen las características básicas de los sistemas de gestión de la seguridad operacional (SMS) y se analiza la función y la importancia de describir adecuadamente el sistema (descripción del sistema) y realizar un análisis de carencias antes de iniciar el proceso de implantación del SMS. En este capítulo también se analiza la relación entre el SMS y los sistemas de gestión de la calidad (QMS). El capítulo comprende los temas siguientes:

- a) conceptos introductorios;
- b) características del SMS;
- c) descripción del sistema;
- d) análisis de las carencias;
- e) SMS y QMS;
- f) SSP/SMS y el proceso de investigación de accidentes;
- g) integración de sistemas de gestión;
- h) aclaración de términos; y
- i) diferencia entre consignas de seguridad operacional y principios de seguridad operacional.

### 7.2 CONCEPTOS INTRODUCTORIOS

7.2.1 Un SMS es como una caja de herramientas. Es una caja de herramientas que contiene las herramientas que necesita una organización de aviación para poder controlar los riesgos de seguridad de las consecuencias de los peligros que debe enfrentar durante la prestación de los servicios con cuyo fin trabaja la organización. En muchos casos, la propia organización genera los peligros durante la prestación de servicios. Es importante reconocer que un SMS en sí no es ni una herramienta ni un proceso. Un SMS es la caja de herramientas, donde están contenidas y protegidas las herramientas reales empleadas para realizar los dos procesos básicos de gestión de la seguridad operacional (identificación de peligros y gestión de los riesgos de seguridad operacional). Lo que un SMS hace para una organización es proporcionar una caja de herramientas que resulta apropiada, en volumen y complejidad, al volumen y complejidad de la organización.

7.2.2 Como caja de herramientas (Figura 7-1), un SMS asegura que cuando se necesitan herramientas específicas para identificar peligros o gestionar los riesgos de seguridad operacional:



**Figura 7-1. SMS — Una caja de herramientas**

- a) las herramientas correctas para la tarea en cuestión están disponibles para que la organización las utilice;
- b) las herramientas y la tarea están adecuadamente relacionadas;
- c) las herramientas son proporcionales a las necesidades y limitaciones de la organización; y
- d) las herramientas pueden encontrarse fácilmente dentro de la caja, sin pérdidas innecesarias de tiempo o recursos.

Esta perspectiva es importante, porque un SMS es sencillamente un caparazón protector que asegura el almacenamiento, la disponibilidad y la utilización adecuados y oportunos de las herramientas necesarias para realizar procesos específicos de gestión de la seguridad operacional en la organización. Sin las herramientas adecuadas en su interior, un SMS es solamente un caparazón vacío.

7.2.3 En el resumen final del Capítulo 3 se indicaron varias características distintivas de la gestión de la seguridad operacional. Una característica importante es que la gestión de la seguridad operacional no se circunscribe a solo una actividad específica de la organización, generalmente la más visible (por ejemplo, operaciones de vuelo de una línea aérea), que puede generar peligros. La gestión de la seguridad operacional trata todas las actividades operacionales de toda la organización. El ámbito de un SMS engloba la mayoría de las actividades de la organización y, ciertamente, todas las actividades operacionales que apoyan la prestación de servicios y contienen la posibilidad de generar peligros. El ámbito de un SMS incluye directamente las operaciones, el mantenimiento, la reparación, los servicios de apoyo, la instrucción y la verificación y otras actividades operacionales. El ámbito de un SMS comprende

indirectamente, según corresponda y sean pertinentes a la prestación de servicios, otras actividades de la organización que apoyan actividades operacionales, como los aspectos de finanzas, recursos humanos y jurídicos, según se vio en el Capítulo 3.

7.2.4 Un SMS debe comenzar desde la administración superior. Esto no es una declaración retórica ni filosófica, sino que está basada en razones muy concretas. La gestión de la seguridad operacional, función empresarial básica de una organización, requiere recursos al igual que cualquier otra función empresarial básica. La asignación de recursos es eminentemente función de la administración superior, en el sentido de que ésta tiene tanto la autoridad como la responsabilidad de la asignación de recursos. Si la administración superior no conoce la función y los objetivos del SMS de la organización o no participa en un nivel apropiado en el SMS de la organización, no podrá apreciar la medida que representan los riesgos de seguridad operacional para las capacidades de la organización. Sin esta apreciación, la asignación de recursos puede no satisfacer las necesidades reales. En otras palabras, es probable que aparezca y permanezca sin resolver el “dilema de las dos P” analizado en el Capítulo 3.

7.2.5 Un SMS apunta a efectuar continuas mejoras en el nivel global de seguridad operacional de una organización. Con arreglo a las características de la gestión de la seguridad operacional como función empresarial básica, el SMS involucra con carácter permanente la identificación diaria de peligros, recolección y análisis, estimación de los riesgos de seguridad operacional e implantación de estrategias de mitigación. No hay punto específico en el cual el SMS se detenga o se haga más lento. Un SMS es una operación constante y que nunca termina dirigida a mantener y, de ser posible, mejorar los niveles de seguridad operacional que son conmensurables con los objetivos estratégicos de la organización y funciones empresariales básicas de apoyo. En este sentido, un SMS es profundamente diferente de la noción tradicional de investigación de accidentes, en la que se espera que ocurra el accidente, para luego extraer y distribuir tantas enseñanzas en materia de seguridad operacional como se puedan obtener de la investigación para evitar accidentes similares. Un SMS busca activamente los peligros, y evalúa continuamente los riesgos de seguridad operacional para contenerlos antes de que resulten en un accidente.

7.2.6 Todos los interesados en la aviación desempeñan una función en el SMS y, una vez más, por razones muy concretas. Es importante identificar e involucrar a los interesados en el sistema de la aviación para asegurar que sus aportes y conocimientos en materia de decisiones sobre riesgos de seguridad operacional se tienen en cuenta antes de adoptar dichas decisiones.

7.2.7 Además, dada la amplia gama de actividades del SMS, es esencial contar con aportes de múltiples sectores al proceso de toma de decisiones sobre riesgos de seguridad operacional. A continuación se presenta una lista de partes interesadas a las que puede apelarse para ayudar o aportar insumos al proceso de toma de decisiones sobre riesgos de seguridad operacional:

- a) profesionales de la aviación;
- b) propietarios de aeronaves y explotadores de servicios aéreos;
- c) fabricantes;
- d) autoridades reglamentadoras de aviación;
- e) asociaciones comerciales de aviación;
- f) proveedores regionales de servicios de tránsito aéreo;
- g) asociaciones y federaciones profesionales;
- h) organizaciones internacionales de aviación;
- i) agencias de investigación; y
- j) público viajero.

7.2.8 Estas partes interesadas pueden ayudar a los encargados de adoptar decisiones en la organización asegurando que la comunicación sobre los riesgos de seguridad operacional que se están considerando tiene lugar al principio y en una forma justa, objetiva y comprensible. Para que la comunicación en materia de seguridad operacional sea creíble, debe ser coherente con los hechos, con declaraciones anteriores de la administración y con los mensajes de otras autoridades. Estos mensajes deben expresarse en términos que los interesados puedan comprender.

### 7.3 CARACTERÍSTICAS DEL SMS

7.3.1 Tres características definen un SMS, a saber:

- a) sistemático;
- b) proactivo; y
- c) explícito.

7.3.2 El SMS es sistemático porque las actividades de gestión de la seguridad operacional están de acuerdo a un plan predeterminado y se aplican de manera coherente a través de toda la organización. Un plan de largo alcance para mantener bajo control los riesgos de seguridad operacional de las consecuencias de los peligros se elabora, aprueba, implanta y pone en funcionamiento con carácter diario e ininterrumpido. Como consecuencia de su carácter sistemático y estratégico, las actividades del SMS se dirigen a una mejora gradual pero constante, y no a un cambio instantáneo y fundamental. El carácter sistemático del SMS también conduce a concentrarse en los procesos en vez de las consecuencias. Aunque las consecuencias (es decir sucesos adversos) se consideran debidamente para extraer conclusiones que apoyen el control de los riesgos de seguridad operacional, el foco principal del SMS es la captura de los peligros, que son los precursores de las consecuencias, en el transcurso de las actividades operacionales rutinarias (procesos) que la organización realiza durante la prestación de sus servicios.

7.3.3 El SMS es proactivo porque se basa en un enfoque que enfatiza la identificación de los peligros y el control y mitigación de los riesgos antes de que puedan ocurrir sucesos que afecten la seguridad. Entraña planificación estratégica que procura mantener los riesgos de seguridad operacional bajo control constante de la organización, en vez de tomar medidas de reparación cuando se experimenta un suceso adverso, y luego regresar al “modo durmiente” hasta que se experimente el siguiente suceso adverso y se vuelva a adoptar medidas correctivas. Para mantener la efectiva identificación de los peligros, se realiza una supervisión constante de las actividades operacionales necesarias para la prestación de los servicios. Esto a su vez permite recopilar datos de seguridad operacional sobre peligros, lo que conduce a la adopción de decisiones en la organización basadas en los riesgos de seguridad operacional y su control, en vez de formular decisiones sobre riesgos de seguridad operacional basadas en opiniones o, incluso peor, en sesgos o prejuicios.

7.3.4 Por último, el SMS es explícito porque todas las actividades de gestión de la seguridad operacional están documentadas, son visibles y, por consiguiente, pueden defenderse. Las actividades de gestión de la seguridad operacional y el subsiguiente conocimiento sobre gestión de la seguridad operacional de la organización son registrados formalmente en documentos oficiales disponibles públicamente. Así pues, las actividades de gestión de la seguridad operacional son transparentes. En este respecto, la “biblioteca de seguridad operacional” a que se hizo referencia en el Capítulo 4 desempeña la función fundamental en garantizar que las actividades y el conocimiento sobre gestión de la seguridad operacional están documentados en estructuras formales de la organización y no residen en las mentes de los individuos. Una organización en la cual las actividades y conocimientos de gestión de la seguridad operacional residen en las mentes de los individuos se expone a una situación altamente volátil en términos de conservación de las actividades y conocimientos de seguridad operacional.



## 7.4 DESCRIPCIÓN DEL SISTEMA

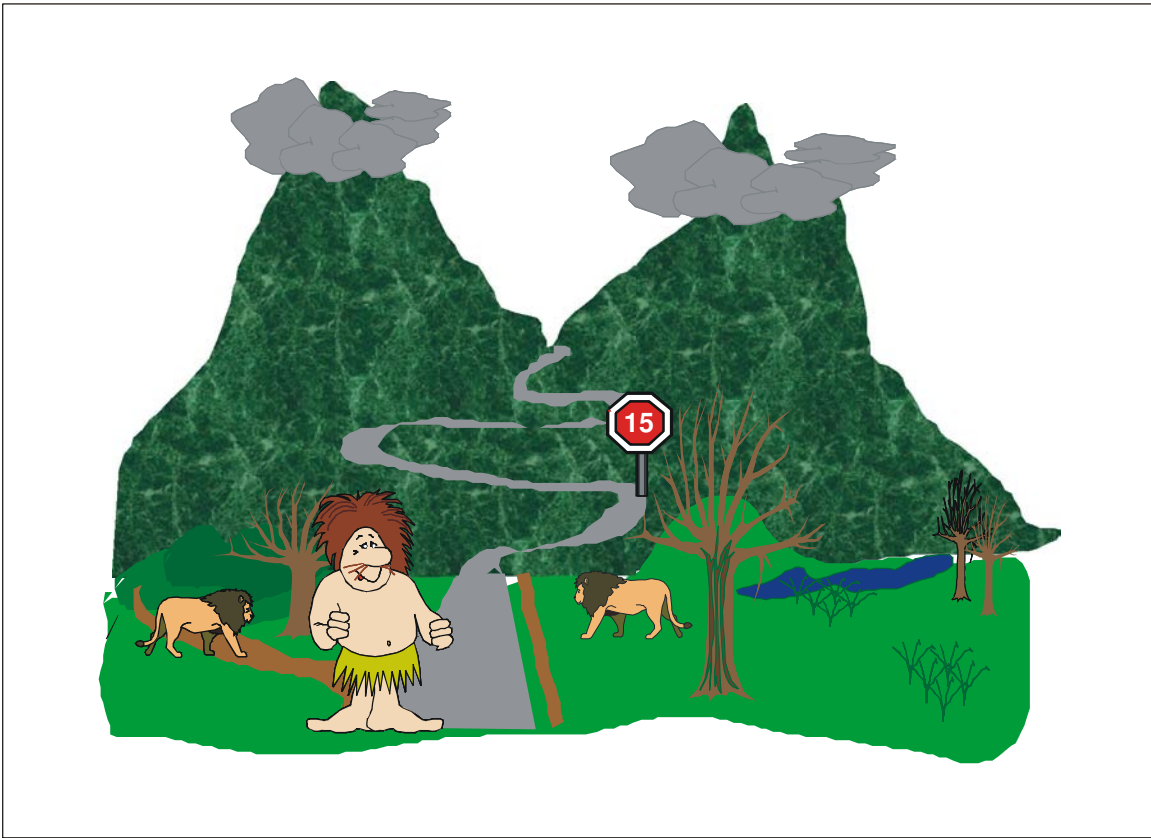
7.4.1 Una descripción del sistema es el primer prerrequisito para la elaboración de un SMS. En el Capítulo 2 se analiza la interrelación entre las personas, el contexto y la seguridad operacional en entornos aeronáuticos. Allí se propone que las fuentes de las vulnerabilidades de seguridad operacional durante la prestación de servicios se encuentran en disparidades en la interfaz entre las personas y los otros componentes del contexto operacional en el que las personas realizan sus actividades de prestación de servicios. Posibles vulnerabilidades de seguridad operacional como consecuencia de las interacciones entre las personas y otros componentes del contexto operacional pueden caracterizarse específicamente en términos de peligros, que tienen elementos identificables y controlables. Los peligros son componentes singulares de los sistemas de producción, y la mayoría de los peligros liberan su potencial perjudicial como consecuencia de interacciones operacionales entre los diferentes componentes del sistema.

7.4.2 Veamos un ejemplo sencillo. El combustible es un componente del sistema de aviación y, al igual que toda otra fuente de energía, constituye un peligro. Mientras está almacenado en tanques subterráneos y no se le manipula, el potencial perjudicial del combustible como peligro es bajo. Las aeronaves son también componentes del sistema de aviación. El abastecimiento de combustible a las aeronaves lo hacen personas. Durante las operaciones de abastecimiento de combustible por personas (una interacción operacional esencial para la prestación del servicio), el potencial perjudicial del combustible como peligro aumenta considerablemente. Entonces se implantan procedimientos de abastecimiento de combustible para llevar los riesgos de seguridad operacional de las operaciones de abastecimiento bajo control de la organización. Estos procedimientos se basan en la identificación y el control de los elementos del peligro. La identificación de los elementos del peligro y, en gran medida, el control, se basan, como etapa primera y esencial, en la descripción del sistema.

7.4.3 El ejemplo utilizado en el Capítulo 2 para explicar la interrelación entre personas, contexto y seguridad operacional en entornos aeronáuticos también resulta útil para explicar la descripción del sistema.

7.4.4 En la Figura 7-2 se muestra un entorno en el que se realiza una actividad de prestación de servicios. El servicio en cuestión es la entrega de pequeños paquetes al otro lado de las montañas por personas (el cavernícola). La combinación de personas involucradas en la prestación del servicio, las herramientas y los medios que utilizarán y las características del entorno constituyen el contexto operacional en el que tendrá lugar la actividad de prestación del servicio. El sistema en cuestión es un sistema sociotécnico (es decir un sistema que combina personas y tecnología) para la entrega de paquetes. Dado que las fuentes de vulnerabilidad de la seguridad operacional están caracterizadas específicamente como peligros que pueden encontrarse en disparidades en la interfaz entre las personas y otros componentes del contexto operacional en el que las personas realizan sus actividades de prestación de servicios, el primer paso en la identificación de tales disparidades consiste en describir el sistema en términos de sus componentes y sus interacciones.

7.4.5 Una descripción de este sistema en términos de sus componentes y sus interacciones, utilizando el modelo SHELL que se analiza en el Capítulo 2, podría ser la siguiente. La función del sistema sociotécnico es la entrega de paquetes. Se interrelaciona con otros sistemas: un sistema topográfico, un sistema meteorológico, un sistema de fauna silvestre. Hay un componente social: las personas. Hay consideraciones de actuación humana que son fundamentales para la operación del sistema: ¿cómo se comportarán las personas cuando interactúen con los leones, con las montañas y con las condiciones meteorológicas? Hay componentes de soporte físico (hardware) del sistema: el camino a través de las montañas, los signos de advertencia. Hay también componentes de soporte lógico (software): documentación, procedimientos e instrucción para orientar a las personas en la operación del sistema e interacción con el mismo (cómo tratar con los leones, cómo manejar las curvas del camino, cómo protegerse contra el mal tiempo) asegurando al mismo tiempo la prestación del servicio (los paquetes deben entregarse intactos al otro lado de la montaña).



**Figura 7-2. Descripción del sistema**

7.4.6 En términos formales o técnicos, una descripción del sistema en aviación debería incluir lo siguiente:

- a) las interacciones del sistema con otros sistemas en el sistema de transporte aéreo;
- b) las funciones del sistema;
- c) las consideraciones de actuación humana requeridas para la operación del sistema;
- d) los componentes "hardware" del sistema;
- e) los componentes "software" del sistema, incluyendo los procedimientos que definen las guías para la operación y el uso del sistema;
- f) el entorno operacional; y
- g) los productos y servicios contratados o adquiridos.

7.4.7 En el Apéndice 1 de este capítulo se proporciona orientación sobre descripción de sistemas.

## 7.5 ANÁLISIS DE LAS CARENCIAS

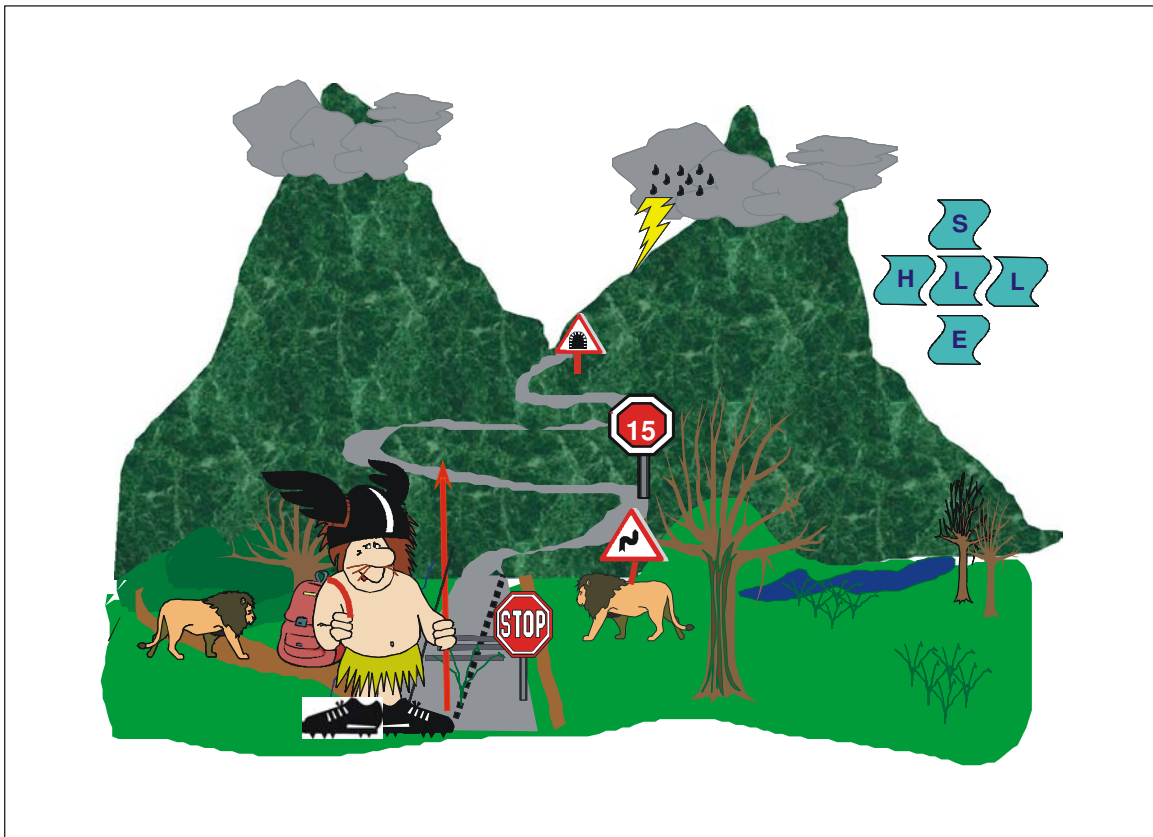
7.5.1 El primer paso para identificar fuentes de vulnerabilidad de la seguridad operacional, especificadas como peligros en las interfaces entre las personas y otros componentes del sistema, es la descripción del sistema. Una vez que el sistema se describe en términos de componentes e interacciones, la segunda etapa es tratar estas vulnerabilidades de la seguridad operacional, especificadas como peligros en las interfaces entre las personas y los otros componentes del sistema, mediante un análisis de los recursos ya presentes en el mismo. El análisis tiene dos objetivos. El primero es identificar las posibles disparidades en las interfaces entre los diferentes componentes identificados en la descripción del sistema. Estas disparidades son las vulnerabilidades de seguridad operacional. El segundo objetivo consiste en identificar los recursos adicionales que podrían considerarse necesarios para suavizar las interfaces rugosas, para ayudar a las personas involucradas en la prestación de servicios en el cumplimiento seguro y eficiente de sus tareas. Este análisis se conoce como análisis de las carencias.

7.5.2 Desde la perspectiva del SMS. Un análisis de carencias es básicamente un análisis de los arreglos de seguridad operacional que ya existen dentro de la organización comparados con los necesarios para el funcionamiento del SMS. El análisis de las carencias es importante porque las estructuras básicas de organización necesarias para comenzar a elaborar un SMS pueden ya existir en la organización: rara vez será necesario construir un SMS a partir de cero debido a que la mayoría de las organizaciones tendrán varias actividades relacionadas a un SMS establecidas y funcionando. La elaboración del SMS debería aprovechar y construirse sobre las estructuras de organización existentes.

7.5.3 Regresando a la Figura 7-2, y teniendo en cuenta que el servicio proporcionado por el sistema es la entrega, por personas, de pequeños paquetes al otro lado de las montañas, veamos un ejemplo de análisis de carencias sencillo. La cuestión rectora para el análisis debería ser: ¿está el personal operacional (en este caso, el cavernícola) que realmente va a prestar el servicio adecuadamente equipado con los recursos necesarios para hacerlo? La respuesta a esta pregunta debe tratar tanto la seguridad operacional (es decir ¿está el personal adecuadamente equipado para prestar el servicio en seguridad?) como la eficiencia (es decir, ¿está el personal adecuadamente equipado para prestar el servicio en forma eficiente?).

7.5.4 El modelo SHELL, analizado en el Capítulo 2, es una herramienta útil para responder a la cuestión y orientar el análisis de las carencias (véase la Figura 7-3). El cavernícola es el elemento humano (L). El camino, el cartel de PARE, el cartel de velocidad y el túnel cerca de la cima del pase montañoso son el soporte físico (H). Los árboles, los leones, las montañas y las nubes son el entorno (E). Aunque no está visible, la instrucción que el cavernícola ha recibido y los procedimientos e instrucciones que debe seguir para prestar el servicio son el soporte lógico (S). Como se indica en la Figura 7-3, el análisis de las carencias produciría los siguientes resultados cuando se le compara con la Figura 7-2:

- a) El cavernícola debe viajar a través de las montañas, por un camino con muchas curvas y probablemente disparejo, pero está descalzo. Por consiguiente puede herirse los pies y experimentar una caída (seguridad operacional) o avanzar a paso lento y, por consiguiente, demorar la entrega de los paquetes (eficiencia). El análisis de las carencias sugiere que sería importante proporcionarle calzado para enfrentar una disparidad en la interfaz entre el cavernícola L y el camino H.
- b) Las nubes en el paso en la cima de las montañas pueden generar lluvia y tormentas. Entonces, proporcionando un sombrero, se protegería al cavernícola y se enfrentaría una disparidad en la interfaz entre el cavernícola (L) y las nubes (E).
- c) Los leones constituyen un claro peligro para el cavernícola y la prestación del servicio. El cartel de PARE es un recurso que ya existe en el sistema, dirigido a alertar al cavernícola con respecto al peligro (es decir ingresar a una zona particularmente peligrosa). No obstante, una herramienta de autodefensa sería un recurso adicional apropiado. Por consiguiente, si se le proporciona una lanza al cavernícola se enfrentaría una disparidad entre el cavernícola (L) y los leones (E).



**Figura 7-3. Análisis de las carencias**

- d) Además del cartel de PARE, líneas amarillas de “espere” pintadas en el camino justo antes de ingresar a la zona particularmente peligrosa aumentarían el conocimiento y llamarían la atención del cavernícola con respecto a los leones, complementando así la lanza como recurso adicional para enfrentar la disparidad entre el cavernícola (L) y los leones (E).
- e) El cavernícola no cuenta con equipo para transportar los pequeños paquetes de modo que sus manos estén libres para manipular la lanza así como para mantener un mejor equilibrio y estabilidad mientras viaja por el áspero y disperejo camino montañoso. Una mochila para llevar los paquetes sería un recurso adicional para enfrentar una disparidad en la interfaz entre el cavernícola (L) y los leones (E) y el cavernícola (L) y el camino (H).
- f) Hay un cartel de velocidad que indirectamente alerta a los viajeros al comienzo del camino ondulante. El cartel de velocidad no transmite un mensaje inequívoco sobre las condiciones del camino. Un cartel de alerta especial y evidente sería un recurso adicional para enfrentar una disparidad en la interfaz entre el cavernícola (L) y el camino (H).
- g) No hay advertencia de que el paso en la cima de las montañas es a través de un túnel. Un cartel en ese sentido sería un recurso adicional para enfrentar la disparidad en la interfaz entre el cavernícola (L) y el camino (H).

7.5.5 Así pues, un análisis de las carencias revela los recursos, estructuras y arreglos de seguridad operacional existentes en el sistema para tratar las vulnerabilidades de seguridad operacional, especificadas en términos de peligro, que surgen como consecuencia de la interacción entre personas y otros componentes del contexto operacional. También revela recursos adicionales, estructuras y arreglos de seguridad operacional que serían necesarias para mitigar las vulnerabilidades de la seguridad operacional y aumentar la resistencia operacional frente a los peligros.

7.5.6 Una vez completado y plenamente documentado el análisis de las carencias, los recursos, estructuras y arreglos que se han identificado como faltantes o deficientes constituirán, conjuntamente con los que ya existen, la base del plan de implantación del SMS. Las organizaciones pueden dar forma a su plan de implantación SMS para adecuarse a sus necesidades individuales; no obstante, un formato de hoja de cálculo, carta Gantt o presentación de tipo MS Project se recomienda para facilitar la visualización y el seguimiento. Cada aspecto será evaluado para determinar cómo la organización creará o modificará políticas, objetivos, procedimientos o procesos para incorporar los componentes y elementos del MS requeridos. En el Apéndice 2 de este capítulo se proporciona un ejemplo de análisis de carencias para proveedores de servicios con preguntas sugeridas para ayudar a la organización a descubrir lo que falta una vez que ha descrito su propio sistema en la organización.

## 7.6 SMS Y QMS

7.6.1 La gestión de la calidad se ha establecido en muchos segmentos del sistema de la aviación desde hace tiempo. Muchas organizaciones aeronáuticas han implantado y operado sistemas de control de calidad (QC) o de garantía de calidad (QA) durante varios años.

7.6.2 Un programa QA define y establece la política y objetivos de calidad de una organización. Asegura que la organización cuenta con los elementos necesarios para mejorar la eficiencia y reducir los riesgos relacionados con el servicio. Si se ha implantado adecuadamente, un QA asegura que los procedimientos se realizan en forma coherente y ajustados a los requisitos aplicables, que los problemas se identifican y resuelven y que la organización examina y mejora continuamente sus procedimientos, productos y servicios. Un QA debería identificar problemas y mejorar procedimientos para satisfacer los objetivos de la empresa.

7.6.3 La aplicación de principios QA a los procesos de gestión de la seguridad operacional contribuye a asegurar que se han adoptado en todo el sistema las medidas de seguridad necesarias para apoyar a la organización en el logro de sus objetivos de seguridad operacional. No obstante, por sí sola la QA no puede, como se propone en el dogma de calidad, "asegurar la seguridad". Es la integración de principios y conceptos de QA en un SMS en el marco del componente de garantía de la seguridad operacional (analizado en el Capítulo 9) lo que ayuda a la organización a asegurar la necesaria normalización de los procesos para lograr el objetivo general de gestionar los riesgos de seguridad operacional de las consecuencias de los peligros que la organización debe enfrentar durante sus actividades relacionadas con la prestación de servicios.

7.6.4 Los principios QA comprenden procedimientos para supervisar la eficacia de todos los aspectos de una organización, incluyendo los siguientes:

- a) diseño y documentación de procedimientos (p. ej., SOP);
- b) métodos de inspección y ensayos;
- c) supervisión de equipo y operaciones;
- d) auditorías internas y externas;

- e) supervisión de medidas correctivas adoptadas; y
- f) uso de análisis estadístico apropiado, cuando sea necesario.

7.6.5 Algunas organizaciones de aviación han integrado sus programas QC y QA en lo que se denomina sistemas de gestión de la calidad (QMS). Actualmente se aplican varias normas de aceptación internacional con respecto a la garantía de calidad. Las normas elegidas dependen del volumen, complejidad y del producto de la organización. Por ejemplo, la norma ISO 9001-2000 es un conjunto de normas internacionales elaboradas por la ISO y aplicadas por muchas organizaciones para implantar un sistema interno de gestión de la calidad. El uso de tales sistemas también asegura que los proveedores o contratistas de la organización han introducido sistemas apropiados de gestión de la calidad.

7.6.6 En vista de la larga historia de QA/QC en la aviación, la relativa juventud de los SMS y el hecho de que los procesos específicos del SMS se nutren de principios de calidad, el potencial para errores de percepción y malentendidos con respecto a la relación entre el SMS y el QMS es real. Es entonces esencial definir esta relación desde una perspectiva sinérgica y no antagónica, así como la contribución relativa del SMS y del QMS al logro de los objetivos generales de la organización y, en particular, los de seguridad operacional.

7.6.7 Es exacto decir que el SMS y el QMS tienen muchos aspectos comunes. Ambos:

- a) deben planificarse y administrarse;
- b) dependen de mediciones y supervisión;
- c) involucran cada función, proceso y persona de la organización; y
- d) procuran lograr mejoramiento continuo.

7.6.8 Debido a que el SMS y QMS tienen muchas cosas en común, puede haber una tendencia a suponer que una organización que ha establecido y aplica un QMS no necesita, o ya tiene, un SMS. No obstante, en la misma manera que el SMS y el QMS tienen aspectos comunes, existen importantes diferencias entre ambos, así como carencias en la efectividad del QMS para lograr por sí mismo el objetivo general de gestionar los riesgos de seguridad operacional de las consecuencias de los peligros que la organización debe enfrentar durante las actividades relacionadas con la prestación de los servicios.

7.6.9 La gestión de la calidad fue introducida en la década de 1960, cuando la comprensión de la actuación humana, los factores de organización y sus consecuencias para la seguridad operacional estaba mucho menos desarrollada que actualmente. Por consiguiente, a pesar de las modificaciones y continua actualización con el tiempo, la gestión de la calidad es menos efectiva en la identificación de problemas de alto nivel/consecuencias graves, como el complejo camino de las fallas latentes, que pueden conducir al desastre. Además, el carácter burocrático de las auditorías y el proceso de lograr una acreditación de calidad oficial tienen el potencial de transformarse en un fin en sí mismo: el objetivo de colgar un cartelito con la acreditación ISO en la entrada de la sede de una empresa puede distraer a la misma respecto de la generación de prácticas de seguridad operacional y hacer que pierda su foco de atención, en el sentido de la seguridad operacional.

7.6.10 El SMS se concentra en la actuación humana, los factores humanos y los factores de organización, e integra en éstos, según corresponda, técnicas y procesos de gestión de la calidad para contribuir al logro de la satisfacción de la seguridad operacional. El objetivo del SMS es identificar los peligros de seguridad que la organización debe enfrentar, y que en muchos casos genera ella misma, durante la prestación de servicios, así como llevar bajo control de la organización los riesgos de seguridad operacional de las consecuencias de estos peligros. En términos generales, el primer imperativo de este objetivo – identificación de peligros – se logra mediante el componente de gestión de los riesgos de seguridad operacional del SMS (que se analiza en el Capítulo 9), y que se basa en principios

y prácticas de gestión de la seguridad operacional. El segundo imperativo – llevar los riesgos de seguridad bajo control de la organización – se logra mediante el componente de garantía de la seguridad operacional del SMS (también se analiza en el Capítulo 9), que se basa en la integración de principios y prácticas de seguridad operacional y gestión de la calidad.

7.6.11 En resumen, el SMS difiere del QMS en que:

- a) el SMS se concentra en la seguridad operacional, los aspectos humanos y los aspectos organizativos de una organización (es decir la satisfacción de la seguridad); mientras que
- b) el QMS se concentra en los productos y servicios de una organización (es decir la satisfacción del cliente).

7.6.12 Una vez establecidos los aspectos comunes y las diferencias entre el SMS y el QMS, es posible establecer una relación sinérgica entre ambos sistemas. Es fundamental considerar que la relación es complementaria, nunca antagonica, y que puede resumirse como sigue:

- a) el SMS se nutre parcialmente en los principios del QMS;
- b) el SMS debería incluir tanto las políticas y prácticas de seguridad como las de calidad; y
- c) la integración de los principios, políticas y prácticas de calidad, por lo que hace al SMS, debería concentrarse en el apoyo a la gestión de la seguridad operacional.

7.6.13 El establecimiento de una relación complementaria entre el SMS y el QMS lleva a las contribuciones complementarias de cada sistema al logro de los objetivos de seguridad de la organización:

- a) el SMS resulta en el diseño e implantación de procesos y procedimientos de organización para identificar los peligros para la seguridad y sus consecuencias y llevar bajo control de la organización los riesgos de seguridad conexos en las operaciones de aviación;
- b) la integración del QMS en el SMS proporciona un enfoque estructurado para supervisar que los procedimientos y procesos para identificar peligros de seguridad y sus consecuencias y llevar los riesgos de seguridad conexos de las operaciones de aviación bajo el control de la organización, funcionan como fuera previsto y, cuando no lo hacen, mejorarlos.

7.6.14 Cabe señalar que los SARPS de la OACI sobre gestión de la seguridad operacional incluidos en los Anexos 1, 6, 8, 11 y 14, que se analizaron en el Capítulo 6, se limitan al SMS. No hay requisitos de la OACI en los Anexos mencionados con respecto al QMS, con la sola excepción de un requisito de contar con organismos de mantenimiento reconocidos (AMO) en el Anexo 6, Parte I, Capítulo 8.

## 7.7 SSP/SMS Y EL PROCESO DE INVESTIGACIÓN DE ACCIDENTES

7.7.1 Al igual que con la relación entre el SMS y el QMS, la relación entre el SSP o el SMS, y el proceso de investigación de accidentes y la función que este desempeña en un entorno de gestión de la seguridad operacional, ha sido objeto de debate dentro de la comunidad de seguridad. Aunque los debates se han concentrado principalmente en la relación entre el SMS y el proceso de investigación de accidentes, el SSP incuestionablemente debe ser parte del debate. Al igual que con la relación entre el SMS y el QMS, es fundamental afirmar enfáticamente que la relación entre SSP/SMS y el proceso de investigación de accidentes es de carácter absolutamente complementario y sinérgico. La investigación de accidentes es una herramienta esencial del proceso de gestión de la seguridad operacional.

7.7.2 En el marco del proceso de gestión de la seguridad operacional, las actividades diarias involucradas en la gestión de la seguridad como otro proceso de organización, según se analiza en el Capítulo 3, son realizadas por el SSP o el SMS de la organización. Un accidente (o incidente grave) representa la falla final del SSP o del SMS (o de ambos), en cuanto sistemas de gestión que orientan las actividades necesarias para gestionar la seguridad operacional en un Estado o en una organización, respectivamente. Cuando ocurre dicha falla final, se pone en movimiento el proceso de investigación de accidentes para encontrar las razones de la falla de las actividades de gestión de la seguridad y generar las contramedidas necesarias para que estas no se repitan. Entonces, en un entorno de gestión de la seguridad operacional, el proceso de investigación de accidentes tiene una función clara. Es el custodio final de la seguridad en el sistema de aviación, que se pone en marcha cuando han fallado todas las defensas, barreras, verificaciones y contrapesos de seguridad operacional en el sistema.

## 7.8 INTEGRACIÓN DE LOS SISTEMAS DE GESTIÓN

7.8.1 Las organizaciones de aviación se describen con frecuencia como “un sistema de sistemas”. Esto se debe a que las organizaciones de aviación deben elaborar, implantar y operar varios sistemas de gestión diferentes para lograr sus objetivos de producción a través de la prestación de servicios. Los sistemas de gestión típicos que una organización de aviación puede tener que explotar comprenden:

- a) sistema de gestión de la calidad (QMS);
- b) sistema de gestión del medio ambiente (EMS);
- c) sistema de gestión de seguridad y salud laboral (OHSMS);
- d) sistema de gestión de la seguridad operacional (SMS); y
- e) sistema de gestión de la seguridad de la aviación (aeroportuaria) (SEMS).

7.8.2 Existe una tendencia en la aviación civil a integrar los diferentes sistemas de gestión. Existen claras ventajas en tal integración:

- a) reduce la duplicación y por lo tanto los costos;
- b) reduce los riesgos generales de la organización y fomenta los beneficios;
- c) equilibra los conflictos potenciales de objetivos;
- d) elimina los potenciales conflictos de responsabilidad e interrelaciones; y
- e) diluye los sistemas de poder.

7.8.3 No obstante, hay diferentes maneras de integrar todos estos sistemas y, en particular, de integrar el SMS con otros sistemas de gestión en la organización. Debería alentarse a las organizaciones de aviación a que integraran sus sistemas de gestión, calidad, seguridad operacional, seguridad aeroportuaria, salud y seguridad laborales y protección del medio ambiente. No obstante, esta integración por el momento está más allá del alcance de los SARPS normalizados de la OACI sobre gestión de la seguridad operacional y de este manual.



## 7.9 ACLARACIÓN DE TÉRMINOS

Es importante elaborar una comprensión común de la terminología empleada en relación con las distintas actividades de gestión de la seguridad operacional que se realizan bajo la responsabilidad de los proveedores de servicios o de las autoridades supervisoras de la aviación civil. Cuando en este manual se utilizan los términos siguientes, tienen los significados que se indican:

- a) **vigilancia de la seguridad operacional** es la actividad que realiza el Estado con respecto al SMS de los explotadores/proveedores de servicios;
- b) **garantía de la seguridad operacional** es la actividad que el Estado realiza con respecto a la eficacia de la seguridad operacional de su SSP y que los explotadores/proveedores de servicios realizan con respecto a la eficacia de la seguridad operacional de sus SMS, comprendiendo la supervisión y la medición; y
- c) **auditoría de la seguridad operacional** es la actividad que realiza el Estado con respecto a la estructura de su SSP y que los explotadores y proveedores de servicios realizan con respecto a la estructura de sus SMS.

*Nota.— Auditoría de la vigilancia de la seguridad operacional es la actividad que realiza el USOAP de la OACI con respecto al programa estatal de seguridad operacional (SSP) de la AAC y sus capacidades de vigilancia de la seguridad operacional con arreglo a los SARPS de la OACI y textos de orientación conexos.*

## 7.10 DIFERENCIA ENTRE CONSIGNAS DE SEGURIDAD OPERACIONAL Y PRINCIPIOS DE SEGURIDAD OPERACIONAL

7.10.1 Existe una tendencia establecida desde hace mucho tiempo en la aviación a basarse en consignas para despertar la conciencia sobre los problemas de seguridad operacional, tendencia que a menudo confunde consignas con principios. Existe una gran diferencia entre consignas y principios. Estos últimos enuncian claramente orientaciones precisas basadas en conocimientos sólidos y proporcionan declaraciones globales sobre cómo realizar una tarea particular. Las consignas articulan referencias oblicuas que se basan en creencias populares convencionales y a veces cuestionables (conocimiento tradicional) y, muy a menudo son representaciones engañosas de cómo enfrentar un problema. Parecería totalmente irracional realizar una tarea crítica como la gestión de la seguridad operacional y la introducción de un SSP/SMS sobre la base de “consignas”. No obstante, existe la posibilidad de que ello suceda. En esta sección se examinan y se presentan para desacreditarlas, principalmente mediante la aplicación de los conceptos básicos de seguridad operacional y su gestión analizados en los Capítulos 2 y 3, cinco de las consignas de seguridad operacional más apreciadas en la aviación:

- a) En la aviación, la seguridad operacional es lo primero.
- b) La seguridad operacional es responsabilidad de todos.
- c) Si no está roto ¿por qué repararlo?
- d) Si cree que la seguridad operacional es costosa, haga la prueba con un accidente.
- e) El 70 % de los accidentes se debe a errores humanos.

7.10.2 **En la aviación, la seguridad operacional es lo primero.** Las organizaciones de sistemas de producción se forman para lograr, como el nombre claramente lo sugiere, algún objetivo de producción, como la fabricación de automóviles, la extracción de petróleo o, en el caso de la aviación comercial, el transporte de personas y mercancías

por vía aérea. Las organizaciones de los sistemas de producción necesitan hacer dinero como consecuencia de sus actividades, de modo de poder asegurar los recursos necesarios para continuar procurando sus objetivos de producción. Por consiguiente, es difícil ver cómo la seguridad operacional podría ser la primera prioridad de la aviación; más bien se pensaría que el dinero es lo primero. Según se analiza en el Capítulo 2, la seguridad operacional en la aviación es cuestión de una jerarquización sensata y coordinada de objetivos de producción y de protección, de modo que las organizaciones aeronáuticas puedan obtener ganancias en condiciones de seguridad. No obstante, la confusión de prioridades que representa esta consigna ha conducido en ocasiones a conductas aberrantes. En realidad, el argumento presentado con mayor frecuencia por las organizaciones disfuncionales cuando les sobrevienen sucesos adversos es que, a pesar de toda evidencia en contrario, no pueden comprender cómo es que les pueda haber sucedido el mal resultado en cuestión dado que “en nuestra compañía, la seguridad es lo primero”. Existe todo un historial en el sentido de que las organizaciones que se han ocultado detrás de esta consigna, y no la han apoyado con medidas apropiadas, se encuentran entre los peores transgresores en materia de seguridad operacional.

7.10.3 **La seguridad operacional es responsabilidad de todos.** Esta consigna es algo desconcertante. Cuando uno se siente enfermo, visita al médico. Cuando uno necesita asesoramiento jurídico, consulta a un abogado. Si el agua no sale del grifo, se llama al plomero. No obstante, cuando se enfrentan problemas de seguridad operacional, todos en la aviación se consideran expertos en la materia. En particular si tienen algunos años de experiencia en la industria. La verdad es que sólo los especialistas capacitados pueden tratar los problemas actuales de seguridad operacional en una forma efectiva, eficiente y pertinente al contexto. Las organizaciones mejor manejadas en la aviación han dedicado personal de seguridad operacional, profesionalmente cualificados con descripciones específicas de sus tareas y con responsabilidades definidas y acceso a toda la organización. Estos profesionales asumen la responsabilidad como supervisores de seguridad operacional de la organización. Coordinan planes para evaluar y reforzar la resistencia intrínseca de la organización frente a los posibles peligros inherentes a la aviación, para que el resto del personal los aplique. No acusan puntualmente cuando descubren peligros y problemas de seguridad no tratados, sino que preparan la documentación y descripción de los problemas, como prerrequisito para la elaboración de soluciones. En el Capítulo 8 se presentan estas ideas con mayor profundidad.

7.10.4 **Si no está roto ¿por qué repararlo?** Esta consigna propone que no hay necesidad de preocuparse por la seguridad operacional mientras no haya accidentes, que el sistema es seguro en la medida que las personas no se lastimen, los metales no se doblen y la organización no se vea expuesta a críticas y situaciones embarazosas. En otras palabras, la consigna propone que los accidentes, o la ausencia de ellos, son indicadores fiables de la seguridad operacional de un sistema. Otra variante de esta forma de pensar propone que, si se cuenta con estructuras y procesos basados en conocimientos modernos para mantener al sistema bajo continua vigilancia para detectar signos de peligro, los accidentes son un desafortunado “ruido en el sistema”. Más allá de otras falsedades inherentes a esta consigna, según se analizó en el Capítulo 3, el esperar hasta que el sistema se descomponga antes de intentar resolver las deficiencias de seguridad puede resultar oneroso más allá de lo razonable. Además, cuando el sistema se descompone, las vidas humanas están en juego, lo que plantea cuestiones éticas en relación con este enfoque. Dado que los costos financieros y humanos relacionados con la adopción de medidas correctivas sólo después de experimentar un accidente son inevitablemente elevados, existen imperiosas razones económicas y éticas para reparar el sistema antes de que se rompa.

7.10.5 **Si cree que la seguridad operacional es costosa, haga la prueba con un accidente.** La creencia popular reflejada por esta consigna es que es posible prever todas las fallas del sistema que puedan conducir eventualmente a accidentes, concretamente observando el comportamiento profesional, ejerciendo disciplina y cumpliendo las reglas. En términos sencillos, el cumplimiento de los reglamentos y “aplicar el librito” son suficiente garantía para la seguridad operacional. Lamentablemente, como ilustra la deriva práctica analizada en el Capítulo 3, el mundo real no funciona así. Una vez introducidas las estructuras y procesos modernos, los accidentes, al igual que las enfermedades y la muerte, son en última instancia asunto de estadística. Aunque es posible, y sensato, realizar verificaciones proactivas de la actuación del sistema y adoptar conductas proactivas, de la misma forma que los humanos visitan a sus médicos de familia y participan en programas de acondicionamiento físico, es imposible eliminar todos los peligros. Los peligros son componentes integrales de los contextos operacionales de la aviación. Las fallas y los errores operacionales ocurrirán en la aviación, a pesar de los esfuerzos mejores y más logrados para evitarlos.

Una organización eficiente, con personal cualificado y equipada con recursos conmensurables con sus objetivos de producción y con procedimientos bien diseñados puede tener de todas maneras un accidente, mientras que una organización mal administrada y con graves carencias de recursos, con personal dudosamente cualificado, prácticas subnormales y un historial de “escapadas por un pelo”, puede lograr evitar un accidente sencillamente por pura suerte.

7.10.6 **El 70% de los accidentes se debe a errores humanos.** Esta consigna ha sido dejada para el final porque muestra claramente cuan engañosas pueden ser las consignas de seguridad. Consideremos el sistema de la aviación: los humanos conciben el plan del sistema y, una vez satisfechos con lo que han concebido, se dedican a diseñarlo. Luego los humanos construyen el sistema y cuando el sistema está funcional, los humanos lo hacen trabajar. A fin de mostrar el comportamiento necesario para conseguir los objetivos del sistema, los humanos capacitan a otros humanos para hacer que el sistema trabaje día tras día. Los humanos adoptan decisiones estratégicas y tácticas sobre la actuación del sistema, y cuando se identifican peligros, los humanos elaboran e introducen las contramedidas necesarias para proteger al sistema de tales peligros. En términos sencillos, los humanos diseñan, fabrican, capacitan, operan, gestionan y defienden el sistema. Por consiguiente, cuando el sistema falla, se debe necesariamente a un error humano. Desde esta perspectiva, y dependiendo del nivel de observación, es claro que el 100% de los accidentes se debe a errores humanos.

---



## Apéndice 1 del Capítulo 7

# ORIENTACIÓN SOBRE DESCRIPCIÓN DEL SISTEMA

### 1. INTRODUCCIÓN

1.1 La descripción del sistema es un primer prerrequisito para la elaboración de un SMS en una organización. Todo sistema contiene posibles vulnerabilidades de seguridad operacional inherentes, que se caracterizan en términos de peligros. El proceso de identificación de peligros puede determinar sólo aquellos peligros que entran en el ámbito de la descripción del sistema. Los límites del sistema, con arreglo a su descripción formal, deben por lo tanto ser lo suficientemente amplios como para abarcar todos los posibles peligros que el sistema podría enfrentar o generar. En particular, es importante que la descripción comprenda las interfaces dentro del sistema, así como las interfaces con los sistemas mayores de los cuales el sistema considerado es parte.

1.2 Una descripción detallada del sistema debería incluir:

- a) el propósito del sistema;
- b) cómo se utilizará el sistema;
- c) las funciones del sistema;
- d) los límites y las interfaces externas del sistema; y
- e) el entorno en que funcionará el sistema.

1.3 Las consecuencias para la seguridad de una potencial pérdida o deterioro del sistema estarán determinadas, en parte, por las características del entorno operacional en que el sistema se integrará. Por consiguiente, la descripción del entorno debería incluir todos los factores que puedan tener consecuencias significativas para la seguridad operacional. Estos factores variarán de una organización a otra. Podrían comprender, por ejemplo, características de tránsito aéreo y terrestre, infraestructura de aeródromos y factores relacionados con las condiciones meteorológicas. La descripción del sistema debería también tratar procedimientos de contingencia y otras operaciones no normales, por ejemplo, fallas de comunicaciones o de ayudas de navegación. A continuación se detalla un ejemplo de descripción de sistema de un aeródromo.

### 2. DESCRIPCIÓN DEL SISTEMA DE UN AERÓDROMO

La descripción del sistema de un aeródromo debería incluir instalaciones y servicios, equipo, personal, procesos y procedimientos necesarios para el funcionamiento del aeródromo. Las diferentes funciones pueden comprender:

#### 1. Gestión operacional

##### 1.1 Control de acceso al área de movimientos

- a) Aéreo
- b) Terrestre
- c) Marítimo

- 1.2 Planificación para emergencias en el aeródromo
  - a) Manual de procedimientos de emergencia
  - b) Prácticas de simulación de emergencias
- 1.3 Salvamento y extinción de incendios
  - a) Capacidad
    - 1) Equipo
    - 2) Velocidad de descarga de espuma/agua/polvo seco
  - b) Mantenimiento de la instalación
  - c) Instrucción y experiencia del personal
  - d) Plan de movilización de equipo
  - e) Reducción de capacidad (aviso)
  - f) Sistema de hidrantes
- 1.4 Inspección y mantenimiento del área de movimientos
  - a) Manual del aeródromo
  - b) Formularios de inspección
  - c) Mantenimiento
- 1.5 Mantenimiento de ayudas visuales
  - a) Inspecciones
  - b) Cronograma
- 1.6 Gestión de la construcción
  - a) Control de obras
  - b) Gestión del sitio
- 1.7 Gestión de la seguridad operacional en la plataforma, incluyendo tránsito de vehículos
  - a) Reglas y reglamentos para operaciones en la parte aeronáutica
  - b) Gestión de la parte aeronáutica
    - 1) Gestión de vehículos en la parte aeronáutica
    - 2) Licencia de vehículos en la parte aeronáutica
    - 3) Examen de vehículos
    - 4) Especificaciones de seguridad operacional
    - 5) Coordinación de servicios a las aeronaves
  - c) Estacionamiento de equipo
  - d) Disciplina en la plataforma
  - e) Operaciones de empuje o remolque
  - f) Carteles y señales de tránsito
  - g) Asignación de puestos de estacionamiento
  - h) Control de daños a aeronaves
  - i) Control de derrames de combustible
  - j) Control de daños a vehículos y equipo
  - k) Listas de verificación de seguridad operacional en la plataforma, incluyendo auditoría de las actividades en rampa
  - l) Actividades contratadas y subcontratadas

- 1.8 Gestión de peligros de la fauna
  - a) Gestión del control aviario
  - b) Observación
  - c) Gestión de informes de choques con aves
- 1.9 Control de obstáculos
  - a) Límites del aeropuerto
  - b) Fuera del aeropuerto
  - c) Franja de pista
  - d) Reglamentación y encuesta
  - e) Aprobación de construcción de edificios debajo de la trayectoria de vuelo
- 1.10 Retiro de aeronaves inutilizadas
  - a) Equipo compatible con el tipo de aeronave
  - b) Mantenimiento para estado de preparación
  - c) Plan de ejecución
  - d) Establecimiento de procedimientos/contactos de contratación externa
- 1.11 Tramitación de mercancías peligrosas
  - a) Limitación de las mercancías peligrosas en las aeronaves
  - b) Almacenamiento y carga
  - c) Establecimiento del programa de instrucción
  - d) Aceptación de mercancías peligrosas por los explotadores
  - e) Guía de respuesta ante emergencias para incidentes de aeronaves que entrañen mercancías peligrosas
- 1.12 Operaciones con poca visibilidad y condiciones meteorológicas adversas
  - a) Procedimientos
  - b) Coordinación con los servicios de tránsito aéreo
  - c) Responsabilidad de las organizaciones involucradas
- 1.13 Instalaciones y mantenimientos de radioayudas para la navegación
  - a) NOTAM
- 2. Gestión de aeródromos
  - 2.1 Negociación y asignación de turnos
  - 2.2 Despacho de vuelo
  - 2.3 Orientación para camión-guía y señales para maniobrar en tierra
  - 2.4 Gestión del área de movimientos y asignación de puestos de parada
  - 2.5 Operaciones de CAT II y CAT III con poca visibilidad
  - 2.6 Control de las reglas de tránsito y reglamentos de otorgamiento de licencias
  - 2.7 Limpieza, eliminación de desechos y control de plagas

3. Gestión del edificio de pasajeros/terminal
    - 3.1 Gestión de pasajeros, movimiento de equipaje e instalaciones y servicios
    - 3.2 Información a los pasajeros e información pública
    - 3.3 Asistencia a VIP y CIP
    - 3.4 Equipaje abandonado
    - 3.5 Ayuda de changadores
    - 3.6 Gestión de los carritos
    - 3.7 Limpieza y control de plagas
  
  4. Servicios de tránsito aéreo, información aeronáutica y comunicaciones
    - 4.1 Control del tránsito aéreo (control del aeródromo en operaciones con poca visibilidad)
    - 4.2 Servicios de información de vuelo y alerta
    - 4.3 Servicios de información aeronáutica (oficina NOTAM internacional y servicio de información previa al vuelo)
    - 4.4 Servicios de telecomunicaciones aeronáuticas
  
  5. Gestión de la seguridad operacional y la seguridad de la aviación
    - 5.1 Implantación y supervisión del SMS
      - a) Gerente de seguridad operacional
      - b) Identificación de peligros y evaluación de las consecuencias
      - c) Evaluación, control y mitigación de los riesgos
      - d) Garantía de seguridad operacional
      - e) Grupos de acción de seguridad operacional
      - f) Manual de sistemas de gestión de la seguridad operacional (SMSM)
  
    - 5.2 Implantación y supervisión del programa de seguridad de la aviación
    - 5.3 Implantación y supervisión del plan de emergencia de aeródromo (AEP)
    - 5.4 Procesamiento de solicitudes para la expedición de tarjetas de acceso
-



## Apéndice 2 del Capítulo 7

# ORIENTACIÓN SOBRE LA ELABORACIÓN DE UN ANÁLISIS DE CARENCIAS DEL SMS PARA PROVEEDORES DE SERVICIOS

*Nota.— En el contexto de este apéndice, el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye a las organizaciones de instrucción reconocidas que están expuestas a los riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados, según corresponda.*

### 1. ANÁLISIS DE LAS CARENCIAS

1.1 La implantación de un SMS exige que el proveedor de servicios realice un análisis de su sistema para determinar qué componentes y elementos del SMS están ya introducidos y cuáles son los componentes y elementos que deben añadirse o modificarse para satisfacer los requisitos de implantación. Este análisis se conoce como análisis de las carencias e involucra comparar los requisitos SMS con los recursos existentes del proveedor de servicios.

1.2 El análisis de las carencias proporciona, en formato de lista de verificación, información para ayudar a evaluar los componentes y elementos que integran el marco de la OACI para SMS e identificar los componentes y elementos que será necesario desarrollar. Una vez completado y documentado, el análisis de las carencias constituirá una de las bases del plan de implantación del SMS.

### 2. MARCO PARA SMS DE LA OACI

El marco para SMS de la OACI comprende cuatro componentes y doce elementos, y su implantación será directamente proporcional al tamaño de la organización y a la complejidad de sus servicios.

1. Política y objetivos de seguridad operacional
  - 1.1 Responsabilidad y compromiso de la administración
  - 1.2 Responsabilidades respecto de la seguridad operacional
  - 1.3 Designación del personal clave de seguridad operacional
  - 1.4 Coordinación del plan de respuesta ante emergencias
  - 1.5 Documentación SMS
2. Gestión de riesgos de seguridad operacional
  - 2.1 Identificación de peligros
  - 2.2 Evaluación y mitigación de riesgos de seguridad operacional

3. Garantía de la seguridad operacional
  - 3.1 Supervisión y medición de la eficacia de la seguridad operacional
  - 3.2 Gestión del cambio
  - 3.3 Mejora continua del SMS
4. Promoción de la seguridad operacional
  - 4.1 Instrucción y educación
  - 4.2 Comunicación de la seguridad operacional.

### 3. ANÁLISIS DE LAS CARENCIAS DEL SMS PARA PROVEEDORES DE SERVICIOS

La siguiente lista de verificación para el análisis de las carencias puede utilizarse como modelo para realizar un análisis de carencias. Cada pregunta está diseñada para obtener una respuesta de “Sí” o “No”. Una respuesta “Sí” indica que el proveedor de servicios ya ha incorporado a su sistema el componente o elemento del marco SMS de la OACI en cuestión y que éste se ajusta o supera al requisito. Una respuesta “No” indica que existe una carencia entre el componente/elemento del marco SMS de la OACI y el sistema del proveedor de servicios.

<i>Referencia de la OACI</i>	<i>Aspecto que ha de analizarse o pregunta que ha de contestarse</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
<b>Componente 1 — POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL</b>			
<b>Elemento 1.1 — Responsabilidad y compromiso de la administración</b>			
Capítulo 8	¿Se ha introducido y se aplica una política de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3 y 8	¿Refleja la política de seguridad operacional los compromisos de la organización con respecto a la gestión de la seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3 y 8	¿Incluye la política de seguridad operacional una declaración clara sobre la provisión de los recursos necesarios para la implantación de la política de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3 y 8	¿Incluye la política de seguridad operacional los procedimientos de notificación de la seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Indica claramente la política de seguridad operacional cuáles son los tipos de comportamientos operacionales que resultan inaceptables?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Incluye la política de seguridad operacional las condiciones en las cuales no se aplicarían medidas disciplinarias?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Está la política de seguridad operacional firmada por el Ejecutivo responsable?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se comunica la política de seguridad operacional, con visible endoso, a toda la [organización]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se examina periódicamente la política de seguridad operacional para asegurar que sigue siendo pertinente y apropiada para la [organización]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

Referencia de la OACI	Aspecto que ha de analizarse o pregunta que ha de contestarse	Respuesta	Estado de implantación
Capítulo 8	¿Existe un proceso formal para elaborar un conjunto coherente de objetivos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Están los objetivos de seguridad operacional relacionados con los indicadores de eficacia de la seguridad operacional, los objetivos de eficacia de la seguridad operacional y los planes de acción?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se publican y distribuyen los objetivos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 1.2 — Responsabilidades respecto de la seguridad operacional</b>			
Capítulos 8 y 10	¿Ha identificado la [organización] un Ejecutivo responsable quien, independientemente de otras funciones, tendrá la responsabilidad final y rendirá cuentas, en nombre de la [organización], de la implantación y mantenimiento del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Tiene el Ejecutivo responsable responsabilidad para asegurar que el sistema de gestión de la seguridad operacional está adecuadamente implantado y funciona con arreglo a los requisitos en todos los sectores de la [organización]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Tiene el Ejecutivo responsable control completo de los recursos financieros necesarios para las operaciones cuya realización se ha autorizado en el marco de un certificado de operaciones?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Tiene el Ejecutivo responsable control completo de los recursos humanos necesarios para las operaciones cuya realización se ha autorizado en el marco del certificado de operaciones?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Tiene el Ejecutivo responsable responsabilidad directa por la realización de las actividades de la organización?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Tiene el Ejecutivo responsable autoridad final con respecto a las operaciones cuya realización se ha autorizado en el marco del certificado de operaciones?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 8 y 10	¿Ha identificado la organización las líneas de rendición de cuentas de todos los miembros de la administración, independientemente de otras funciones, así como la de los empleados, con respecto a la eficacia de la seguridad operacional del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se documentan y comunican en toda la [organización] las responsabilidades, rendición de cuentas y autoridades de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Ha incluido la [organización] una definición de los niveles de administración con autoridad para tomar decisiones con respecto a la aceptabilidad de los riesgos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 1.3 — Designación del personal clave de seguridad operacional</b>			
Capítulo 8	¿Ha designado la organización una persona cualificada para gestionar y supervisar el funcionamiento diario del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Cumple la persona que supervisa el funcionamiento del SMS las funciones y responsabilidades requeridas de su cargo?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Están definidas y documentadas las facultades, responsabilidades y rendición de cuentas de seguridad operacional del personal a todos los niveles de la organización?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

<i>Referencia de la OACI</i>	<i>Aspecto que ha de analizarse o pregunta que ha de contestarse</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
<b>Elemento 1.4 — Coordinación del plan de respuesta ante emergencias</b>			
Capítulo 8	¿Cuenta la [organización] con un plan de respuestas ante emergencias/plan de contingencia apropiado al tamaño, carácter y complejidad de la organización?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Coordina la [organización] sus procedimientos de respuesta ante emergencias/contingencias con los procedimientos de respuesta ante emergencias/contingencias de otras organizaciones con las que debe interrelacionarse durante la prestación de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Cuenta la [organización] con un proceso para distribuir y comunicar los procedimientos de coordinación al personal involucrado en dicha interacción?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 1.5 — Documentación SMS</b>			
Capítulos 4 y 8	¿Ha elaborado y mantiene la [organización] una biblioteca de seguridad operacional para la documentación sobre peligros y la gestión de la documentación?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 4 y 8	¿Ha elaborado y mantiene la [organización] documentación SMS en papel o formato electrónico?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 7, 8 y 10	¿Se ha elaborado la documentación SMS para que describa el SMS y las interrelaciones consolidadas entre todos los componentes del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 8 y 10	¿Ha elaborado el proveedor de servicios un plan de implantación del SMS que asegure que el SMS satisface los objetivos de seguridad operacional de la organización?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 8 y 10	¿Se ha elaborado el plan de implantación SMS por una persona o por un grupo de planificación que comprenda una base de experiencia apropiada?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 8 y 10	¿Ha recibido la persona o grupo de planificación recursos suficientes (incluyendo tiempo para reuniones) para la elaboración del plan de implantación SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Está endosado el plan de implantación SMS por la administración superior de la [organización]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Es revisado regularmente el plan de implantación SMS por la administración superior de la [organización]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 8 y 10	¿Propone el plan de implantación SMS la introducción del SMS en fases?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Trata explícitamente el plan de implantación SMS la coordinación entre el SMS del proveedor de servicios y el SMS de otras organizaciones con las cuales la [organización] debe interactuar durante la prestación de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Ha elaborado el proveedor de servicios un manual de sistemas de gestión de la seguridad operacional (SMSM) como instrumento básico para comunicar a toda la [organización] el enfoque de seguridad operacional de la misma?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se documentan en el SMSM todos los aspectos del SMS comprendidos, entre otros, la política de seguridad operacional, sus objetivos, procedimientos y responsabilidades individuales de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

Referencia de la OACI	Aspecto que ha de analizarse o pregunta que ha de contestarse	Respuesta	Estado de implantación
Capítulo 8	¿Articula claramente el SMSM la función de la gestión del riesgo de seguridad operacional como una actividad del diseño inicial y la función de la garantía de seguridad operacional como actividad continua?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se han incorporado partes pertinentes de la documentación relacionada con el SMS en la documentación aprobada, como el manual de operaciones de la compañía, manual de control/política de mantenimiento y manual de operaciones aeroportuarias, según corresponda?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Cuenta el proveedor de servicios con un sistema de registros que asegure la generación y conservación de todos los registros necesarios para documentar y apoyar los requisitos operacionales?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Se ajusta el sistema de registros del proveedor de servicios a los requisitos normativos aplicables y mejores prácticas industriales?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 8	¿Proporciona el sistema de registros los procesos de control necesarios para asegurar la apropiada identificación, legibilidad, almacenamiento, protección, archivo, recuperación, tiempo de retención y disposición de los registros?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Componente 2 — GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL</b>			
<b>Elemento 2.1 — Identificación de peligros</b>			
Capítulos 3 y 9	¿Tiene la [organización] un sistema formal de recopilación y procesamiento de datos de seguridad operacional (SDCPS) para la eficaz recolección de información sobre peligros en las operaciones?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3, 4 y 9	¿Incluye el SDCPS de la [organización] una combinación de métodos reactivos, proactivos y predictivos para recoger datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3, 9 y 10	¿Cuenta la [organización] con procesos reactivos que permitan la captación de información pertinente a la gestión de la seguridad operacional y de los riesgos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 9 y 10	¿Ha desarrollado el proveedor de servicios un sistema de instrucción pertinente a métodos reactivos de recolección de datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 9 y 10	¿Ha desarrollado el proveedor de servicios un sistema de comunicaciones pertinente a los métodos reactivos de recolección de datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Es la notificación reactiva sencilla, accesible y conmensurable con el tamaño del proveedor de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 9 y 10	¿Se examinan los informes reactivos al nivel apropiado de la administración?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un proceso de retroinformación para notificar a los contribuyentes que sus informes se han recibido y compartir los resultados de los análisis?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3, 9 y 10	¿Cuenta el proveedor de servicios con procesos proactivos que busquen activamente identificar los riesgos de seguridad operacional mediante el análisis de las actividades de la organización?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

<i>Referencia de la OACI</i>	<i>Aspecto que ha de analizarse o pregunta que ha de contestarse</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
Capítulos 9 y 10	¿Existe instrucción pertinente a los métodos proactivos de recolección de datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 9 y 10	¿Ha elaborado el proveedor de servicios un sistema de comunicación pertinente a los métodos proactivos de recolección de datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Es la notificación proactiva sencilla, accesible y conmensurable con el tamaño del proveedor de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 3, 9 y 10	¿Cuenta el proveedor de servicios con procesos predictivos que permitan la captación de la eficacia del sistema en las operaciones normales en tiempo real?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 9 y 10	¿Existe instrucción pertinente a los métodos predictivos de recolección de datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Ha elaborado el proveedor de servicios un sistema de comunicación pertinente a los métodos predictivos de recolección de datos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Es el proceso predictivo de captación de datos de seguridad operacional conmensurable con el tamaño del proveedor de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 2.2 — Evaluación y mitigación de riesgos de seguridad operacional</b>			
Capítulos 9 y 10	¿Ha elaborado y mantiene la [organización] un protocolo que asegure el análisis, evaluación y control de los riesgos de seguridad operacional en las operaciones de la organización?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 4, 9 y 10	¿Articula claramente la documentación SMS de la [organización] la relación entre peligros, consecuencias y riesgos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 5 y 9	¿Existe un proceso estructurado para el análisis de los riesgos de seguridad operacional relacionados con las consecuencias de peligros identificados, expresados en términos de probabilidad y gravedad del suceso?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 5 y 9	¿Existen criterios para evaluar los riesgos de seguridad operacional y establecer la aceptabilidad de los riesgos (es decir el nivel aceptable de riesgos de seguridad operacional que la organización está dispuesta a aceptar)?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulos 5 y 9	¿Cuenta el proveedor de servicios con estrategias de mitigación de riesgos de seguridad operacional que comprendan planes de acción correctiva/preventiva para evitar la repetición de sucesos y deficiencias notificadas?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Componente 3 — GARANTÍA DE LA SEGURIDAD OPERACIONAL</b>			
<b>Elemento 3.1 — Supervisión y medición de la eficacia de la seguridad operacional</b>			
Capítulos 9 y 10	¿Ha implantado la [organización] un proceso interno para verificar la eficacia de la seguridad operacional de la organización y validar la efectividad de los controles de riesgo de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

Referencia de la OACI	Aspecto que ha de analizarse o pregunta que ha de contestarse	Respuesta	Estado de implantación
Capítulo 9	¿Se incluyen en esos procesos las herramientas siguientes? Sistemas de notificación de seguridad Operacional <input type="checkbox"/> Sí <input type="checkbox"/> No Estudios de seguridad operacional <input type="checkbox"/> Sí <input type="checkbox"/> No Exámenes de seguridad operacional <input type="checkbox"/> Sí <input type="checkbox"/> No Auditorías de la seguridad operacional <input type="checkbox"/> Sí <input type="checkbox"/> No Encuestas de seguridad operacional <input type="checkbox"/> Sí <input type="checkbox"/> No Investigaciones internas de seguridad operacional <input type="checkbox"/> Sí <input type="checkbox"/> No		
Capítulos 6 y 9	¿Se verifica la eficacia de la seguridad operacional de la organización con referencia a los indicadores de eficacia de seguridad operacional y objetivos de eficacia de seguridad del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se examinan los informes de seguridad operacional al nivel apropiado de la administración?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un proceso de retroinformación para notificar a los contribuyentes que sus informes se han recibido y compartir los resultados de los análisis?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se generan medidas correctivas y preventivas en respuesta de la identificación de peligros?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se aplican procedimientos para la realización de investigaciones internas?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un proceso que asegure que los sucesos y deficiencias notificados se analizan para identificar todos los peligros conexos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Cuenta el proveedor de servicios con un proceso para evaluar la efectividad de las medidas correctivas/preventivas que se han elaborado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Cuenta el proveedor de servicios con un sistema para supervisar el proceso de notificación interno y las medidas correctivas conexas?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe una función de auditoría con la independencia y autoridad requeridas para realizar evaluaciones internas efectivas?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Cubre el sistema de auditoría todas las funciones, actividades y organizaciones dentro del proveedor de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existen procesos de selección/instrucción para asegurar la objetividad y competencia de los auditores así como la imparcialidad del proceso de auditoría?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un proceso para notificar los resultados de las auditorías y mantener registros?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un procedimiento que establezca los requisitos para la oportuna adopción de medidas correctivas y preventivas en respuesta a los resultados de las auditorías?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un procedimiento para registrar la verificación de las medidas adoptadas y la notificación de los resultados de verificación?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un proceso para supervisar y analizar tendencias?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

<i>Referencia de la OACI</i>	<i>Aspecto que ha de analizarse o pregunta que ha de contestarse</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
<b>Elemento 3.2 — Gestión del cambio</b>			
Capítulo 9	¿Ha elaborado y mantiene la [organización] un protocolo para identificar cambios dentro de la organización que puedan afectar a procesos y servicios establecidos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Analiza el protocolo para la gestión del cambio los cambios a las operaciones o personal fundamental debidos a riesgos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Ha establecido la [organización] arreglos para asegurar la eficacia de la seguridad operacional antes de intentar los cambios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Ha establecido la [organización] un proceso para eliminar o modificar los controles de riesgos de seguridad operacional que ya no se necesitan debido a los cambios introducidos en el entorno operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 3.3 — Mejora continua del SMS</b>			
Capítulo 9	¿Ha elaborado y mantiene la [organización] un protocolo para identificar las causas del bajo nivel de eficacia del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Ha establecido la [organización] un mecanismo para determinar las consecuencias del bajo nivel de eficacia del SMS sobre las operaciones?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Ha establecido la organización un mecanismo para eliminar o mitigar las causas de la baja eficacia del SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Cuenta la organización con un proceso para la evaluación proactiva de instalaciones, equipo, documentación y procedimientos (mediante auditorías y encuestas, etc.)?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Cuenta la organización con un proceso para la evaluación proactiva de la actuación de un individuo, para verificar el cumplimiento de las responsabilidades de seguridad operacional de dicho individuo?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Componente 4 — PROMOCIÓN DE LA SEGURIDAD OPERACIONAL</b>			
<b>Elemento 4.1 — Instrucción y educación</b>			
Capítulo 9	¿Existe un proceso documentado para identificar requisitos de instrucción de modo que el personal esté capacitado y sea competente para realizar sus tareas en SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se corresponde la instrucción en seguridad operacional con la participación del individuo en el SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se ha incorporado la instrucción en seguridad operacional en la instrucción de adoctrinamiento después de la contratación?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe instrucción sobre respuesta a emergencias/contingencia para el personal afectado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un proceso que mida la efectividad de la instrucción?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 4.2 — Comunicación de la seguridad operacional</b>			
Capítulo 9	¿Existen procesos de comunicación en la [organización] que permitan que el sistema de gestión de la seguridad operacional funcione efectivamente?	<input type="checkbox"/> Sí <input type="checkbox"/> No	



<i>Referencia de la OACI</i>	<i>Aspecto que ha de analizarse o pregunta que ha de contestarse</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
Capítulo 9	¿Existen procesos de comunicación (escrita, reuniones, electrónica, etc.) conmensurables con el tamaño y alcance del proveedor de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se ha establecido y mantiene la información crítica para la seguridad operacional en un medio adecuado que proporcione dirección con respecto a documentos SMS pertinentes?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Se difunde en toda la [organización] la información crítica para la seguridad operacional y se supervisa la efectividad de dicha comunicación?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 9	¿Existe un procedimiento que explique por qué se adoptan medidas de seguridad operacional particulares y por qué se introducen o modifican los procedimientos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	



# Capítulo 8

## PLANIFICACIÓN DEL SMS

### 8.1 OBJETIVO Y CONTENIDO

En este capítulo se describen los requisitos relacionados con la planificación de un SMS, incluyendo la estructura de un plan de implantación del SMS. Estos requisitos se describen tomando como referencia el marco de la OACI para SMS. Aunque el marco de la OACI para SMS se introduce en su totalidad, en este capítulo se analiza solamente el primer componente del marco, política y objetivos de seguridad operacional; los otros tres componentes del marco de la OACI para SMS (gestión de riesgos de seguridad operacional, garantía de la seguridad operacional y promoción de la seguridad operacional) se analizan en el Capítulo 9. Este capítulo comprende los temas siguientes:

- a) Componentes y elementos del SMS;
- b) Marco SMS de la OACI;
- c) Responsabilidad y compromiso de la administración;
- d) Responsabilidades respecto de la seguridad operacional;
- e) Designación del personal clave de seguridad operacional;
- f) Coordinación del plan de respuesta ante emergencias;
- g) Documentación SMS; y
- h) Plan de implantación del SMS.

### 8.2 COMPONENTES Y ELEMENTOS DEL SMS

8.2.1 Existen cuatro componentes del SMS que representan los dos procesos operacionales básicos en los que se basa el SMS, así como los arreglos de organización necesarios para apoyar ambos procesos operacionales básicos. Los cuatro componentes del SMS son:

- a) política y objetivos de seguridad operacional;
- b) gestión de riesgos de seguridad operacional;
- c) garantía de la seguridad operacional; y
- d) promoción de la seguridad operacional.

8.2.2 Las dos actividades operacionales básicas de un SMS son la gestión de riesgos de seguridad operacional y la garantía de la seguridad operacional. La gestión de riesgos de seguridad debe considerarse como una de las primeras actividades de diseño del sistema, dirigida a la identificación inicial de peligros en el contexto en el cual se realizan las operaciones relacionadas con la prestación de servicios. La garantía de la calidad debe considerarse como una actividad de ejecución continua dirigida a:

- a) asegurar que la identificación inicial de peligros e hipótesis con respecto a la evaluación de las consecuencias de los riesgos de seguridad operacional, y las defensas que existen en el sistema como medio de control, permanecen válidas y aplicables a medida que el sistema evoluciona con el tiempo; o
- b) introducir cambios en las defensas según sea necesario.

Así pues, la identificación de peligros puede considerarse como una actividad de aplicación única que se realiza ya sea durante el diseño del sistema o cuando se enfrentan cambios importantes al sistema original. Por otra parte, la garantía de la seguridad operacional es una actividad cotidiana que se realiza ininterrumpidamente para asegurar que las operaciones que apoyan la prestación de servicios están adecuadamente protegidas contra los peligros. En términos sencillos, la identificación de peligros proporciona el marco de referencia inicial con respecto al cual se realiza la garantía de la seguridad operacional con carácter cotidiano.

8.2.3 Estas dos actividades operacionales básicas tienen lugar en el marco proporcionado por la política y objetivos de seguridad operacional y están apoyadas por la promoción de la seguridad operacional. Estos dos componentes del SMS engloban los necesarios arreglos de organización sin los cuales serían imposibles, o se verían gravemente afectadas, la identificación de peligros y la gestión de riesgos de seguridad operacional. Por consiguiente, puede considerarse que la gestión de riesgos de seguridad operacional y la garantía de seguridad operacional son las "actividades hacedoras" reales del SMS; son las actividades operacionales subyacentes de un SMS eficaz. Las políticas y objetivos de seguridad operacional y la promoción de la seguridad operacional por otra parte, proporcionan el marco de referencia así como el apoyo que permiten la realización efectiva de las actividades operacionales subyacentes en la gestión de riesgos de seguridad operacional y garantía de la seguridad operacional.

8.2.4 Los cuatro componentes analizados en los párrafos anteriores constituyen los bloques básicos de un SMS, en el sentido de que representan cuatro procesos de gestión de la seguridad operacional generales en que se basa el sistema real de gestión (SMS). Cada componente se subdivide en elementos, que abarcan los subprocesos específicos, tareas específicas o herramientas específicas que el sistema de gestión real debe aplicar o utilizar para realizar la gestión de la seguridad operacional al igual que cualquier otra función empresarial básica o proceso de organización.

8.2.5 La política y objetivos de seguridad operacional se componen de cinco elementos:

- a) responsabilidad y compromiso de la administración;
- b) responsabilidades respecto de la seguridad operacional;
- c) designación del personal clave de seguridad operacional;
- d) coordinación del plan de respuesta ante emergencias; y
- e) documentación SMS.

8.2.6 El componente de gestión de riesgos de seguridad operacional está compuesto por dos elementos:

- a) identificación de peligros; y
- b) evaluación y mitigación de riesgos de seguridad operacional.

8.2.7 El componente de garantía de la seguridad operacional está compuesto de tres elementos:

- a) supervisión y medición de la eficacia de la seguridad operacional;
- b) gestión del cambio; y
- c) mejora continua del SMS.

- 8.2.8 El componente de promoción de la seguridad operacional está compuesto de dos elementos:
- a) instrucción y educación; y
  - b) comunicación de la seguridad operacional.

### 8.3 MARCO SMS DE LA OACI

*Nota.— En el Apéndice 1 de este capítulo figuran detalles del marco de la OACI para SMS.*

Los cuatro componentes, combinados con los doce elementos analizados en la sección 8.2, integran el marco de la OACI para SMS, concebido como guía principal para la elaboración e implantación del SMS de un proveedor de servicios, como sigue:

1. Política y objetivos de seguridad operacional
  - 1.1 Responsabilidad y compromiso de la administración
  - 1.2 Responsabilidades respecto de la seguridad operacional
  - 1.3 Designación del personal clave de seguridad operacional
  - 1.4 Coordinación del plan de respuesta ante emergencias
  - 1.5 Documentación SMS
2. Gestión de riesgos de seguridad operacional
  - 2.1 Identificación de peligros
  - 2.2 Evaluación y mitigación de riesgos de seguridad operacional
3. Garantía de la seguridad operacional
  - 3.1 Supervisión y medición de la eficacia de la seguridad operacional
  - 3.2 Gestión del cambio
  - 3.3 Mejora continua del SMS
4. Promoción de la seguridad operacional
  - 4.1 Instrucción y educación
  - 4.2 Comunicación de la seguridad operacional.

### 8.4 RESPONSABILIDAD Y COMPROMISO DE LA ADMINISTRACIÓN

8.4.1 En toda organización, la administración controla las actividades del personal y el uso de recursos directamente relacionados con la prestación de servicios o necesarios para esta. La exposición de la organización a peligros de seguridad operacional es consecuencia de las actividades directamente relacionadas con la prestación de servicios. Mediante actividades específicas del personal y el uso de recursos, la administración puede controlar activamente los riesgos de seguridad operacional relacionados con las consecuencias de los peligros. Como ejemplo de estas actividades, la administración contrata, capacita y supervisa empleados, y adquiere equipo para apoyar las actividades de prestación de servicios. La administración debe asegurar que los empleados cumplen las directivas y controles de seguridad de la organización y que su equipo permanece en condiciones de servicio. La responsabilidad principal de la administración en cuanto a gestionar la seguridad operacional resulta entonces obvia y se ejerce mediante el funcionamiento de un sistema especializado que incorpora los necesarios controles de riesgos de seguridad operacional. El SMS del proveedor de servicios es el medio con que cuenta la administración para cumplir estas responsabilidades. El SMS es un sistema de gestión que garantiza operaciones seguras y eficientes.

8.4.2 El punto de partida para asegurar la eficacia y la eficiencia del SMS de la organización es la política de seguridad operacional de ésta. La administración superior debe definir la política de seguridad operacional de la organización, firmada por el ejecutivo responsable. En la Figura 8-1 se presenta un ejemplo de política de seguridad operacional. En términos generales, la política de seguridad debe incluir un compromiso para:

- a) lograr las normas de seguridad operacional más elevadas;
- b) observar todos los requisitos jurídicos y normas internacionales aplicables así como las prácticas más efectivas;
- c) proporcionar todos los recursos necesarios;
- d) hacer valer la seguridad operacional como responsabilidad principal de todos los administradores; y
- e) asegurar que la política se comprende, implanta y mantiene a todos los niveles.

8.4.3 Una vez elaborada la política de seguridad operacional, la administración superior debe comunicarla, con visible endoso, a todo el personal.

8.4.4 La administración superior también debe establecer objetivos de seguridad, así como las normas de eficacia de la seguridad operacional para el SMS y, por consiguiente, para toda la organización. Los objetivos de seguridad deben identificar lo que la organización desea lograr en términos de gestión de la seguridad y establecer las etapas que debe emprender para lograr esos objetivos. Las normas de eficacia de la seguridad permiten medir el comportamiento de la organización con respecto a la eficacia de la seguridad y con respecto a la gestión de la seguridad operacional. Los objetivos de seguridad y las normas de eficacia de la seguridad deben relacionarse con los indicadores y los objetivos de eficacia de la seguridad y los planes de acción del SMS, analizados en el Capítulo 6.

8.4.5 La organización debe identificar al Ejecutivo responsable, que debe ser una persona única e identificable, con responsabilidad final por la actuación efectiva y eficiente del SMS de la organización. Dependiendo del tamaño y complejidad de ésta, el Ejecutivo responsable puede ser:

- a) el Director general;
- b) el Presidente de la junta de directores;
- c) un socio; o
- d) el propietario.

8.4.6. Existe una tendencia a determinar quién debería ser el Ejecutivo responsable desde el punto de vista de la función asignada a la persona dentro de la organización. No obstante, más importante que quién debería ser el Ejecutivo responsable, son las facultades y responsabilidades que éste debería tener para rendir cuentas adecuadamente de la eficacia de la seguridad operacional del SMS. Estas facultades y responsabilidades comprenden, sin limitarse a ellas:

- a) plena autoridad en cuestiones de recursos humanos;
- b) autoridad en cuestiones financieras significativas;
- c) responsabilidad directa en la conducción de los asuntos de la organización;
- d) autoridad final sobre las operaciones autorizadas en certificado; y
- e) responsabilidad final sobre todos los asuntos de seguridad operacional.

### DECLARACIÓN DE POLÍTICA DE SEGURIDAD OPERACIONAL

La seguridad operacional es una de nuestras funciones empresariales básicas. Estamos comprometidos a elaborar, implantar, mantener y mejorar constantemente estrategias y procesos para asegurar que todas nuestras actividades de aviación tienen lugar en el marco de una asignación equilibrada de recursos de la organización, dirigidos a lograr el nivel más elevado de eficacia de la seguridad operacional y a satisfacer las normas nacionales e internacionales en la prestación de nuestros servicios.

Todos los niveles de administración y todos los empleados son responsables del logro de este nivel más elevado de eficacia de la seguridad, comenzando con el [Director general/Gerente general o según corresponda a la organización].

Nuestro compromiso es:

- **Apoyar** la gestión de la seguridad operacional mediante el suministro de todos los recursos apropiados, que resultará en una cultura de la organización que fomente las prácticas seguras, aliente a la efectiva notificación y comunicación de seguridad operacional y gestione activamente la seguridad con la misma atención a los resultados que la atención a los resultados de los otros sistemas de gestión de la organización;
- **Hacer valer** la gestión de la seguridad operacional como responsabilidad principal de todos los administradores y empleados;
- **Definir claramente** para todo el personal, administradores y empleados por igual, sus líneas de rendición de cuentas y responsabilidades para el logro de la eficacia de la seguridad operacional de la organización y la eficacia de nuestro sistema de gestión de la seguridad;
- **Establecer y operar** procesos de identificación de peligros y de gestión de riesgos, incluyendo un sistema de notificación de peligros, para eliminar o mitigar los riesgos de seguridad operacional de las consecuencias de los peligros que resultan de nuestras operaciones o actividades al punto más bajo como sea razonable en la práctica (ALARP);
- **Asegurar** que no se adoptará ninguna medida contra ningún empleado que revele un problema de seguridad operacional mediante el sistema de notificación de peligros, a menos que dicha revelación indique, más allá de toda duda razonable, que se ha cometido un acto ilícito, una negligencia grave, o un incumplimiento deliberado o voluntario de reglamentos o procedimientos;
- **Cumplir** y, cuando sea posible, sobrepasar los requisitos y las normas legislativas y reglamentarias;
- **Asegurar** que se dispone de recursos humanos con conocimientos e instrucción suficientes para poner en práctica las estrategias y procesos de seguridad operacional;
- **Asegurar** que todos los miembros del personal poseen información e instrucción sobre seguridad operacional de la aviación adecuadas y apropiadas, que son competentes en cuestiones de seguridad operacional y que solamente se les asignan tareas acordes con sus competencias;
- **Establecer y medir** nuestra eficacia de la seguridad operacional con respecto a los indicadores de eficacia de seguridad operacional y objetivos de eficacia de la seguridad operacional realistas;
- **Mejorar continuamente** nuestra eficacia de seguridad operacional mediante procesos de gestión que aseguren que se adoptan, y son eficaces, las medidas de seguridad pertinentes; y
- **Asegurar** que los sistemas y servicios suministrados del exterior para apoyar nuestras operaciones satisfacen nuestras normas de eficacia de la seguridad operacional.

(Firmado)

\_\_\_\_\_  
Director general/Gerente general /  
o quien corresponda

Figura 8-1. Ejemplo de política de seguridad operacional

8.4.7 En el Capítulo 2 se analiza la asignación de recursos como proceso fundamental de la organización. Por consiguiente, la asignación de recursos es una de las funciones primordiales de la administración. En el párrafo 8.4.1 se analiza con más detalle la función de administración como una función de control de las actividades del personal y del uso de recursos directamente relacionados con la prestación de servicios, como consecuencia de los cuales la organización se ve expuesta a peligros de seguridad. Lo anterior subraya la justificación de las responsabilidades y facultades del Ejecutivo responsable establecidas en 8.4.6: tales responsabilidades y facultades se refieren a la asignación de recursos o control de actividades, exclusivamente. Una organización que designe un Ejecutivo responsable que no tenga estas facultades y responsabilidades coloca a la persona designada en una posición en que no cuenta con los atributos esenciales para desempeñar su función.

8.4.8 El Ejecutivo responsable puede asignar la gestión del SMS a otra persona, siempre que dicha asignación esté adecuadamente documentada y descrita en el manual de sistemas de gestión de la seguridad operacional (SMSM) de la organización, que se tratará más adelante en este capítulo. La obligación de rendición de cuentas del Ejecutivo responsable no se ve afectada, no obstante, por la asignación de la gestión del SMS a otra persona: el Ejecutivo responsable conserva la obligación de rendición de cuentas y responsabilidad final por la eficacia del SMS de la organización.

## 8.5 RESPONSABILIDADES RESPECTO DE LA SEGURIDAD OPERACIONAL

8.5.1 En el Capítulo 3 se analiza la gestión de la seguridad operacional como una función empresarial básica que contribuye al análisis de los recursos y objetivos de una organización. Este análisis constituye la base de una asignación balanceada y realista de recursos entre los objetivos de protección y de producción que apoya las necesidades generales en la prestación de servicios de la organización. En el párrafo 8.4.1 se analiza el SMS como sistema de gestión para garantizar las operaciones seguras. Las operaciones seguras son improbables a menos que se logre una asignación balanceada y realista de recursos entre los objetivos de protección y producción, que apoyan las necesidades generales de prestación de servicios de la organización. En términos generales, las responsabilidades respecto de la seguridad operacional en cuanto garantizar las operaciones seguras y el logro de equilibrio y realismo en la atribución de recursos, se materializan mediante la organización del propio SMS y, en particular, mediante un elemento específico del SMS: la definición de las responsabilidades respecto de la seguridad operacional de todo el personal, pero principalmente, del personal clave.

8.5.2 Las responsabilidades de seguridad operacional de los administradores con respecto a la organización del SMS se refieren a la definición de una arquitectura del SMS de la organización que corresponda al tamaño, características y complejidad de las operaciones y a los peligros y riesgos de seguridad relacionados con las actividades necesarias para la prestación de los servicios. Las responsabilidades de seguridad operacional de los administradores con respecto a la organización del SMS comprenden, además, la asignación de recursos humanos, técnicos, financieros o de otro tipo necesarios para lograr el funcionamiento efectivo y eficiente del SMS.

8.5.3 Aunque las descripciones de tareas de todos los empleados, independientemente del nivel, deberían incluir las responsabilidades respecto de la seguridad operacional y la rendición de cuentas, las obligaciones de rendición de cuentas con respecto a la definición de responsabilidades y facultades de seguridad operacional del personal clave se refieren a la inclusión en la descripción de tareas de cada administrador superior (jefe de departamento o persona encargada de una dependencia funcional), de las responsabilidades relativas al funcionamiento del SMS, en la medida apropiada, además de las responsabilidades específicas por el funcionamiento del departamento o dependencia en cuestión. En el marco de la gestión de la seguridad operacional como función empresarial básica, cada jefe de departamento o persona responsable de una dependencia funcional tendrá un grado de participación en la operación del SMS y su eficacia de la seguridad operacional. Esta participación será por cierto más profunda para los encargados de los departamentos operacionales o dependencias funcionales directamente involucrados en la prestación de los servicios básicos de la organización (operaciones, mantenimiento, ingeniería, instrucción y despacho, denominados en lo que sigue "gerentes de línea") que para los encargados de las funciones de apoyo (recursos humanos, administración, asuntos jurídicos y financieros).



8.5.4 Las obligaciones de rendición de cuentas, responsabilidades y facultades de todos los jefes de departamentos o personas encargadas de dependencias funcionales, y en particular los gerentes de línea, deben describirse en el manual de sistemas de gestión de la seguridad operacional (SMSM) de la organización, que se analizará posteriormente en este capítulo. Las obligaciones de rendición de cuentas, responsabilidades y facultades deben mostrarse gráficamente en una carta de funciones que indique las interfaces e interrelaciones en términos de la gestión de la seguridad operacional entre los diversos sectores de la organización. En la Figura 8-2 se presenta un ejemplo de carta de funciones.

8.5.5 Es muy importante observar que la Figura 8-2 muestra las funciones más que la organización. No se pretende presentar a la organización de la gestión de la seguridad operacional en términos de departamentos y dependencias funcionales y su relativa posición jerárquica dentro de la empresa, sino más bien las funciones de cada departamento o dependencia en términos del logro de la seguridad operacional como proceso empresarial básico. Esta advertencia es importante porque habrá tantas cartas de organización como organizaciones pueden existir en la aviación. Por consiguiente, para los fines de este manual, la Figura 8-2 debe considerarse como una carta de funciones y no como una carta de organización.

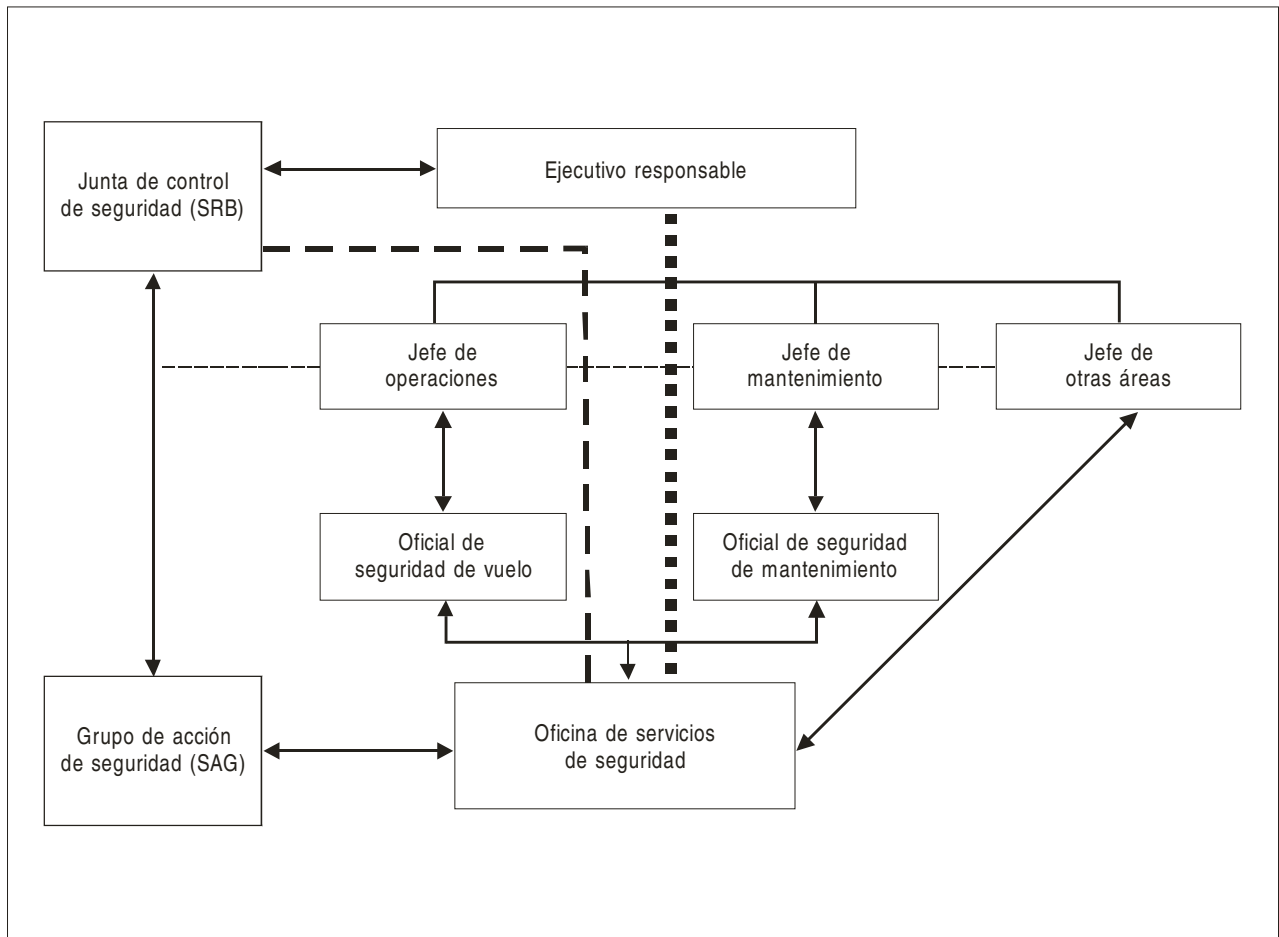


Figura 8-2. Responsabilidades de seguridad operacional

8.5.6 La Oficina de servicios de seguridad operacional está en el centro de la carta funcional. El concepto de Oficina de servicios de seguridad es clave para la noción de gestión de la seguridad operacional como proceso empresarial básico, y de SMS como sistema que la administración emplea para tales fines. La Oficina de servicios de seguridad es independiente y neutral en términos de los procesos y decisiones adoptadas con respecto a la prestación de servicios por los gerentes de línea de las dependencias operacionales. En un entorno SMS, la Oficina de servicios de seguridad realiza cuatro funciones corporativas esenciales:

- a) gestiona y supervisa el sistema de identificación de peligros;
- b) supervisa la eficacia de la seguridad de las dependencias operacionales que participan directamente en la prestación de servicios;
- c) asesora a la administración superior en asuntos de gestión de la seguridad operacional; y
- d) asiste a los gerentes de línea en asuntos de gestión de la seguridad operacional.

8.5.7 En el enfoque tradicional de la seguridad operacional analizado en el Capítulo 2, la Oficina de seguridad era el “propietario” exclusivo de todo el proceso de seguridad dentro de la organización. El gerente de seguridad, a menudo conocido como oficial de prevención de accidentes, era la persona a cargo de identificar los problemas de seguridad operacional, proponer soluciones, participar en la implantación de las mismas, y supervisar la eficacia de las soluciones. En años recientes, la noción de que la “propiedad” del proceso de seguridad era exclusivamente de la Oficina de seguridad se vio involuntariamente reforzada por una práctica adoptada en toda la industria por la que se establecía un enlace directo de notificación y comunicación entre el gerente de seguridad y el Director general de la organización.

8.5.8 La intención de esta extendida práctica era doble. En primer lugar, se dirigía a elevar el nivel jerárquico y la visibilidad de la Oficina de seguridad estableciendo un enlace directo entre ésta y el Director general. En segundo lugar, el enlace directo se dirigía a generar neutralidad apartando a los encargados de gestionar las actividades operacionales directamente relacionadas con la prestación de servicios (gerentes de línea) de la evaluación y resolución de problemas de seguridad. Se consideraba que existía una gran probabilidad de que los gerentes de línea pudieran, en diversos grados, ser partes interesadas, lo que llevaría a un posible conflicto de intereses en la evaluación y resolución de problemas de seguridad. La relación directa entre el gerente de seguridad y el Director general se estableció para eliminar este presunto conflicto de intereses.

8.5.9 Aunque claramente bien intencionada, esta práctica presentaba dos graves carencias. En primer lugar, otorgando la propiedad del proceso de seguridad enteramente a la Oficina de seguridad, alejaba a los gerentes de línea del proceso de toma de decisiones de seguridad. Esto nutrió la percepción de que “los problemas de seguridad eran problemas del gerente de línea; los problemas de seguridad pertenecían a la Oficina de seguridad y al gerente de seguridad”. La línea de rendición de cuentas se redujo efectivamente a un diálogo entre el Director general y el gerente de seguridad. Considerando la carga de trabajo de un Director general, este diálogo tenía todas las posibilidades de transformarse en monólogo. En segundo lugar, y muy importante, dejaba de lado el valioso aporte, en términos de conocimientos, que las dependencias operacionales podrían llevar al proceso de toma de decisiones de seguridad operacional de la organización.

8.5.10 El entorno SMS plantea una perspectiva diferente. El nombre de la Oficina de seguridad se ha modificado a Oficina de servicios de seguridad operacional, para reflejar que proporciona un servicio a la organización, a la administración superior y a los gerentes de línea, con respecto a la gestión de la seguridad como proceso empresarial básico. El axioma “no se puede administrar lo que no se puede medir” analizado en el Capítulo 3, se trata con el SMS. La Oficina de servicios de seguridad es fundamentalmente una dependencia de recolección y análisis de datos de seguridad operacional. Mediante una combinación de métodos predictivos, proactivos y reactivos (analizada en el Capítulo 3), la Oficina de servicios de seguridad capta lo que sucede dentro de la deriva operacional (también analizada en el Capítulo 3), mediante la recolección continua y regular de datos de seguridad operacional sobre peligros durante las actividades de prestación de servicios.

8.5.11 Una vez identificados los peligros, evaluadas sus consecuencias y estimados los riesgos de seguridad operacional de tales consecuencias (es decir una vez que la información de seguridad se ha extraído de los datos de seguridad), la información de seguridad operacional se transmite a los gerentes de línea para la resolución de los problemas de seguridad subyacentes. Los gerentes de línea son los verdaderos expertos temáticos en sus respectivos sectores y, por consiguiente, los mejor ubicados para diseñar soluciones efectivas y eficientes e implantarlas. Además, los gerentes de línea pueden encargarse de la última etapa del proceso de análisis de datos de seguridad operacional, transformando la información de seguridad en inteligencia de seguridad y proporcionando un contexto para la información sobre peligros obtenida por la oficina de servicios de seguridad.

8.5.12 Al igual que la organización en su totalidad, la responsabilidad principal de la gestión de la seguridad operacional corresponde a los “dueños” de las actividades de producción. Es durante las actividades de producción cuando los peligros se enfrentan directamente, donde las deficiencias en los procesos organizativos contribuyen a desencadenar las consecuencias perjudiciales de los peligros, y donde el control de supervisión directo y la asignación de recursos pueden mitigar los riesgos de seguridad operacional a un valor ALARP. Además, los propietarios de los procesos son los expertos técnicos, temáticos en toda organización y, entonces los que tienen mayores conocimientos de los procesos técnicos de producción.

8.5.13 Después de que la información de seguridad se ha entregado a los gerentes de línea apropiados, la Oficina de servicios de seguridad reanuda sus actividades regulares de recolección y análisis de datos de seguridad. A intervalos convenidos entre la Oficina de servicios de seguridad y los gerentes de línea en cuestión, la Oficina de servicios de seguridad presentará a los gerentes de línea de las áreas en que haya un problema de seguridad nueva información sobre el problema que se está considerando. La información de seguridad operacional indicará si las soluciones de mitigación implantadas por los gerentes de línea han solucionado el problema de seguridad o si éste persiste. En este último caso, se introducen más soluciones de mitigación, se conviene un nuevo intervalo de tiempo, se recogen y analizan datos de seguridad, se entrega la información de seguridad y este ciclo se repite tantas veces como sea necesario hasta que el análisis de los datos de seguridad comprueba que el problema de seguridad operacional se ha resuelto. En todo este proceso, los gerentes de línea no responden ante la Oficina de servicios de seguridad, sino ante el Ejecutivo responsable, como persona con responsabilidad final por el SMS de la organización, a través de cualquiera de los dos órganos formales de seguridad operacional de la organización que se analizan en la sección 8.6.

## 8.6 DESIGNACIÓN DEL PERSONAL CLAVE DE SEGURIDAD OPERACIONAL

8.6.1 Fundamental para la implantación y funcionamiento efectivos de una Oficina de servicios de seguridad es la designación de la persona a cargo de la operación cotidiana de dicha oficina. Esta persona estará identificada por diferentes nombres en diferentes organizaciones, pero para los fines de este manual se conserva el término genérico de gerente de seguridad.

8.6.2 El gerente de seguridad, en la mayoría de las organizaciones, será la persona a quien el Ejecutivo responsable ha asignado las funciones cotidianas de gestión del SMS. El gerente de seguridad es el individuo responsable y punto focal para la puesta en práctica y mantenimiento de un SMS efectivo. El gerente de seguridad también asesora al Ejecutivo responsable y gerentes de línea en asuntos relativos a la gestión de la seguridad operacional y es responsable de coordinar y comunicar asuntos de seguridad dentro de la organización, así como con agencias externas, contratistas y partes interesadas, según corresponda. Las funciones de gerente de seguridad comprenden, pero sin limitarse a ellas:

- a) administrar el plan de implantación del SMS en nombre del Ejecutivo responsable;
- b) realizar y facilitar la identificación de peligros y el análisis de gestión de riesgos;
- c) supervisar las medidas correctivas y evaluar sus resultados;

- d) proporcionar informes periódicos sobre la eficacia de la seguridad operacional de la organización;
- e) mantener registros y documentación de seguridad;
- f) planificar y organizar la instrucción del personal en seguridad;
- g) proporcionar asesoramiento independiente sobre asuntos de seguridad;
- h) supervisar problemas de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones de la organización dirigidas a la prestación de servicios;
- i) coordinar y comunicarse (en nombre del Ejecutivo responsable) con la autoridad de vigilancia del Estado y otras agencias estatales según corresponda sobre problemas relacionados con la seguridad operacional; y
- j) coordinar y comunicarse (en nombre del Ejecutivo responsable) con agencias internacionales sobre cuestiones relativas a la seguridad operacional.

8.6.3 El gerente de seguridad puede ser la única persona que maneja la Oficina de servicios de seguridad o puede estar apoyado por personal adicional, principalmente analistas de datos de seguridad. Esto dependerá del tamaño de la organización y del carácter y complejidad de las operaciones que apoyan la prestación de servicios. Independientemente del tamaño de la Oficina de servicios de seguridad y el nivel de su personal, sus funciones son las mismas. El gerente de seguridad se comunica directamente con los gerentes de línea (operaciones, mantenimiento, ingeniería, instrucción, etc.). Esto se indica con las flechas de trazo lleno en la carta de funciones de la Figura 8-2. Si, debido al tamaño de la organización los jefes de las dependencias operacionales cuentan con un oficial de seguridad especializado con experiencia temática y responsabilidad delegada para la gestión de problemas de seguridad en un área determinada, ese oficial de seguridad será el primer punto de contacto para el gerente de seguridad.

8.6.4 En circunstancias normales, el gerente de seguridad tiene acceso al Ejecutivo responsable o se comunica con éste mediante dos canales: el Grupo de acción de seguridad operacional y, a través de él la Junta de control de seguridad. Estos grupos se analizan posteriormente en este capítulo. En circunstancias excepcionales o urgentes, el gerente de seguridad debe tener acceso directo de emergencia al Ejecutivo responsable, según se indica con la línea de puntos que conecta las casillas respectivas de la Figura 8-2. Este canal de comunicación debería utilizarse en raras ocasiones y, cuando se haga, debería justificarse y documentarse adecuadamente.

8.6.5 En un entorno SMS, el gerente de seguridad es la persona responsable de la recolección y análisis de los datos de seguridad sobre peligros y de la distribución, a los gerentes de línea, de información de seguridad sobre peligros y los riesgos de seguridad de las consecuencias de los peligros. Como tal, el gerente de seguridad será a menudo el portador de malas noticias. Por esta razón, los criterios de selección del gerente de seguridad operacional adquieren especial importancia y deberían incluir, pero sin limitarse a ellos, los siguientes:

- a) experiencia en gestión operacional;
- b) antecedentes técnicos para comprender los sistemas necesarios para las operaciones;
- c) habilidades interpersonales;
- d) habilidades analíticas y de resolución de problemas;
- e) habilidades de gestión de proyectos; y
- f) habilidades de comunicación oral y escrita.

*Nota.— Un ejemplo de descripción de tareas para el gerente de seguridad figura en el Apéndice 2 de este capítulo.*

8.6.6 La distribución de información sobre el riesgo de seguridad operacional de las consecuencias de los peligros por la Oficina de servicios de seguridad es sólo la primera etapa del proceso de gestión de riesgos de seguridad operacional. Los gerentes de línea deben actuar sobre esta información. La mitigación de problemas de seguridad inevitablemente exige recursos. A veces estos recursos están directamente disponibles a los gerentes de línea. A menudo se requieren recursos adicionales, cuya asignación puede no estar en las facultades del gerente de línea, y debe ser aprobada por niveles superiores de la organización. Análogamente, debe haber algún protocolo en la organización para asegurar una evaluación neutral de la eficacia y eficiencia de las estrategias de mitigación en relación con la eficacia de la seguridad operacional convenida de la organización. La Junta de control de la seguridad (SRB) proporciona la plataforma para lograr los objetivos de asignación de recursos y evaluación neutral de la eficacia y eficiencia de las estrategias de mitigación.

8.6.7 La SRB es un comité de muy alto nivel, presidido por el Ejecutivo responsable e integrado por los administradores superiores, incluyendo los gerentes de línea responsables de las áreas funcionales. El gerente de seguridad participa en la SRB solamente como asesor. La SRB tiene carácter eminentemente estratégico, trata problemas de alto nivel en relación con las políticas, asignación de recursos y supervisión del desempeño de la organización y se reúne con poca frecuencia, a menos que circunstancias excepcionales impongan otra cosa. La SRB:

- a) monitorea la eficacia del plan de implantación del SMS;
- b) monitorea que toda medida correctiva necesaria se adopta en forma oportuna;
- c) monitorea la eficacia de la seguridad operacional con respecto de la política y objetivos de seguridad de la organización;
- d) monitorea la efectividad de los procesos de gestión de la seguridad operacional de la organización que apoyan la prioridad declarada por la empresa de la gestión de la seguridad como otro proceso empresarial básico;
- e) monitorea la efectividad de la supervisión de la seguridad operacional de las operaciones subcontratadas;
- f) asegura que se asignan recursos apropiados para lograr la eficacia de la seguridad operacional más allá de lo requerido por el cumplimiento de los reglamentos; y
- g) proporciona orientación estratégica al SAG.

8.6.8 Una vez que la SRB ha elaborado una dirección estratégica, debe realizarse en forma coordinada la implantación concertada de las estrategias en toda la organización. Esta es la función principal del Grupo de acción de seguridad operacional (SAG). El SAG es un comité de alto nivel, integrado por gerentes de línea y representantes del personal operativo y presidido en turnos por gerentes de línea designados: el gerente de seguridad es el secretario del SAG. El SAG tiene carácter eminentemente táctico y trata de asuntos de implantación para satisfacer las directivas estratégicas de la SRB. Mientras el SAG trata de aspectos de implantación "a nivel de base" relativos a actividades específicas para asegurar el control de los riesgos de seguridad operacional de las consecuencias de los peligros durante las operaciones de línea, la SRB trata de la coordinación de esos aspectos, para asegurar la coherencia con la dirección estratégica proporcionada por la SRB. El SAG:

- a) supervisa la eficacia de la seguridad operacional dentro de las áreas funcionales y asegura que la identificación de peligros y la gestión de riesgos de seguridad se realizan según corresponda, con la necesaria participación del personal para crear conciencia de la seguridad operacional;

- b) coordina la resolución de estrategias de mitigación para las consecuencias de peligros identificadas y asegura que existen arreglos satisfactorios para la captura de datos de seguridad operacional y la retroinformación de los empleados;
- c) evalúa el impacto de los cambios operacionales en la seguridad;
- d) coordina la implantación de planes de medidas correctivas y convoca a reuniones o sesiones de información, según corresponda, para asegurar que todos los empleados cuentan con amplias oportunidades para participar plenamente en la gestión de la seguridad;
- e) asegura que las medidas correctivas se adoptan en forma oportuna;
- f) examina la efectividad de las recomendaciones de seguridad anteriores; y
- g) supervisa la promoción de la seguridad operacional y asegura que se imparte al personal instrucción apropiada en seguridad operacional, emergencias y técnicas que satisface o supera los requisitos normativos mínimos.

## **8.7 COORDINACIÓN DEL PLAN DE RESPUESTA ANTE EMERGENCIAS**

8.7.1 Un plan de respuesta ante emergencias (ERP) detalla por escrito las acciones que deberían adoptarse después de un accidente y designa los responsables de cada acción. La finalidad de un ERP es asegurar que existe una transición ordenada y eficiente de las operaciones normales a las de emergencia, incluyendo la delegación de autoridad de emergencia y asignación de responsabilidades de emergencia. La autorización para las medidas que deben llevar a cabo el personal clave también figura en el plan, así como la coordinación de las actividades para enfrentar la emergencia. El objetivo general es la continuación en condiciones de seguridad de las operaciones o el retorno a operaciones normales tan pronto como sea posible.

8.7.2 Los aeropuertos deben elaborar un plan de emergencia de aeropuerto (AEP), los proveedores de servicios de tránsito aéreo deben elaborar planes de contingencia y las líneas aéreas deben elaborar un plan de respuesta ante emergencias. Dado que las operaciones de aeropuerto, ATC y líneas aéreas se superponen, es obvio que estos planes deberían ser compatibles. La coordinación de los diferentes planes debería describirse en el manual SMS.

## **8.8 DOCUMENTACIÓN SMS**

8.8.1 Como se analizó en el Capítulo 7, una característica explícita del SMS es que todas las actividades de gestión de la seguridad operacional deben estar documentadas y ser visibles. Por lo tanto, la documentación es un elemento esencial del SMS.

8.8.2 La documentación SMS debe incluir y hacer referencia, según corresponda, a todos los reglamentos pertinentes y aplicables, tanto nacionales como internacionales. También debe incluir registros y documentación específicos del SMS, como formularios de notificación de peligros, líneas de rendición de cuentas, responsabilidad y facultades relativas a la gestión de la seguridad operacional y la estructura de la organización de gestión de la seguridad. Además debe documentar directrices explícitas para la gestión de los registros, incluyendo tratamiento, almacenamiento, recuperación y conservación. Pero indudablemente, la documentación más importante del SMS es el manual SMS (SMSM).

8.8.3 El SMSM es un instrumento clave para comunicar el enfoque de la organización respecto de la seguridad a toda la organización. En él se documentan todos los aspectos del SMS, incluyendo la política y los objetivos de seguridad operacional, los procedimientos y las responsabilidades individuales en la materia.

8.8.4 Normalmente, el SMSM comprende:

- a) ámbito del sistema de gestión de la seguridad operacional;
- b) política y objetivos de seguridad operacional;
- c) responsabilidades y rendición de cuentas respecto de la seguridad;
- d) personal clave de seguridad;
- e) procedimientos de control de documentación;
- f) coordinación de la planificación de respuesta ante emergencias;
- g) planes de identificación de peligros y de gestión de riesgos;
- h) garantías de la seguridad;
- i) supervisión de la eficacia de la seguridad;
- j) auditorías de la seguridad operacional;
- k) gestión del cambio;
- l) promoción de la seguridad; y
- m) actividades contratadas.

## 8.9 PLAN DE IMPLANTACIÓN DEL SMS

8.9.1 El plan de implantación del SMS define el enfoque de la organización respecto de la gestión de la seguridad operacional. Como tal, constituye una estrategia realista para la implantación del SMS que satisfará los objetivos de seguridad de la organización apoyando al mismo tiempo la prestación efectiva y eficiente de los servicios. En el se describe cómo logrará la organización sus objetivos empresariales de seguridad y cómo satisfará cualquier requisito de seguridad nuevo o revisado, reglamentario o de otro tipo. Los aspectos significativos del plan se incluirán normalmente en el plan administrativo de la organización. Un plan de implantación del SMS, que puede consistir en más de un documento, detalla las medidas que han de adoptarse, por quienes y según que cronogramas.

8.9.2 Dependiendo del tamaño de la organización y la complejidad de sus operaciones, el plan de implantación del SMS puede ser elaborado por una persona, o por un grupo de planificación que comprenda una base de experiencia apropiada. El grupo de planificación debería reunirse regularmente con la administración superior para evaluar el progreso del plan de implantación y para que se le asignen recursos (incluyendo el tiempo para las reuniones), conmensurables con la tarea que debe realizar.

8.9.3 Normalmente, el contenido de un plan de implantación del SMS comprende:

- a) políticas y objetivos de seguridad operacional;
- b) descripción del sistema;
- c) análisis de las carencias;
- d) componentes del SMS;
- e) funciones y responsabilidades de seguridad operacional;
- f) política de notificación de peligros;
- g) medios para la participación de los empleados;
- h) medición de la eficacia de la seguridad;
- i) comunicación de seguridad;
- j) instrucción de seguridad; y
- k) revisión por la administración de la eficacia de la seguridad operacional.

8.9.4 Una vez completado, la administración superior debe endosar el plan de implantación del SMS. La duración típica de la implantación de un SMS es de uno a cuatro años. La implantación del SMS, incluyendo un enfoque por etapas, según se analizará en el Capítulo 10, y orientación sobre la metodología para elaborar el plan de implantación SMS y cronograma conexo, figuran en el Apéndice 2 de ese capítulo.

---



## Apéndice 1 del Capítulo 8

# MARCO PARA LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

Un SMS es una herramienta de gestión para la gestión de la seguridad operacional por una organización. En este apéndice se introduce un marco para la implantación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS) por una organización. La implantación del marco será conmensurable con el tamaño de la organización y la complejidad de los servicios proporcionados. El marco incluye los siguientes cuatro componentes y doce elementos que representan los requisitos mínimos para la implantación de un SMS.

1. Política y objetivos de seguridad operacional
  - 1.1 Responsabilidad y compromiso de la administración
  - 1.2 Responsabilidades respecto de la seguridad operacional
  - 1.3 Designación del personal clave de seguridad operacional
  - 1.4 Coordinación del plan de respuesta ante emergencias
  - 1.5 Documentación SMS
2. Gestión de riesgos de seguridad operacional
  - 2.1 Identificación de peligros
  - 2.2 Evaluación y mitigación de riesgos de seguridad operacional
3. Garantía de la seguridad operacional
  - 3.1 Supervisión y medición de la eficacia de la seguridad operacional
  - 3.2 Gestión del cambio
  - 3.3 Mejora continua del SMS
4. Promoción de la seguridad operacional
  - 4.1 Instrucción y educación
  - 4.2 Comunicación de la seguridad operacional.

### 1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

#### 1.1 Responsabilidad y compromiso de la administración

La [organización] definirá la política de seguridad operacional de la organización de conformidad con los requisitos nacionales e internacionales, y la misma llevará la firma del Ejecutivo responsable de la organización. La política de seguridad operacional reflejará los compromisos de la organización respecto de la seguridad operacional; incluirá una declaración clara acerca de la provisión de los recursos necesarios para su puesta en práctica; y se comunicará, con visible endorso, a toda la organización. La política de seguridad operacional incluirá procedimientos de presentación de

informes en la materia; indicará claramente qué tipos de comportamientos operacionales son inaceptables; e incluirá las condiciones en las que no se podrían aplicar medidas disciplinarias. La política de seguridad operacional se examinará periódicamente para garantizar que continúa siendo pertinente y apropiada para la organización.

### **1.2 Responsabilidades respecto de la seguridad operacional**

La [organización] identificará al Ejecutivo responsable quien, independientemente de sus otras funciones, será el responsable último y rendirá cuentas, en nombre de la [organización], respecto de la implantación y mantenimiento del SMS. La [organización] también identificará las responsabilidades de rendición de cuentas de todos los miembros de la administración, independientemente de las demás funciones que desempeñen, así como las de los empleados, en relación con la eficacia de la seguridad operacional del SMS. Las responsabilidades, rendición de cuentas y facultades de seguridad operacional se documentarán y comunicarán a toda la organización e incluirán una definición de los niveles de gestión que tienen autoridad para tomar decisiones relativas a la aceptabilidad de los riesgos de seguridad operacional.

### **1.3 Designación del personal clave de seguridad operacional**

La [organización] identificará un gerente de seguridad que será la persona responsable y de contacto para la implantación y el mantenimiento de un SMS eficaz.

### **1.4 Coordinación del plan de respuesta ante emergencias**

La [organización] garantizará que el plan de respuesta ante emergencias, que permitirá la transición ordenada y eficiente de las operaciones normales a las operaciones de emergencia y el posterior restablecimiento de las operaciones normales, se coordine en forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que deba interactuar al prestar sus servicios.

### **1.5 Documentación SMS**

La [organización] elaborará un plan de implantación del SMS, endosado por la administración superior de la organización, que defina el enfoque de la organización respecto de la gestión de la seguridad operacional de un modo que cumpla con los objetivos de la organización en materia de seguridad operacional. La [organización] elaborará y mantendrá actualizada la documentación del SMS en la que se describirán la política y los objetivos del SMS, sus requisitos, procesos y procedimientos, la rendición de cuentas, actividades y facultades respecto de los procesos y procedimientos, así como los resultados del SMS. También, como parte de la documentación relativa al SMS, la [organización] elaborará y mantendrá un manual de sistemas de gestión de la seguridad operacional (SMSM) para comunicar a toda la organización su enfoque respecto de la gestión de la seguridad operacional.

## **2. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL**

### **2.1 Identificación de peligros**

La [organización] elaborará y mantendrá un protocolo que garantice la identificación de los peligros operacionales. La identificación de los peligros se basará en una combinación de métodos reactivos, proactivos y predictivos para recopilar datos sobre seguridad operacional.

## **2.2 Evaluación y mitigación de riesgos de seguridad operacional**

La [organización] elaborará y mantendrá un protocolo que garantice el análisis, la evaluación y el control de los riesgos de seguridad operacional en las operaciones de la [organización].

## **3. GARANTÍA DE LA SEGURIDAD OPERACIONAL**

### **3.1 Supervisión y medición de la eficacia de la seguridad operacional**

La [organización] elaborará y mantendrá los medios para verificar la eficacia de la seguridad operacional de la organización y validar la efectividad de los controles de los riesgos de seguridad operacional. La eficacia de la seguridad operacional de la organización se verificará con referencia a los indicadores y los objetivos de eficacia de la seguridad operacional del SMS.

### **3.2 Gestión del cambio**

La [organización] elaborará y mantendrá un protocolo para identificar los cambios dentro de la organización que puedan afectar a los procesos y servicios establecidos; describir las disposiciones adoptadas para garantizar una buena eficacia de la seguridad operacional antes de introducir cualquier cambio y eliminar o modificar los controles de riesgos de seguridad operacional que ya no sean necesarios o efectivos debido a modificaciones del entorno operacional.

### **3.3 Mejora continua del SMS**

La [organización] elaborará y mantendrá un protocolo para identificar las causas de una actuación deficiente del SMS, determinar las consecuencias de las deficiencias del SMS en las operaciones y eliminar o mitigar las causas identificadas.

## **4. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL**

### **4.1 Instrucción y educación**

La [organización] elaborará y mantendrá un programa de instrucción en seguridad operacional que asegure que el personal cuente con la instrucción y competencia necesarias para cumplir con sus funciones en el marco del SMS. El alcance de la instrucción en seguridad se adaptará al grado de participación en el SMS de cada persona.

### **4.2 Comunicación de la seguridad operacional**

La [organización] elaborará y mantendrá un medio formal para la comunicación sobre seguridad operacional que asegure que todo el personal tiene pleno conocimiento del SMS, difunda información crítica respecto de la seguridad operacional y explique por qué se toman determinadas medidas de seguridad operacional y por qué se introducen o modifican procedimientos de seguridad operacional.

---



## Apéndice 2 del Capítulo 8

# EJEMPLO DE DESCRIPCIÓN DE TAREAS PARA UN GERENTE DE SEGURIDAD OPERACIONAL

### 1. PROPÓSITO GENERAL

El gerente de seguridad es responsable de proporcionar orientación y dirección para la planificación, implantación y funcionamiento del sistema de gestión de la seguridad operacional (SMS) de la organización.

### 2. FUNCIONES CLAVE

#### ***Promotor y defensor de la seguridad operacional***

- Demuestra un excelente comportamiento y actitud con respecto a la seguridad operacional, cumple con las prácticas reglamentarias y las reglas, reconoce y notifica los peligros y promueve la efectiva presentación de informes de seguridad operacional.

#### ***Líder***

- Modeliza y promueve una cultura de la organización que fomente las prácticas de seguridad operacional mediante una conducción efectiva.

#### ***Comunicador***

- Actúa como conducto de información para llevar los aspectos de seguridad operacional a la atención de la administración y presentar información de seguridad operacional al personal de la organización, sus contratistas y partes interesadas.
- Proporciona y articula información con respecto a asuntos de seguridad operacional dentro de la organización.

#### ***Innovador***

- Ayuda a la continua mejora de los planes de identificación de peligros y evaluación de riesgos de seguridad operacional y del SMS de la organización.

#### ***Forjador de relaciones***

- Forja y mantiene una excelente relación de trabajo con el Grupo de acción de seguridad operacional (SAG) y dentro de la Oficina de servicios de seguridad (SSO) de la organización.

#### ***Embajador***

- Representa a la organización en comités gubernamentales, de organismos internacionales y de la industria (p. ej., OACI, IATA, AAC, AIB, etc.).

**Analista**

- Analiza datos técnicos buscando tendencias relativas a peligros, sucesos y ocurrencias.

**Gestor de procesos**

- Utiliza efectivamente procesos y procedimientos aplicables para cumplir funciones y responsabilidades.
- Investiga oportunidades para aumentar la eficiencia de los procesos.
- Mide la efectividad y procura mejorar continuamente la calidad de los procesos.

**3. RESPONSABILIDADES**

3.1 El puesto requiere la capacidad de hacer frente, con poca supervisión, a circunstancias y situaciones cambiantes. El gerente de seguridad actúa independientemente de otros gerentes de la organización.

3.2 El gerente de seguridad es responsable de proporcionar información y asesoramiento a la administración superior y al Ejecutivo responsable sobre asuntos relacionados con la realización de operaciones seguras. Tacto, diplomacia y un alto grado de integridad son requisitos para el puesto.

3.3 El puesto exige flexibilidad, dado que puede ser necesario realizar las tareas con poco, o ningún, tiempo de aviso y fuera del horario de trabajo normal.

**4. CARÁCTER Y ÁMBITO DE LA FUNCIÓN**

El gerente de seguridad debe interactuar con el personal de operaciones, los administradores superiores y los jefes de departamentos de toda la organización. El gerente de seguridad debería fomentar relaciones positivas con las autoridades de reglamentación y con organismos y proveedores de servicio fuera de la organización. Cuando corresponda, se establecerán otras relaciones de trabajo.

**5. CUALIFICACIONES**

Entre las cualidades y cualificaciones necesarias figuran:

- a) amplios conocimientos y experiencia operacionales respecto a las funciones de la organización (p. ej., gestión de la instrucción, operaciones de aeronaves, gestión del tránsito aéreo, operaciones de aeródromo y gestión de la organización de mantenimiento);
- b) sólido conocimiento de los principios y prácticas de la gestión de la seguridad operacional;
- c) aptitud para comunicar bien, oralmente y por escrito;
- d) capacidad bien desarrollada para las relaciones interpersonales;
- e) capacidad para utilizar computadoras;

- f) capacidad para relacionarse en todos los niveles, tanto dentro como fuera de la organización;
- g) capacidad de organización;
- h) capacidad para trabajar sin supervisión;
- i) buena capacidad analítica;
- j) condiciones de liderazgo y autoridad; y
- k) merecer el respeto de sus pares y superiores.

## 6. AUTORIDAD

6.1 En cuestiones de seguridad operacional, el gerente de seguridad tiene acceso directo al Ejecutivo responsable y a la administración superior y media que corresponda.

6.2 El gerente de seguridad está autorizado a realizar auditorías de la seguridad operacional, encuestas e inspecciones de cualquier aspecto de las actividades.

6.3 El gerente de seguridad tiene autoridad para iniciar investigaciones de sucesos internos de seguridad operacional con arreglo a los procedimientos especificados en el manual de sistemas de gestión de la seguridad operacional (SMSM) de la organización.

---





## Capítulo 9

# FUNCIONAMIENTO DEL SMS

### 9.1 OBJETIVO Y CONTENIDO

En este capítulo se describen los requisitos relacionados con el funcionamiento de un SMS, utilizando como referencia el marco para SMS de la OACI. El primer componente del marco para SMS de la OACI se trató en el Capítulo 8. En este capítulo se analizan los tres componentes restantes del marco. El capítulo comprende los temas siguientes:

- a) Gestión de riesgos de seguridad operacional — Generalidades;
- b) Identificación de peligros;
- c) Evaluación y mitigación de riesgos de seguridad operacional;
- d) Garantía de la seguridad operacional — Generalidades;
- e) Supervisión y medición de la eficacia de la seguridad operacional;
- f) Protección de las fuentes de información de seguridad operacional;
- g) Gestión del cambio;
- h) Mejora continua del SMS;
- i) Relación entre gestión de riesgos de seguridad operacional (SRM) y garantía de la seguridad operacional (SA);
- j) Promoción de la seguridad operacional — Instrucción y educación; y
- k) Promoción de la seguridad operacional — Comunicación de seguridad operacional.

### 9.2 GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL — GENERALIDADES

9.2.1 Una organización gestiona la seguridad operacional garantizando que, en todo su proceso de gestión de la seguridad, los riesgos de seguridad de las consecuencias de los peligros en actividades críticas relativas a la prestación de servicios están controlados hasta un nivel tan bajo como sea razonable en la práctica (ALARP). Esto se conoce como gestión de riesgos de seguridad operacional, término genérico que engloba dos actividades distintas: identificación de peligros y evaluación y mitigación de los riesgos de seguridad operacional.

9.2.2 La gestión de los riesgos de seguridad operacional se apoya en un diseño de sistema en el cual están integrados controles apropiados de los riesgos de seguridad para eliminar o mitigar las consecuencias de los peligros previstos. Esto es cierto tanto si el “sistema” en cuestión es un sistema físico como una aeronave, o un sistema de organización como una línea aérea, un aeródromo o un proveedor de servicios de tránsito aéreo. En términos de este

manual, este último — sistema de organización — es el “sistema” al que se hace referencia más comúnmente. Una organización es un sistema que consiste en estructuras, procesos y procedimientos, así como personas, equipo e instalaciones, necesarios para cumplir su misión.

### 9.3 IDENTIFICACIÓN DE PELIGROS

9.3.1 La gestión de los riesgos de seguridad operacional comienza con una descripción de las funciones del sistema como base para la identificación de peligros (véase el Capítulo 7). En la descripción del sistema, los componentes y sus interfaces con el entorno operacional del sistema se analizan buscando peligros, así como para identificar los controles de los riesgos de seguridad operacional que ya existen en el sistema, o la ausencia de los mismos (proceso conocido como análisis de las carencias, también analizado en el Capítulo 7). Los peligros se analizan en el contexto del sistema descrito, se identifican sus consecuencias posiblemente perjudiciales, y se evalúan dichas consecuencias en términos de los riesgos de seguridad operacional (la probabilidad y la gravedad resultante del potencial perjudicial de las consecuencias identificadas, que se analizaron en el Capítulo 5). Donde se evalúa que los riesgos de seguridad operacional de las consecuencias de los peligros son demasiado elevados para ser aceptables, deben introducirse en el sistema controles adicionales de riesgo de seguridad operacional. La evaluación del diseño del sistema y la verificación de que controla adecuadamente las consecuencias del peligro es, por consiguiente, un elemento fundamental de la gestión de la seguridad operacional.

9.3.2 La identificación de los peligros es, entonces, la primera etapa de un protocolo de recoger, registrar, adoptar medidas y generar retroinformación sobre peligros y riesgos de seguridad en las operaciones. En un SMS adecuadamente implantado, las fuentes de identificación de peligros deben incluir los tres métodos analizados en el Capítulo 3: métodos reactivos, proactivos y predictivos. El propio proceso de identificación de peligros se analiza en el Capítulo 4.

9.3.3 Un enfoque estructurado de la identificación de peligros asegura que, en la medida posible, se identifican la mayoría de los peligros en el entorno operacional del sistema. Las técnicas adecuadas para asegurar dicho enfoque estructurado pueden incluir:

- a) **Listas de verificación.** Examen de la experiencia y datos disponibles del sistema similares y establecimiento de una lista de verificación de peligros. Los sectores potencialmente peligrosos exigirán mayor evaluación.
- b) **Examen de grupo.** Pueden utilizarse sesiones de grupos para examinar la lista de verificación de peligros, estudiar más ampliamente dichos peligros o llevar a cabo un detallado análisis del escenario.

9.3.4 Las sesiones de identificación de peligros exigen una gama de personal operacional y técnico experimentado y normalmente se realizan en forma de debates de grupo dirigidos. Un facilitador familiarizado con las técnicas de generar ideas en forma grupal (brainstorming) debería dirigir las sesiones del grupo. El gerente de seguridad, si está designado, normalmente cumpliría esta función. Si bien el uso de sesiones de grupo se trata aquí en el contexto de la identificación de peligros, el mismo grupo trataría también la evaluación de la probabilidad y gravedad de los riesgos de seguridad operacional de las consecuencias de los peligros que ha identificado.

9.3.5 En la evaluación de peligros se deberían tener en cuenta todas las posibilidades, desde la más pequeña hasta la más probable. Hay que prever adecuadamente las “peores” condiciones, pero también es importante que los peligros que se incluyan en el análisis final sean peligros “creíbles”. A menudo es difícil definir el límite entre un caso más desfavorable creíble y uno que depende tanto de coincidencias que no debería tenerse en cuenta. Para decidir sobre esto puede emplearse las definiciones siguientes:

- a) **Caso más desfavorable.** Se prevén las condiciones más desfavorables; p. ej., niveles de tránsito extremadamente elevados y perturbaciones meteorológicas extremas.
- b) **Caso creíble.** Esto supone que no es exagerado esperar que ocurra la combinación de condiciones extremas durante el ciclo de vida operacional del sistema.

9.3.6 Debería asignarse un número a cada uno de los peligros identificados y registrarlos en un registro de peligros (ejemplos de registro de peligros figuran en los apéndices del Capítulo 5). El registro de peligros debería contener una descripción de cada uno de los peligros, sus consecuencias, la evaluación de la probabilidad y gravedad de los riesgos de seguridad de las consecuencias, y los controles de los riesgos de seguridad operacional requeridos, generalmente, medidas de mitigación. El registro de peligros debería actualizarse a medida que se identifiquen nuevos peligros y se presenten propuestas para mejorar los controles de los riesgos de seguridad (es decir más medidas de mitigación).

## 9.4 EVALUACIÓN Y MITIGACIÓN DE RIESGOS

9.4.1 Una vez identificados los peligros, deben evaluarse los riesgos de seguridad de sus posibles consecuencias (Capítulo 5). La evaluación de los riesgos de seguridad operacional es el análisis de los riesgos de seguridad de las consecuencias de los peligros que se han determinado como que amenazan la capacidad de una organización. Los análisis de los riesgos de seguridad operacional utilizan un desglose convencional del riesgo en dos componentes — la probabilidad de ocurrencia de un suceso o condición perjudicial, y la gravedad del suceso o condición, en caso de que ocurra. Las decisiones del riesgo de seguridad operacional y su aceptación se especifican mediante el empleo de una matriz de aceptabilidad de los riesgos. Si bien se requiere una matriz, también se requiere discreción. Debería dejarse a la organización del proveedor de servicios el diseño de la definición y construcción final de la matriz, sujeta a aprobación de su organización de supervisión. Esto es para asegurar que las herramientas de decisión de cada organización son pertinentes a sus operaciones y entorno operacional, reconociendo la amplia diversidad en este sector.

9.4.2 Después de que los riesgos de seguridad operacional se han evaluado mediante el paso anterior, debe realizarse la eliminación o mitigación a nivel ALARP. Esto se conoce como mitigación de riesgo de seguridad operacional. Deben diseñarse e implantarse controles de riesgo de seguridad. Estos pueden ser procedimientos adicionales o modificados, nuevos controles de supervisión, cambios en la instrucción, equipo adicional o modificado o cualquier otra alternativa de eliminación/mitigación. Casi invariablemente, estas alternativas entrañarán la introducción o reintroducción de alguna de las tres defensas tradicionales de la aviación (tecnología, instrucción y reglamentación), o combinaciones de ellas. Después de haberse diseñado los controles de los riesgos de seguridad operacional, pero antes de que el sistema se coloque “en línea”, debe realizarse una evaluación para ver si los controles introducen nuevos peligros al sistema.

9.4.3 En este punto, el sistema está listo para la introducción/reintroducción operacional, suponiendo que los controles de los riesgos de seguridad operacional se consideran aceptables. El siguiente componente del SMS, la garantía de la seguridad operacional, emplea auditorías, análisis, examen y técnicas similares, armonizadas con las que se utilizan en los sistemas de gestión de la calidad. Estas técnicas se emplean para supervisar los controles de los riesgos de seguridad operacional y asegurar que continúan implantándose con arreglo al diseño y que también continúan siendo efectivos en el entorno operacional dinámico.

## 9.5 GARANTÍA DE LA SEGURIDAD OPERACIONAL — GENERALIDADES

9.5.1 La gestión de los riesgos de seguridad operacional requiere retroinformación sobre eficacia en la seguridad operacional para completar el ciclo de gestión de la seguridad. Mediante la supervisión y la retroinformación puede evaluarse la eficacia del SMS y efectuar los cambios al sistema que sean necesarios. Además, la garantía de la seguridad operacional proporciona a las partes interesadas una indicación del nivel de eficacia de la seguridad del sistema.

9.5.2 La garantía puede definirse sencillamente como “algo que da confianza”. El proceso de gestión de los riesgos de seguridad operacional en el SMS comienza con la obtención por la organización de una buena comprensión de sus procesos operacionales y los entornos en que funciona, avanza a través de la identificación de peligros, la evaluación de los riesgos de seguridad operacional y la mitigación de los riesgos de seguridad, y culmina en la elaboración e implantación de controles apropiados de los riesgos de seguridad operacional. Una vez que estos controles de riesgos de seguridad operacional de las consecuencias de los peligros se diseñan, consideran que son capaces de controlar los riesgos de seguridad y se ponen en funcionamiento, la garantía de la seguridad operacional se impone a la gestión de los riesgos de seguridad.

9.5.3 Una vez elaborados e implantados los controles de los riesgos de seguridad operacional, es responsabilidad de la organización asegurar que continúan instalados y que funcionan según lo previsto. En el marco de la definición anterior de “garantía”, ésta consiste en procesos y actividades emprendidas por la organización para brindar confianza en cuanto a la eficacia y efectividad de los controles. La organización debe supervisar continuamente sus operaciones y el entorno para asegurar que reconoce los cambios que puedan producirse en el entorno operacional y que podrían indicar el surgimiento de peligros nuevos y no mitigados, así como el deterioro de los procesos operacionales, instalaciones, condiciones del equipo o actuación humana que pudieran reducir la efectividad de los controles de riesgos de seguridad existentes. Esto indicaría la necesidad de regresar al proceso de gestión de los riesgos de seguridad para examinar y, si es necesario, revisar los controles existentes de los riesgos de seguridad o elaborar nuevos controles.

9.5.4 El proceso de examen, análisis y evaluación permanentes de estos controles debe continuar durante toda la operación cotidiana del sistema. El proceso de garantía de seguridad operacional es análogo al de garantía de la calidad, con requisitos relativos al análisis, documentación, auditoría, y exámenes por la administración de la efectividad de los controles de los riesgos de seguridad. La diferencia es que el énfasis en la garantía de la seguridad operacional está en la garantía de que están instalados los controles de los riesgos de seguridad, se les aplica y permanecen efectivos. El énfasis tradicional en la garantía de la calidad es normalmente la satisfacción del cliente que, a menos que se respeten las perspectivas adecuadas, puede o no ser plenamente paralela con la satisfacción de la seguridad operacional. A continuación se presenta un breve análisis.

9.5.5 La garantía de la calidad en la aviación se ha relacionado tradicionalmente con las operaciones de mantenimiento y fabricación y menos a menudo con las operaciones relacionadas con los vuelos, excepto por un uso limitado en la instrucción y verificación. En algunos de los primeros reglamentos se exhortaba a la introducción de programas de garantía de la calidad, aunque los requisitos a menudo no eran completos o bien definidos para todas las funciones de la organización. No obstante, permanece el hecho de que la garantía de la calidad es un término familiar aunque relacionado a menudo con la satisfacción del cliente y el logro de los objetivos comerciales más que la seguridad operacional. No obstante, como medio de asegurar el logro de los objetivos de la organización, las técnicas de garantía de la calidad son aplicables a la garantía de la seguridad operacional. Para aplicar esas técnicas a la garantía de la seguridad operacional, la organización debe establecer y medir cuidadosamente los objetivos con respecto de la seguridad.

9.5.6 El aspecto más importante es que la organización diseñe e implante todos los procesos operacionales en una forma que incorpore los controles de los riesgos de seguridad sobre la base de una correcta aplicación de los principios de gestión de los riesgos de seguridad y proporcione garantía de esos controles. La elección por la organización del título — “calidad” o “seguridad operacional” — para el proceso de garantía tiene menor importancia en la medida en que el foco en la seguridad operacional se mantenga en el SMS.

9.5.7 En el Capítulo 6 se analizan enfoques de la gestión de la seguridad operacional basados en el cumplimiento y en la eficacia. Un aspecto que puede no tenerse en cuenta al asegurar la eficacia, a menos que se observe una perspectiva adecuada, es la inclusión de la garantía de cumplimiento reglamentario. En el Capítulo 6 se introduce la noción de reglamentos como controles de los riesgos de seguridad operacional. En ese carácter, los reglamentos son parte integral del proceso de gestión de los riesgos de seguridad. En un SMS adecuadamente introducido, no debería haber conflictos entre la garantía de los riesgos de seguridad y la garantía de cumplimiento de

los reglamentos. Los reglamentos deberían ser parte del diseño del sistema y el cumplimiento de ellos y la gestión de los riesgos de seguridad son partes del mismo todo. El cumplimiento de los reglamentos es todavía una expectativa y debería integrar el ámbito de la garantía de seguridad como actividad dirigida a “dar confianza” en la eficacia del SMS.

9.5.8 En conclusión, la administración superior debe asegurar que los objetivos de satisfacción de la seguridad operacional y satisfacción del cliente están equilibrados a efectos de mantener la viabilidad comercial manteniendo también la seguridad de las operaciones. Si bien la integración de los objetivos del SMS y QMS podría resultar en economías de recursos, la posibilidad de disparidades entre los objetivos de satisfacción de la seguridad y los objetivos de satisfacción del cliente significa que ambos no son automáticamente intercambiables o coincidentes. La administración de la organización debe tener en cuenta este tipo de integración. La evaluación de la eficacia del sistema y la verificación de que la actuación del sistema continúa controlando los riesgos de seguridad en su entorno operacional actual sigue siendo la preocupación fundamental, desde la perspectiva de la gestión de la seguridad.

9.5.9 Por último, las actividades de garantía de la seguridad operacional deberían incluir procedimientos que aseguren la elaboración de medidas correctivas en respuesta a conclusiones de informes, estudios, encuestas, auditorías, evaluaciones, etc., y verificar su implantación oportuna y efectiva. La responsabilidad de la organización en cuanto al desarrollo e implantación de medidas correctivas debería corresponder a los departamentos operacionales que se mencionen en las conclusiones. Si se descubren nuevos peligros, el proceso de gestión de los riesgos de seguridad debería ampliarse para determinar si es necesario elaborar nuevos controles de riesgo de seguridad.

## 9.6 SUPERVISIÓN Y MEDICIÓN DE LA EFICACIA DE LA SEGURIDAD OPERACIONAL

9.6.1 La tarea principal de la garantía de la seguridad operacional es el control. Esto se logra mediante supervisión y medición de la eficacia de la seguridad, proceso por el cual se verifica la eficacia de la seguridad de la organización en comparación con la política de seguridad y objetivos de seguridad aprobados. El control de la garantía de la seguridad operacional se realiza supervisando y midiendo los resultados de las actividades que el personal operacional debe realizar para la prestación de servicios por la organización.

9.6.2 La norma internacional de gestión de la calidad, ISO-9000, proporciona la siguiente definición de proceso: “... un conjunto de actividades interrelacionadas que transforma insumos en productos”. El énfasis en “actividades” como básicamente “las cosas que hace la gente” es la razón por la cual se subraya tanto el error humano y las condiciones del lugar de trabajo en los análisis de seguridad y gestión de la seguridad en los Capítulos 2 y 3, y que en última instancia se traslada a la gestión de los riesgos de seguridad operacional. Estas condiciones están en la raíz de la mayoría de los peligros, y son el foco de atención de la mayoría de los controles de los riesgos de seguridad. Así pues, la mayoría de las actividades de garantía en el marco de la eficacia y supervisión de la seguridad operacional se concentran en las condiciones del lugar de trabajo que afectan la forma en que las personas realizan las actividades necesarias para la prestación de servicios. Por esta razón también el modelo SHELL — modelo de los sistemas que apoyan la realización de las actividades operacionales que llevan a la prestación de servicio — se propone como guía para la descripción del sistema y el análisis de las carencias.

9.6.3 A continuación se presenta una lista de aspectos o áreas genéricos que han de considerarse para “asegurar la seguridad” mediante supervisión y medición de la eficacia de la seguridad:

- a) **Responsabilidad.** Quién es responsable de la gestión de las actividades operacionales (planificación, organización, dirección, control) y su logro final.
- b) **Autoridad.** Quién puede dirigir, controlar o modificar los procedimientos y quién no, así como quién puede adoptar decisiones clave como las decisiones de aceptación de los riesgos de seguridad.
- c) **Procedimientos.** Formas especificadas de realizar actividades operacionales y que transforman el “qué” (objetivos) en “cómo” (actividades prácticas).

- d) **Controles.** Elementos del sistema, comprendiendo soporte físico, soporte lógico, procedimientos especiales o etapas de procedimiento así como prácticas de supervisión diseñadas para la realización correcta de las actividades operacionales.
- e) **Interfaces.** Examen de las líneas de autoridad entre departamentos, líneas de comunicación entre empleados, coherencia de procedimientos y clara delineación de responsabilidades entre organizaciones, dependencias laborales y empleados.
- f) **Medidas de proceso.** Medios de proporcionar a las partes responsables información de que las actividades requeridas se están realizando, los productos requeridos se están produciendo y los resultados previstos se están alcanzando.

9.6.4 La información para la eficacia y la supervisión de la seguridad operacional procede de varias fuentes, incluyendo auditorías formales y evaluación, investigaciones de sucesos relacionados con la seguridad, supervisión continua de las actividades cotidianas relacionadas con la prestación de servicios y aportes de los empleados a través de los sistemas de notificación de peligros. Cada uno de estos tipos de fuentes de información puede existir en alguna medida en toda organización. No obstante, las especificaciones con respecto a lo que estas fuentes deberían ser o qué aspecto deberían adoptar, deberían corresponder a un nivel operacional, dejando a cada organización que las adapte al ámbito y escala adecuados al tamaño y tipo de organización. Las fuentes de información para la supervisión y medición de la eficacia de la seguridad operacional comprenden:

- a) informes sobre peligros;
- b) estudios de seguridad;
- c) exámenes de seguridad;
- d) auditorías;
- e) encuestas de seguridad; y
- f) investigaciones internas de seguridad.

9.6.5 La notificación de peligros y los sistemas para ello son elementos esenciales en la identificación de los peligros. Nadie conoce mejor la actuación real del sistema que el personal operacional. Una organización que desee saber cómo funciona realmente todos los días, frente a cómo debería funcionar con arreglo “al librito”, debería preguntar al personal operacional, de ahí la importancia de los sistemas de presentación de informes. Hay tres tipos de sistemas de notificación:

- a) sistemas de notificación obligatoria;
- b) sistemas de notificación voluntaria; y
- c) sistemas de notificación confidencial.

9.6.6 En los **sistemas de notificación obligatoria**, las personas deben notificar ciertos tipos de sucesos o peligros. Esto exige reglamentos detallados que establezcan quienes deberán informar y qué deberá informarse. Dado que los sistemas obligatorios tratan principalmente de asuntos de “soporte físico” tienden a recoger más información sobre fallas técnicas que sobre otros aspectos de actividades operacionales. Para superar ese sesgo, los sistemas de notificación voluntaria se dirigen a adquirir más información sobre esos otros aspectos.

9.6.7 En los **sistemas de notificación voluntaria** el informante, sin ningún requisito jurídico o administrativo de hacerlo, presenta información voluntaria sobre sucesos o peligros. En estos sistemas, los organismos u organizaciones de reglamentación pueden ofrecer un incentivo para informar, por ejemplo, pueden no aplicarse medidas disciplinarias

para sucesos que se notifiquen destacando errores o violaciones involuntarias. La información notificada no debería emplearse contra los informantes, es decir, que tales sistemas deben ser no punitivos y brindar protección de las fuentes de información para fomentar la presentación de dicha información.

9.6.8 Los **sistemas de notificación confidencial** se dirigen a proteger la identidad del informante. Esta es una forma de asegurar que los sistemas de notificación voluntaria son no punitivos. La confidencialidad se logra normalmente mediante la no identificación, y cualquier información de identificación sobre el informante será conocida solamente por los “porteros” para hacer lugar al seguimiento o “rellenar blancos” en los sucesos notificados. Los sistemas de presentación de informes confidenciales sobre incidentes facilitan la revelación de peligros que conducen al error humano, sin temor a castigos o situaciones embarazosas y permitir la adquisición más amplia de información sobre peligros.

9.6.9 Si bien los procesos básicos en que se basan los sistemas de notificación son normalizados, los requisitos reales de presentación de informes pueden variar entre los Estados y las organizaciones. Es también importante señalar, para asegurar el éxito de los sistemas de presentación de informes, que existe una reticencia normal del personal operacional a informar. Esta afirmación es válida para todos los tipos de notificación, y se aplica en particular cuando se trata de notificar los errores propios. Hay razones para esta reticencia: el temor de represalias, la autoincriminación y las situaciones difíciles son las tres principales. La enseñanza en términos de la importancia de presentar informes de seguridad en los sistemas de identificación de peligros, analizada en el Capítulo 2, y la protección de las fuentes de la información de seguridad (que se verá en la sección 9.7) son estrategias esenciales para superar la reticencia a informar y asegurar un entorno efectivo de presentación de informes de seguridad. Las cualidades típicas de los sistemas de notificación de seguridad exitosos comprenden:

- a) los informes son fáciles de hacer;
- b) no hay medidas disciplinarias como resultado de los informes;
- c) los informes son confidenciales; y
- d) la retroinformación es rápida, accesible e informativa.

9.6.10 Los **estudios de seguridad operacional** son análisis más bien grandes que abarcan amplias preocupaciones de seguridad. Algunos penetrantes problemas de seguridad pueden comprenderse mejor mediante un examen en el contexto más amplio posible. Una organización podría experimentar un problema de seguridad que no es de carácter global, y que puede haber sido tratado a escala industrial o estatal. Por ejemplo, una línea aérea puede experimentar un aumento del número de sucesos relacionados con la aproximación y el aterrizaje (aproximaciones no estabilizadas, aterrizajes en pérdida profunda, aterrizajes con excesiva velocidad, etc.). A nivel global, la industria se ha visto preocupada por la frecuencia y gravedad de los accidentes de aproximación y aterrizaje (ALA) y ha emprendido importantes estudios, producido muchas recomendaciones de seguridad e implantado medidas mundiales para reducir tales sucesos durante las fases críticas de vuelo de aproximación y aterrizaje. Así pues, la línea aérea en cuestión puede encontrar en estas recomendaciones y estudios globales argumentos convincentes para sus propios análisis de seguridad internos. Dichos argumentos son necesarios para lograr cambios en gran escala que requieran datos significativos, análisis apropiados y comunicaciones efectivas. Los argumentos de seguridad operacional basados en sucesos aislados e información anecdótica pueden no ser suficientes. Debido a su carácter, los estudios de seguridad operacional son más apropiados para tratar las deficiencias de seguridad del sistema que para identificar peligros específicos e individuales.

9.6.11 Los **exámenes de seguridad operacional** se realizan durante la introducción y distribución de nuevas tecnologías, cambio o implantación de procedimientos, o en situaciones de cambio estructural en las operaciones. Los exámenes de seguridad operacional son un componente fundamental de la gestión del cambio, que se analizará en la sección 9.8. Tienen un objetivo claramente definido que está relacionado con el cambio en consideración. Por ejemplo, un aeropuerto está considerando implantar equipo de detección en la superficie del aeropuerto (ASDE). Por lo tanto, el objetivo del examen de seguridad operacional sería evaluar los riesgos de seguridad relacionados con la implantación

de un ASDE en el aeropuerto XYZ valorando la adecuación y eficacia de las actividades de gestión de la seguridad operacional relacionadas con el proyecto. Los exámenes de seguridad son efectuadas por los Grupos de acción de seguridad operacional (SAG), que procuran establecer la realización efectiva de las siguientes actividades de gestión de la seguridad en el marco de los cambios propuestos:

- a) identificación de peligros y evaluación/mitigación de los riesgos de seguridad;
- b) medición de la seguridad operacional;
- c) responsabilidades de la administración;
- d) competencia del personal operacional;
- e) sistemas técnicos; y
- f) operaciones anormales.

9.6.12 Una vez examinada la eficacia de cada actividad de gestión de la seguridad en el marco de los cambios propuestos, el SAG produce una lista de peligros para cada actividad, la respuesta/mitigación propuesta por el gerente de línea y una evaluación de la adecuación y efectividad de las mitigaciones para tratar los peligros. La mitigación será apropiada si trata realmente el peligro. La mitigación será efectiva si gestiona coherentemente los riesgos de seguridad operacional en las condiciones operacionales normales para reducir los riesgos de seguridad a un nivel ALARP. El SAG también propone establecer prioridades en las respuestas/mitigaciones, asignando importancia y urgencia a cada peligro. Así pues, los exámenes de seguridad operacional aseguran la eficacia de la seguridad durante períodos de cambio, proporcionando una hoja de ruta hacia el cambio seguro y efectivo.

9.6.13 Las **auditorías** se concentran en la integridad del SMS de la organización y evalúan periódicamente el estado de los controles de los riesgos de seguridad operacional. Al igual que otros requisitos, los requisitos de auditoría corresponden al nivel funcional, haciendo lugar a una amplia gama de complejidad, conmensurable con la complejidad de la organización. Si bien las auditorías son “externas” a las dependencias involucradas en las actividades directamente relacionadas con la provisión de servicios, aún son “internas” a la organización en su totalidad. Las auditorías no están concebidas para ser auditorías profundas de los procesos técnicos sino más bien para proporcionar garantías de las funciones de gestión de la seguridad, así como las actividades y recursos de las dependencias en línea. Las auditorías se utilizan para asegurar que la estructura del SMS es sólida en términos de niveles apropiados de personal, cumplimiento de los procedimientos e instrucciones aprobados, niveles de competencia e instrucción para operar el equipo e instalaciones y mantener niveles requeridos de desempeño, etc.

9.6.14 Las **encuestas de seguridad** examinan elementos particulares o procesos de una operación específica, como las áreas con problemas o cuellos de botella en las operaciones diarias, las percepciones y opiniones del personal operativo y las áreas de disenso o confusión. Las encuestas de seguridad pueden entrañar el uso de listas de verificación, cuestionarios y entrevistas confidenciales informales. Dado que la información de las encuestas es subjetiva, es necesaria una verificación antes de poner en marcha las medidas correctivas. Las encuestas pueden ser una fuente poco costosa de importante información de seguridad.

9.6.15 Las **investigaciones internas de seguridad** incluyen sucesos que no requieren ser investigados o notificados al Estado, aunque en algunos casos las organizaciones pueden realizar investigaciones internas aunque el suceso en cuestión esté siendo investigado por el Estado. Entre los ejemplos de ocurrencias o sucesos que corresponden al ámbito de las investigaciones internas de seguridad figuran: turbulencia en vuelo (operaciones de vuelo), congestión de frecuencias (ATC), falla del material (mantenimiento) y operaciones de vehículos en la rampa (aeródromos).



9.6.16 En conclusión, la contribución de las fuentes de información sobre eficacia y supervisión de la seguridad operacional al SMS de una organización pueden resumirse como sigue:

- a) la notificación sobre peligros es una fuente principal de información sobre peligros en las operaciones;
- b) los estudios de seguridad son una fuente de información sobre problemas genéricos de seguridad operacional o deficiencias sistémicas de seguridad operacional;
- c) los exámenes de seguridad están relacionados con la gestión del cambio y garantizan la eficacia de la seguridad en condiciones operacionales cambiantes;
- d) las auditorías aseguran la integridad de estructuras y procesos del SMS;
- e) las encuestas de seguridad recaban la opinión de los expertos y sus percepciones sobre áreas problemáticas específicas en las operaciones cotidianas; y
- f) las investigaciones internas de seguridad tratan los resultados de menor magnitud que no requieren ser investigados por el Estado.

## 9.7 PROTECCIÓN DE LAS FUENTES DE INFORMACIÓN DE SEGURIDAD OPERACIONAL

9.7.1 El notable historial de seguridad operacional de la aviación civil internacional se debe, entre otras cosas, a dos factores principales: un continuo proceso de aprendizaje, basado en la elaboración y libre intercambio de información de seguridad y la capacidad de transformar los errores en medidas preventivas. Desde hace tiempo se ha reconocido que las actividades dirigidas a mejorar la seguridad operacional de la aviación civil contemporánea deben basarse en datos empíricos. Existen varias fuentes de tales datos disponibles a la aviación civil. Combinados, proporcionan la base para una sólida comprensión de las virtudes y defectos de las operaciones aeronáuticas.

9.7.2 Durante años, la información de investigaciones de accidentes e incidentes constituyó la columna vertebral de las actividades dirigidas a mejorar el diseño del equipo, procedimientos de mantenimiento, instrucción de tripulaciones de vuelo, sistemas de control de tránsito aéreo, diseño y funciones de aeródromo, servicios de apoyo meteorológico y otros aspectos críticos para la seguridad del sistema de transporte aéreo. En los últimos años, la disponibilidad de medios tecnológicos ha llevado a un desarrollo acelerado de la recolección de datos de seguridad operacional, sistemas de procesamiento e intercambio de los mismos [denominados en lo que sigue, en combinación con la investigación y notificación de accidentes e incidentes, sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS)]. Los SDCPS, según se analizó en el Capítulo 3, son fundamentales para el SMS y generan información que se utiliza para implantar medidas de seguridad correctivas y estrategias continuas.

9.7.3 Los SDCPS han permitido a la aviación civil obtener una comprensión más profunda de los errores operacionales: por qué suceden, qué puede hacerse para minimizar su ocurrencia, y cómo contener sus consecuencias negativas para la seguridad operacional. Sigue siendo evidente que los peligros conducen a errores operacionales en la aviación, la amplia mayoría de los cuales son inadvertidos. Las personas bien capacitadas y bien intencionadas cometen errores cuando mantienen, operan o controlan equipo bien diseñado. Para esas raras situaciones en que los errores son resultado de actos voluntarios, abuso de sustancias adictivas, sabotaje o violaciones, existen sistemas de observancia que garantizan que la cadena de responsabilidades permanece intacta. Este enfoque doble, combinar una mejor comprensión de los errores operacionales inadvertidos con la apropiada observancia de las reglas en caso de mala conducta, ha servido muy bien a la aviación civil en términos de seguridad, garantizando al mismo tiempo que no hay en ella lugar para transgresores.

9.7.4 No obstante, en los últimos años se ha registrado una tendencia en la aviación civil cuando trata de errores operacionales que llevan a ocurrencias, de que la información del SDCPS se ha utilizado para fines disciplinarios y represivos. También se han admitido como prueba en procedimientos judiciales, lo que ha resultado en la presentación de acusaciones criminales contra individuos involucrados en tales ocurrencias. La presentación de acusaciones criminales en ocurrencias aeronáuticas resultantes de errores operacionales inadvertidos pueden perjudicar el desarrollo y el libre intercambio de información de seguridad operacional que es esencial para mejorar la seguridad aeronáutica.

9.7.5 Varias iniciativas dentro de la comunidad de la aviación civil internacional han intentado tratar la protección del SDCPS. No obstante, dado el carácter delicado de la cuestión, es esencial contar con un marco que proporcione unidad de propósito y coherencia entre todas las actividades de la aviación civil. Las actividades para asegurar la protección de la información de seguridad deben lograr un muy delicado equilibrio entre la necesidad de proteger la información de seguridad y la responsabilidad de administrar justicia. Debería adoptarse un cauteloso enfoque a este respecto para evitar formular propuestas que puedan ser incompatibles con las leyes correspondientes a la administración de justicia en los Estados contratantes.

9.7.6 El 35º período de sesiones de la Asamblea de la OACI consideró el tema de la protección de las fuentes y la libre circulación de la información de seguridad y adoptó la Resolución A35-17 de la Asamblea — *Protección de la información obtenida por medio de sistemas de recopilación y procesamiento de datos sobre seguridad operacional para mejorar la seguridad operacional de la aviación*. Esta resolución instaba al Consejo de la OACI a “elaborar orientación jurídica apropiada con el propósito de asistir a los Estados en la promulgación de sus leyes y reglamentos nacionales para proteger la información obtenida de todos los sistemas de recopilación y procesamiento de datos sobre seguridad operacional pertinentes, permitiendo al mismo tiempo la administración apropiada de la justicia en el Estado”.

9.7.7 Como primer paso en la elaboración de la orientación jurídica pedida en la Resolución A35-17 de la Asamblea, la OACI pidió a algunos Estados que proporcionaran ejemplos de sus leyes y reglamentos pertinentes relativos a la protección de la información del SDCPS. Posteriormente, la OACI realizó un análisis de los textos recibidos de los Estados, buscando líneas y puntos conceptuales comunes en las leyes y reglamentos proporcionados.

9.7.8 La consecuente orientación jurídica (contenida en el Adjunto E del Anexo 13 — *Investigación de accidentes e incidentes de aviación*) tiene el propósito de asistir a los Estados en la promulgación de sus leyes y reglamentos nacionales para proteger la información obtenida de los SDCPS, permitiendo al mismo tiempo la administración apropiada de la justicia. El objetivo consiste en impedir que sea un uso inapropiado de la información recopilada exclusivamente con la finalidad de mejorar la seguridad operacional de la aviación. Teniendo en cuenta que debería permitirse a los Estados contar con flexibilidad para redactar sus leyes y reglamentos de acuerdo con sus políticas y prácticas nacionales, la orientación jurídica toma la forma de una serie de principios que pueden adaptarse para satisfacer las necesidades particulares de los Estados que promulguen las leyes y reglamentos para proteger la información sobre seguridad operacional. A continuación se presenta un breve esbozo de la orientación.

9.7.9 La orientación jurídica incluye principios generales que declaran:

- a) el único propósito de proteger la información sobre seguridad operacional del uso inapropiado es asegurar la continua disponibilidad a fin de poder tomar medidas preventivas adecuadas y oportunas y mejorar la seguridad operacional de la aviación;
- b) la protección de la información sobre seguridad operacional no tiene el propósito de interferir con la debida administración de la justicia en los Estados;
- c) las leyes y reglamentos nacionales que protegen la información sobre seguridad operacional deben garantizar un equilibrio entre la necesidad de proteger dicha información, a fin de mejorar la seguridad operacional de la aviación, y la de administrar debidamente la justicia;

- d) las leyes y reglamentos nacionales que protegen la información sobre seguridad operacional deben impedir que ésta se utilice en forma inapropiada; y
- e) ofrecer protección para información calificada sobre seguridad operacional en condiciones específicas es parte de las responsabilidades que en materia de seguridad operacional tiene un Estado.

9.7.10 La orientación incluye principios de protección, como sigue:

- a) la información sobre seguridad operacional debe reunir los requisitos para ser protegida del uso inapropiado de acuerdo con condiciones específicas que deberían incluir, sin limitarse necesariamente a ellas: la recopilación de información se hace para fines explícitos de seguridad operacional y su divulgación impediría su continua disponibilidad;
- b) la protección debe ser específica para cada SDCPS, dependiendo de la naturaleza de la información sobre seguridad operacional que contenga;
- c) debe establecerse un procedimiento formal para proteger información calificada sobre seguridad operacional, de acuerdo con condiciones específicas;
- d) la información sobre seguridad operacional no deberá utilizarse para fines distintos de aquellos para los que fue recopilada; y
- e) el uso de información sobre seguridad operacional en procedimientos disciplinarios, civiles, administrativos y criminales, se llevará a cabo sólo bajo garantías adecuadas de la legislación nacional.

9.7.11 La orientación señala que se harán excepciones respecto de la protección de la información sobre seguridad operacional sólo mediante leyes y reglamentos nacionales cuando:

- a) exista evidencia de que el evento ha sido originado por un acto que, de acuerdo con la ley, se considere que ha sido con la intención de causar daño, o con el conocimiento de la posibilidad de que éste se originaría, y equivalga a una conducta temeraria, a negligencia grave o a acto doloso;
- b) una autoridad competente considere que las circunstancias indican razonablemente que el evento puede haber sido originado con la intención de causar daño, o con el conocimiento de la posibilidad de que éste se originaría, y equivalga a una conducta temeraria, a negligencia grave o a acto doloso; o
- c) mediante un examen de una autoridad competente, se determine que la divulgación de la información sobre seguridad operacional es necesaria para la administración apropiada de la justicia y que su divulgación pesa más que las repercusiones adversas que a escala nacional e internacional dicha divulgación pueda tener en la futura disponibilidad de la información sobre seguridad operacional.

9.7.12 La orientación también trata el tema de la divulgación al público, proponiendo que, con sujeción a los principios de protección y excepción resumidos anteriormente, cualquier persona que busque divulgar información sobre seguridad operacional tendrá que justificar dicha divulgación. Deberán establecerse criterios formales para la divulgación de información de seguridad operacional, y estos comprenderán, entre otras cosas, lo siguiente:

- a) la divulgación de la información sobre seguridad operacional es necesaria para corregir las condiciones que comprometen la seguridad operacional y para cambiar políticas y reglamentos;
- b) la divulgación de la información sobre seguridad operacional no impide su futura disponibilidad a fin de mejorar la seguridad operacional;

- c) la divulgación de información personal pertinente incluida en la información sobre seguridad operacional cumple con las leyes de confidencialidad que resulten aplicables; y
- d) la divulgación de la información sobre seguridad operacional se hace sin revelar las identidades y en forma resumida o combinada.

9.7.13 La orientación también analiza la responsabilidad del custodio de la información sobre seguridad operacional, proponiendo que cada SDCPS deberá contar con la designación de un custodio. Es responsabilidad del custodio de la información sobre seguridad operacional aplicar toda la protección posible en relación con la divulgación de la información, a menos que:

- a) el custodio de la información sobre seguridad operacional cuente con el consentimiento del originador de la información para que ésta se divulgue; o
- b) el custodio de la información sobre seguridad operacional tenga la seguridad de que la divulgación de la información sobre seguridad operacional se hace de acuerdo con los principios de excepción.

9.7.14 Por último, la orientación analiza la protección de la información registrada y, considerando que las grabaciones ambiente de las conversaciones en el lugar de trabajo exigidas por la delegación como es el caso de los registradores de la voz en el puesto de pilotaje (CVR) pueden percibirse como una invasión de la privacidad en el caso del personal de operaciones, situación a la que otras profesiones no están expuestas propone que:

- a) con sujeción a los principios de protección y excepción anteriores, las leyes y reglamentos nacionales deberán considerar las grabaciones ambiente de las conversaciones en el lugar de trabajo exigidas por la legislación como información protegida y privilegiada, es decir como información que merece mayor protección; y
- b) las leyes y reglamentos nacionales deberán proporcionar medidas específicas para proteger dichas narraciones en cuanto a su carácter confidencial y a su acceso al público. Dichas medidas específicas de protección de las grabaciones de las conversaciones en el lugar de trabajo que exige la legislación pueden incluir la emisión de órdenes judiciales de no divulgación al público.

## 9.8 GESTIÓN DEL CAMBIO

9.8.1 Las organizaciones de aviación experimentan cambios permanentes debido a expansión, contracción, cambios a los sistemas existentes, equipo, programas, productos y servicios e introducción de nuevos equipos o procedimientos. Los peligros pueden introducirse inadvertidamente en una operación cuando ocurren cambios. Las prácticas de gestión de la seguridad operacional exigen que los peligros que son resultados secundarios de los cambios sean sistemática y proactivamente identificados y que las estrategias para gestionar los riesgos de seguridad de las consecuencias de los peligros se elaboren, implanten y evalúen posteriormente. Los exámenes de seguridad, analizados en 9.6.11, son una valiosa fuente de información y de adopción de decisiones en circunstancias de cambio.

9.8.2 El cambio puede introducir nuevos peligros, impactar la adecuación de las estrategias de mitigación de los riesgos de seguridad existentes o afectar la eficacia de esas estrategias. Los cambios pueden ser externos a la organización o internos. Entre los cambios externos figuran los cambios de los requisitos reglamentarios, cambios en los requisitos de seguridad aeroportuaria y reorganización del control del tránsito aéreo. Entre los cambios internos figuran los cambios de administración, equipo nuevo y nuevos procedimientos.

9.8.3 Un protocolo para la gestión del cambio debería tener en cuenta las tres consideraciones siguientes:

- a) **Criticidad de los sistemas y actividades.** La criticidad se relaciona estrechamente con el riesgo de seguridad operacional. La criticidad se refiere a las consecuencias potenciales de que el equipo sea inadecuadamente operado o que una actividad se ejecute en forma incorrecta, y esencialmente responde a la pregunta: “¿cuán importante es este equipo/actividad para las operaciones seguras del sistema?”. Si bien esta es una consideración que debería tenerse en cuenta durante el proceso de diseño del sistema, se hace más evidente durante una situación de cambio. Claramente, algunas actividades son más esenciales para la prestación segura de servicios que otras. Por ejemplo, los cambios en actividades o procedimientos relativos al retorno al servicio de una aeronave después de un mantenimiento importante en una organización que ha implantado por primera vez su propia organización de mantenimiento después de subcontratar previamente dicho mantenimiento por terceros, podría considerarse como más crítica para la seguridad que un escenario similar respecto de cambios en las actividades de los servicios de comidas. El equipo y las actividades que tienen una criticidad más elevada respecto de la seguridad deberían examinarse después de los cambios para asegurar que pueden adoptarse medidas correctivas a fin de controlar posibles riesgos de seguridad operacional emergentes.
- b) **Estabilidad de sistemas y entornos operacionales.** Los cambios pueden ser resultado de cambios programados como crecimiento, operaciones a nuevos destinos, cambios en las flotas, cambios en los servicios contratados u otros cambios directamente bajo control de la organización. Los cambios en el entorno operacional son también importantes, tales como la situación económica o financiera, la agitación laboral, cambios en entornos políticos o normativos o cambios en el entorno físico como los que se producen cíclicamente en los sistemas meteorológicos. Si bien estos factores no están bajo control directo de la organización, ésta debe adoptar medidas para responder a ellos. Los cambios frecuentes en los sistemas o entornos operacionales hacen que la administración deba actualizar la información clave con mayor frecuencia que en situaciones más estables. Esta es una condición esencial para la gestión del cambio.
- c) **Desempeño anterior.** El desempeño anterior de los sistemas críticos es un indicador reconocido del desempeño futuro. Es aquí donde entra en juego el carácter de círculo cerrado de la garantía de la seguridad operacional. Deberían emplearse análisis de tendencias en el proceso de garantía de la seguridad para hacer el seguimiento en el tiempo de las medidas de eficacia de la seguridad operacional e incluir esta información en la planificación de actividades futuras en situaciones de cambio. Además, donde se hayan encontrado y corregido deficiencias como resultado de auditorías, evaluaciones, investigaciones o informes anteriores, es esencial que dicha información se tenga en cuenta para asegurar la efectividad de las medidas correctivas.

9.8.4 Entonces, un protocolo de gestión del cambio debería identificar los cambios en la organización que puedan afectar los procesos, procedimientos, productos y servicios establecidos. Antes de implantar cambios, un proceso de gestión del cambio debería describir los arreglos para asegurar la eficacia de la seguridad. El resultado de este proceso es la reducción a nivel ALARP de los riesgos de seguridad operacional que resultan de los cambios en el suministro de servicios por la organización.

9.8.5 En el Capítulo 7 se analiza la importancia de describir el sistema (descripción del sistema) como una de las actividades preliminares fundamentales en la planificación de un SMS. El objetivo de la descripción del sistema es determinar un análisis de peligros de referencia para el sistema de referencia. A medida que el sistema evoluciona, pueden acumularse con el tiempo cambios aparentemente pequeños y graduales en el sistema (o en el entorno que proporciona el contexto para la operación del sistema), que harán que la descripción inicial del sistema no resulte adecuada. Por consiguiente, como parte del protocolo de gestión del cambio, la descripción del sistema y el análisis de peligros de referencia deberían examinarse periódicamente, incluso si no existen circunstancias de cambio, para determinar su validez continua. Cuando se introducen cambios en el sistema, y después periódicamente, la organización

debería examinar todo el sistema, su entorno operacional previsto y su entorno operacional real, para asegurar que continúa teniendo un panorama claro de las circunstancias en que tiene lugar la prestación de servicios.

## 9.9 MEJORA CONTINUA DEL SMS

9.9.1 La garantía de la seguridad se basa en el principio del ciclo de mejora continua. Casi de la misma forma en que la garantía de la calidad facilita las mejoras continuas de la calidad, la garantía de la seguridad asegura el control de la eficacia de la seguridad operacional incluyendo el cumplimiento de los reglamentos mediante una verificación y mejoramiento constantes del sistema operacional. Estos objetivos se logran con la aplicación de herramientas similares: evaluaciones internas y auditorías independientes (tanto internas como externas), estrictos controles de los documentos y supervisión continua de los controles de seguridad y medidas de mitigación.

9.9.2 Las **evaluaciones internas** entrañan la evaluación de las actividades operacionales de la organización así como las funciones específicas del SMS. Las evaluaciones que se realizan para estos fines deben ser efectuadas por personas u organizaciones que sean funcionalmente independientes del proceso técnico que se evalúa (es decir, un departamento especializado en garantía de la seguridad o de la calidad u otra suborganización según lo decida la administración superior). La función de evaluación interna también requiere la auditoría y la evaluación de las funciones de gestión de la seguridad operacional, la adopción de políticas, la gestión de los riesgos de seguridad, la garantía de la seguridad y la promoción de la seguridad. Estas auditorías proporcionan a los administradores responsabilidad designada para que el SMS haga el inventario de los procesos en el propio SMS.

9.9.3 Las **auditorías internas** son una herramienta importante para los administradores a fin de obtener información con la cual adoptar decisiones y mantener en marcha las actividades operacionales. La responsabilidad principal de la gestión de la seguridad corresponde a aquellos a quienes “pertenecen” las actividades técnicas de la organización en apoyo de la prestación de servicios. Es aquí donde los peligros se encuentran con mayor frecuencia, donde las deficiencias de las actividades contribuyen a los riesgos de seguridad y donde el control de supervisión directo y la asignación de recursos pueden mitigar los riesgos de seguridad operacional a un nivel ALARP. Si bien a menudo se piensa que las auditorías internas son un ensayo o “clasificación” de las actividades de la organización, son en verdad una herramienta esencial para la garantía de la seguridad, que ayuda a los administradores a cargo de las actividades que apoyan la prestación de servicios a controlar que, una vez implantado los controles de los riesgos, continúan funcionando y son efectivos en el mantenimiento de la seguridad operacional continua.

9.9.4 Las **auditorías externas** del SMS pueden ser efectuadas por el reglamentador, socios en código compartido, organizaciones de clientes u otras terceras partes seleccionadas por la organización. Estas auditorías no sólo proporcionan una sólida interfaz con el sistema de supervisión sino también constituyen un sistema de garantía secundario.

9.9.5 La continua mejora del SMS está entonces dirigida a determinar las causas inmediatas del desempeño inferior a las normas y sus consecuencias en el funcionamiento del SMS, así como rectificar las situaciones que entrañen desempeño inferior a las normas identificadas mediante las actividades de garantía de la seguridad operacional. La mejora continua se logra mediante evaluaciones internas, auditorías internas y externas y se aplica a:

- a) la evaluación proactiva de las instalaciones, equipo, documentación y procedimientos, por ejemplo evaluaciones internas;
- b) la evaluación proactiva del desempeño individual para verificar el cumplimiento de las responsabilidades de seguridad del individuo, por ejemplo, mediante verificaciones periódicas de la competencia (una forma de evaluación/auditoría); y
- c) una evaluación reactiva para verificar la eficacia del sistema de control y mitigación de riesgo de seguridad, por ejemplo, mediante auditorías internas y externas.

9.9.6 Como conclusión, la mejora continua puede ocurrir solamente cuando la organización desarrolla una vigilancia constante respecto de la efectividad de sus operaciones técnicas y sus medidas correctivas. En verdad, sin una supervisión continua de los controles de seguridad y medidas de mitigación, no hay forma de establecer si el proceso de gestión de la seguridad operacional está alcanzando sus objetivos. Análogamente, no hay forma de medir si el SMS está cumpliendo su finalidad con eficiencia.

## **9.10 RELACIÓN ENTRE GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL (SRM) Y GARANTÍA DE LA SEGURIDAD OPERACIONAL (SA)**

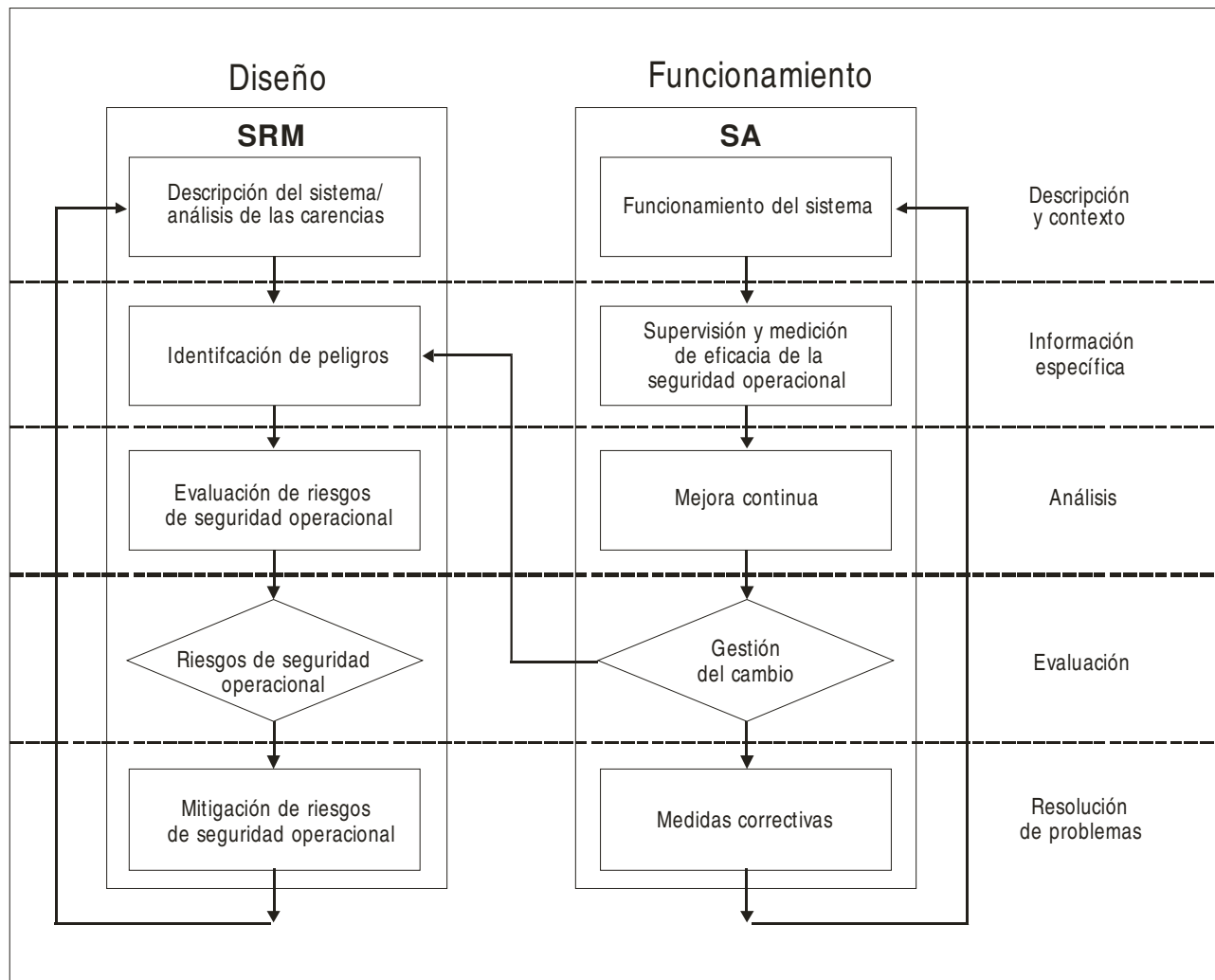
9.10.1 Las sutilezas de la relación entre la gestión de los riesgos de seguridad operacional y la garantía de la seguridad operacional son a menudo fuente de confusión. Una de las primeras tareas en la gestión efectiva de riesgos de seguridad y de garantía de la seguridad es que tanto el proveedor de servicios como la autoridad supervisora de aviación civil tengan una plena comprensión de la configuración y estructura del sistema de la organización y sus actividades. Existe un número considerable de peligros y riesgos de seguridad debidos al diseño inadecuado de estas actividades o a una defectuosa adaptación entre el sistema y su entorno operacional. En estos casos, puede que no se comprendan bien los peligros para la seguridad operacional y, por lo tanto, tampoco se controlen adecuadamente.

9.10.2 La función de gestión de los riesgos de seguridad operacional de un SMS comprende la identificación inicial de peligros y la evaluación de los riesgos de seguridad operacional. Se elaboran controles de los riesgos de seguridad operacional en la organización y, una vez que se haya determinado su capacidad de reducir a nivel ALARP el riesgo de seguridad, se emplean en las operaciones cotidianas. La función de garantía de la seguridad operacional se inicia en este punto para asegurar que los controles de los riesgos de seguridad se ejercen con arreglo a lo previsto y que continúan logrando sus objetivos previstos. La función de garantía de la seguridad operacional también permite la identificación de la necesidad de nuevos controles de los riesgos de seguridad debido a la introducción de cambios en el entorno operacional.

9.10.3 En un SMS, los requisitos de seguridad operacional del sistema se elaboran basándose en una evaluación objetiva de los riesgos de seguridad en las actividades de la organización que apoyan la prestación de servicios. El aspecto garantía del sistema se concentra en el hecho de que la organización demuestre (a ella misma y a las partes externas apropiadas), mediante recolección y análisis de pruebas objetivas, que dichos requisitos sean han satisfecho.

9.10.4 La función de gestión de los riesgos de seguridad operacional de un SMS permite, por lo tanto, la evaluación de los riesgos de seguridad operacional en las operaciones que apoyan la prestación de servicios, así como el desarrollo de controles para llevar a nivel ALARP los riesgos evaluados. También apoya las decisiones de seguridad operacional en relación con esas actividades. Una vez instalada, la función de garantía de la seguridad operacional del SMS funciona en forma muy similar a la función de garantía de la calidad en un QMS. En realidad, las funciones de garantía de la seguridad operacional del SMS se han derivado casi directamente de la norma ISO 9001-2000, norma internacional de gestión de la calidad. Como ya se ha visto, existe una diferencia importante: si bien los requisitos típicos de QMS son orientados al cliente y se basan en la satisfacción de éste, los requisitos del SMS son requisitos de seguridad operacional y se basan en la satisfacción de la seguridad.

9.10.5 Es importante reiterar los papeles de las dos funciones dentro de los procesos integrados del SMS. El proceso de gestión de los riesgos de seguridad operacional (SRM) permite la identificación inicial de peligros y la evaluación de los riesgos. Se elaboran controles de los riesgos de seguridad operacional y, una vez que se haya determinado que son capaces a llevar a un nivel ALARP el riesgo de seguridad, estos controles se emplean en las operaciones cotidianas. Es en este punto que la función de garantía de la seguridad operacional (SA) comienza a actuar. La garantía de la seguridad operacional asegura (es decir, da confianza) que los controles de la organización se están aplicando y que todos los tipos de control continúan logrando sus objetivos previstos. Este sistema también permite evaluar la necesidad de nuevos controles debida a cambios en el entorno operacional. En la Figura 9-1 se presenta visualmente este concepto.



**Figura 9-1. Relación entre gestión de riesgos de seguridad operacional y garantía de la seguridad operacional**

## 9.11 PROMOCIÓN DE LA SEGURIDAD OPERACIONAL — INSTRUCCIÓN Y EDUCACIÓN

9.11.1 Una actividad de seguridad operacional en una organización no puede tener éxito por mandato o estrictamente mediante la implantación mecánica de políticas. La promoción de la seguridad operacional marca las pautas que predisponen al comportamiento individual y de la organización y llena vacíos en las políticas, procedimientos y procesos de la organización, proporcionando un sentido de finalidad a las actividades de seguridad.

9.11.2 La mayoría de los procesos y procedimientos especificados en la política y objetivos de la seguridad operacional y en los componentes de gestión de riesgo de seguridad y de garantía de seguridad del SMS proporcionan los elementos básicos estructurales del sistema. No obstante, la organización también debe establecer procesos y procedimientos que permitan la comunicación entre el personal operativo y con la administración de la organización.



Las organizaciones deben hacer lo posible por comunicar sus objetivos, así como la situación actual de las actividades de la organización y sucesos significativos. Análogamente, las organizaciones deben proporcionar un medio de comunicación hacia arriba en un entorno sin restricciones.

9.11.3 La promoción de la seguridad operacional comprende:

- a) instrucción y educación, incluyendo la competencia en seguridad operacional; y
- b) comunicación de la seguridad operacional.

9.11.4 El gerente de seguridad operacional proporciona la información actualizada y la instrucción relacionada con los aspectos de seguridad pertinentes a las operaciones específicas y las dependencias operacionales de la organización. El suministro de instrucción apropiada a todo el personal, independientemente de su nivel en la organización, es una indicación del compromiso de la administración de contar con un SMS efectivo. La instrucción y educación en seguridad operacional debería comprender lo siguiente:

- a) un proceso documentado para identificar requisitos de instrucción;
- b) un proceso de validación que mida la efectividad de la instrucción;
- c) instrucción inicial (seguridad general) específica de la tarea;
- d) adoctrinamiento/instrucción inicial que incorpora el SMS, incluyendo factores humanos y factores de organización; y
- e) instrucción periódica en seguridad operacional.

9.11.5 Los requisitos y actividades de instrucción deberían documentarse para cada área de actividad dentro de la organización. Debería elaborarse un fichero de instrucción para cada empleado, incluyendo los administradores, para ayudar a identificar y hacer el seguimiento de los requisitos de instrucción del empleado y verificar que el personal ha recibido la instrucción prevista. Los programas de instrucción deberían adaptarse a las necesidades y complejidad de la organización.

9.11.6 La instrucción en seguridad operacional dentro de una organización debe asegurar que el personal está instruido y es competente para realizar sus tareas de gestión de la seguridad operacional. El manual SMS (SMSM) debería especificar normas de instrucción en seguridad, inicial y periódica, para el personal operativo, gerentes y supervisores, administradores superiores y el Ejecutivo responsable. El volumen de instrucción de seguridad debería adecuarse a la responsabilidad del individuo y su participación en el SMS. El SMSM también debería especificar responsabilidades de instrucción en seguridad, incluyendo contenido, frecuencia, validación y gestión de registros de instrucción en seguridad.

9.11.7 La instrucción en seguridad operacional debería seguir un enfoque de elementos fundamentales. La instrucción en seguridad para el personal operativo debería tratar la responsabilidad de seguridad, incluyendo el cumplimiento de todos los procedimientos operacionales y de seguridad, y el reconocimiento y notificación de peligros. Los objetivos de la instrucción deberían incluir la política de seguridad de la organización y los fundamentos y panorama general del SMS. La instrucción debería incluir la definición de peligros, consecuencias y riesgos, el proceso de gestión de los riesgos de seguridad, comprendiendo funciones y responsabilidades y, fundamentalmente, la notificación de seguridad operacional y los sistemas de notificación de seguridad de la organización.

9.11.8 La instrucción en seguridad operacional para gerentes y supervisores debería tratar las responsabilidades de seguridad, incluyendo promover el SMS y hacer que el personal operacional participe en la notificación de peligros. Además de los objetivos de instrucción establecidos para el personal operativo, los objetivos de instrucción para

gerentes y supervisores deberían incluir un detallado conocimiento del proceso de seguridad operacional, la identificación de peligros y la evaluación y mitigación de los riesgos de seguridad operacional, así como la gestión del cambio. Además del contenido especificado para el personal operativo, el contenido de la instrucción para supervisores y gerentes debería incluir el análisis de datos de seguridad operacional.

9.11.9 La instrucción en seguridad operacional para la administración superior debería incluir responsabilidades de seguridad operacional, incluyendo el cumplimiento de los requisitos de seguridad nacionales y de la organización, asignación de recursos, asegurar una efectiva comunicación de seguridad entre departamentos y promover activamente el SMS. Además de los objetivos de los dos grupos de empleados anteriores, la instrucción en seguridad operacional para los administradores superiores debería incluir la garantía de la seguridad operacional y la promoción de la seguridad operacional, funciones y responsabilidades de seguridad operacional y el establecimiento de niveles aceptables de seguridad (Figura 9-2).

9.11.10 Por último, la instrucción en seguridad operacional debería incluir una instrucción especial para el Ejecutivo responsable. Esta sesión de instrucción debería ser razonablemente breve (no mayor de medio día), y proporcionar al Ejecutivo responsable concientización general del SMS de la organización, incluyendo funciones y responsabilidades del SMS, política y objetivos de seguridad operacional, gestión de riesgos de seguridad operacional y garantía de seguridad operacional.

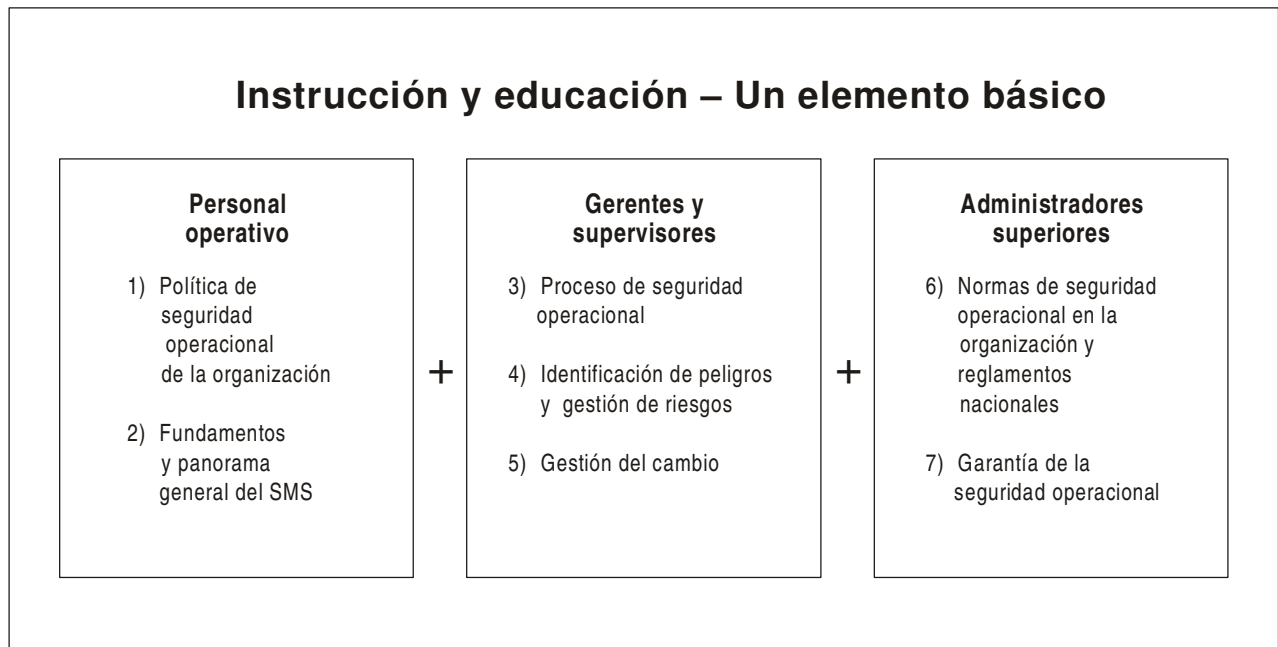
## **9.12 PROMOCIÓN DE LA SEGURIDAD OPERACIONAL — COMUNICACIÓN DE LA SEGURIDAD OPERACIONAL**

9.12.1 La organización debería comunicar los objetivos y procedimientos del SMS a todo su personal operativo y el SMS debería ser visible en todos los aspectos de las operaciones de la organización que apoyan la prestación de servicios. El gerente de seguridad operacional debería comunicar la eficacia del programa SMS de la organización mediante boletines y sesiones de información. El gerente de seguridad operacional también debería asegurar que las enseñanzas obtenidas de las investigaciones, historias de casos o experiencias, tanto internamente como de otras organizaciones, tienen amplia divulgación. Debería existir una corriente de comunicación entre el gerente de seguridad operacional y el personal operativo de toda la organización. La eficacia de la seguridad operacional será mayor si se alienta activamente al personal operativo a que identifique y notifique peligros. Por consiguiente, la comunicación de seguridad operacional se dirige a:

- a) asegurar que todo el personal tiene pleno conocimiento del SMS;
- b) transmitir información crítica para la seguridad operacional;
- c) explicar por qué se adoptan medidas particulares;
- d) explicar por qué se introducen o modifican procedimientos de seguridad operacional; y
- e) transmitir información que pueda ser útil.

9.12.2 Entre los ejemplos de comunicación en la organización figuran:

- a) el manual de sistemas de gestión de la seguridad operacional (SMSM);
- b) los procesos y procedimientos de seguridad operacional;
- c) boletines informativos, avisos y anuncios de seguridad operacional; y
- d) sitios web o correo electrónico.



**Figura 9-2. Instrucción en seguridad operacional**



# Capítulo 10

## ENFOQUE EN FASES DE LA IMPLANTACIÓN DEL SMS

### 10.1 OBJETIVO Y CONTENIDO

El objetivo de este capítulo es introducir una propuesta para la implantación de un SMS en fases. El capítulo comprende los temas siguientes:

- a) Por qué adoptar un enfoque en fases de la implantación del SMS;
- b) Fase I — Planificación de la implantación del SMS;
- c) Fase II — Procesos reactivos de gestión de la seguridad operacional;
- d) Fase III — Procesos proactivos y predictivos de gestión de la seguridad operacional; y
- e) Fase IV — Garantía de la seguridad operacional.

### 10.2 POR QUÉ ADOPTAR UN ENFOQUE EN FASES DE LA IMPLANTACIÓN DEL SMS

10.2.1 La implantación de un SMS es un proceso directo. No obstante, dependiendo de varios factores, como la disponibilidad de textos de orientación publicados por la autoridad supervisora de aviación civil, el conocimiento de los proveedores de servicio con respecto al SMS y los recursos para la implantación, este proceso directo puede transformarse en una tarea atemorizante.

10.2.2 Es un axioma en la gestión de proyectos que los proyectos complejos avanzan mejor si se divide la complejidad general de la tarea en subcomponentes más pequeños y manejables de la misma. De esta forma, una complejidad abrumadora y a veces confusa, y su carga de trabajo subyacente, puede transformarse en subconjuntos de actividades más sencillas y transparentes que exijan solamente una carga de trabajo manejable. Análogamente, los recursos necesarios para implantar el SMS “de una vez” pueden sencillamente no estar disponibles en la organización. Así pues, la división de la complejidad general en subconjuntos de actividades más pequeños permite asignar a subconjuntos completos de actividades recursos parciales o de menor volumen. Esta asignación parcial de recursos puede ser más conmensurable con los requisitos de cada actividad así como con los recursos disponibles en la organización. Por consiguiente, dos razones que justifican por qué se propone un enfoque en fases de la implantación del SMS son:

- a) proporciona una serie de pasos manejables durante la implantación del SMS, incluyendo la asignación de recursos; y
- b) administra con eficacia la carga de trabajo relacionada con la implantación del SMS.

10.2.3 Una tercera razón, muy distinta de las dos anteriores, pero igualmente importante, es evitar el “cumplimiento cosmético”. Una organización debería tener como objetivo la implantación realista de un SMS eficaz, y no una figura simbólica del mismo. Una organización indebidamente sobrecargada con requisitos y sin los recursos para implantar plenamente un SMS en un período de tiempo insuficiente, puede verse impulsada a producir todo el papelerío que se ajustaría a las demandas y requisitos de una autoridad supervisora de aviación civil. En otras palabras, una situación conocida como “marque las casillas apropiadas” podría surgir como resultado de requisitos de

implantación con un nivel infundado de exigencias. Si esto sucediera, el SMS resultante, aunque completo y ajustado a normas en papel, no sería más que un caparazón vacío. Proporcionando una serie de pasos pequeños, graduales y, principalmente medibles, se desalienta el cumplimiento cosmético y la “marcación de casillas apropiadas”. La implantación completa del SMS llevará por cierto más tiempo, pero la solidez del SMS resultante se irá mejorando a medida que se complete cada fase de implantación y se inicien procesos de gestión de la seguridad más sencillos antes de avanzar a las fases sucesivas que involucren procesos de gestión de la seguridad operacional de mayor complejidad.

10.2.4 En resumen, la propuesta de una implantación en fases del SMS tiene por objeto:

- a) proporcionar una serie de pasos manejables en la implantación del SMS, incluyendo la asignación de recursos;
- b) administrar con eficacia la carga de trabajo relacionada con la implantación del SMS; y
- c) proporcionar un SMS sólido y no simplemente un caparazón vacío (es decir “marque las casillas apropiadas”).

10.2.5 Se proponen cuatro fases de implantación para el SMS. Cada fase se relaciona con un componente del marco de la OACI para SMS introducido en el Capítulo 8. La implantación de cada fase se basa en la introducción de elementos específicos de cada componente del marco de la OACI durante la fase en cuestión.

### 10.3 FASE I — PLANIFICACIÓN DE LA IMPLANTACIÓN DEL SMS

10.3.1 El objetivo de la Fase I de la implantación del SMS es proporcionar un plan de trabajo sobre cómo se satisfarán los requisitos del SMS y se integrarán en las actividades laborales de la organización, así como un marco de responsabilidad para la implantación del SMS.

10.3.2 Durante la Fase I, se establecen la planificación básica y la asignación de responsabilidades. Fundamental para la Fase I es el análisis de las carencias. A partir del análisis de las carencias, una organización puede determinar la situación actual de sus procesos de gestión de la seguridad operacional y puede comenzar a planificar en detalle el desarrollo de ulteriores procesos de gestión de la seguridad operacional. Un resultado importante de la Fase I es el plan de implantación del SMS.

10.3.3 Al terminar la Fase I, las actividades siguientes deberían estar finalizadas en forma tal que satisfagan las expectativas de la actividad supervisora de aviación civil, según se ha establecido en los requisitos y textos de orientación pertinentes:

- a) Identificar al Ejecutivo responsable y las responsabilidades de seguridad de los gerentes. Esta actividad se basa en los Elementos 1.1 y 1.2 del marco de la OACI para SMS y se analiza en el Capítulo 8.
- b) Identificar a la persona (o grupo de planificación) dentro de la organización responsable de implantar el SMS. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en el Capítulo 8.
- c) Describir el sistema (organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, explotadores de aeronaves, organismos de mantenimiento reconocidos, organizaciones responsables del diseño de tipo o fabricantes de aeronaves, proveedores de servicios de tránsito aéreo y aeródromos certificados). Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en el Capítulo 7. En el Apéndice 1 del Capítulo 7 se proporciona orientación sobre la descripción del sistema.

- d) Realizar un análisis de carencias de los recursos existentes en la organización en relación con los requisitos nacionales e internacionales para establecer el SMS. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en el Capítulo 7. En el Apéndice 2 del Capítulo 7 se proporciona orientación sobre un análisis de las carencias del SMS para un proveedor de servicios.
- e) Elaborar un plan de implantación del SMS que explique cómo la organización implantará el SMS sobre la base de los requisitos nacionales y los SARPS internacionales, la descripción del sistema y los resultados del análisis de las carencias. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en el Capítulo 8.
- f) Elaborar documentación pertinente de la política y objetivos de seguridad operacional. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en el Capítulo 8, que también comprende un ejemplo de declaración de política de seguridad operacional.
- g) Elaborar y establecer medios para la comunicación de seguridad operacional. Esta actividad se basa en el Elemento 4.2 del marco de la OACI para SMS y se analiza en el Capítulo 9.

#### 10.4 FASE II — PROCESOS REACTIVOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

10.4.1 El objetivo de la Fase II es poner en práctica procesos esenciales de gestión de la seguridad operacional, corrigiendo al mismo tiempo las posibles deficiencias en los procesos de gestión de la seguridad operacional existentes. La mayoría de las organizaciones tendrá en funcionamiento algunas actividades básicas de gestión de la seguridad operacional, a diversos niveles de implantación y con diferentes grados de efectividad. Estas actividades pueden incluir inspecciones e informes de auditoría, análisis de información obtenida en investigaciones de accidentes e incidentes, e informes de empleados. Esta fase se dirige a solidificar las actividades existentes y desarrollar aquellas que todavía no existen. No obstante, debido a que todavía hay que desarrollar e implantar sistemas orientados al futuro, esta fase se considera reactiva. Hacia el final de la Fase I, la organización estará en condiciones de realizar análisis coordinados de la seguridad operacional basados en la información obtenida mediante métodos reactivos de recolección de datos de seguridad.

10.4.2 Al terminar la Fase II, habrán finalizado las actividades siguientes en forma tal que satisfagan las expectativas de la autoridad supervisora de aviación civil, según se establece en los requisitos y textos de orientación pertinentes:

- a) Poner en práctica aquellos aspectos del plan de implantación del SMS que involucren la gestión de riesgos de seguridad operacional basadas en procesos reactivos. Esta actividad se basa en los Elementos 2.1 y 2.2 del marco para SMS de la OACI y se analiza en los Capítulos 3 y 8.
- b) Proporcionar instrucción pertinente a los componentes del plan de implantación del SMS y a la gestión de riesgos de seguridad operacional basándose en procesos reactivos. Esta actividad se basa en el Elemento 4.1 de marco de la OACI para SMS y se analiza en los Capítulos 3, 8 y 9.
- c) Elaborar documentación relativa a los componentes del plan de implantación del SMS y a la gestión de riesgos de seguridad operacional basándose en procesos reactivos. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en los Capítulos 3, 8 y 9.
- d) Desarrollar y mantener medios formales para las comunicaciones de seguridad operacional. Esta actividad se basa en el Elemento 4.2 del marco de la OACI para SMS y se analiza en el Capítulo 9.

### **10.5 FASE III — PROCESOS PROACTIVOS Y PREDICTIVOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL**

10.5.1 El objetivo de la Fase III es estructurar procesos de gestión de la seguridad operacional orientados al futuro. Se refinan los procesos de gestión y análisis de la información de seguridad operacional. Hacia el final de la Fase III, la organización estará en condiciones de realizar análisis de seguridad operacional coordinados sobre la base de la información obtenida mediante métodos reactivos, proactivos y predictivos de recolección de datos de seguridad operacional.

10.5.2 Al terminar la Fase III, las actividades siguientes habrán finalizado en forma tal que satisfagan las expectativas de la autoridad supervisora de aviación civil, según se establece en los requisitos y textos de orientación pertinentes:

- a) Poner en práctica aquellos elementos del plan de implantación del SMS que se refieren a la gestión de riesgos de seguridad operacional basándose en procesos proactivos y predictivos. Esta actividad se basa en los Elementos 2.1 y 2.2 del marco de la OACI para SMS y se analiza en los Capítulos 3 y 8.
- b) Desarrollar instrucción pertinente a los componentes del plan de implantación del SMS y a la gestión de riesgos de seguridad operacional basándose en procesos proactivos y predictivos. Esta actividad se basa en el Elemento 4.1 del marco de la OACI para SMS y se analiza en los Capítulos 3, 8 y 9.
- c) Elaboración de documentación relativa a los componentes del plan de implantación del SMS y a la gestión de riesgo de seguridad operacional sobre la base de procesos proactivos y predictivos. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en los Capítulos 3, 8 y 9.
- d) Desarrollar y mantener medios formales para las comunicaciones de seguridad operacional. Esta actividad se basa en el Elemento 4.2 del marco de la OACI para SMS y se analiza en el Capítulo 9.

### **10.6 FASE IV — GARANTÍA DE LA SEGURIDAD OPERACIONAL**

10.6.1 La Fase IV es la fase final del SMS. En esta fase se evalúa la garantía de la seguridad operacional mediante la implantación de supervisión periódica, retroinformación y medidas correctivas continuas para mantener la efectividad de los controles de riesgos de seguridad en situaciones operacionales cambiantes. Al final de la Fase IV, los procesos de gestión y análisis de la información de seguridad operacional garantizan la sostenibilidad de los procesos de organización seguros a lo largo del tiempo y durante períodos de cambio en el entorno operacional.

10.6.2 Al terminar la Fase IV, habrán finalizado las actividades siguientes en forma tal que satisfagan las expectativas de la autoridad supervisora de aviación civil, según se establece en los requisitos y textos de orientación pertinentes:

- a) Desarrollar y ponerse de acuerdo sobre los indicadores de eficacia de la seguridad operacional, los objetivos de eficacia de la seguridad operacional y la mejora continua del SMS. Esta actividad se basa en los Elementos 1.1, 3.1, 3.2 y 3.3 del marco de la OACI para SMS y se analiza en los Capítulos 6 y 9.
- b) Desarrollar instrucción pertinente a la garantía de la seguridad operacional. Esta actividad se basa en el Elemento 4.1 del marco de la OACI para SMS y se analiza en el Capítulo 9.
- c) Elaborar documentación relativa a la garantía de la seguridad operacional. Esta actividad se basa en el Elemento 1.5 del marco de la OACI para SMS y se analiza en el Capítulo 9.
- d) Desarrollar y mantener medios formales para la comunicación de seguridad operacional. Esta actividad se basa en el Elemento 4.2 del marco de la OACI para SMS y se analiza en el Capítulo 9.

10.6.3 En la Figura 10-1 se presenta un resumen de las diferentes etapas de la implantación del SMS y sus elementos correspondientes.



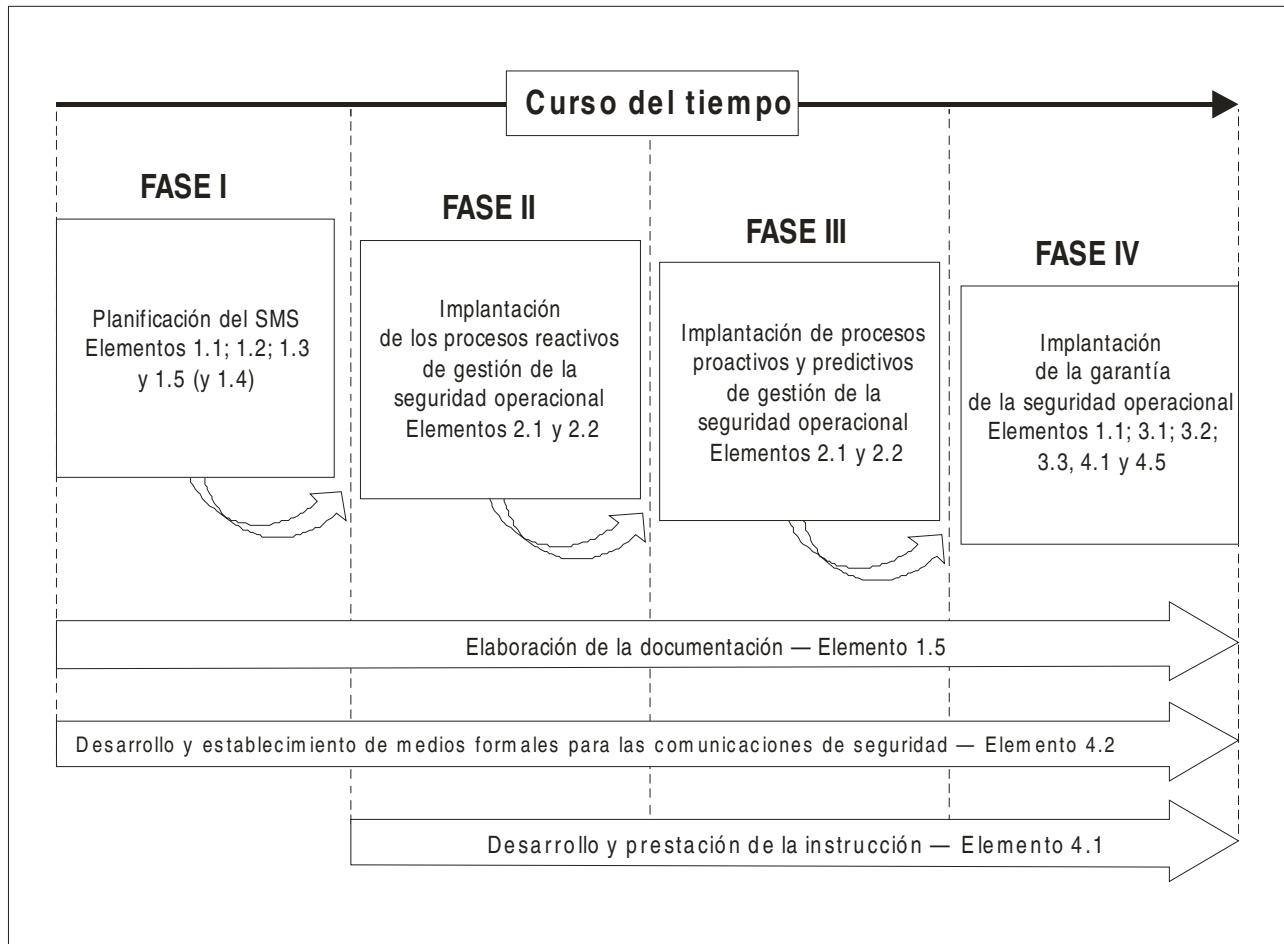


Figura 10-1. Resumen de las diferentes fases de implantación del SMS



# Apéndice 1 del Capítulo 10

## ORIENTACIÓN PARA LA ELABORACIÓN DE UN REGLAMENTO DEL ESTADO SOBRE EL SMS

### 1. BASE LEGAL

Este reglamento se promulga bajo responsabilidad legal en [reglamentos de aviación civil aplicables del Estado, órdenes de navegación aérea o normas reglamentarias].

### 2. ALCANCE Y APLICACIÓN

#### 2.1 Alcance

2.1.1 Este reglamento especifica los requisitos para el sistema de gestión de la seguridad operacional (SMS) de un proveedor de servicios que funciona con arreglo al Anexo 1 — *Licencias al personal*; Anexo 6 — *Operación de aeronaves*, Parte I — *Transporte aéreo comercial internacional — Aviones* y Parte III — *Operaciones internacionales — Helicópteros*; Anexo 8 — *Aeronavegabilidad*; Anexo 11 — *Servicios de tránsito aéreo*; y Anexo 14 — *Aeródromos*, Volumen I — *Diseño y operaciones de aeródromos*.

2.1.2 En el contexto de este reglamento el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye a las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicio de tránsito aéreo y los aeródromos certificados, según corresponda.

2.1.3 Este reglamento abarca los procesos, procedimientos y actividades relacionados con la seguridad operacional de la aviación y no la seguridad laboral, la protección del medio ambiente, los servicios a la clientela o la calidad de los productos.

2.1.4 El proveedor de servicios es responsable de la seguridad de los servicios o productos contratados o subcontratados a otras organizaciones o adquiridos de otras organizaciones.

2.1.5 Este reglamento establece los requisitos mínimos aceptables; el proveedor de servicios puede establecer requisitos más estrictos.

#### 2.2 Aplicación y aceptación

2.2.1 Con efecto el [fecha(s)], el proveedor de servicios habrá implantado un sistema de gestión de la seguridad operacional (SMS) aceptable para [Estado] y que, como mínimo:

2.2.1.1 identifique los peligros para la seguridad operacional;

- 2.2.1.2 garantice la aplicación de las medidas correctivas necesarias para mantener la eficacia convenida respecto de la seguridad operacional;
- 2.2.1.3 provea supervisión continua y evaluación periódica de la eficacia de la seguridad operacional; y
- 2.2.1.4 tenga como objetivo el mejoramiento continuo de la actuación global del sistema de gestión de la seguridad operacional.
- 2.2.2 Para que sea aceptable al Estado, el SMS del proveedor de servicios deberá satisfacer los requisitos establecidos en este reglamento.

*Nota de información.— Un reglamento sobre SMS debería incluir información respecto del proceso de aceptación para el SMS. El proceso de aceptación debería incluir, según corresponda, la solicitud de aceptación del SMS, los procedimientos para presentar dicha solicitud, la duración de la aceptación, la renovación de la aceptación y la suspensión o revocación de la aceptación.*

### 3. REFERENCIAS

- 3.1 Este reglamento se ajusta al Anexo 1 — *Licencias al personal*; Anexo 6 — *Operación de aeronaves, Parte I — Transporte aéreo comercial internacional — Aviones y Parte III — Operaciones internacionales — Helicópteros*; Anexo 8 — *Aeronavegabilidad*; Anexo 11 — *Servicios de tránsito aéreo*; y Anexo 14 — *Aeródromos, Volumen I — Diseño y operaciones de aeródromos*; así como al *Manual de gestión de la seguridad operacional*, de la OACI (Doc 9859).
- 3.2 Este reglamento está de acuerdo con *[textos normativos o de orientación aplicables del Estado]*.

### 4. DEFINICIONES

*Nota.— Esta lista se incluye con fines de orientación solamente.*

- Accidente
- Análisis de las carencias
- Auditoría de la seguridad operacional
- Consecuencia
- Descripción del sistema
- Eficacia de la seguridad operacional
- Ejecutivo responsable
- Encuesta de seguridad operacional
- Evaluación de la seguridad operacional
- Garantía de la seguridad operacional
- Gerente de seguridad operacional
- Gravedad
- Incidente
- Indicador de eficacia de la seguridad operacional
- Investigaciones internas de seguridad operacional
- Mitigación
- Nivel aceptable de seguridad operacional (ALoS)
- Objetivo de eficacia de la seguridad operacional

- Ocurrencia
- Peligro
- Política de seguridad operacional
- Predictivo
- Proactivo
- Probabilidad
- Procedimiento
- Proceso
- Programa estatal de seguridad operacional (SSP)
- Reactivo
- Requisito de seguridad operacional
- Riesgo
- Riesgo de seguridad operacional
- Seguridad operacional
- Sistema de gestión de la seguridad operacional (SMS)
- Supervisión continua
- Vigilancia.

## 5. GENERALIDADES

El proveedor de servicios elaborará, establecerá, mantendrá y adherirá a un sistema de gestión de la seguridad operacional (SMS) que sea apropiado al tamaño, carácter y complejidad de las operaciones cuya realización se ha autorizado en el marco de su certificado de operaciones, y a los peligros y riesgos de seguridad operacional relacionados con dichas operaciones.

## 6. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

### 6.1 Requisitos generales

- 6.1.1 El proveedor de servicios definirá la política de seguridad operacional de la organización.
- 6.1.2 La política de seguridad operacional deberá ser firmada por el Ejecutivo responsable de la organización.
- 6.1.3 La política de seguridad operacional incluirá las responsabilidades de la administración y de los empleados con respecto a la eficacia de la seguridad operacional del SMS.
- 6.1.4 La política de seguridad operacional deberá incluir también una declaración clara sobre la provisión de los recursos necesarios para su implantación.
- 6.1.5 La política de seguridad operacional se comunicará, con visible endoso, a toda la organización.
- 6.1.6 La política de seguridad operacional también incluirá, entre otras cosas:
  - 6.1.6.1 un compromiso respecto de la mejora continua del nivel de seguridad operacional;
  - 6.1.6.2 los procedimientos de notificación de peligros; y
  - 6.1.6.3 las condiciones bajo las cuales las medidas disciplinarias no serían aplicables después de la notificación de peligros por los empleados.

6.1.7 La política de seguridad operacional estará de acuerdo con todos los requisitos jurídicos y normas internacionales aplicables, así como las mejores prácticas de la industria y reflejará los compromisos de la organización con respecto de la seguridad operacional.

6.1.8 La política de seguridad operacional será revisada periódicamente para asegurar que sigue siendo pertinente y apropiada a la organización.

6.1.9 El proveedor de servicios establecerá objetivos de seguridad operacional para el SMS.

6.1.10 Los objetivos de seguridad operacional estarán relacionados con los indicadores de eficacia de la seguridad operacional, objetivos de eficacia de la seguridad operacional y planes de acción del SMS del proveedor de servicios.

## **6.2 Arreglos de organización del SMS y responsabilidades y rendición de cuentas respecto de la seguridad operacional**

6.2.1 El proveedor de servicios identificará un Ejecutivo responsable quien se encargará y será responsable en nombre del proveedor de servicios de la satisfacción de los requisitos de este reglamento, y notificará a [Estado] en nombre de dicha persona.

6.2.2 El Ejecutivo responsable será una persona única e identificable que, con independencia de otras funciones, tendrá la responsabilidad final y de rendición de cuentas, en nombre de [organización], sobre la implantación y mantenimiento del SMS.

6.2.3 El Ejecutivo responsable tendrá:

6.2.3.1 pleno control de los recursos humanos necesarios para las operaciones cuya realización se ha autorizado en el certificado de operaciones;

6.2.3.2 pleno control de los recursos financieros para las operaciones cuya realización se ha autorizado en el certificado de operaciones;

6.2.3.3 autoridad final sobre las operaciones cuya realización se ha autorizado en el certificado de operaciones;

6.2.3.4 responsabilidad directa sobre la conducción de los asuntos de la organización; y

6.2.3.5 responsabilidad final por todos los asuntos de seguridad operacional.

6.2.4 El proveedor de servicios establecerá los arreglos de organización necesarios para la implantación, el cumplimiento y el mantenimiento del SMS de la organización.

6.2.5 El proveedor de servicios identificará las líneas de rendición de cuentas, las responsabilidades y las facultades de todos los miembros de la administración, así como de todos los empleados, independientemente de otras responsabilidades.

6.2.6 Las líneas de rendición de cuentas, responsabilidades y facultades relacionadas con la seguridad operacional serán definidas, documentadas y comunicadas a toda la organización.

6.2.7 El proveedor de servicio designará a una persona de la administración para ser gerente de seguridad operacional, punto individual y focal responsable de la implantación y mantenimiento de un SMS efectivo.

6.2.8 El gerente de seguridad, entre otras cosas:

- 6.2.8.1 asegurará que los procesos necesarios para el SMS se elaboran, implantan, cumplen y mantienen;
- 6.2.8.2 informará al Ejecutivo responsable sobre la eficacia del SMS y sobre cualquier necesidad de mejoras; y
- 6.2.8.3 asegurará la promoción de la seguridad operacional en toda la organización.

### **6.3 Coordinación del plan de respuesta ante emergencias**

6.3.1 El proveedor de servicios asegurará que su plan de respuesta ante emergencias está adecuadamente coordinado con los planes de respuesta ante emergencias de las organizaciones con las que debe interactuar durante la prestación de sus servicios.

6.3.2 La coordinación del plan de respuesta ante emergencias asegurará la transición ordenada y eficiente de las operaciones normales a las de emergencia y el reinicio de las operaciones normales.

6.3.3 La coordinación del plan de respuesta ante emergencias incluirá, entre otras cosas:

- 6.3.3.1 la delegación de autoridad ante emergencias;
- 6.3.3.2 la asignación de responsabilidades de emergencia durante las actividades coordinadas;
- 6.3.3.3 la coordinación de los esfuerzos para enfrentar la emergencia; y
- 6.3.3.4 la compatibilidad con otros planes de respuesta ante emergencias de otras organizaciones.

### **6.4 Documentación**

6.4.1 El proveedor de servicios elaborará y mantendrá documentación sobre SMS para describir:

- 6.4.1.1 la política y objetivos de seguridad operacional;
- 6.4.1.2 los requisitos del SMS;
- 6.4.1.3 los procesos y procedimientos del SMS;
- 6.4.1.4 las líneas de rendición de cuentas, responsabilidades y facultades para los procesos y procedimientos; y
- 6.4.1.5 los resultados del SMS.

6.4.2 Como parte de la documentación sobre SMS el proveedor de servicios completará una descripción del sistema.

6.4.3 La descripción del sistema incluirá los aspectos siguientes:

- 6.4.3.1 las interacciones del sistema con otros sistemas del sistema de transporte aéreo;
- 6.4.3.2 las funciones del sistema;
- 6.4.3.3 las consideraciones en materia de actuación humana requerida para el funcionamiento del sistema;
- 6.4.3.4 componentes de soporte físico del sistema;
- 6.4.3.5 componentes del soporte lógico del sistema;
- 6.4.3.6 procedimientos conexos que definen orientación para el funcionamiento y uso del sistema;
- 6.4.3.7 entorno operacional; y
- 6.4.3.8 productos o servicios contratados, subcontratados y adquiridos.

6.4.4 Como parte de la documentación del SMS, el proveedor de servicios realizará un análisis de las carencias, para:

- 6.4.4.1 identificar los arreglos y estructuras de seguridad operacional que ya pueden existir en su organización; y
- 6.4.4.2 determinar los arreglos de seguridad operacional adicionales requeridos para implantar y mantener el SMS de la organización.

6.4.5 Como parte de la documentación del SMS, el proveedor de servicios elaborará, cumplirá y mantendrá un plan de implantación del SMS.

6.4.6 El plan de implantación del SMS será la definición del enfoque de la organización en la gestión de la seguridad operacional de manera de alcanzar los objetivos de la seguridad operacional de la organización.

6.4.7 El plan de implantación del SMS tratará explícitamente la coordinación entre el SMS del proveedor de servicios y el SMS de otras organizaciones con las cuales el proveedor de servicios debe interactuar durante la prestación de los servicios.

6.4.8 El plan de implantación del SMS incluirá los aspectos siguientes:

- 6.4.8.1 políticas y objetivos de seguridad operacional;
- 6.4.8.2 descripción del sistema;
- 6.4.8.3 análisis de las carencias;
- 6.4.8.4 componentes del SMS;
- 6.4.8.5 funciones y responsabilidades de seguridad operacional;
- 6.4.8.6 política de notificación de peligros;
- 6.4.8.7 medios de participación de los empleados;



- 6.4.8.8 medición de la eficacia de la seguridad operacional;
  - 6.4.8.9 instrucción en seguridad operacional;
  - 6.4.8.10 comunicación de la seguridad operacional; y
  - 6.4.8.11 examen por la administración de la eficacia de la seguridad operacional.
- 6.4.9 El plan de implantación del SMS será endosado por la administración superior de la organización.
- 6.4.10 Como parte de la documentación del SMS, el proveedor de servicios elaborará y mantendrá un manual de sistemas de gestión de la seguridad operacional (SMSM), para comunicar a toda la organización su enfoque de la gestión de la seguridad operacional.
- 6.4.11 El SMSM documentará todos los aspectos del SMS y su contenido será el siguiente:
- 6.4.11.1 alcance del sistema de gestión de la seguridad operacional;
  - 6.4.11.2 política y objetivos de seguridad operacional;
  - 6.4.11.3 responsabilidades (rendición de cuentas) de seguridad operacional;
  - 6.4.11.4 personal clave de seguridad operacional;
  - 6.4.11.5 procedimientos de control de la documentación;
  - 6.4.11.6 coordinación de la planificación de respuestas ante emergencias;
  - 6.4.11.7 planes de identificación de peligros y gestión de riesgos de seguridad operacional;
  - 6.4.11.8 supervisión de la eficacia de la seguridad operacional;
  - 6.4.11.9 auditoría de la seguridad operacional;
  - 6.4.11.10 procedimientos para la gestión del cambio;
  - 6.4.11.11 promoción de la seguridad operacional; y
  - 6.4.11.12 control de las actividades contratadas.

*Nota de información.— Las directrices genéricas para la elaboración y mantenimiento de documentación sobre el SMS figuran en el Adjunto H del Anexo 6 de la OACI, Parte I, y en el Adjunto G del Anexo 6 de la OACI, Parte III, Sistema de documentos de seguridad de vuelo del explotador.*

## **7. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL**

### **7.1 Generalidades**

- 7.1.1 El proveedor de servicios elaborará y mantendrá un protocolo que asegure que se identifican los peligros en las operaciones.

7.1.2 El proveedor de servicios desarrollará y mantendrá sistemas de recopilación y procesamiento de datos de seguridad operacional (SDCPS) que permitan la identificación de peligros y el análisis, evaluación y mitigación de los riesgos de seguridad operacional.

7.1.3 El SDCPS del proveedor de servicios incluirá métodos reactivos, proactivos y predictivos de recolección de datos de seguridad operacional.

## **7.2 Identificación de peligros**

7.2.1 El proveedor de servicios elaborará y mantendrá protocolos para la eficaz recolección y registro de información sobre peligros en las operaciones así como la adopción de medidas y la generación de retroinformación sobre ellos, que combinen métodos reactivos, proactivos y predictivos para la recolección de datos de seguridad operacional. Los protocolos de recolección de datos de seguridad operacional comprenderán sistemas de notificación obligatoria, voluntaria y confidencial.

7.2.2 El proceso de identificación de peligros comprenderá los pasos siguientes:

7.2.2.1 notificación de peligros, sucesos o problemas de seguridad operacional;

7.2.2.2 recolección y almacenamiento de datos de seguridad operacional;

7.2.2.3 análisis de los datos de seguridad operacional; y

7.2.2.4 distribución de la información de seguridad operacional obtenida de los datos de seguridad operacional.

## **7.3 Evaluación y mitigación de riesgos de seguridad operacional**

7.3.1 El proveedor de servicios elaborará y mantendrá un protocolo que garantice el análisis, la evaluación y el control de los riesgos de seguridad operacional de las consecuencias de los peligros durante la prestación de sus servicios.

7.3.2 Los riesgos de seguridad operacional de las consecuencias de cada peligro identificado mediante los procesos de identificación de peligros descritos en la sección 7.2 de este reglamento se analizarán en cuanto a su probabilidad y gravedad de ocurrencia y se evaluarán en cuanto a su aceptabilidad.

7.3.3 La organización definirá los niveles de administración con autoridad para tomar decisiones sobre la aceptabilidad de los riesgos de seguridad operacional.

7.3.4 La organización definirá controles de seguridad para cada riesgo de seguridad operacional evaluado como tolerable.

# **8. GARANTÍA DE LA SEGURIDAD OPERACIONAL**

## **8.1 Generalidades**

8.1.1 El proveedor de servicios elaborará y mantendrá procesos de garantía de la seguridad operacional para asegurar que los controles de riesgos de seguridad operacional elaborados como consecuencia de la identificación de peligros y las actividades de gestión de riesgos de seguridad operacional indicados en el párrafo 7 logran sus objetivos previstos.

8.1.2 Los procesos de garantía de la seguridad operacional se aplicarán al SMS independientemente de si las actividades u operaciones se realizan internamente o se contratan exteriormente.

## **8.2 Supervisión y medición de la eficacia de la seguridad operacional**

8.2.1 Como parte de sus actividades de garantía de la seguridad operacional del SMS, el proveedor de servicios elaborará y mantendrá los medios necesarios para verificar la eficacia de la seguridad operacional de la organización con referencia a los indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional del SMS, y confirmará la efectividad de los controles de riesgos de seguridad.

8.2.2 Los medios para la supervisión y medición de la eficacia de la seguridad operacional comprenderán los siguientes:

- 8.2.2.1 sistemas de notificación de peligros;
- 8.2.2.2 auditorías de la seguridad operacional;
- 8.2.2.3 encuestas de seguridad operacional;
- 8.2.2.4 exámenes de la seguridad operacional;
- 8.2.2.5 estudios de la seguridad operacional; y
- 8.2.2.6 investigaciones internas de la seguridad operacional.

8.2.3 Los procedimientos de notificación de peligros establecerán las condiciones para asegurar una notificación efectiva, incluyendo las condiciones en que no se aplicarán medidas disciplinarias o administrativas.

## **8.3 Gestión del cambio**

8.3.1 Como parte de las actividades de garantía de la seguridad operacional de su SMS, el proveedor de servicios elaborará y mantendrá un protocolo para la gestión del cambio.

8.3.2 El protocolo para la gestión del cambio:

- 8.3.2.1 identificará los cambios dentro de la organización que puedan afectar a los procesos y servicios establecidos;
- 8.3.2.2 establecerá disposiciones para garantizar la eficacia de la seguridad operacional antes de introducir cualquier cambio; y
- 8.3.2.3 eliminará o modificará los controles de riesgo de seguridad operacional que ya no sean necesarios debido a modificaciones del entorno operacional.

## **8.4 Mejora continua del sistema de seguridad operacional**

8.4.1 Como parte de las actividades de garantía de la seguridad operacional de su SMS, el proveedor de servicios elaborará y mantendrá protocolos para identificar las causas de una actuación deficiente del SMS, determinar las consecuencias para sus operaciones y rectificar las situaciones que entrañen una actuación deficiente a efectos de asegurar la mejora continua del SMS.

- 8.4.2 La mejora continua del SMS del proveedor de servicio comprenderá:
- 8.4.2.1 evaluaciones proactivas y reactivas de instalaciones, equipo, documentación y procedimientos, para verificar la efectividad de las estrategias de control de riesgo de seguridad operacional; y
  - 8.4.2.2 evaluación proactiva de la actuación de los individuos para verificar el cumplimiento de sus responsabilidades de seguridad operacional.

## **9. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL**

### **9.1 Generalidades**

Los proveedores de servicio elaborarán y mantendrán actividades normales de instrucción en seguridad operacional y comunicación de la seguridad operacional para crear un entorno en el que puedan lograrse los objetivos de seguridad operacional de la organización.

### **9.2 Instrucción en seguridad operacional**

- 9.2.1 Como parte de sus actividades de promoción de la seguridad operacional, el proveedor de servicios elaborará y mantendrá un programa de instrucción de seguridad operacional que asegure que el personal cuenta con la instrucción y competencias necesarias para cumplir sus funciones en el marco del SMS.
- 9.2.2 El alcance de la instrucción en seguridad operacional se adaptará al grado de participación en el SMS de cada persona.
- 9.2.3 El ejecutivo responsable recibirá instrucción sobre conciencia de la seguridad operacional con respecto a:
- 9.2.3.1 política y objetivos de seguridad operacional;
  - 9.2.3.2 funciones y responsabilidades en el SMS;
  - 9.2.3.3 normas del SMS; y
  - 9.2.3.4 garantía de la seguridad operacional.

### **9.3 Comunicación de la seguridad operacional**

- 9.3.1 Como parte de sus actividades de promoción de la seguridad operacional el proveedor de servicios elaborará y mantendrá medios formales para la comunicación de la seguridad operacional a efectos de:
- 9.3.1.1 asegurar que todo el personal tiene pleno conocimiento del SMS;
  - 9.3.1.2 difundir información crítica respecto de seguridad operacional;
  - 9.3.1.3 explicar por qué se toman determinadas medidas de seguridad operacional;
  - 9.3.1.4 explicar por qué se introducen o modifican procedimientos de seguridad operacional; y
  - 9.3.1.5 difundir la información genérica de seguridad operacional.

9.3.2 Los medios formales para la comunicación de la seguridad operacional comprenderán, entre otros:

9.3.2.1 políticas y procedimientos de seguridad operacional;

9.3.2.2 boletines;

9.3.2.3 anuncios; y

9.3.2.4 sitios web.

## 10. POLÍTICA DE CALIDAD

El proveedor de servicios asegurará que la política de calidad de la organización es coherente con las actividades del SMS y apoya su realización.

## 11. IMPLANTACIÓN DEL SMS

11.1 Este reglamento propone, con carácter no obligatorio, una implantación en fases del SMS del proveedor de servicios que comprenda las cuatro fases descritas en 11.2 a 11.5.

11.2 **Fase I** — La planificación debería proporcionar un plan sobre cómo se satisfarán los requisitos SMS y se integrarán en las actividades laborales de la organización, así como un marco de responsabilidades y rendición de cuentas para la implantación del SMS, que:

11.2.1 identifique al Ejecutivo responsable y las responsabilidades de seguridad operacional de los gerentes;

11.2.2 identifique a la persona (o grupo de planificación) dentro de la organización responsable de implantar el SMS;

11.2.3 describa el sistema (ATO, explotadores aéreos, AMO, organizaciones responsables del diseño de tipo o fabricación de aeronaves, proveedores de servicios ATC, aeródromos certificados);

11.2.4 realice un análisis de las carencias de los recursos existentes en la organización con respecto a los requisitos nacionales e internacionales para establecer un SMS;

11.2.5 elabore un plan de implantación del SMS que explique cómo la organización pondrá en práctica el SMS sobre la base de los requisitos nacionales y SARPS internacionales, descripción del sistema y resultados del análisis de las carencias;

11.2.6 elabore documentación pertinente a la política y objetivos de seguridad operacional; y

11.2.7 elabore y establezca medios para la comunicación de la seguridad operacional.

11.3 **Fase II** — Los procesos reactivos deberían poner en práctica los elementos del plan de implantación del SMS que se refieren a la gestión de riesgo de la seguridad operacional sobre la base de los procesos reactivos siguientes:

11.3.1 identificación de peligros y gestión de riesgos de seguridad operacional aplicando procesos reactivos;

- 11.3.2 instrucción pertinente a:
  - 11.3.2.1 componentes del plan de implantación SMS; y
  - 11.3.2.2 gestión de riesgos de seguridad operacional (procesos reactivos).
- 11.3.3 documentación pertinente a:
  - 11.3.3.1 componentes del plan de implantación del SMS; y
  - 11.3.3.2 gestión de riesgos de seguridad operacional (procesos reactivos).

11.4 **Fase III** — Los procedimientos proactivos y predictivos deberían poner en práctica los elementos del plan de implantación del SMS que se refieren a la gestión de riesgos de seguridad operacional sobre la base de los procesos proactivos y predictivos siguientes:

- 11.4.1 identificación de peligros y gestión de riesgos de seguridad operacional aplicando procesos proactivos y predictivos;
- 11.4.2 instrucción pertinente a:
  - 11.4.2.1 componentes del plan de implantación del SMS; y
  - 11.4.2.2 gestión de riesgos de seguridad operacional (procesos proactivos y predictivos).
- 11.4.3 documentación pertinente a:
  - 11.4.3.1 componentes del plan de implantación SMS; y
  - 11.4.3.2 gestión de riesgos de seguridad operacional (procesos proactivos y predictivos).

11.5 **Fase IV** — La garantía de la seguridad operacional debería poner en práctica la garantía de la seguridad operacional mediante:

- 11.5.1 el desarrollo y acuerdo sobre indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional;
  - 11.5.2 mejora continua del SMS;
  - 11.5.3 instrucción pertinente a la garantía de seguridad operacional;
  - 11.5.4 documentación pertinente a la garantía de la seguridad operacional; y
  - 11.5.5 elaboración y mantenimiento de medios formales para la comunicación de la seguridad operacional.
-

## Apéndice 2 del Capítulo 10

# ORIENTACIÓN SOBRE LA ELABORACIÓN DE UN PLAN DE IMPLANTACIÓN DEL SMS PARA PROVEEDORES DE SERVICIOS

### ANTECEDENTES

1. En este apéndice se proporciona orientación para ayudar a los proveedores de servicios en la elaboración de un plan de implantación del SMS que defina el enfoque de su organización a la gestión de la seguridad operacional. El plan de implantación del SMS será endosado por la administración superior de la organización y se elaborará sobre la base de los reglamentos nacionales, normas y métodos recomendados internacionales (SARPS), la descripción del sistema y los resultados de un análisis de carencias.
2. La elaboración de un plan de implantación del SMS también:
  - a) ayudará a los proveedores de servicios a preparar una estrategia realista para la implantación de un SMS que satisfaga los objetivos de seguridad operacional de la organización;
  - b) proporcionará una serie manejable de pasos para seguir en la implantación del SMS; y
  - c) proporcionará un marco de rendición de cuentas para la implantación del SMS.
3. Se propone un enfoque en etapas para ayudar a la efectiva gestión de la carga de trabajo relacionada con la implantación del SMS. Cada fase se basa en la introducción de elementos específicos del marco de la OACI para SMS.
4. El tiempo que insuma la implantación de cada fase será proporcional al tamaño de la organización y a la complejidad de los servicios que presta.

*Nota 1.— En este apéndice se incluye un modelo de carta Gantt para la elaboración de un plan de implantación del SMS. Esta orientación se incluye solamente como referencia, y puede tener que ajustarse para satisfacer las necesidades de cada proveedor de servicio. También puede descargarse un fichero sobre gestión de proyectos del modelo de carta Gantt de [www.icao.int/fsix](http://www.icao.int/fsix) o [www.icao.int/anb/safetymanagement](http://www.icao.int/anb/safetymanagement).*

*Nota 2.— En el contexto de este apéndice, el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicio, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicio de tránsito aéreo y los aeródromos certificados, según corresponda.*

## Plan de implantación del SMS

### 1. FASE I — PLANIFICACIÓN DE LA IMPLANTACIÓN DEL SMS

#### 1.1 *El Ejecutivo responsable*

- Identificar al Ejecutivo responsable y a la persona o grupo de planificación que elaborará el plan de implantación del SMS (analizado en el Capítulo 8).

#### 1.2 *Descripción del sistema y análisis de las carencias* (analizado en el Capítulo 7).

##### *Descripción del sistema*

- Realizar la descripción del sistema, que es la primera actividad de requisito para la elaboración de un SMS en una organización. Debería incluir las interfaces dentro del sistema, así como las interfaces con otros sistemas del sistema de transporte aéreo. En el Apéndice 1 del Capítulo 7 se brinda orientación sobre la descripción del sistema.

##### *Análisis de las carencias*

- Realizar un análisis de las carencias, con respecto a los cuatro componentes y doce elementos del marco para SMS de la OACI, a efectos de identificar disposiciones de seguridad operacional existentes en la organización así como las ausentes. En el Apéndice 2 del Capítulo 7 se brinda orientación sobre la elaboración de un análisis de las carencias del SMS.
- Sobre la base de los resultados del análisis de las carencias, la persona o grupo de planificación debería estar en condiciones de elaborar el plan de implantación del SMS teniendo en cuenta:
  - la identificación de posibles carencias que puedan afectar la implantación del SMS; y
  - la elaboración de estrategias para solucionar dichas carencias.

#### 1.3 *Política y objetivos de seguridad operacional* (analizado en el Capítulo 8)

##### *Política de seguridad operacional*

- Elaborar una política de seguridad operacional.
- La política de seguridad operacional deberá ser firmada por el Ejecutivo responsable.
- Comunicar la política de seguridad operacional, con visible endoso, a toda la organización.
- Establecer un plan de examen de la política de seguridad operacional para garantizar que sigue siendo pertinente y apropiada a la organización.

En el Capítulo 8 figura un ejemplo de declaración de política de seguridad operacional.



*Objetivos de seguridad operacional*

- Establecer objetivos de seguridad operacional para el SMS, elaborando normas de eficacia de la seguridad operacional en términos de:
  - indicadores de eficacia de la seguridad operacional;
  - objetivos de eficacia de la seguridad operacional; y
  - planes de acción.
- Establecer requisitos de SMS para subcontratistas:
  - establecer un procedimiento para incluir por escrito los requisitos del SMS en el proceso de contratación; y
  - establecer los requisitos SMS en la documentación para licitaciones.

1.4 **Responsabilidades y rendición de cuentas de seguridad operacional y designación de personal clave de seguridad operacional** (analizado en el Capítulo 8 de este manual)

*Estructura de organización del SMS*

- Establecer la Oficina de servicios de seguridad operacional.
- Designar un gerente de seguridad operacional como individuo responsable y punto focal para la elaboración y mantenimiento de un SMS efectivo.
- Evaluar y establecer líneas de comunicación entre la Oficina de servicios de seguridad operacional y el Ejecutivo responsable, el Grupo de acción de seguridad operacional (SAG) y la Junta de control de seguridad (SRB).
- Asegurar que las líneas funcionales de comunicación son acordes con el tamaño de la organización y la complejidad de los servicios que brinda.
- Establecer la Junta de control de seguridad (SRB) presidida por el Ejecutivo responsable.
- Designar para que integren la SRB a administradores superiores, incluyendo los gerentes responsables de las áreas funcionales.
- Asignar a la SRB funciones estratégicas apropiadas.
- Establecer el Grupo de acción de seguridad operacional (SAG).
- Designar para que integren el SAG a gerentes de línea y representantes del personal operativo.
- Asignar a la SRB funciones tácticas apropiadas.
- Documentar todas las responsabilidades, líneas de rendición de cuentas y facultades de seguridad operacional y comunicarlas a toda la organización, incluyendo una definición de los niveles de administración con autoridad para tomar decisiones sobre tolerabilidad de riesgos de seguridad operacional.
- Elaborar un calendario de reuniones para que la Oficina de servicios de seguridad operacional se reúna con la SRB y el SAG según sea necesario.

**1.5 Coordinación del plan de respuesta ante emergencias (ERP)** (analizado en el Capítulo 8)*Coordinación interna*

- Examinar la reseña del ERP respecto de la delegación de autoridad y asignación de responsabilidades para casos de emergencia.
- Establecer procedimientos de coordinación para el personal clave durante la emergencia y el retorno a las operaciones normales.

*Coordinación externa*

- Identificar entidades externas que interactuarán con la organización durante situaciones de emergencias.
- Evaluar sus respectivos ERP.
- Establecer coordinación entre los diferentes ERP.
- Incorporar la coordinación entre diferentes ERP en el Manual de sistemas de gestión de la seguridad operacional (SMSM) de la organización.

**1.6 Documentación SMS** (analizado en el Capítulo 8)*Documentación SMS*

- Establecer el mecanismo para recoger y almacenar registros y documentación específicos del SMS.
- Hacer referencia a todos los reglamentos nacionales y normas internacionales pertinentes y aplicables.
- Elaborar directrices para la gestión de registros que incluyan el plan de implantación del SMS y el SMSM.

*Plan de implantación del SMS*

- Designar la persona, o establecer el grupo de planificación, responsable de la elaboración del plan de implantación del SMS.
- Recoger todos los documentos aplicables que integran el plan de implantación del SMS.
- Celebrar reuniones regulares con la administración superior para evaluar los progresos.
- Asignar recursos (incluyendo el tiempo para reuniones) conmensurables con las tareas que han de realizarse.
- Incluir aspectos significativos del plan de implantación del SMS en el plan administrativo de la organización.
- Identificar los costos relacionados con la instrucción y planificación requeridas para la implantación del SMS.
- Asignar tiempo para la elaboración e introducción del plan de implantación del SMS entre los diferentes niveles administrativos de la organización.

- Redactar un presupuesto para la implantación del SMS.
- Aprobar el presupuesto inicial para la implantación del SMS.
- Presentar el plan de implantación del SMS para endoso por la administración superior.

*Manual de sistemas de gestión de la seguridad operacional (SMSM)*

- Redactar el SMSM para comunicar a toda la organización el enfoque de ésta sobre la seguridad operacional.
- Ampliar, revisar y enmendar el contenido del SMSM (que es un documento “viviente”) a medida que evoluciona el enfoque en fases del SMS.

**1.7 Promoción de la seguridad operacional — Instrucción** (analizado en el Capítulo 9)

*Instrucción en seguridad operacional*

- Elaborar un proceso documentado para identificar requisitos de instrucción.
- Elaborar un proceso de validación que mida la efectividad de la instrucción.
- Elaborar instrucción en seguridad operacional considerando:
  - instrucción inicial (seguridad general) específica de la tarea;
  - adoctrinamiento/instrucción inicial que incorpore el SMS, incluyendo factores humanos y factores de organización;
  - instrucción periódica.
- Identificar los costos relacionados con la instrucción.
- Organizar y establecer programas para la instrucción apropiada de todo el personal con arreglo a sus responsabilidades individuales y participación en el SMS.
- Elaborar ficheros de instrucción para cada empleado, incluyendo los gerentes.

**1.8 Promoción de la seguridad operacional — Comunicación de la seguridad operacional**  
(analizado en el Capítulo 9)

- Establecer un medio para transmitir la información de organización sobre la Fase I, incluyendo:
  - boletines informativos, anuncios y avisos de seguridad operacional;
  - sitio web;
  - correo electrónico.

**1.9 Cronograma para la implantación y resultados que han de lograrse**

El cronograma previsto para la implantación de la Fase I podría insumir de 1 a 6 meses, dependiendo del tamaño de la organización y la complejidad de los servicios que presta.

**Resultados**

- 1) Política de seguridad operacional firmada por el Ejecutivo responsable.
- 2) Política de seguridad operacional comunicada a todo el personal.
- 3) Descripción del sistema completada.
- 4) Análisis de las carencias completado.
- 5) Estructura de organización del SMS implantada.
- 6) Plan de implantación del SMS aprobado.
- 7) Instrucción sobre la fase de planificación del SMS brindada.
- 8) Proyecto inicial de SMSM publicado.
- 9) Medios para comunicar aspectos de seguridad operacional establecidos.

**2. FASE II — PROCESOS REACTIVOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL****2.1 Identificación y análisis de peligros basados en procesos reactivos**  
(analizado en los Capítulos 3, 4 y 9)*Identificación de peligros*

- Identificar las fuentes internas y externas que se utilizarán para recoger información reactiva sobre peligros.
- Implantar un enfoque estructurado de la identificación reactiva de peligros.

**2.2 Gestión de riesgos de seguridad operacional basada en procesos reactivos**  
(analizado en los Capítulos 5 y 9)*Evaluación de riesgos de seguridad operacional*

- Elaborar y adoptar una matriz de riesgos de seguridad operacional pertinente al entorno operacional de la organización.
- Elaborar instrucciones para la matriz de riesgos de seguridad e incluirlas en el programa de instrucción.

**2.3 Instrucción** (analizado en el Capítulo 9)

- Elaborar un programa de instrucción en seguridad operacional para el personal operativo, gerentes y supervisores sobre:

- los componentes pertinentes del plan de implantación del SMS;
- identificación de peligros y gestión de riesgos de seguridad operacional basadas en procesos reactivos (el personal operativo se instruirá en identificación y notificación de peligros a partir de sucesos activadores, y los supervisores se instruirán en gestión de peligros y riesgos de seguridad operacional);
- formulario/plantilla de notificación de peligros.

#### 2.4 **Documentación sobre procesos reactivos** (analizado en los Capítulos 4 y 9)

- Establecer una biblioteca de seguridad operacional.
- Agregar información sobre procesos reactivos de gestión de riesgos de seguridad operacional al SMSM. (La información sobre procesos reactivos de gestión de la seguridad operacional se empleará en una etapa posterior para establecer indicadores y objetivos de eficacia de la seguridad operacional).
- Redactar requisitos para la identificación de peligros y gestión de riesgos de seguridad operacional basados en procesos reactivos que se integrarán en la documentación para licitaciones de contratistas, de ser necesario, y se notificarán por escrito a contratistas y subcontratistas.

#### 2.5 **Promoción de la seguridad operacional — Comunicación de la seguridad operacional** (analizado en el Capítulo 9)

- Establecer un medio de transmitir la información de la organización sobre la Fase II:
  - boletines informativos, avisos y anuncios;
  - sitios web;
  - correo electrónico.

#### 2.6 **Cronograma para la implantación y resultados que han de lograrse**

El cronograma previsto para la implantación de la Fase II podría insumir de 9 a 12 meses dependiendo del tamaño de la organización y la complejidad de los servicios que brinda.

#### **Resultados**

- 1) Biblioteca de seguridad operacional establecida.
- 2) Procesos reactivos de gestión de la seguridad operacional implantados.
- 3) Instrucción pertinente a los componentes del plan de implantación del SMS y gestión de riesgos de seguridad operacional basados en procesos reactivos completados.
- 4) Información crítica para la seguridad operacional basada en los datos de seguridad operacional obtenidos de los procesos reactivos distribuidos a la organización.

### 3. FASE III — PROCESOS PROACTIVOS Y PREDICTIVOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

#### 3.1 **Identificación y análisis de peligros basados en procesos proactivos y predictivos**

(analizados en los Capítulos 3, 4 y 9)

##### *Identificación de peligros*

- Identificar las fuentes internas y externas que han de utilizarse para recoger información proactiva y predictiva sobre peligros.
- Implantar un enfoque estructurado de la identificación proactiva y predictiva de peligros.

#### 3.2 **Gestión de riesgo de seguridad operacional basada en procesos proactivos y predictivos**

(analizada en los Capítulos 5 y 9)

##### *Evaluación de riesgos de seguridad operacional*

- Elaborar y adoptar una matriz de riesgos de seguridad operacional pertinente al entorno operacional de la organización.
- Elaborar instrucciones para la matriz de riesgos de seguridad operacional e incluirlas en el programa de instrucción.

#### 3.3 **Instrucción** (analizada en el Capítulo 9)

- Instruir al personal de la oficina de servicio de seguridad operacional sobre medios específicos proactivos y predictivos de recoger datos relacionados con la seguridad operacional.
- Informar a los supervisores y al personal operativo sobre procesos proactivos y predictivos.
- Elaborar un programa de instrucción en seguridad operacional para el personal operativo, gerentes y supervisores:
  - los componentes pertinentes de plan de implantación SMS;
  - identificación de peligros y gestión de riesgos de seguridad operacional basadas en procesos proactivos y predictivos (el personal operativo se instruirá en identificación y notificación de peligros a partir de sucesos activadores menos graves o durante operaciones normales en tiempo real, y los supervisores se instruirán en gestión de peligros y riesgos de seguridad operacional basada en procesos proactivos y predictivos).

#### 3.4 **Documentación sobre procesos proactivos y predictivos**

(analizados en los Capítulos 4 y 9 de este manual)

- Almacenar información sobre gestión de riesgos de seguridad operacional basada en procesos proactivos y predictivos en la biblioteca de seguridad operacional.
- Agregar información sobre procesos proactivos y predictivos de gestión de riesgos de seguridad operacional en el SMSM.

- Elaborar indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional.
- Redactar requisitos para la identificación de peligros y gestión de riesgos de seguridad operacional basados en procesos proactivos y predictivos e incorporar en la documentación de licitaciones para contratistas, de ser necesario, y notificar por escrito a contratistas y subcontratistas.

### 3.5 **Promoción de la seguridad operacional — Comunicación de la seguridad operacional** (analizadas en el Capítulo 9)

- Establecer un medio de transmitir la información de organización sobre la Fase III:
  - boletines informativos, avisos y anuncios de seguridad operacional;
  - sitios web;
  - correo electrónico.

### 3.6 **Cronograma para la implantación y resultados que han de lograrse**

El cronograma previsto para la implantación de la Fase III podría insumir de 12 a 16 meses, dependiendo del tamaño de la organización y la complejidad de los servicios que presta.

#### **Resultados**

- 1) Período de prueba inicial establecido para medios proactivos y predictivos de recoger identificación de peligros.
- 2) Procesos proactivos y predictivos de gestión de la seguridad operacional implantados.
- 3) Instrucción pertinente a los componentes del plan de implantación del SMS y gestión de riesgos de seguridad operacional basados en procesos proactivos y predictivos completadas.
- 4) Indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional elaborados.
- 5) Información crítica sobre seguridad operacional basada en datos de seguridad capturados por procesos reactivos, proactivos y predictivos distribuida a la organización.

## **4. FASE IV — GARANTÍA DE LA SEGURIDAD OPERACIONAL**

### 4.1 **Eficacia de la seguridad operacional del SMS** (analizada en el Capítulo 9)

- Establecer indicadores de eficacia de la seguridad operacional.
- Establecer objetivos de eficacia de la seguridad operacional.
- Establecer planes de acción.
- Definir medidas de fiabilidad, disponibilidad o exactitud relativas a los planes de acción, según corresponda.

- Convenir en una medición de la eficacia de la seguridad operacional con la autoridad supervisora del Estado.

#### 4.2 **Supervisión y medición de la eficacia de la seguridad operacional** (analizadas en el Capítulo 9)

- Definir y desarrollar fuentes de información para la eficacia y supervisión de la seguridad operacional.

#### 4.3 **Gestión del cambio** (analizada en el Capítulo 9)

- Establecer un protocolo para la gestión del cambio que tenga en cuenta:
  - criticidad de los sistemas y actividades;
  - estabilidad de los sistemas y entornos operacionales;
  - eficacia anterior.
- Identificar cambios que puedan afectar los procesos, procedimientos, productos y servicios establecidos.
- Antes de implantar cambios, definir arreglos para garantizar la eficacia de la seguridad operacional.

#### 4.4 **Mejora continua del SMS** (analizada en el Capítulo 9)

- Elaborar formularios para evaluaciones internas y asegurar independencia respecto de los procesos técnicos que se evalúan.
- Definir un proceso de auditoría interna.
- Definir un proceso de auditoría externa.
- Definir un programa para la evaluación proactiva de instalaciones, equipo, documentación y procedimientos, que se completarán mediante auditorías y encuestas.
- Definir un programa para la evaluación proactiva de la performance de un individuo.
- Elaborar documentación pertinente a la garantía de la seguridad operacional.

#### 4.5 **Instrucción** (analizada en el Capítulo 9)

- Elaborar instrucción pertinente a la garantía de la seguridad operacional para el personal involucrado en la fase de garantía de la seguridad operacional.

#### 4.6 **Promoción de la seguridad operacional — Comunicación de la seguridad operacional** (analizadas en el Capítulo 9)

- Establecer un medio para transmitir información de la organización sobre la Fase IV:
  - boletines informativos, anuncios y avisos;
  - sitios web;
  - correo electrónico.



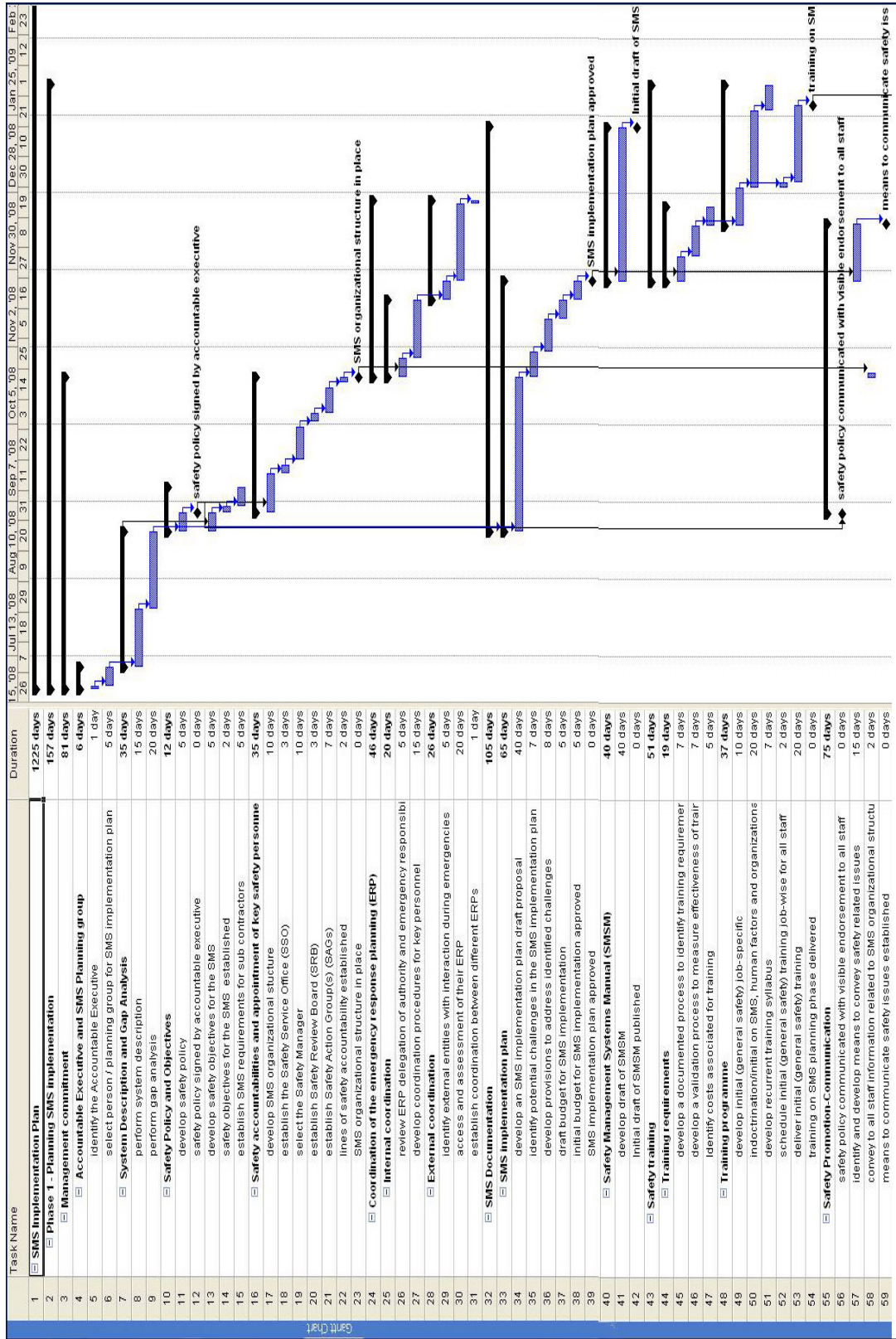
#### 4.7 **Cronograma para la implantación y resultados que han de obtenerse**

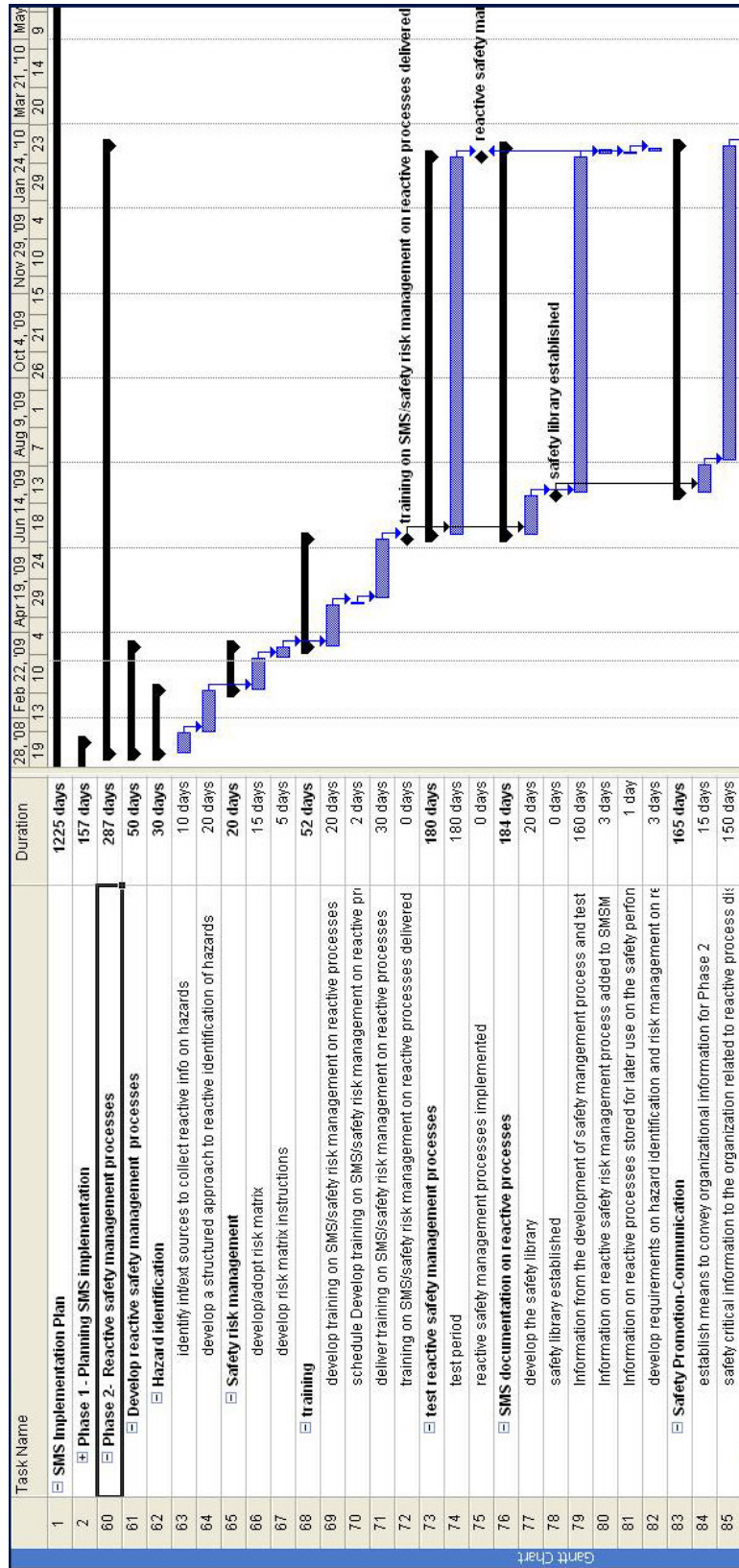
El cronograma previsto para la implantación de la Fase IV podía insumir de 9 a 12 meses, dependiendo del tamaño de la organización y la complejidad de los servicios que presta.

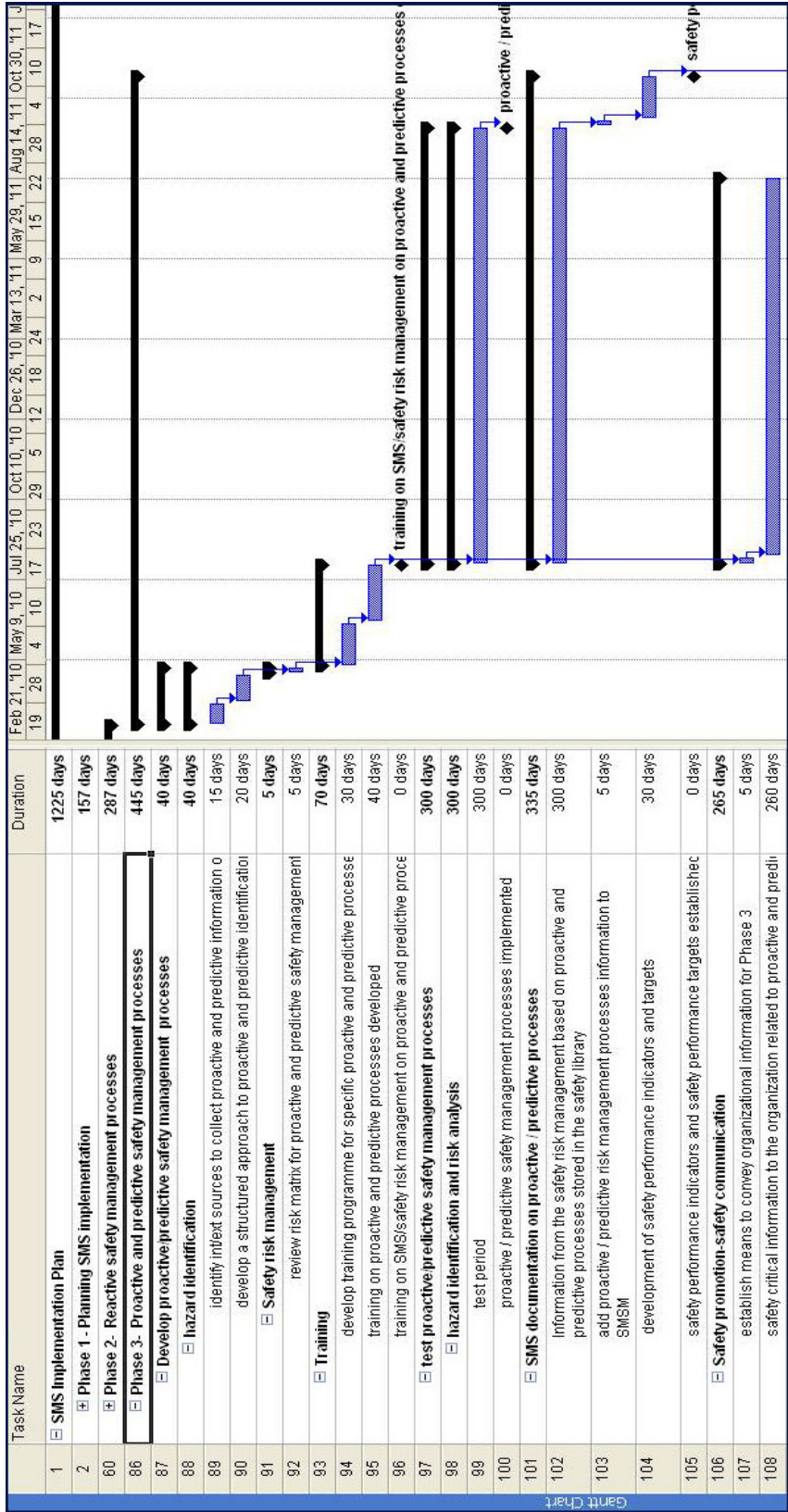
#### **Resultados**

- 1) Acuerdo alcanzado con la autoridad supervisora del Estado sobre indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional.
- 2) Instrucción completada sobre garantía de la seguridad operacional para el personal operativo, gerentes y supervisores.
- 3) Documentación pertinente a la garantía de la seguridad operacional incluida en la biblioteca de seguridad operacional.

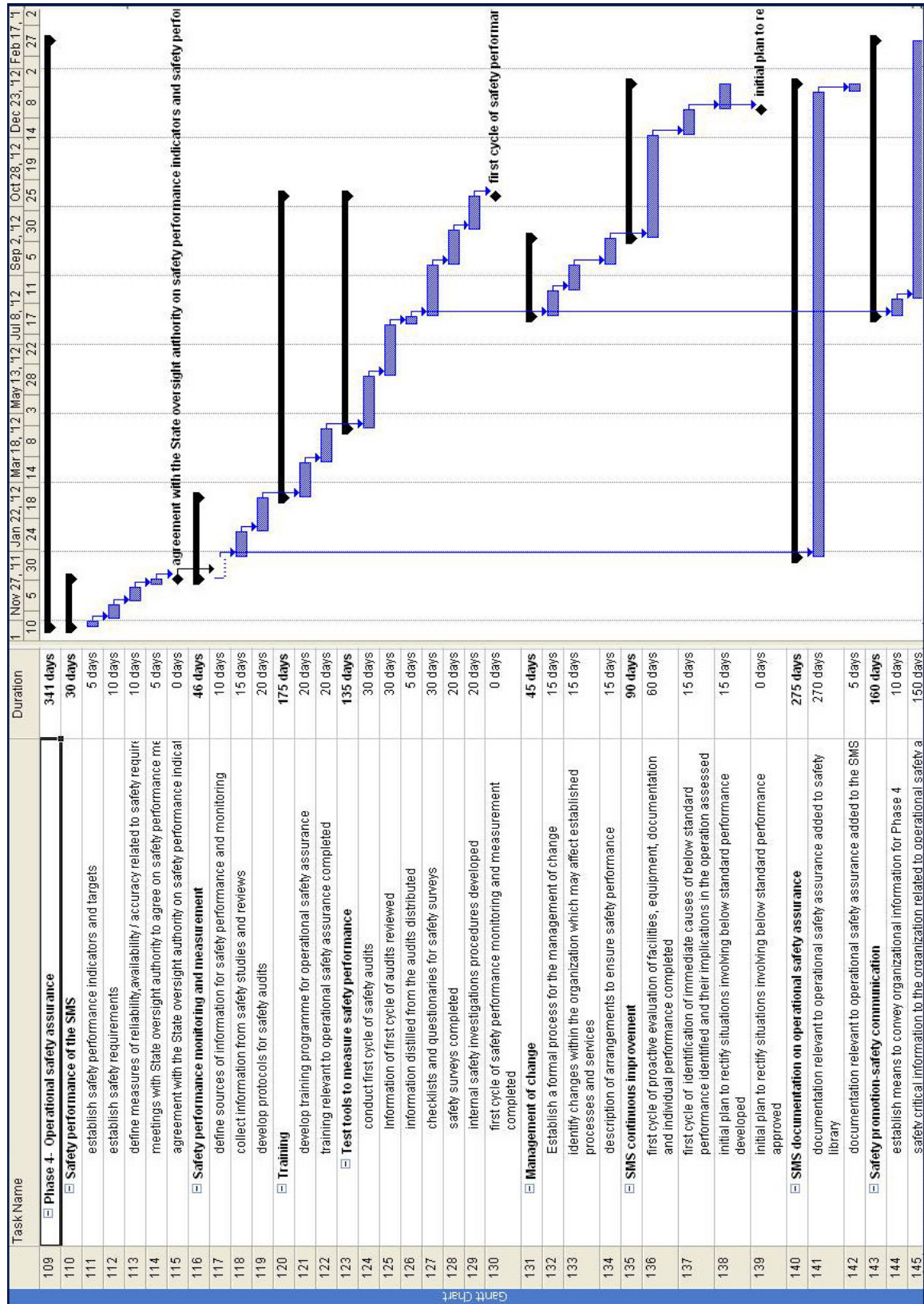
Carta de Gantt — Plan de implantación del SMS







Gantt Chart





# **Capítulo 11**

## **PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)**

### **11.1 OBJETIVO Y CONTENIDO**

En este capítulo se introduce un marco para la elaboración e implantación de un programa estatal de seguridad operacional (SSP) que combina elementos de los enfoques prescriptivos, y basado en la eficacia respecto de la gestión de la seguridad operacional. En este capítulo también se analiza la importancia de una implantación realista del SSP como prerrequisito para la implantación de un SMS por los proveedores de servicios. El capítulo comprende los temas siguientes:

- a) componentes y elementos de un SSP;
- b) marco para el SSP de la OACI;
- c) elaboración del SSP;
- d) implantación del SSP; y
- e) función del SSP en apoyo de la implantación del SMS.

### **11.2 COMPONENTES Y ELEMENTOS DE UN SSP**

11.2.1 Un SSP es un sistema para la gestión de la seguridad operacional por los Estados. La implantación de un SSP debe ser directamente proporcional al tamaño y complejidad del sistema de aviación del Estado y puede requerir coordinación entre las distintas autoridades responsables de las funciones de aviación civil correspondientes a cada elemento en el Estado.

11.2.2 El SSP tiene cuatro componentes, que representan las dos actividades operacionales básicas que el SSP debe emprender, así como los arreglos de organización necesarios para apoyar dichas actividades operacionales básicas. Los cuatro componentes del SSP son:

- a) política y objetivos de seguridad operacional de los Estados;
- b) gestión de riesgos de seguridad operacional por los Estados;
- c) garantía de la seguridad operacional por los Estados; y
- d) promoción de la seguridad operacional por los Estados.

11.2.3 Desde el punto de vista de las intervenciones de seguridad operacional y estrategias de mitigación, las dos actividades operacionales básicas de un SSP son la gestión de riesgo de seguridad operacional por los Estados y la garantía de la seguridad operacional por los Estados. Estas dos actividades operacionales básicas tienen lugar en el

marco proporcionado por la política y objetivos de seguridad operacional de los Estados y son apoyadas por la promoción de la seguridad operacional por los Estados. La mayoría de los componentes equivalentes de un SMS presentados en el Capítulo 8, 8.2 y 8.3 también se aplican al SSP. No obstante, existe una diferencia: en el marco del SSP, el proceso de investigación de accidentes e incidentes graves, si bien considerado formalmente como elemento de la política y objetivos de los Estados, también es una actividad operacional básica que contribuye a la recopilación, análisis e intercambio de datos de seguridad operacional, así como a la fijación de objetivos para la vigilancia de los elementos más preocupantes (garantía de la seguridad operacional por los Estados).

11.2.4 Los cuatro componentes analizados en 11.2.2 constituyen los bloques fundamentales básicos de un SSP, en el sentido de que representan los cuatro procesos generales de gestión de la seguridad operacional subyacentes en el sistema de gestión real (SSP). Cada componente se subdivide en elementos, que comprenden los subprocesos específicos, actividades específicas o herramientas específicas que el sistema de gestión real de los Estados deben realizar o utilizar para llevar a cabo la gestión de la seguridad operacional en una forma que combine los enfoques prescriptivos y basado en la eficacia y apoya la implantación de SMS por los proveedores de servicios.

11.2.5 El componente de política y objetivos de seguridad operacional de los Estados comprende cuatro elementos:

- a) marco legislativo estatal de la seguridad operacional;
- b) responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional;
- c) investigación de accidentes e incidentes; y
- d) política de cumplimiento.

11.2.6 El componente de gestión de riesgos de seguridad operacional por los Estados comprende dos elementos:

- a) requisitos de seguridad operacional para los SMS de los proveedores de servicios;
- b) acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional.

11.2.7 El componente de garantía de la seguridad operacional por los Estados comprende tres elementos:

- a) vigilancia de la seguridad operacional;
- b) recopilación, análisis e intercambio de datos sobre seguridad operacional; y
- c) fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención.

11.2.8 El componente de promoción de la seguridad operacional por los Estados comprende dos elementos:

- a) instrucción, comunicación y divulgación internas de la información sobre seguridad operacional; y
- b) instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

*Nota.— En el contexto del SSP, el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye a las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo y/o los fabricantes de aeronaves, los proveedores de servicio de tránsito aéreo y los aeródromos certificados, según corresponda.*



### 11.3 EL MARCO PARA SSP DE LA OACI

*Nota.— En el Apéndice 1 de este capítulo figura información detallada del marco de la OACI para SSP.*

11.3.1 Los cuatro componentes, combinados con los elementos analizados en la sección 11.2, constituyen el marco de la OACI para SSP, concebido como guía de principios para la elaboración, implantación y mantenimiento de un SSP, como sigue:

1. Política y objetivos de seguridad operacional de los Estados
  - 1.1 Marco legislativo estatal de la seguridad operacional
  - 1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
  - 1.3 Investigación de accidentes e incidentes
  - 1.4 Política de cumplimiento
2. Gestión de riesgos de seguridad operacional por los Estados
  - 2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
  - 2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional
3. Garantía de la seguridad operacional por los Estados
  - 3.1 Vigilancia de la seguridad operacional
  - 3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
  - 3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención
4. Promoción de la seguridad operacional por los Estados
  - 4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
  - 4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

11.3.2 El marco para SSP que se introduce en este capítulo, y el marco para el sistema de gestión de la seguridad operacional (SMS) especificado en el Capítulo 8, deben considerarse como complementarios aunque distintos.

### 11.4 ELABORACIÓN DE UN SSP

11.4.1 Se propone que los Estados elaboren su SSP en torno a los cuatro componentes y once elementos del marco para SSP de la OACI.

11.4.2 **Política y objetivos de seguridad operacional de los Estados.** Descripción de cómo supervisará el Estado la gestión de la seguridad operacional de sus actividades de aviación. Esto comprende una definición de los requisitos, responsabilidades y rendición de cuentas de las diferentes organizaciones estatales en lo que respecta al SSP, así como el nivel aceptable de seguridad operacional (ALoS) que debe alcanzar el SSP.

11.4.3 Los tres componentes SSP analizados en los párrafos siguientes pueden implantarse eficazmente sólo como parte de un marco general de rendición de cuentas y responsabilidades. Este marco general se transforma en un “paraguas protector”, bajo el cual tienen lugar la gestión de riesgo de seguridad operacional, la garantía de la seguridad operacional y la promoción de la seguridad operacional por los Estados. El componente de política y objetivos de seguridad operacional de los Estados proporciona políticas explícitas de gestión y de personal, procedimientos, controles administrativos, documentación y procesos de medidas correctivas que mantienen correctamente encausados

los esfuerzos de gestión de la seguridad operacional de la administración de aviación civil de los Estados. Este componente también es esencial en la generación de confianza en la capacidad de los Estados de proporcionar liderazgo en seguridad operacional en un sistema de transporte aéreo cada vez más complejo y constantemente cambiante. Una actividad central en el marco de este componente es la elaboración de la política de seguridad operacional de los Estados. En el Apéndice 2 de este capítulo se proporciona orientación sobre la elaboración de una declaración de política de seguridad operacional de los Estados.

11.4.4 **Gestión de riesgos de seguridad operacional por los Estados.** Descripción de cómo identificarán los Estados los peligros y cómo evaluarán los riesgos de seguridad operacional de las consecuencias de los peligros en las operaciones de aviación de los Estados. Esto comprende el establecimiento de controles (reglas o reglamentos) que rigen la forma en que los Estados gestionarán la seguridad operacional, reglas o reglamentos que rigen cómo funciona el SMS del proveedor de servicios, así como un acuerdo sobre la eficacia de la seguridad operacional del SMS del proveedor de servicios.

11.4.5 Los principios de gestión de la seguridad operacional afectan a la mayoría de las actividades de la administración de aviación civil de los Estados, comenzando con la formulación de reglas y el desarrollo de políticas. En vez de buscar solamente las causas del accidente más reciente, la formulación de reglas del SSP se basa en análisis completos del sistema de aviación de los Estados. Los reglamentos se basan en los peligros identificados y en el análisis de los riesgos de seguridad operacional de las consecuencias de los peligros. Los propios reglamentos proporcionan un marco para el control de riesgos, cuando se les integra en el SMS del proveedor de servicios.

11.4.6 **Garantía de la seguridad operacional por los Estados.** Una descripción de cómo asegurarán los Estados que la gestión de la seguridad operacional dentro de los Estados y el funcionamiento del SMS del proveedor de servicios se ajustan a controles establecidos (cumplimiento de los reglamentos), cuán realista será la implantación del SSP (ALoS), mediante una combinación de medidas de seguridad operacional por los Estados y de eficacia de la seguridad operacional por los proveedores de servicios, y cómo la actuación real del SMS del proveedor de servicios (eficacia de la seguridad operacional) se demostrará (medición de la eficacia de la seguridad operacional). Esto comprende el establecimiento de los arreglos necesarios (vigilancia, inspecciones, auditorías, análisis de datos de seguridad operacional y así sucesivamente) necesarios para verificar el cumplimiento y medir la eficacia.

11.4.7 **Actividades de vigilancia del SSP.** Las actividades de vigilancia del SSP, más allá de la formulación de reglas, están apoyadas por análisis, y las prioridades de asignación de recursos de la administración de aviación civil de los Estados se basan en los riesgos de seguridad operacional de las consecuencias de los peligros identificados mediante los análisis. La certificación y las decisiones continuas sobre seguridad operacional se basan en evaluaciones de la eficacia de los procesos del proveedor de servicios, sus productos o servicios. Avanzando desde los reglamentos que tratan peligros definidos, las decisiones de cumplimiento se basan en si el SMS de un proveedor de servicios encara los peligros en los reglamentos dentro del entorno operacional específico del proveedor de servicios. Los procesos de garantía de la seguridad operacional por los Estados se utilizan para obtener confianza en la capacidad de gestión de la seguridad operacional del proveedor de servicios según lo demuestren las evaluaciones de su SMS. Es importante destacar que en el marco del SSP no se requiere establecer mecanismos específicos para dar seguimiento a los ocho elementos críticos esbozados en el Doc 9734 de la OACI, Parte A, *Establecimiento y gestión de un sistema estatal de vigilancia de la seguridad operacional*.

11.4.8 **Promoción de la seguridad operacional por los Estados.** Una descripción de los arreglos establecidos por los Estados para asegurar que se realiza la instrucción en seguridad operacional y la comunicación y difusión de información de seguridad operacional. En el marco de un SSP, esto es una promoción doble; tanto dentro de las organizaciones aeronáuticas de los Estados como entre los proveedores de servicios que éstos supervisan. Comprende el establecimiento de los medios necesarios para proporcionar instrucción y comunicar información de seguridad operacional.

11.4.9 Nada de lo mencionado anteriormente modifica la función de los Estados y sus organizaciones de aviación con respecto al establecimiento de los reglamentos y normas de los Estados o al requisito de que el personal

de aviación civil de los Estados posea altos niveles de conocimiento y competencia. Por el contrario, exige competencias adicionales en áreas tales como análisis de riesgos de seguridad operacional, valoración del sistema y evaluación del sistema de gestión, así como en las muchas nuevas tecnologías fundamentales para que la industria de la aviación logre sus objetivos de producción. Esto hace que corresponda a los Estados proporcionar estas competencias mediante instrucción, contratación y gestión de recursos humanos.

11.4.10 Al elaborar el SSP, los principios de gestión de la seguridad operacional proporcionan una plataforma conceptual para el desarrollo paralelo del SSP por los Estados y el SMS por los proveedores de servicios. Un SSP elaborado a partir de principios de gestión de la seguridad operacional y basado en los mismos constituye el puente que cierra la brecha que de otra manera surgiría inevitablemente entre los procesos internos y externos de seguridad operacional dentro de las organizaciones de aviación civil de los Estados y los procesos internos de seguridad operacional de los proveedores de servicios (véase la Figura 11-1). Como parte del SSP, los Estados promulgan requisitos de SMS para los proveedores de servicios que les exigen demostrar su capacidad de gestión de la seguridad operacional directamente, en vez de esperar que ocurran accidentes, incidentes o casos de incumplimiento de normas de seguridad operacional. Esto permite tanto a los Estados como a los proveedores de servicios adelantarse a los riesgos de seguridad operacional. Los requisitos de SMS en el marco del SSP también proporcionan un marco estructurado que permite a los Estados y a los proveedores de servicios interactuar más efectivamente en la solución de problemas de seguridad operacional. De esta manera el carácter compartido e interactivo del SSP y el SMS rinde sus mejores frutos.

## 11.5 IMPLANTACIÓN DEL SSP

11.5.1 La implantación del SSP se facilita mediante la identificación de los procesos relacionados con cada uno de los cuatro componentes del SSP analizados en los párrafos anteriores. Estos procedimientos pueden transformarse a su vez en elementos discretos de cada componente del SSP y, análogamente al marco para SMS analizado en el Capítulo 8, la combinación de elementos y componentes pasa a ser el marco para el SSP. La disponibilidad de dicho marco proporciona una guía de principios para la implantación del SSP. La OACI ha elaborado orientación para la elaboración de un marco para SSP a efectos de facilitar la implantación del SSP de la OACI y dicho marco figura en el Apéndice 1 de este capítulo. En el Apéndice 5 de este capítulo se presenta orientación sobre el plan de implantación del SSP.

11.5.2 En el sitio web de la AAC del Reino Unido [www.caa.co.uk](http://www.caa.co.uk) figura un ejemplo de SSP elaborado por un Estado, el Programa estatal de seguridad operacional para el Reino Unido, publicado en la Publicación de aviación civil (CAP) 784 del Reino Unido.

## 11.6 FUNCIÓN DEL SSP EN APOYO DE LA IMPLANTACIÓN DEL SMS

11.6.1 Uno de los objetivos del SSP es generar un contexto que apoye la implantación de un SMS por los proveedores de servicios. El SMS del proveedor de servicios no puede funcionar eficazmente en un vacío normativo o en un entorno exclusivamente orientado al cumplimiento. En tales entornos, los proveedores de servicios implantarán y demostrarán solamente los aspectos exteriores de un SMS y las autoridades estatales sólo evaluarán los mismos. El SMS de un proveedor de servicios puede desarrollarse plenamente sólo bajo la cobertura proporcionada por un SSP. Por consiguiente, el SSP es un capacitador fundamental de la implantación de un SMS efectivo por los proveedores de servicios. Por esta razón, dentro del alcance de la implantación general de un SSP presentada en el Capítulo 5, cuatro pasos, dos globales y dos específicos, están concebidos para apoyar la implantación del SMS por los proveedores de servicios.



**Figura 11-1. El SMS constituye el puente que cierra la brecha entre los procesos de seguridad operacional de los Estados y los del proveedor de servicios**

11.6.2 El primer paso, general, que ha de adoptar un Estado al implantar su SSP es realizar un análisis de carencias, para evaluar la existencia y el grado de madurez, dentro del Estado, de los elementos de un SSP. Un ejemplo de análisis de carencias para un SSP se incluye en el Apéndice 3 de este capítulo. Después del análisis de carencias, el Estado está en condiciones de redactar legislación nacional de reglamentos de operación que rigen el funcionamiento del SSP. Entre estos estarán los requisitos para SMS de los proveedores de servicios.

11.6.3 Uno de los primeros pasos en la implantación del SSP es elaborar un programa de instrucción para el personal de la administración de los Estados. El programa de instrucción debería tener dos objetivos básicos. El primero es proporcionar conocimientos sobre conceptos de gestión de la seguridad operacional, incluyendo los SARPS de la OACI que figuran en los Anexos 1, 6, 8, 11, 13 y 14, y textos de orientación conexos. Este aspecto de la instrucción se aplica al SSP con carácter general. El segundo objetivo es desarrollar conocimientos para aceptar y supervisar la implantación de componentes clave de un SMS, en cumplimiento de los reglamentos nacionales y SARPS pertinentes de la OACI. Este aspecto de la instrucción se dirige a apoyar la implantación del SMS.

11.6.4 El primer paso en la implantación del SSP, especialmente dirigido a apoyar la implantación del SMS, es la elaboración de requisitos sobre SMS para proveedores de servicios, así como textos de orientación para la implantación del SMS. En el Apéndice 1 del Capítulo 10 figura orientación sobre la elaboración de un reglamento sobre SMS de los Estados. Dicha orientación utiliza como referencia los componentes y elementos del marco de la OACI para SMS analizado en el Capítulo 8. Este manual y los cursos de instrucción sobre SMS y SSP de la OACI son fuentes de información para la elaboración de textos de orientación.

11.6.5 El segundo paso en la implantación de un SSP, dirigido específicamente a apoyar la implantación del SMS, es la revisión de la política de cumplimiento de la autoridad supervisora de la aviación civil. Este paso merece mención especial.

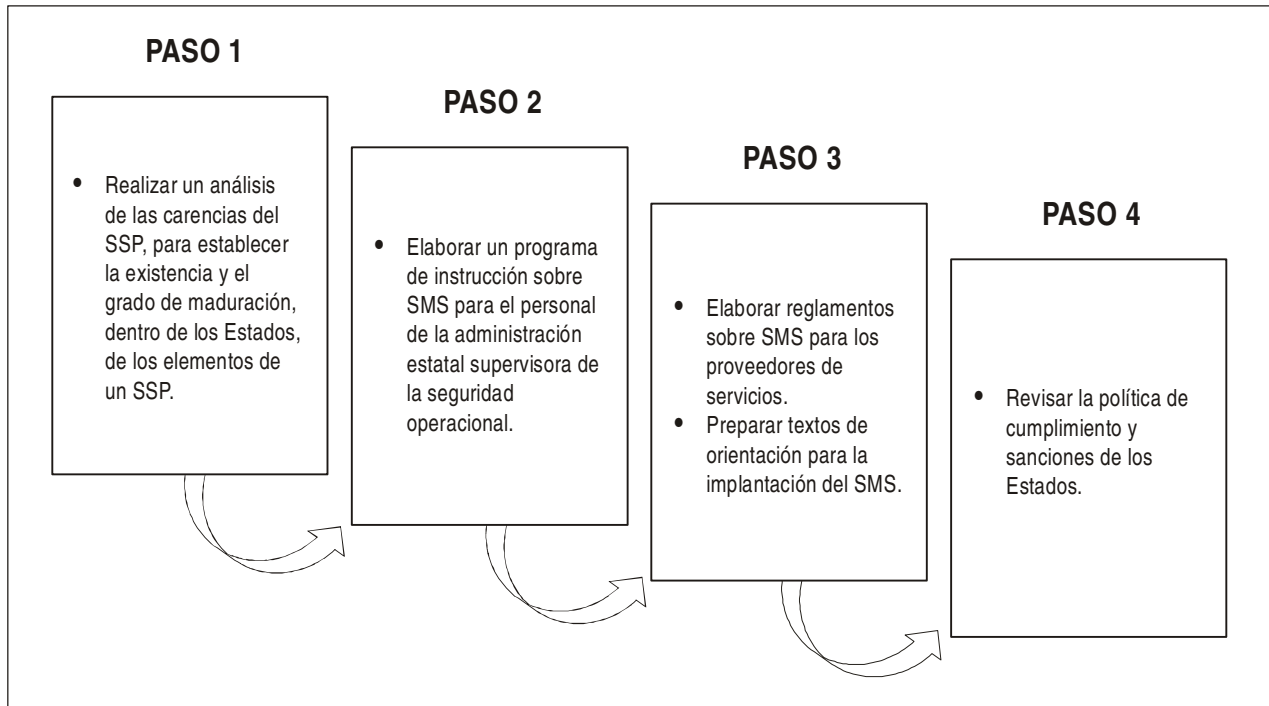
11.6.6 La esencia del SSP y del SMS es adelantarse a los riesgos de seguridad operacional mediante la elaboración de capacidades de gestión de la seguridad operacional dentro de los Estados así como en la industria, en vez de esperar que ocurran accidentes, incidentes o sucesos de incumplimiento. Una esencia de la gestión, según se analiza en diversas partes de este manual, es la medición, dado que no es posible gestionar lo que no puede medirse. A su vez, la medición requiere datos. Se deduce que la recopilación, análisis e intercambio de datos de seguridad operacional constituye la médula del carácter interactivo del SSP y del SMS analizados en 11.4.10.

11.6.7 Durante el transcurso de las actividades normales de gestión de la seguridad operacional en el marco del SSP y SMS, respectivamente, los Estados y los proveedores de servicios intercambiarán datos de seguridad operacional. Los datos de seguridad operacional del proveedor de servicios recibidos por los Estados serán datos privados, parte de los cuales los Estados convertirán en datos colectivos. Un volumen considerable de todos estos datos se referirá razonablemente a problemas de seguridad operacional identificados en el transcurso normal de los procesos SMS del proveedor de servicio. Si la respuesta de la autoridad supervisora de aviación civil a estos datos es la aplicación de sanciones, el proceso de gestión de la seguridad operacional en los Estados se detendrá repentinamente. Por consiguiente, es esencial que, como parte del SSP, la autoridad supervisora de la aviación civil revise sus políticas de cumplimiento para asegurar la continua circulación e intercambio de datos proactivos y predictivos de gestión de la seguridad operacional con los proveedores de servicios que operan en un entorno SMS. Se proponen las siguientes directrices para esa revisión:

- a) debería permitirse a los proveedores de servicios que se encarguen internamente de ciertos problemas de seguridad operacional, dentro del contexto de su SMS;
- b) los proveedores de servicios deberían proporcionar a los Estados una clara definición del problema de seguridad operacional, incluyendo desviaciones o violaciones menores, y un plan de mitigación para su solución, que satisfaga a los Estados;
- c) el plan de mitigación debería incluir fechas, de modo que los Estados puedan supervisar satisfactoriamente el progreso de las actividades de mitigación; y
- d) la negligencia grave, la conducta temeraria y las desviaciones intencionales deberían abordarse mediante procedimientos establecidos en cuanto a cumplimiento y sanción.

En el Apéndice 4 de este capítulo se presenta orientación sobre la elaboración de una política estatal de cumplimiento y procedimientos de sanciones en un entorno SMS.

11.6.8 En la Figura 11-2 se presenta un resumen de la función del SSP en apoyo de la implantación del SMS y medidas propuestas.



**Figura 11-2. Resumen de la función del SSP en apoyo de la implantación del SMS**

-----

## Apéndice 1 del Capítulo 11

### MARCO PARA EL PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

*Nota.— En el contexto de este apéndice el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye a las organizaciones de instrucción reconocidas que están expuestas a riesgo de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicio de tránsito aéreo y los aeródromos certificados, según corresponda.*

En este apéndice se presenta un marco para la implantación y el mantenimiento de un programa estatal de seguridad operacional (SSP) por cada Estado. El marco está compuesto por los siguientes cuatro componentes y once elementos:

1. Política y objetivos de seguridad operacional de los Estados
  - 1.1 Marco legislativo estatal de la seguridad operacional
  - 1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
  - 1.3 Investigación de accidentes e incidentes
  - 1.4 Política de cumplimiento
2. Gestión de riesgos de seguridad operacional por los Estados
  - 2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
  - 2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional
3. Garantía de la seguridad operacional por los Estados
  - 3.1 Vigilancia de la seguridad operacional
  - 3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
  - 3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención
4. Promoción de la seguridad operacional por los Estados
  - 4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
  - 4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

Sigue una breve descripción de cada elemento.

## **1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL DE LOS ESTADOS**

### **1.1 Marco legislativo estatal de la seguridad operacional**

El Estado ha promulgado un marco legislativo nacional de seguridad operacional y reglamentos específicos de conformidad con normas nacionales e internacionales, que definen la forma en que el Estado llevará a cabo la gestión de la seguridad operacional en el Estado. Esto incluye la participación de las organizaciones de aviación estatales en actividades específicas relacionadas con la gestión de la seguridad operacional en el Estado, y la creación de los roles, las responsabilidades y las relaciones de dichas organizaciones. El marco legislativo de la seguridad operacional y la reglamentación específica se examinan periódicamente para asegurar que sigan siendo pertinentes y apropiados para el Estado.

### **1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional**

El Estado ha identificado, definido y documentado los requisitos, las responsabilidades y la rendición de cuentas relativas a la creación y el mantenimiento del SSP. Esto incluye las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional del Estado. Incluye además una declaración clara sobre la provisión de los recursos necesarios para la implantación del SSP.

### **1.3 Investigación de accidentes e incidentes**

El Estado ha establecido un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes, y no la asignación de culpa o responsabilidad. Estas investigaciones respaldan la gestión de la seguridad operacional en el Estado. En el marco del SSP, el Estado mantiene la independencia de la organización de investigación de accidentes e incidentes respecto de otras organizaciones estatales de aviación.

### **1.4 Política de cumplimiento**

El Estado ha promulgado una política de cumplimiento que establece las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional, y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, a satisfacción de la autoridad estatal competente. La política de cumplimiento establece además las condiciones y circunstancias en las cuales las desviaciones con respecto de la seguridad operacional deben abordarse mediante procedimientos establecidos en cuanto a cumplimiento.

## **2. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL POR LOS ESTADOS**

### **2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios**

El Estado ha establecido los controles que rigen la forma en que los proveedores de servicios detectarán los peligros y gestionarán los riesgos de seguridad operacional. Esto incluye los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para los SMS de los proveedores de servicios. Los requisitos, reglamentos específicos de funcionamiento y políticas de implantación se examinan periódicamente para asegurar que sigan siendo pertinentes y apropiados para los proveedores de servicios.



## **2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional**

El Estado ha acordado con cada proveedor de servicios la actuación de sus SMS respecto de la seguridad operacional. La eficacia de la seguridad operacional acordada de los SMS de cada proveedor de servicios se examina periódicamente para asegurar que siga siendo pertinente y apropiada para los proveedores de servicios.

## **3. GARANTÍA DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS**

### **3.1 Vigilancia de la seguridad operacional**

El Estado ha establecido mecanismos para asegurar la supervisión eficaz de los ocho elementos críticos de la función de vigilancia de la seguridad operacional. El Estado ha creado además mecanismos para garantizar que la detección de peligros y la gestión de riesgos de seguridad operacional por los proveedores de servicios se ajusten a los controles reguladores establecidos (requisitos, reglamentos de funcionamiento específicos y políticas de implantación). Estos mecanismos incluyen inspecciones, auditorías y encuestas para asegurar que los controles reguladores de los riesgos de seguridad operacional se integren apropiadamente en los SMS de los proveedores de servicios, que se lleven a la práctica conforme a su diseño, y que tengan el efecto previsto en los riesgos de seguridad operacional.

### **3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional**

El Estado ha establecido mecanismos para asegurar la captura y almacenamiento de datos sobre peligros y riesgos de seguridad operacional a nivel tanto individual como global. El Estado ha establecido además mecanismos para preparar información a partir de los datos almacenados y para intercambiar activamente información sobre seguridad operacional con los proveedores de servicios y otros Estados, según corresponda.

### **3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención**

El Estado ha establecido procedimientos para priorizar las inspecciones, auditorías y encuestas relacionadas con los elementos que plantean más preocupación o que requieren mayor atención, según lo detectado en el análisis de los datos sobre peligros, sus consecuencias en las operaciones y los riesgos de seguridad operacional evaluados.

## **4. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS**

### **4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional**

El Estado proporciona instrucción y fomenta el conocimiento y el intercambio de información relacionada con la seguridad operacional para respaldar, en las organizaciones estatales de aviación, el desarrollo de una cultura organizativa que promueva SSP eficaces.

#### **4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional**

El Estado proporciona educación y promueve el conocimiento con respecto a los riesgos de seguridad operacional y el intercambio de información relativa a la seguridad operacional para respaldar, entre los proveedores de servicios, el desarrollo de una cultura organizativa que promueva SMS eficaces.

-----

## Apéndice 2 del Capítulo 11

# ORIENTACIÓN SOBRE LA ELABORACIÓN DE UNA DECLARACIÓN ESTATAL DE POLÍTICA DE SEGURIDAD OPERACIONAL

La gestión de la seguridad operacional de la aviación civil es una de las principales responsabilidades de [Estado]. [Estado] se compromete a elaborar, implantar, mantener y mejorar constantemente estrategias y procesos para asegurar que todas las actividades de aviación que tienen lugar bajo su supervisión lograrán el mayor nivel de eficacia de seguridad operacional, satisfaciendo al mismo tiempo las normas nacionales e internacionales.

Los titulares de certificados de aviación de [Estado] deberán demostrar que sus sistemas de gestión reflejan adecuadamente un enfoque de SMS. El resultado previsto de este enfoque es una gestión de la seguridad operacional y prácticas de seguridad operacional mejoradas, incluyendo la notificación de seguridad dentro de la industria de aviación civil.

En [Estado], todos los niveles de administración son responsables por el logro del más alto nivel de eficacia de la seguridad operacional dentro de [Estado], comenzando por el Ejecutivo responsable [según corresponda a la organización].

[Estado] se compromete a:

- a) elaborar la formulación de reglas generales y políticas operacionales específicas, fundadas en principios de gestión de la seguridad operacional, sobre la base de un análisis completo del sistema de aviación del Estado;
- b) consultar a todos los sectores de la industria de la aviación sobre aspectos relativos a la elaboración de reglamentos;
- c) apoyar la gestión de la seguridad operacional en el Estado mediante un sistema efectivo de notificación y comunicación de la seguridad operacional;
- d) interactuar eficazmente con los proveedores de servicios para la resolución de problemas de seguridad operacional;
- e) asegurar que dentro de [la administración estatal supervisora de la seguridad operacional], se asignan suficientes recursos y que el personal cuenta con las competencias y la instrucción adecuadas para realizar sus tareas, tanto relacionadas con la seguridad operacional como de otro tipo;
- f) realizar actividades de supervisión tanto basadas en la eficacia como en el cumplimiento, apoyadas por análisis y asignación priorizada de recursos basada en los riesgos de seguridad operacional;
- g) cumplir y, cuando sea posible, superar, los requisitos y normas internacionales de seguridad operacional;
- h) promover conceptos y principios de gestión de la seguridad operacional y educar a la industria de la aviación al respecto;

- i) supervisar la implantación de SMS dentro de las organizaciones de aviación;
- j) asegurar que todas las actividades bajo supervisión logran las más altas normas de seguridad operacional;
- k) establecer disposiciones para la protección de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS), de modo que se aliente a las personas a proporcionar información esencial relacionada con la seguridad operacional sobre peligros, y que existe una corriente e intercambio continuos de datos de gestión de la seguridad operacional entre [Estado] y los proveedores de servicios;
- l) establecer y medir la implantación realista de nuestro SSP con respecto a los indicadores de seguridad operacional y a los objetivos de seguridad operacional que están claramente identificados; y
- m) promulgar una política de cumplimiento que asegure que ninguna información obtenida de SDCPS establecidos en el marco del SSP o el SMS se utilizará como base para la imposición de sanciones, excepto en caso de negligencia grave o desviaciones intencionales.

Esta política debe ser comprendida, implantada y observada por todo el personal que participa en actividades relacionadas con [administración estatal de supervisión de la seguridad operacional].

(Firma) \_\_\_\_\_  
Ejecutivo responsable

-----

## Apéndice 3 del Capítulo 11

# ORIENTACIÓN SOBRE LA ELABORACIÓN DE UN ANÁLISIS DE LAS CARENCIAS DEL PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

*Nota.— En el contexto de esta orientación el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye a las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicio de tránsito aéreo y los aeródromos certificados, según corresponda.*

### 1. ANÁLISIS DE LAS CARENCIAS

1.1 La implantación de un SSP requiere que el Estado realice un análisis de su sistema de seguridad operacional para determinar cuáles son los componentes y elementos del SSP que están actualmente implantados y cuáles deben añadirse o modificarse para satisfacer los requisitos de implantación. Este análisis se conoce como análisis de las carencias y entraña la comparación de los requisitos del SSP respecto de los recursos existentes en un Estado.

1.2 El análisis de las carencias proporciona, en forma de lista de verificación, información para ayudar en la evaluación de los componentes y elementos que integran el marco de la OACI para SSP e identificar los componentes y elementos que deben elaborarse. Una vez completado y documentado el análisis de carencias, constituye una de las bases del plan de implantación del SSP.

### 2. MARCO DE LA OACI PARA SSP

El marco de la OACI para SSP consta de cuatro componentes y once elementos, a saber:

1. Política y objetivos de seguridad operacional de los Estados
  - 1.1 Marco legislativo estatal de la seguridad operacional
  - 1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
  - 1.3 Investigación de accidentes e incidentes
  - 1.4 Política de cumplimiento
2. Gestión de riesgos de seguridad operacional por los Estados
  - 2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
  - 2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

3. Garantía de la seguridad operacional por los Estados
  - 3.1 Vigilancia de la seguridad operacional
  - 3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
  - 3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención
4. Promoción de la seguridad operacional por los Estados
  - 4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
  - 4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

### 3. ANÁLISIS DE LAS CARENCIAS DEL PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

La siguiente lista para análisis de las carencias puede utilizarse como modelo para realizar un análisis de ese tipo. Cada pregunta está concebida para obtener una respuesta “sí” o “no”. Una respuesta “sí” indica que el Estado ya ha incorporado a su sistema de seguridad operacional el componente o elemento del marco de la OACI para SSP en cuestión y que cumple o supera el requisito. Una respuesta “no” indica que existe una brecha (carencia) entre el componente/elemento del marco de la OACI para SSP y el sistema de seguridad operacional en el Estado.

<i>Referencia OACI (Doc 9859)</i>	<i>Aspecto para analizar o pregunta para contestar</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
<b>Componente 1 — POLÍTICAS Y OBJETIVOS DE SEGURIDAD OPERACIONAL DE LOS ESTADOS</b>			
<b>Elemento 1.1 — Marco legislativo estatal de seguridad operacional</b>			
Capítulo 11	¿Ha promulgado [Estado] un marco legislativo nacional de seguridad operacional y las reglamentaciones específicas que definen la gestión de la seguridad operacional en el Estado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Ha definido [Estado] las actividades específicas relacionadas con la gestión de la seguridad operacional en el Estado en las cuales cada organización de aviación de [Estado] debe participar?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Ha establecido [Estado] los requisitos, las responsabilidades y las obligaciones de rendir cuentas con respecto a la gestión de la seguridad operacional en todas las organizaciones de aviación de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se examinan periódicamente el marco legislativo y la reglamentación específica para asegurar que sigan siendo pertinentes y apropiadas para el Estado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se examinan periódicamente el marco legislativo y la reglamentación específica de [Estado] para asegurar que están actualizados con respecto a las normas internacionales?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

Referencia OACI (Doc 9859)	Aspecto para analizar o pregunta para contestar	Respuesta	Estado de implantación
Capítulo 11	¿Ha establecido [Estado] una política de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿La política de seguridad operacional de [Estado] está firmada por el Ejecutivo responsable del SSP de [Estado] o una autoridad superior dentro de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se examina periódicamente la política de seguridad operacional de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿La política de seguridad operacional de [Estado] se comunica con visible endoso a todos los empleados de todas las organizaciones de aviación de [Estado] para que tomen conciencia de sus responsabilidades individuales de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Ha elaborado [Estado] documentación que describa el SSP, incluyendo las interrelaciones entre sus componentes y elementos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Cuenta [Estado] con un sistema de registro que asegure que la generación y conservación de todos los registros necesarios para documentar y apoyar las actividades del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Proporciona el sistema de registro los procesos de control necesarios para asegurar la apropiada identificación, legibilidad, almacenamiento, protección, archivo, recuperación, tiempo de conservación y disposición de los registros?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 1.2 — Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional</b>			
Capítulo 11	¿Ha identificado y definido [Estado] los requisitos, las responsabilidades y la rendición de cuentas estatales relativos a la creación y mantenimiento del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Incluyen los requisitos directrices y actividades para planificar, organizar, desarrollar, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Incluyen los requisitos una declaración clara sobre la provisión de los recursos necesarios para la implantación y mantenimiento del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Ha identificado y designado [Estado] un Ejecutivo responsable como persona cualificada con responsabilidad directa por la implantación, funcionamiento y supervisión del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Cumple el Ejecutivo responsable del SSP de [Estado] las funciones y responsabilidades requeridas de su tarea?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Coordina el Ejecutivo responsable de SSP de [Estado], según corresponda, las actividades de las diferentes organizaciones de aviación del Estado en el marco del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

<i>Referencia OACI (Doc 9859)</i>	<i>Aspecto para analizar o pregunta para contestar</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
Capítulo 11	¿Tiene el Ejecutivo responsable del SSP de [Estado] control sobre los recursos necesarios requeridos para la ejecución adecuada del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Verifica el Ejecutivo responsable del SSP de [Estado] que todo el personal de las organizaciones de aviación de [Estado] comprenden sus facultades, responsabilidades y obligaciones de rendir cuentas con respecto al SSP y todos los procesos, decisiones y medidas de gestión de la seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Están definidas y documentadas, en todos los niveles, las responsabilidades y obligaciones de rendición de cuentas de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 1.3 — Investigación de accidentes e incidentes</b>			
Capítulo 11	¿Ha establecido [Estado], como parte de la gestión de la seguridad operacional, un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes y no la asignación de culpa o responsabilidad?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Mantiene [Estado] la independencia de la organización de investigación de accidentes e incidentes respecto de otras organizaciones estatales de aviación?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 1.4 — Política de cumplimiento</b>			
Capítulo 11	¿Ha promulgado [Estado] una política de cumplimiento?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Establece la política de cumplimiento las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional, y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, a satisfacción de la autoridad estatal competente?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Establece la política de cumplimiento las condiciones y circunstancias en las cuales las desviaciones respecto de la seguridad operacional deben abordarse mediante procedimientos establecidos en cuanto a cumplimiento?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Componente 2 — GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL POR LOS ESTADOS</b>			
<b>Elemento 2.1 — Requisitos de seguridad operacional para los SMS de los proveedores de servicios</b>			
Capítulo 11	¿Ha establecido [Estado] los controles que rigen la forma en que los proveedores de servicios detectarán los peligros y gestionarán los riesgos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	



Referencia OACI (Doc 9859)	Aspecto para analizar o pregunta para contestar	Respuesta	Estado de implantación
Capítulo 11	¿Incluyen esos controles los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para los SMS de los proveedores de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se basan todos los requisitos, reglamentos operacionales específicos y políticas de implantación en los peligros identificados y en el análisis de los riesgos de seguridad operacional que se corren a consecuencia de los peligros?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se examinan periódicamente los requisitos, reglamentos específicos del funcionamiento y políticas de implantación para asegurar que siguen siendo pertinentes y apropiados para los proveedores de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existe un proceso estructurado dentro de [Estado] para evaluar cómo los proveedores de servicios gestionarán los riesgos de seguridad operacional relacionados con peligros identificados, expresados en términos de probabilidad y gravedad de ocurrencia?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existe una política de [Estado] que asegure la notificación efectiva de las deficiencias, peligros u ocurrencias de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Incluye la política de [Estado] sobre notificación de deficiencias, peligros u ocurrencias de seguridad operacional las condiciones en las cuales se aplica la protección con respecto a medidas disciplinarias o administrativas?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 2.2 — Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional</b>			
Capítulo 11	¿Ha acordado [Estado] con cada proveedor de servicios la eficacia de la seguridad operacional de sus SMS?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Es la eficacia de la seguridad operacional acordada proporcional a la complejidad del contexto operacional específico de cada proveedor de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Considera la eficacia de la seguridad operacional acordada los recursos de cada proveedor de servicios para tratar los riesgos de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se expresa la eficacia de la seguridad operacional acordada mediante múltiples indicadores de seguridad operacional y objetivos de seguridad operacional, en vez de uno solo, así como mediante planes de acción?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se examina periódicamente la eficacia de la seguridad operacional acordada para asegurar que siga siendo pertinente y apropiada para los proveedores de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

Referencia OACI (Doc 9859)	Aspecto para analizar o pregunta para contestar	Respuesta	Estado de implantación
<b>Componente 3 — GARANTÍA DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS</b>			
<b>Elemento 3.1 — Vigilancia de la seguridad operacional</b>			
Capítulo 11	¿Ha establecido [Estado] mecanismos para asegurar que la identificación de peligros y la gestión de riesgos de seguridad operacional por los proveedores de servicios se ajusten a los controles reguladores establecidos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Incluyen los mecanismos establecidos inspecciones, auditorías y encuestas para asegurar que los controles reguladores de los riesgos de seguridad operacional se integran apropiadamente en los SMS de los proveedores de servicios?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Aseguran los mecanismos establecidos que los controles regulares de los riesgos de seguridad operacional se llevan a la práctica conforme a su diseño?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Aseguran los mecanismos establecidos que los controles regulares de los riesgos de seguridad operacional tienen el efecto previsto en dichos riesgos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se realizan exámenes regulares y periódicos respecto del ALoS de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Consideran los exámenes cambios que puedan afectar al SSP de [Estado] y su ALoS, recomendaciones de mejoras y mejores prácticas compartidas en todo el Estado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se realizan exámenes regulares y periódicos para evaluar si el SSP de [Estado] y su ALoS siguen siendo apropiados al alcance y complejidad de las operaciones de aviación en el Estado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existe un proceso para evaluar la efectividad de los cambios relacionados con el SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 3.2 — Recopilación, análisis e intercambio de datos sobre seguridad operacional</b>			
Capítulo 11	¿Ha establecido [Estado] mecanismos para asegurar la captura y almacenamiento de datos sobre peligros y riesgos de seguridad operacional a nivel tanto individual como global en el Estado?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Ha establecido [Estado] mecanismos para preparar información a partir de los datos almacenados y promover el intercambio de información de seguridad operacional con los proveedores de servicios u otros Estados, según corresponda?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Ha establecido [Estado] un nivel aceptable de seguridad operacional (ALoS) relativo a su SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

Referencia OACI (Doc 9859)	Aspecto para analizar o pregunta para contestar	Respuesta	Estado de implantación
Capítulo 11	¿Combina el ALoS relativo al SSP de [Estado] elementos de medición de la seguridad operacional y medición de la eficacia de la seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Es el ALoS de [Estado] proporcional a la complejidad de las actividades de aviación dentro de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existe dentro de [Estado] un protocolo para elaborar y mantener un conjunto de parámetros para medir la implantación realista del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Elemento 3.3 — Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención</b>			
Capítulo 11	¿Ha elaborado [Estado] procedimientos para priorizar las inspecciones, auditorías y encuestas relacionadas con los elementos que plantean más preocupación o que requieren mayor atención en materia de seguridad operacional?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Es la priorización de inspecciones y auditorías resultado del análisis de datos sobre peligros, sus consecuencias en las operaciones y los riesgos de seguridad operacional evaluados?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
<b>Componente 4 — PROMOCIÓN DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS</b>			
<b>Elemento 4.1 — Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional</b>			
Capítulo 11	¿Proporciona [Estado] instrucción interna, conocimiento e intercambio de información relacionada con la seguridad operacional dentro de las organizaciones de aviación de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existen procesos de comunicación dentro de [Estado] para asegurar que la información sobre las funciones y productos del SSP se dan a conocer a las organizaciones de aviación de [Estado] en forma oportuna?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existe un proceso para la difusión de información de seguridad operacional en todas las organizaciones de aviación de [Estado] y un medio para supervisar la efectividad de este proceso?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Son los procesos de comunicación (escritos, reuniones, electrónicos, etc.) proporcionales al tamaño y alcance de las organizaciones de aviación de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se mantienen en un medio adecuado la información de seguridad y la información sobre funciones y productos del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

<i>Referencia OACI (Doc 9859)</i>	<i>Aspecto para analizar o pregunta para contestar</i>	<i>Respuesta</i>	<i>Estado de implantación</i>
<b>Elemento 4.2 — Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional</b>			
Capítulo 11	¿Proporciona [Estado] educación, conocimiento de los riesgos de seguridad operacional e intercambio de información relacionada con la seguridad operacional externos?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existen procesos de comunicación dentro de [Estado] que permitan promover el SSP tanto nacional como internacionalmente?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existe un protocolo para la divulgación externa de información de seguridad operacional a los proveedores de servicios de [Estado] y medios para supervisar la efectividad de dicho proceso?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existen en [Estado] procesos de comunicación para asegurar que la información sobre funciones y productos del SSP se ponen en conocimiento de los proveedores de servicios de [Estado] en forma oportuna?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Existen procesos de comunicación (escrita, reuniones, electrónico, etc.) proporcionales al tamaño y alcance de los proveedores de servicios de [Estado]?	<input type="checkbox"/> Sí <input type="checkbox"/> No	
Capítulo 11	¿Se establecen y mantienen en un medio adecuado la información de seguridad operacional y la información sobre funciones y productos del SSP?	<input type="checkbox"/> Sí <input type="checkbox"/> No	

-----

## Apéndice 4 del Capítulo 11

# ORIENTACIÓN PARA LA ELABORACIÓN DE UNA POLÍTICA DE CUMPLIMIENTO Y PROCEDIMIENTOS DE CUMPLIMIENTO DEL ESTADO EN UN ENTORNO SMS

## POLÍTICA DE CUMPLIMIENTO

### 1. INTRODUCCIÓN

La presente política de cumplimiento se promulga bajo responsabilidad legal en [reglamentos de aviación civil aplicables del Estado, órdenes de navegación aérea o normas regulatorias].

### 2. PRINCIPIOS

2.1 Esta política de cumplimiento es la culminación de un examen completo por [AAC del Estado] de su capacidad y reglamentos para evaluar las actividades de seguridad operacional de los proveedores de servicios.

2.2 La implantación de sistemas de gestión de la seguridad operacional (SMS) exige que [AAC del Estado] elabore un enfoque flexible del cumplimiento en este marco de seguridad operacional en evolución realizando, al mismo tiempo, funciones de cumplimiento en forma equitativa, práctica y coherente. Un enfoque flexible del cumplimiento en un entorno SMS debería basarse en dos principios generales.

2.3 El primer principio general es elaborar procedimientos de cumplimiento que permita a los proveedores de servicios encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional, y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios y a satisfacción de la autoridad competente. Las transgresiones intencionales de [Ley de aviación civil del Estado] y [Reglamentos de aviación civil del Estado] se investigarán y pueden ser objeto de medidas disciplinarias convencionales, si corresponde.

2.4 El segundo principio general es que ninguna información obtenida de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) establecidos en el marco del SMS se utilizará como base para la adopción de medidas disciplinarias.

### 3. ALCANCE

3.1 Los principios subyacentes de esta declaración de política de cumplimiento procedimientos de cumplimiento conexos se aplican a los proveedores de servicio que funcionan con arreglo a los siguientes documentos de la OACI: Anexo 1 — *Licencias al personal*; Anexo 6 — *Operación de aeronaves*, Parte I — *Transporte aéreo comercial internacional — Aviones*, y Parte III — *Operaciones internacionales — Helicópteros*; Anexo 8 — *Aeronavegabilidad*; Anexo 11 — *Servicios de tránsito aéreo*; y Anexo 14 — *Aeródromos*, Volumen I — *Diseño y operaciones de aeródromos*.

3.2 En el contexto de esta orientación, el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye además a las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados, según corresponda.

#### 4. GENERALIDADES

4.1 [Proveedor de servicios] establecerá, mantendrá y cumplirá un SMS proporcional al tamaño, carácter y complejidad de las operaciones cuya realización se autoriza en su certificado de operaciones y a los peligros y riesgo de seguridad operacional relacionados con esas operaciones.

4.2 Para elaborar una política de cumplimiento que apoye la implantación del SMS, inspectores de [AAC del Estado] mantendrán una comunicación abierta con los proveedores de servicios.

4.3 Cuando un proveedor de servicios que opera en el marco de un SMS transgrede involuntariamente [Ley de aviación civil o reglamentos de aviación civil], se aplicarán procedimientos de examen específicos. Estos procedimientos permitirán al inspector de [AAC del Estado] responsable de la vigilancia del proveedor de servicios la oportunidad de entablar un diálogo con la organización regida por el SMS. El objetivo de este diálogo es convenir medidas correctivas propuestas y un plan de acción que trate adecuadamente las deficiencias que llevaron a la transgresión y brindar al proveedor de servicios tiempo razonable para implantarlas. Este enfoque se dirige a nutrir y mantener una efectiva notificación de seguridad operacional, por la cual los empleados del proveedor de servicios pueden notificar deficiencias y peligros de seguridad operacional sin temor a medidas punitivas. Por consiguiente, el proveedor de servicios puede, sin asignar culpas y sin temor de medidas disciplinarias, analizar el suceso y los factores de la organización o individuales que puedan haber conducido al mismo, a efectos de incorporar medidas correctivas que mejor contribuyan a prevenir repeticiones.

#### 5. MEDIDAS CORRECTIVAS

[AAC del Estado], mediante el inspector responsable de la vigilancia del proveedor de servicios, evaluará las medidas correctivas propuestas por el proveedor de servicios o los sistemas actualmente implantados para tratar el suceso que llevó a la transgresión. Si las medidas correctivas se consideran apropiadas y que podrían prevenir repeticiones y fomentar el futuro cumplimiento, el examen de la violación se dará por concluido sin medidas disciplinarias. En los casos en que las medidas correctivas o los sistemas implantados se consideren inapropiados, [AAC del Estado] continuará interactuando con el proveedor de servicios para encontrar una solución satisfactoria a efectos de prevenir la adopción de medidas disciplinarias. No obstante, en casos en que el proveedor de servicios se niegue a tratar el suceso y proporcionar medidas correctivas efectivas, [AAC del Estado] considerará la adopción de medidas disciplinarias u otras medidas administrativas con respecto al certificado.

#### 6. PROCEDIMIENTOS DE CUMPLIMIENTO

Las transgresiones de los reglamentos de aviación pueden ocurrir por muchas razones diferentes, desde una genuina mala interpretación de los reglamentos a la desconsideración total por la seguridad operacional. [AAC del Estado] cuenta con una gama de procedimientos de cumplimiento para tratar efectivamente las obligaciones de seguridad operacional en el marco de [Ley estatal aplicable] a la luz de circunstancias diferentes. Estos procedimientos pueden resultar en una variedad de medidas, a saber:

- a) asesoramiento profesional;

- b) instrucción correctiva; o
- c) variación, suspensión y cancelación de autorizaciones.

## **7. IMPARCIALIDAD DE LAS MEDIDAS DE CUMPLIMIENTO**

Las decisiones en materia de cumplimiento no deben estar influidas por:

- a) conflictos personales;
- b) consideraciones de género, raza, religión, opiniones o afiliación política; o
- c) el poder personal, político o financiero de los involucrados.

## **8. PROPORCIONALIDAD DE LAS RESPUESTAS**

Las decisiones de cumplimiento deben ser proporcionales a las transgresiones identificadas y a los riesgos de seguridad operacional que ellas provocarían, sobre la base de dos principios:

- a) [AAC del Estado] adoptará medidas contra aquellos que en forma continua y deliberada operan sin respetar los reglamentos de aviación civil; y
- b) [AAC del Estado] procurará educar y promover la instrucción o supervisión de aquellos que demuestren compromiso a resolver deficiencias de seguridad operacional.

## **9. JUSTICIA NATURAL Y RENDICIÓN DE CUENTAS**

Las decisiones de cumplimiento deben:

- a) ser justas y ajustarse al debido proceso;
- b) ser transparentes para todos los involucrados;
- c) tener en cuenta las circunstancias del caso y la actitud/acciones del proveedor de servicios cuando se considere la aplicación de medidas;
- d) ser medidas o decisiones coherentes con circunstancias iguales o similares; y
- e) estar sujetas a exámenes internos y externos apropiados.

## **10. EXCEPCIONES**

10.1 Esta política no se aplica si hay pruebas de intentos deliberados de ocultar el incumplimiento.

10.2 Esta política no se aplica si el proveedor de servicios no está en condiciones de proporcionar confianza en sus medios de identificación de peligros y de gestión de riesgo de seguridad operacional.

10.3 Esta política no se aplica si el proveedor de servicios es un violador reiterado. Un violador reiterado es un violador que, en el [período], pasado, ha ejecutado las mismas violaciones o violaciones muy similares.

10.4 En tales circunstancias, se aplicará la matriz de sanciones (o medición aplicable) de los procedimientos de cumplimiento establecidos.

(Firma) \_\_\_\_\_  
Ejecutivo responsable del Estado

-----



## Procedimientos de cumplimiento en un entorno SMS

### 1. GENERALIDADES

En el marco del programa estatal de seguridad operacional (SSP) de [Estado], [AAC del Estado] es responsable de la vigilancia de los titulares de certificados que operan en un entorno SMS. Los procedimientos de cumplimiento proporcionan orientación para los responsables de la vigilancia de los proveedores de servicios que operan en un entorno SMS asesorándoles sobre la repuesta apropiada a acciones u omisiones para garantizar que si se adoptan medidas de cumplimiento éstas tendrán éxito. Los procedimientos de cumplimiento desempeñan una función de apoyo en el proceso, y la decisión final sobre cualquier aspecto de cumplimiento es responsabilidad del Ejecutivo responsable.

### 2. APLICACIÓN

2.1 Estos procedimientos se aplican a transgresiones que pueden haber sido cometidas por personas o proveedores de servicios que realizan actividades en el marco de un SMS.

2.2 Estos procedimientos entran en vigor el [fecha]. Reemplazan y sustituyen procedimientos anteriores indicados en [Reglamentos de aviación civil del Estado].

2.3 Cuando los proveedores de servicios han demostrado su disposición a realizar sus operaciones en el marco de un SMS, pueden aplicarse procedimientos de cumplimiento de SMS con respecto a aquellos proveedores de servicios que, aunque no cuentan con un SMS aceptado, han implantado algunos componentes básicos esenciales de un SMS y están tramitando la plena implantación.

2.4 [AAC del Estado] no aplicará procedimientos de cumplimiento SMS a los proveedores de servicios que, después de iniciarse una investigación de una transgresión, aducen arbitrariamente que están elaborando un SMS. Estos procedimientos se aplicarán a los proveedores de servicios que han participado diligentemente en el desarrollo de un SMS que en última instancia satisfaría los requisitos de los reglamentos SMS pertinentes, y están aplicando un “enfoque en fases” similar al indicado en los textos de asesoramiento publicados [AM-xxx] de [AAC del Estado] — Guía de procedimientos de implantación para SMS.

2.5 Cuando los proveedores de servicios no han demostrado estar funcionando en un entorno SMS, las medidas de cumplimiento pueden aplicarse sin las ventajas de los procedimientos que se explican en el párrafo 3.

### 3. PROCEDIMIENTOS

3.1 Para fines de determinar si debe realizarse una investigación aplicando procedimientos de cumplimiento SMS, será necesario que los investigadores disciplinarios de la aviación determinen la condición de implantación del SMS del proveedor de servicios específico. Esta determinación podría efectuarse inicialmente mediante comunicación entre los investigadores y el inspector principal responsable de la vigilancia y certificación del proveedor de servicios que se está investigando.

3.2 El inspector principal determinará si el proveedor de servicios satisface los criterios mencionados anteriormente para los procedimientos de cumplimiento SMS. Para facilitar la evaluación inicial, [AAC del Estado] puede preparar una lista de proveedores de servicios que han iniciado el proceso de elaboración e implantación de un SMS. Si esta lista se pone en conocimiento de los encargados del cumplimiento, ello ayudará a los investigadores en la adopción de decisiones respecto de la aplicación de procedimientos de cumplimiento SMS.

3.3 Durante el “enfoque en fases” del SMS del proveedor de servicios, [AAC del Estado] aplicará los procedimientos de cumplimiento del SMS a los proveedores de servicios que no han implantado plenamente el SMS, siempre que se satisfagan ciertas condiciones.

3.4 [AAC del Estado] exigirá, como mínimo, que se satisfagan las tres condiciones siguientes antes de poder aplicar los procedimientos de cumplimiento SMS:

- a) el proveedor de servicios cuenta con un programa efectivo de notificación interna de peligros apoyado por la administración superior;
- b) el proveedor de servicios cuenta con un proceso proactivo de análisis de sucesos proporcional al tamaño y complejidad de sus operaciones y adecuado para determinar factores causales y elaborar medidas correctivas;
- c) la información obtenida del proceso a que se hace referencia en el párrafo 3, adecuadamente protegida para no poner en peligro el SDCPS, se comunica, a petición, al inspector principal asignado al proveedor de servicios específicos.

#### **Informe inicial de violación**

3.5 Los inspectores de cumplimiento de la aviación deben realizar un análisis preliminar en todos los casos en que se detecte una transgresión o cuando se recibe información sobre una posible transgresión.

#### **Análisis preliminar**

3.6 Las preguntas siguientes deberían considerarse sobre la base de la información recibida:

- a) ¿Hay motivo razonable para creer que una persona u organización que realiza actividades en el marco de un SMS puede haber cometido una transgresión?
- b) ¿Es el carácter del suceso tan grave que sería necesario considerar medidas disciplinarias?
- c) ¿Existen pruebas percederas que deberían protegerse para las acciones disciplinarias?

#### **Provisión de apoyo efectivo**

3.7 Cuando las tres preguntas tienen respuesta afirmativa, deberá notificarse al inspector principal identificando el suceso y la transgresión.

3.8 Cuando se solicite, los investigadores de cumplimiento en aviación proporcionarán apoyo efectivo al Ejecutivo responsable brindando asesoramiento sobre la respuesta apropiada a la transgresión, para asegurar que si se adoptan medidas disciplinarias, éstas tendrán éxito. El apoyo al Ejecutivo responsable comprende recoger y asegurar pruebas percederas.

#### **Iniciación de una investigación de cumplimiento**

3.9 Una investigación de cumplimiento se iniciará solamente a petición del inspector principal, no de los investigadores de cumplimiento.

### Inmunidad

3.10 Ninguna información obtenida de un SDCPS establecido en el marco de un SMS se utilizará como base para la adopción de medidas disciplinarias.

*Nota.— La política de cumplimiento de SMS y procedimientos conexos también pueden aplicarse a explotadores extranjeros de servicios aéreos que funcionan en el marco de los reglamentos SMS, se ajustan a los requisitos y orientación establecidos por la Organización de Aviación Civil Internacional (OACI) y satisfacen las condiciones del párrafo 3.*

-----



## Apéndice 5 del Capítulo 11

# ORIENTACIÓN SOBRE LA ELABORACIÓN DE UN PLAN DE IMPLANTACIÓN DEL SSP

### 1. ANTECEDENTES

1.1 En el presente apéndice se proporciona orientación para ayudar a los Estados a elaborar un plan de implantación del SSP. El plan de implantación del SSP describe la forma en que el Estado pondrá en práctica, en forma secuencial y basada en principios, los procesos, procedimientos y medios que le permitirán cumplir sus responsabilidades relacionadas con la gestión de la seguridad operacional en la aviación civil.

1.2 La implantación de un SSP debe ser proporcional al tamaño y complejidad del sistema de aviación del Estado, y puede requerir la coordinación entre las múltiples autoridades responsables de cada elemento de las funciones de aviación civil en el Estado. Esta orientación está concebida como referencia y puede tener que adaptarse para satisfacer las necesidades particulares de los Estados.

1.3 La elaboración de un plan implantación del SSP permitirá a los Estados:

- a) formular una estrategia general para la gestión de la seguridad operacional en el Estado;
- b) coordinar los procesos ejecutados por las diferentes organizaciones de aviación del Estado en el marco del SSP;
- c) establecer los controles que gobiernan la forma en que funcionará el sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios;
- d) asegurar que el funcionamiento del SMS del proveedor de servicios se ajusta a los controles establecidos; y
- e) apoyar la interacción entre el SSP y el funcionamiento del SMS del proveedor de servicios.

1.4 Cuando el Estado es responsable de la provisión de servicios específicos (p. ej., servicios de aeródromo, servicios de navegación aérea) la organización que proporciona estos servicios debería elaborar e implantar un SMS (véase el plan de implantación del SMS en el Apéndice 2 del Capítulo 10).

*Nota.— En el contexto de este apéndice, el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye a las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados, según corresponda.*

### 2. ANÁLISIS DE LAS CARENCIAS DEL SSP

2.1 Para elaborar un plan de implantación del SSP, debería realizarse un análisis de las carencias, de las estructuras y procesos que existen en el Estado con respecto al marco para SSP de la OACI. Esto permitirá al Estado evaluar la existencia y grado de maduración de los elementos del SSP dentro del propio Estado. Una vez completado y

documentado el análisis de las carencias, los componentes/elementos identificados como faltantes o deficientes formarán junto con los que ya existen o son eficaces, la base para el plan de implantación del SSP.

2.2 Cada componente/elemento debería evaluarse para determinar si el Estado debe crear o modificar reglamentos, políticas o procedimientos para desarrollar los componentes/elementos requeridos del SSP. El marco para SSP de la OACI que constituye la base para la elaboración del plan de implantación del SSP comprende cuatro componentes y once elementos, como sigue:

1. Política y objetivos de seguridad operacional de los Estados
  - 1.1 Marco legislativo estatal de la seguridad operacional
  - 1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
  - 1.3 Investigación de accidentes e incidentes
  - 1.4 Política de cumplimiento
2. Gestión de riesgos de seguridad operacional por los Estados
  - 2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
  - 2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional
3. Garantía de la seguridad operacional por los Estados
  - 3.1 Vigilancia de la seguridad operacional
  - 3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
  - 3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención
4. Promoción de la seguridad operacional por los Estados
  - 4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
  - 4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

### 3. PLAN DE IMPLANTACIÓN DEL SSP

3.1 El plan de implantación del SSP es un plan de trabajo sobre cómo se elaborará e integrará el SSP en las actividades de gestión de la seguridad operacional del Estado. Dada la potencial magnitud de la empresa, es importante gestionar adecuadamente la carga de trabajo relacionada con las actividades en que se basan la elaboración e implantación del SSP. Se propone que los cuatro componentes y once elementos del marco para SSP de la OACI se implanten en forma secuencial que permita lograr los resultados específicos. El orden de esta secuencia dependerá del resultado del análisis de las carencias y de la complejidad y alcance del sistema de aviación dentro de cada Estado.

3.2 Uno de los objetivos específicos de un SSP es generar un contexto que apoye la implantación del SMS por los proveedores de servicios. Por consiguiente, dentro del alcance de las actividades del SSP, cuatro pasos específicos apoyan la implantación del SMS por los proveedores de servicios. Estos cuatro pasos se analizan en el Capítulo 11.

## **1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL DE LOS ESTADOS**

### **1.1 Marco legislativo estatal de la seguridad operacional**

- a) Examinar, elaborar y promulgar, según sea necesario, un marco legislativo nacional de la seguridad operacional y reglamentos específicos, en cumplimiento de las normas internacionales y nacionales que definen la forma en que el Estado supervisará la gestión de la seguridad operacional dentro de su jurisdicción.
- b) Establecer un grupo a nivel nacional dentro del Estado en forma de junta, comité, etc., para asegurar la participación coordinada de las organizaciones aeronáuticas del Estado en actividades específicas relativas a la gestión de la seguridad operacional en el Estado, y el establecimiento de funciones, responsabilidades y relaciones de tales organizaciones.
- c) Establecer un cronograma para examinar periódicamente la legislación de seguridad operacional y los reglamentos de funcionamiento específicos para asegurar que siguen siendo pertinentes y apropiados para el Estado.

### **1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional**

- a) Identificar, definir y documentar los requisitos, las responsabilidades y la rendición de cuentas relativas a la creación y el mantenimiento del SSP. Esto incluye las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional del Estado. Incluir, además, una declaración clara sobre la provisión de los recursos necesarios para la implantación del SSP.
- b) Identificar y designar al Ejecutivo responsable del SSP del Estado quien tendrá, entre otras cosas:
  - 1) la responsabilidad final y la obligación administrativa de rendir cuentas en nombre del Estado para la implantación y mantenimiento del SSP;
  - 2) plena autoridad sobre asuntos de recursos humanos relativos a la organización de aviación del Estado que ha sido designada como depositaria del SSP;
  - 3) plena autoridad sobre los aspectos financieros de la organización de aviación del Estado que ha sido designada como depositaria del SSP;
  - 4) autoridad final sobre los aspectos de gestión de los certificados del proveedor de servicios; y
  - 5) responsabilidad final en la resolución de todos los asuntos de seguridad operacional de la aviación en el Estado.
- c) Establecer el equipo de implantación del SSP.
- d) Asignar el tiempo necesario para cada tarea relacionada con la implantación del SSP entre los diferentes niveles de gestión de las organizaciones de aviación del Estado.
- e) Presentar a todo el personal los conceptos del SSP a un nivel de acuerdo con su participación individual en el SSP.

- f) Elaborar e implantar una política de seguridad operacional del Estado que incluya, pero sin limitarse necesariamente a ellos, los puntos siguientes:
  - 1) el compromiso de elaborar e implantar estrategias y procesos para asegurar que todas las actividades de aviación bajo vigilancia alcanzarán el nivel más elevado de eficacia de la seguridad operacional;
  - 2) la elaboración y promulgación de un marco legislativo nacional de seguridad operacional y reglamentos de funcionamiento aplicables para la gestión de la seguridad operacional en el Estado;
  - 3) el compromiso de asignar los recursos necesarios a las organizaciones de aviación del Estado para permitir que su personal cumpla sus responsabilidades, tanto relacionadas con la seguridad operacional como de otro tipo;
  - 4) el apoyo a la gestión de la seguridad operacional en el Estado mediante un sistema efectivo de notificación y comunicación de peligros;
  - 5) el establecimiento de disposiciones para la protección de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS);
  - 6) el compromiso de una interacción efectiva con los proveedores de servicios en la resolución de los problemas de seguridad operacional;
  - 7) el compromiso de comunicar, con visible endoso, la política de seguridad operacional del Estado a todo el personal; y
  - 8) una política de cumplimiento adecuada a las operaciones del proveedor de servicios en un entorno SMS.
- g) Establecer los medios necesarios para asegurar que la política de seguridad operacional del Estado es comprendida, implantada y observada en todos los niveles dentro de las organizaciones de aviación del Estado.

### **1.3 Investigación de accidentes e incidentes**

- a) Elaborar y establecer los mecanismos para asegurar un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes, en apoyo de la gestión de la seguridad operacional en el Estado, y no la asignación de culpa o responsabilidad.
- b) Elaborar y establecer los arreglos necesarios para asegurar la independencia de la organización de investigación de accidentes e incidentes respecto de otras organizaciones estatales de aviación.

### **1.4 Política de cumplimiento**

- a) Elaborar y promulgar una política de cumplimiento que establezca las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional y resolverlos, internamente, en el contexto del



sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, y a satisfacción de la autoridad estatal competente. La política de cumplimiento establece también las condiciones y circunstancias en las cuales las desviaciones respecto de la seguridad operacional deben abordarse mediante procedimientos establecidos en cuanto a cumplimiento.

- b) La política también debería asegurar que ninguna información obtenida de un sistema de notificación interna de peligros o un sistema de vigilancia de datos de vuelo establecidos en el marco del SMS se utilizará para la aplicación de medidas disciplinarias.

### 1.5 Documentación del SSP

- a) Elaborar y establecer una biblioteca de seguridad operacional del Estado que documente los requisitos, responsabilidades y líneas de rendición de cuentas relativas al establecimiento y mantenimiento del SSP. Esta biblioteca de seguridad operacional mantendrá y actualizará, según sea necesario, la documentación del SSP relativa al marco legislativo nacional de seguridad operacional, las políticas y objetivos de seguridad operacional del Estado, los requisitos del SSP, los procedimientos y procesos del SSP, las líneas de rendición de cuentas, responsabilidades y facultades para procesos y procedimientos, y el nivel aceptable de seguridad operacional (ALoS) del Estado relacionados con el SSP.

#### Resultados

1. Marco legislativo estatal de seguridad operacional promulgado.
2. Responsabilidades y rendición de cuentas establecidas, documentadas y publicadas del Estado respecto de la seguridad operacional.
3. Políticas de seguridad operacional y de cumplimiento del Estado firmadas por el Ejecutivo responsable.
4. Políticas de seguridad operacional y de cumplimiento del Estado distribuidas dentro de las organizaciones de aviación del Estado y entre los proveedores de servicio bajo vigilancia.
5. Procesos independientes de investigación de accidentes e incidentes establecidos.
6. Estructura de organización del SSP implantada.

#### Hitos

1. Ejecutivo responsable identificado.
2. Propuesta de política de seguridad operacional redactada.
3. Líneas de responsabilidad y rendición de cuentas respecto a la seguridad operacional establecidas.
4. Propuesta de estructura de organización del SSP aprobada.
5. Presupuesto para procesos del SSP aprobado.

*Nota.— Los resultados e hitos propuestos en este apéndice son solamente un ejemplo y no deberían limitarse a otros resultados que podrían preverse de la implantación de los componentes del marco para SSP en Estados con distinto alcance y complejidad en sus actividades aeronáuticas.*

## 2. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL POR LOS ESTADOS

### 2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios

- a) Establecer los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para el SMS del proveedor de servicios (marco normativo para SMS, circular de asesoramiento, etc.) como controles que rigen la forma en que los proveedores de servicios identificarán los peligros y gestionarán y controlarán los riesgos de seguridad operacional.
- b) Establecer un cronograma para consulta con los proveedores de servicios sobre estos requisitos.
- c) Establecer un cronograma para examinar periódicamente los requisitos y reglamentos específicos de funcionamiento a efectos de asegurar que siguen siendo pertinentes y apropiados para los proveedores de servicios.

### 2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

- a) Elaborar y establecer un procedimiento para acordar con cada proveedor de servicios la eficacia de la seguridad operacional de sus SMS sobre la base de:
  - 1) valores de indicador de la eficacia de la seguridad operacional;
  - 2) valores de objetivo de la eficacia de la seguridad operacional; y
  - 3) planes de acción.
- b) Incluir en el procedimiento acordado que la eficacia de la seguridad operacional del proveedor de servicios debería ser proporcional a:
  - 1) la complejidad de los contextos operacionales y específicos de cada proveedor de servicios; y
  - 2) la disponibilidad de recursos en cada proveedor de servicios para enfrentar los riesgos de seguridad operacional.
- c) Medir la eficacia de la seguridad operacional del SMS del proveedor de servicios mediante exámenes periódicos de la eficacia de seguridad del SMS acordada para asegurar que los indicadores de eficacia de la seguridad y objetivos de eficacia de la seguridad siguen siendo pertinentes y apropiados para los proveedores de servicios.
- d) Elaborar un medio para evaluar resultados de bajo nivel y procesos más frecuentes entre diferentes proveedores de servicios.
- e) Determinar resultados de eficacia medibles dentro de los diferentes SMS.

#### **Resultados**

- 1. Reglamentos sobre SMS promulgados.
- 2. Textos de orientación sobre implantación del SMS distribuidos a los proveedores de servicios.

3. Primer examen anual de la eficacia de la seguridad operacional de los proveedores de servicios acordada completado.

### **Hitos**

1. Proyecto de propuesta de reglamentos sobre SMS distribuidos a los proveedores de servicios para su examen.
2. Proyecto de propuesta de textos de orientación sobre SMS distribuido a los proveedores de servicios para su examen.
3. Instrucción de personal técnico del Estado en identificación de peligros y gestión de riesgos de seguridad operacional completada.
4. Procedimiento para acuerdo sobre la eficacia de seguridad operacional de los proveedores de servicios completados.

## **3. GARANTÍA DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS**

### **3.1 Vigilancia de la seguridad operacional**

- a) Establecer mecanismos que garanticen que la identificación de peligros y la gestión de riesgos de seguridad operacional por los proveedores de servicios se ajustan a controles reglamentarios establecidos.
- b) Establecer mecanismos que garanticen que los controles de riesgo de seguridad operacional se integran en el SMS del proveedor de servicios.
- c) Desarrollar una auditoría interna del SSP.

### **3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional**

- a) Elaborar y establecer un medio para recopilar, analizar y almacenar datos sobre peligros y riesgos de seguridad operacional a nivel del Estado:
  - 1) establecer un sistema de notificación obligatoria de peligros;
  - 2) establecer un sistema de notificación confidencial de peligros;
  - 3) elaborar una base de datos estatal sobre peligros;
  - 4) establecer un mecanismo para elaborar información a partir de los datos almacenados;
  - 5) establecer un medio para recopilar datos sobre peligros a nivel global del Estado y a nivel de cada proveedor de servicios; y
  - 6) establecer un medio para implantar planes de medidas correctivas.

- b) Asegurar que los procesos de identificación de peligros y de gestión de riesgos de seguridad operacional del proveedor de servicios se ajustan a los requisitos normativos establecidos y que los controles de riesgos de seguridad operacional están adecuadamente integrados en el SMS del proveedor de servicios, incluyendo, entre otros:
  - 1) inspecciones;
  - 2) auditorías; y
  - 3) encuestas.
- c) Observar la secuencia siguiente para la implantación:
  - 1) controles normativos de riesgos de seguridad operacional integrados en el SMS del proveedor de servicios;
  - 2) actividades de vigilancia para asegurar que los procesos de identificación de peligros y gestión de riesgos de seguridad operacional del proveedor de servicios se ajustan a los requisitos normativos establecidos; y
  - 3) actividades de vigilancia para verificar que los proveedores de servicios aplican los controles de riesgos de seguridad operacional.
- d) Establecer el nivel aceptable de seguridad (ALoS) relativo al SSP, comprendiendo una combinación de medición de la seguridad operacional y medición de la eficacia de la seguridad operacional:
  - 1) La medición de la seguridad operacional comprende la cuantificación de los resultados de sucesos de alto nivel, consecuencias graves o funciones estatales de alto nivel, tales como proporciones de accidentes, proporciones de incidentes graves y cumplimiento de los reglamentos.
  - 2) La medición de la eficacia de la seguridad operacional comprende la cuantificación de los resultados de procesos de bajo nivel y consecuencias leves que proporciona una medida de la implantación realista de cada SSP más allá de las proporciones de accidentes o cumplimiento de los reglamentos.

### **3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención**

- a) Establecer procedimientos para priorizar las inspecciones, auditorías y encuestas, basadas en análisis de peligros y riesgos de seguridad operacional.

#### **Resultados**

1. Sistemas estatales de notificación obligatoria y confidencial de peligros implantados.
2. Primer examen anual de la política y objetivos de seguridad operacional realizado.
3. Primer examen anual de la política de cumplimiento realizado.
4. ALoS establecido.

**Hitos**

1. Almacenamiento y procesamiento de datos de peligros y riesgos de seguridad operacional a nivel del Estado.
2. Información sobre peligros y riesgos de seguridad operacional a nivel global del Estado y a nivel de cada proveedor de servicios recopilados.

**4. PROMOCION DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS**

**4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional**

- a) Identificar requisitos de instrucción internos.
- b) Elaborar y proporcionar instrucción genérica en seguridad operacional a todo el personal.
- c) Elaborar un programa de instrucción sobre componentes clave del SSP y el SMS para el personal que incluya:
  - 1) adoctrinamiento/instrucción inicial en seguridad operacional;
  - 2) instrucción en seguridad operacional en el puesto de trabajo (OJT);
  - 3) instrucción periódica en seguridad operacional.
- d) Establecer un medio para medir la efectividad de la instrucción.
- e) Elaborar un medio para comunicar internamente cuestiones relacionadas con la seguridad operacional, incluyendo:
  - 1) políticas y procedimientos de seguridad operacional;
  - 2) boletines de noticias;
  - 3) avisos; y
  - 4) un sitio web.

**4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional**

- a) Establecer los medios para proporcionar intercambio de información relacionada con la seguridad operacional para apoyar la implantación del SMS entre proveedores de servicios, incluyendo los operadores menores.
- b) Elaborar instrucción y textos de orientación sobre implantación del SMS para proveedores de servicios.

- c) Establecer los medios para comunicar externamente asuntos relacionados con la seguridad operacional incluyendo:
  - 1) políticas y procedimientos de la seguridad operacional;
  - 2) boletines de noticias;
  - 3) avisos; y
  - 4) un sitio web.

**Resultados**

- 1. Primer ciclo de instrucción genérica en seguridad operacional para el personal completado.
- 2. Programa de instrucción sobre componentes clave de un SSP y SMS para personal técnico y de apoyo completado.
- 3. Texto de orientación sobre SMS distribuido a los proveedores de servicios, incluyendo los explotadores menores.
- 4. Primer ciclo de instrucción para proveedores de servicios sobre implantación de SMS completado.
- 5. Medios para comunicar interna y externamente la información relacionada con la seguridad operacional establecidos.

**Hitos**

- 1. Requisitos mínimos de conocimientos y experiencia para personal técnico que realiza funciones de vigilancia de la seguridad operacional establecidos.
  - 2. Texto de orientación sobre SMS elaborado y publicado.
  - 3. Programas de instrucción sobre SMS para organizaciones de aviación del Estado y proveedores de servicios elaborados.
  - 4. Boletín de noticias y avisos del Estado elaborados.
-

# Adjunto A

## SISTEMA DE NOTIFICACIÓN DE DATOS SOBRE ACCIDENTES/INCIDENTES (ADREP) DE LA OACI

De conformidad con el Anexo 13, *Investigación de accidentes e incidentes de aviación*, los Estados notifican a la OACI la información sobre todos los accidentes de aviación cuando se trata de una aeronave con una masa máxima certificada de despegue de más de 2 250 kg. La OACI también recoge información sobre incidentes de aviación de aeronaves de más de 5 700 kg. Este sistema de notificación se conoce como ADREP. Los Estados notifican a la OACI datos específicos en un formato predeterminado (y codificado). Cuando se reciben de los Estados informes ADREP, la información se verifica y se almacena electrónicamente, constituyéndose así un banco de datos sobre sucesos de todo el mundo.

### LISTA DE EJEMPLOS DE INCIDENTES GRAVES

La expresión “incidente grave” se define en el Anexo 13, Capítulo 1, como sigue:

**Incidente grave.** Incidente en el que intervienen circunstancias que indican que casi ocurrió un accidente.

Los incidentes que se enumeran a continuación constituyen ejemplos característicos de incidentes que podrían ser graves. La lista no es exhaustiva y sólo se proporciona como orientación respecto a la definición de incidente grave.

- Cuasicolisiones que requieren una maniobra evasiva para evitar la colisión o una situación de peligro para la seguridad, o cuando habría correspondido realizar una acción evasiva.
- Impacto contra el suelo sin pérdida de control sólo marginalmente evitado.
- Despegues interrumpidos en una pista cerrada o comprometida, desde una calle de rodaje<sup>1</sup> o una pista no asignada
- Despegues efectuados desde una pista cerrada o comprometida, desde una calle de rodaje<sup>1</sup> o una pista no asignada.
- Aterrizajes o intentos de aterrizaje en una pista cerrada o comprometida, en una calle de rodaje<sup>1</sup> o una pista no asignada.
- Incapacidad grave de lograr la performance prevista durante el recorrido de despegue o el ascenso inicial.

---

1. Excluyendo operaciones autorizadas de helicópteros.

- Incendio o humo producido en la cabina de pasajeros, en los compartimientos de carga o en los motores, aun cuando tales incendios se hayan apagado mediante agentes extintores.
  - Sucesos que obliguen a la tripulación de vuelo a utilizar el oxígeno de emergencia.
  - Fallas estructurales de la aeronave o desintegraciones de motores que no se clasifiquen como accidente.
  - Mal funcionamiento de uno o más sistemas de la aeronave que afecten gravemente el funcionamiento de ésta.
  - Incapacitación de la tripulación de vuelo durante el mismo.
  - Cantidad de combustible que obligue al piloto a declarar una situación de emergencia.
  - Incursiones en las pistas clasificadas como de gravedad A. En el *Manual sobre prevención de las incursiones en la pista* (Doc 9870) figura información sobre las clasificaciones de gravedad.
  - Incidentes ocurridos en el despegue o aterrizaje. Se trata de incidentes como los aterrizajes demasiado cortos o demasiado largos o salidas de la pista por el costado.
  - Fallas de los sistemas, fenómenos meteorológicos, operaciones efectuadas fuera de la envolvente de vuelo aprobada, u otros acontecimientos que hubieran podido ocasionar dificultades para controlar la aeronave.
  - Fallas de más de un sistema, cuando se trata de un sistema redundante de carácter obligatorio para la guía de vuelo y la navegación.
-



## Adjunto B

# PLAN DE RESPUESTA ANTE EMERGENCIAS

### 1. INTRODUCCIÓN

1.1 Quizás porque los accidentes de aviación son sucesos raros, pocas organizaciones están preparadas cuando uno de estos accidentes ocurre. Muchas organizaciones no tienen planes eficaces para manejar la situación durante o después de una emergencia o de una crisis. Como se desempeña una organización como resultado de un accidente u otra emergencia puede depender de cuan bien manejó las primeras horas de un suceso importante desde el punto de vista de la seguridad operacional y los días siguientes. Un plan de respuesta ante emergencias describe por escrito lo que debe hacerse después de un accidente y quién es el responsable de cada acción. En las operaciones de aeródromos, esta planificación de emergencia se conoce como plan de emergencia de aeropuerto (AEP). En este manual se emplea la expresión genérica plan de respuesta ante emergencias (ERP).

1.2 Si bien es normal pensar en la planificación de la respuesta ante emergencias con respecto a operaciones de aeronaves o de aeródromo, normalmente como resultado de un accidente de aviación, el concepto puede aplicarse igualmente a otros proveedores de servicios. En el caso de los proveedores ATS esto puede incluir un gran corte de energía, o pérdida de servicio radar, de comunicaciones o de otras instalaciones importantes. Para una organización de mantenimiento puede involucrar un incendio en un hangar o un gran derramamiento de combustible. En este contexto, se considera que una emergencia es un suceso que podría causar un perjuicio o un trastorno importante a una organización.

1.3 A primera vista, la planificación de emergencia puede parecer que tiene poco que ver con la gestión de la seguridad operacional. No obstante, una efectiva respuesta ante emergencias proporciona una oportunidad para aprender, y también para aplicar, lecciones de seguridad dirigidas a minimizar los daños o las lesiones.

1.4 La exitosa respuesta ante una emergencia comienza con una efectiva planificación. El plan de respuesta ante emergencias (ERP) proporciona la base para un enfoque sistemático de la gestión de los asuntos de la organización después de un suceso importante no previsto — en el peor de los casos, un gran accidente.

1.5 La finalidad de un plan de respuesta ante emergencias es asegurar los siguientes aspectos:

- a) transición ordenada y eficiente de las operaciones normales a las operaciones de emergencia;
- b) delegación de poderes de emergencia;
- c) asignación de responsabilidades de emergencia;
- d) autorización del personal clave para las medidas que contiene el plan;
- e) coordinación de esfuerzos para hacer frente a la emergencia; y
- f) continuación segura de las operaciones o retorno a las operaciones normales tan pronto como sea posible.

## 2. REQUISITOS DE LA OACI

2.1 Toda organización que realiza operaciones de vuelo o presta servicios de apoyo a dichas operaciones debería tener un plan de respuesta ante emergencias. Por ejemplo:

- a) En el Anexo 14 — *Aeródromos* se dispone que, en un aeródromo deberá establecerse un plan de emergencia de aeródromo que guarde relación con las operaciones de las aeronaves y demás actividades que se realicen en un aeropuerto. El plan deberá prever la coordinación de las medidas que deben tomarse en una emergencia que ocurra en un aeródromo o en sus inmediaciones.
- b) En *Preparación de un manual de operaciones* (Doc 9376) se señala que el manual de operaciones de una empresa debería contener instrucciones y orientación sobre las funciones y obligaciones del personal después de un accidente. Dicho manual debería incluir orientación sobre establecimiento y funcionamiento de un centro de respuesta para accidentes y emergencias – el centro de coordinación para la gestión de crisis. Además de orientación sobre accidentes de aeronaves de la empresa, debería contener también orientación sobre accidentes de aeronaves de las cuales la empresa es el agente de despacho (por ejemplo, por medio de acuerdos de código compartido o servicios contratados). Las grandes empresas pueden optar por compilar toda esta información sobre planificación para caso de emergencia en un volumen separado de su manual de operaciones.
- c) En el *Manual de servicios de aeropuerto* (Doc 9137), Parte 7 — *Planificación de emergencia en los aeropuertos* se presenta orientación para las autoridades aeroportuarias y explotadores de aeronave sobre la planificación previa para emergencias, así como sobre la coordinación entre las diferentes entidades del aeropuerto incluyendo el explotador.

2.2 Para ser eficaz, un ERP debería:

- a) ser pertinente y útil para la gente que probablemente esté en servicio en el momento del accidente;
- b) incluir listas de verificación y referencias para contactar con rapidez al personal pertinente;
- c) ser objeto de ensayos periódicos por medio de ejercicios; y
- d) ser actualizado cuando cambian los detalles.

## 3. CONTENIDO DEL ERP

Un plan de respuesta ante emergencias (ERP) debería documentarse normalmente en forma de manual. Dicho plan debería establecer las responsabilidades y las funciones y actividades que corresponden a los diversos organismos y al personal que debe actuar para ser frente a las emergencias. El ERP debería tener en cuenta consideraciones tales como:

- a) **Principios rectores.** El ERP debería proporcionar orientación para responder ante emergencias, tales como leyes y reglamentos aplicables a las investigaciones, acuerdos con autoridades locales, políticas y prioridades de la empresa.
- b) **Organización.** El ERP debería describir las intenciones de la administración con respecto a los organismos encargados de la respuesta:
  - 1) designando a quienes dirigirán y a quienes integrarán los equipos de respuesta;

- 2) definiendo las funciones y responsabilidades del personal asignado a los equipos de respuesta;
- 3) aclarando las líneas de autoridad de rendición de cuentas;
- 4) estableciendo un centro de gestión de crisis (CMC);
- 5) estableciendo procedimientos para recibir un gran número de solicitudes de información, especialmente durante los primeros días después de un accidente importante;
- 6) designando al portavoz de la empresa para tratar con los medios de comunicación;
- 7) definiendo qué recursos estarán disponibles, incluidas las autorizaciones financieras para las actividades inmediatas;
- 8) designando al representante de la empresa para toda investigación oficial emprendida por funcionarios del Estado; y
- 9) definiendo un plan de llamadas para el personal clave, etc.

Podría emplearse un organigrama para indicar las funciones y las relaciones de comunicación en la organización.

c) **Notificaciones.** El plan debería especificar a quién, en la organización, se debe notificar en caso de emergencia, quién debe hacer las notificaciones externas y por qué medios. Debería considerarse la necesidad de informar a las personas y entidades siguientes:

- 1) la administración;
- 2) las autoridades del Estado (búsqueda y salvamento, autoridad de reglamentación, junta de investigación de accidentes, etc.);
- 3) los servicios locales de respuesta ante emergencias (autoridades aeroportuarias, bomberos, policía, ambulancias, organismos médicos, etc.);
- 4) familiares de las víctimas (una cuestión delicada que, en muchos Estados, atiende la policía);
- 5) el personal de la empresa;
- 6) los medios de comunicación; y
- 7) entidades jurídicas, contables, aseguradores, etc.

d) **Respuesta inicial.** Dependiendo de las circunstancias, inicialmente podrá enviarse a un equipo de respuesta al lugar del accidente para aumentar los recursos locales y supervisar los intereses de la organización. Entre los factores que deben considerarse para dicho equipo figuran los siguientes:

- 1) ¿Quién debería dirigir el equipo de respuesta inicial?
- 2) ¿Quién debería ser incluido en el equipo de respuesta inicial?
- 3) ¿Quién debería hablar en nombre de la organización en el lugar del accidente?
- 4) ¿Qué se necesitaría como equipo especial, ropa, documentación, transporte, alojamiento, etc.?

- e) **Asistencia adicional.** Los empleados que tienen instrucción y experiencia apropiadas pueden proporcionar apoyo útil durante la preparación, la práctica y la actualización para la organización del ERP. La experiencia de estas personas puede ser útil para planificar y ejecutar tareas como:
- 1) actuar como pasajeros en simulacros de accidentes;
  - 2) ocuparse de los sobrevivientes;
  - 3) tratar con los familiares más próximos, etc.
- f) **Centro de gestión de crisis (CMC).** Una vez que se han cumplido los criterios de activación, en la sede de la organización debería establecerse un CMC. Además, podría establecerse un puesto de mando (CP) en el lugar del accidente o en un lugar cercano. El ERP debería prever cómo atender a las necesidades siguientes:
- 1) personal (quizás 24 horas por día, 7 días por semana durante el período de respuesta inicial);
  - 2) equipo de comunicaciones (teléfonos, fax, internet, etc.);
  - 3) requisitos de documentación, mantenimiento de registros de actividades de emergencia;
  - 4) acumulación de registros de la empresa conexos;
  - 5) útiles y accesorios de oficina; y
  - 6) documentos de referencia (tales como lista de verificación y procedimientos de respuesta ante emergencias, manuales de la empresa, planes de emergencias de aeropuerto y listas de teléfonos).
- En caso de una crisis en un lugar alejado de la base de la empresa, podrían contratarse los servicios del centro de crisis de una línea aérea o de otro organismo especializado para que atienda los intereses del explotador. El personal de la empresa normalmente complementará los servicios del centro contratado lo antes posible.
- g) **Registros.** Además de la necesidad de mantener registros de sucesos y actividades, la organización también tendrá que proporcionar información a cualquier equipo de investigación del Estado. El ERP debería prever los siguientes tipos de información para los investigadores:
- 1) todos los registros pertinentes sobre la aeronave, la tripulación de vuelo y las operaciones;
  - 2) listas de punto de contacto y del personal relacionado con el suceso;
  - 3) notas de todas las entrevistas (y declaraciones) con toda persona relacionada con el suceso;
  - 4) toda prueba fotográfica o de otro tipo.
- h) **Lugar del accidente.** Después de un gran accidente, los representantes de varias jurisdicciones tienen razones legítimas para tener acceso al lugar del accidente, por ejemplo, policía, bomberos, personal médico, autoridades aeroportuarias, peritos forenses (médicos examinadores) para ocuparse de los muertos, investigadores del Estado del suceso, organismos de socorro (como la Cruz Roja) e incluso los medios de comunicación. Si bien la coordinación de las actividades de estos interesados es responsabilidad de la policía del Estado o de la autoridad investigadora, el explotador de la aeronave debería aclarar los siguientes aspectos de las actividades en el lugar del accidente:

- 1) nombramiento de un representante de alto nivel de la empresa en el lugar del accidente ya sea:
    - en la base principal;
    - fuera de la base principal;
    - fuera de la costa o en un Estado extranjero.
  - 2) gestión de la atención de los pasajeros sobrevivientes;
  - 3) necesidades de los familiares de las víctimas;
  - 4) seguridad de los restos de la aeronave;
  - 5) tratamiento de los restos humanos y bienes personales de las víctimas;
  - 6) preservación de pruebas;
  - 7) suministro de asistencia (según sea necesario) a las autoridades de la investigación;
  - 8) traslado y eliminación de los restos de la aeronave; etc.
- i) **Medios de comunicación.** La forma en que la empresa responde a los medios de comunicación puede afectar a la recuperación de la misma respecto del suceso. Es necesaria una orientación clara. Por ejemplo:
- 1) qué información está protegida por ley (datos del FDR, registros del CVR y ATC, declaraciones de testigos, etc.);
  - 2) quién puede hablar en nombre de la sociedad matriz en la sede y en el lugar del accidente (Director de relaciones públicas, Director general u otro directivo de alto nivel, gerente, propietario);
  - 3) directrices respecto de una declaración preparada para responder inmediatamente a preguntas de los medios de comunicación;
  - 4) qué información se puede divulgar (qué debería evitarse);
  - 5) oportunidad y contenido de la declaración inicial de la empresa; y
  - 6) disposiciones para autorizaciones periódicas a los medios de comunicación.
- j) **Investigaciones oficiales.** Debería proporcionarse orientación para el personal de la empresa que trata con los investigadores y la policía del Estado.
- k) **Asistencia a los familiares.** El EPR debería incluir también orientación sobre el enfoque de la organización para prestar asistencia a los familiares de las víctimas de accidentes (tripulación y pasajeros). Esta orientación puede incluir aspectos tales como:
- 1) requisitos del Estado para la prestación de servicios de asistencia a los familiares;
  - 2) arreglos de viaje y alojamiento para visitar el lugar del accidente y a los sobrevivientes;
  - 3) coordinador del programa y puntos de contacto para cada familia;

- 4) suministro de información actualizada;
- 5) asistencia psicológica para duelo, etc.;
- 6) asistencia financiera inmediata para las víctimas y sus familiares;
- 7) servicios conmemorativos, etc.

Algunos Estados definen los tipos de asistencia que debe proporcionar un explotador.

- l) **Terapia para estrés causado por incidentes graves.** Para el personal que trabaja en situaciones de estrés, el ERP puede incluir orientación que especifique los límites de las funciones y prevea terapia para el estrés causado por incidentes graves.
- m) **Examen posterior al suceso.** Deberían preverse directrices para que, después de la emergencia, el personal clave lleve a cabo una sesión completa de información y registro de toda la experiencia importante adquirida que pueda resultar en enmiendas al ERP y las listas de verificación correspondientes.

#### 4. RESPONSABILIDADES DEL EXPLOTADOR DE LA AERONAVE

4.1 El plan de respuesta ante emergencias (ERP) del explotador de la aeronave debería estar coordinado con el plan de emergencia de aeropuerto (AEP) de modo que el personal del explotador sepa qué responsabilidades asumirá el aeropuerto y qué respuestas se espera del explotador. Como parte de su planificación de respuesta ante emergencias, los explotadores de aeronaves juntamente con el explotador del aeropuerto deben:

- a) proporcionar instrucción al personal a fin de prepararlo para emergencias;
- b) tomar disposiciones para atender las consultas telefónicas relacionadas con la emergencia;
- c) designar una zona de espera apropiada para las personas que no están lesionadas (“parientes y amigos”);
- d) proporcionar una descripción de las funciones del personal de la empresa (p. ej., persona al mando y recepcionistas para recibir a los pasajeros en la zona de espera);
- e) recoger información esencial sobre los pasajeros y coordinar la atención de sus necesidades;
- f) hacer arreglos con otros explotadores y organismos para la provisión de apoyo mutuo durante la emergencia;
- g) preparar y mantener un maletín de urgencia que contenga:
  - 1) los útiles administrativos necesarios (formularios, papel, etiquetas de nombres, computadoras, etc.); y
  - 2) números de teléfonos indispensables (médicos, hoteles locales, traductores e intérpretes, abastecedores, empresas de transporte de la línea aérea, etc.).

4.2 En el caso de un accidente de aviación en el aeropuerto, o cerca del mismo, los explotadores deberán tomar ciertas medidas, por ejemplo:

- a) informar al puesto de mando del aeropuerto para coordinar las actividades del explotador de la aeronave;
- b) ayudar a ubicar y recuperar los registradores de vuelo;
- c) ayudar a los investigadores a identificar los componentes de la aeronave y asegurarse de que los componentes peligrosos no presentan riesgos;
- d) proporcionar información respecto a los pasajeros y la tripulación de vuelo y a la existencia de cualquier mercancía peligrosa a bordo;
- e) transportar a las personas que no están lesionadas a una zona de espera designada;
- f) hacer arreglos para las personas que no están lesionadas y que desean continuar su viaje o que necesitan alojamiento u otro tipo de asistencia;
- g) brindar información a los medios de comunicación en coordinación con el funcionario de información al público del aeropuerto y la policía; y
- h) trasladar la aeronave (o sus restos) una vez obtenida la autorización de la autoridad encargada de la investigación.

Si bien este párrafo está orientado a un accidente de aeronave, algunos de los conceptos se aplican también a la planificación de emergencia por los explotadores de aeródromos y proveedores de servicios de tránsito aéreo.

## 5. LISTAS DE VERIFICACIÓN

Toda persona que deba participar en la respuesta inicial a un accidente grave de aviación sufrirá cierto grado de choque nervioso. Por lo tanto, el proceso de respuesta ante emergencias tiende por sí mismo al empleo de listas de verificación. Estas listas de verificación pueden formar parte integrante de los manuales de operaciones o de respuesta ante emergencias de la empresa. Para ser eficaces, las listas de verificación deben ser regularmente:

- a) examinadas y actualizadas (p. ej., vigencia de las listas de llamada y detalles de puntos de contacto); y
- b) puestas a prueba por medio de ejercicios realistas.

## 6. INSTRUCCIÓN Y EJERCICIOS

Un plan de respuesta ante emergencias es un documento de intención escrito. Se espera que gran parte del ERP nunca se pondrá a prueba en condiciones reales. La instrucción es necesaria para asegurarse de que estas intenciones están respaldadas por capacidades para actuar. Puesto que la instrucción tiene una "vida útil", breve, es aconsejable efectuar simulacros y ejercicios. Algunas partes del ERP, tales como los planes de llamada y de comunicaciones, pueden someterse a prueba mediante ejercicios de simulación en la oficina. Otros aspectos, como las actividades "en el lugar" en que participan otros organismos, deben practicarse a intervalos regulares. Dichos ejercicios tienen la ventaja de demostrar las deficiencias del plan, que pueden rectificarse antes de que ocurra una verdadera emergencia.





# Adjunto C

## TEXTOS DE ORIENTACIÓN CONEXOS DE LA OACI

### MANUALES

*Auditoría de la seguridad de las operaciones de línea aérea (LOSA) (Doc 9803)*

*Concepto operacional de gestión del tránsito aéreo mundial (Doc 9854)*

*Directrices sobre factores humanos para los sistemas de gestión del tránsito aéreo (ATM) (Doc 9758)*

*Directrices sobre los factores humanos en el mantenimiento de aeronaves (Doc 9824)*

*Estudio de la seguridad de las operaciones normales (NOSS) (Doc 9910)*

*Manual de aeronavegabilidad (Doc 9760)*

*Manual de certificación de aeródromos (Doc 9774)*

*Manual de diseño de aeródromos (Doc 9157)*

*Manual de implantación de una separación vertical mínima de 300 m (1 000 ft) entre FL 290 y FL 410 inclusive (Doc 9574)*

*Manual de instrucción sobre factores humanos (Doc 9683)*

*Manual de investigación de accidentes e incidentes de aviación (Doc 9756)*

*Parte I — Organización y planificación*

*Parte III — Investigación<sup>1</sup>*

*Parte IV — Redacción de informes*

*Manual de medicina aeronáutica civil (Doc 8984)*

*Manual de navegación basada en la performance (PBN) (Doc 9613)*

*Manual de operaciones de deshielo y antihielo para aeronaves en tierra (Doc 9640)*

*Manual de operaciones todo tiempo (Doc 9365)*

*Manual de orientación sobre factores humanos para las auditorías de la seguridad operacional (Doc 9806)*

*Manual de radiotelefonía (Doc 9432)*

---

<sup>1</sup> En preparación

*Manual de servicios de aeropuertos (Doc 9137)*

*Manual de sistemas avanzados de guía y control del movimiento en la superficie (A-SMGCS) (Doc 9830)*

*Manual de sistemas de guía y control del movimiento en la superficie (SMGCS) (Doc 9476)*

*Manual de vigilancia de la seguridad operacional (Doc 9734)*

*Manual sobre auditoría de la vigilancia de la seguridad operacional (Doc 9735)*

*Manual sobre el sistema de notificación de la OACI de los choques con aves (IBIS) (Doc 9332)*

*Manual sobre la interceptación de aeronaves civiles (Doc 9433)*

*Manual sobre la metodología de planificación del espacio aéreo para determinar las mínimas de separación (Doc 9689)*

*Manual sobre la performance mundial del sistema de navegación aérea (Doc 9883)*

*Manual sobre las medidas de seguridad relativas a las actividades militares potencialmente peligrosas para las operaciones de aeronaves civiles (Doc 9554)*

*Manual sobre operaciones simultáneas en pistas de vuelo por instrumentos paralelas o casi paralelas (SOIR) (Doc 9643)*

*Manual sobre performance de comunicación requerida (RCP) (Doc 9869)*

*Manual sobre procedimientos para la inspección, certificación y supervisión permanente de las operaciones (Doc 8335)*

*Manual sobre requisitos del sistema de gestión del tránsito aéreo (Doc 9882)*

*Plan mundial de navegación aérea (Doc 9750)*

*Preparación de un manual de operaciones (Doc 9376)*

## **CIRCULARES**

*Compendio sobre factores humanos Núm. 15 — Los factores humanos en la seguridad de cabina (Cir 300)*

*Compendio sobre factores humanos Núm. 16 — Factores transculturales en la seguridad aeronáutica (Cir 302)*

*Compendio sobre factores humanos Núm. 17 — Manejo de amenazas y errores (TEM) en el control de tránsito aéreo (Cir 314)*

*Evaluación de la ADS-B para apoyar los servicios de tránsito aéreo y directrices para su implantación (Cir 311)<sup>1</sup>*

*Guía de instrucción para investigadores de accidentes de aviación (Cir 298)*

*Marco unificado para modelos de riesgo de colisión en apoyo del Manual sobre la metodología de planificación del espacio aéreo para determinar las mínimas de separación (Doc 9689) (Cir 319)<sup>1</sup>*

---

<sup>1</sup> En preparación

*Operación de nuevos aviones de mayor tamaño en los aeródromos existentes (Cir 305)*

*Orientación sobre asistencia a las víctimas de accidentes de aviación y sus familiares (Cir 285)*

*Riesgos en los lugares de accidentes de aviación (Cir 315)*

**VARIOS**

Notificación ADREP (<http://www.icao.int/anb/aig/Reporting.html>)

— FIN —





ISBN 978-92-9231-480-4



9 789292 314804