OACI

Doc 9859

Manual de gestión de la seguridad operacional

Cuarta edición, 2018



Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Doc 9859

Manual de gestión de la seguridad operacional

Cuarta edición, 2018

Aprobado y publicado bajo la responsabilidad de la Secretaria General

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

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

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

Primera edición, 2006
Tercera edición, 2013
Cuarta edición, 2018

Doc 9859, ***Manual de gestión de la seguridad operacional***
Núm. de pedido: 9859
ISBN 978-92-9258-655-3

© OACI 2019

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.

PREÁMBULO

Esta cuarta edición del Manual de gestión de la seguridad operacional (SMM) remplaza a la tercera edición, publicada en mayo de 2013, en su totalidad. La preparación de la presente edición se inició después de la adopción de la Enmienda 1 del Anexo 19 para abordar los cambios introducidos por dicha enmienda y reflejar los conocimientos y experiencia obtenidos después de la última revisión.

Para abordar las necesidades de la diversa comunidad de la aviación en la implantación de la gestión de la seguridad operacional y una recomendación de la segunda Conferencia de Alto Nivel sobre seguridad operacional celebrada en 2015, se ha elaborado el sitio web sobre implantación de la gestión de la seguridad operacional (SMI) (www.icao.int/SMI) a efectos de complementar el SMM que constituye, además, un repositorio para compartir mejores prácticas. En dicho sitio, y con carácter continuo, se recogerán, revisarán y presentarán ejemplos prácticos, herramientas y material didáctico de apoyo.



Esta edición tiene por objeto apoyar a los Estados en la implementación de programas estatales de seguridad operacional (SSP) eficaces. Esto comprende asegurar que los proveedores de servicios implantan sistemas de gestión de la seguridad operacional (SMS) con arreglo a las disposiciones del Anexo 19. A efectos de ser coherentes con los principios de gestión de la seguridad operacional, se ha realizado un esfuerzo concertado para centrarse en el resultado previsto de cada norma y método recomendado evitando expresamente ser demasiado prescriptivo. Se ha hecho hincapié en la importancia de que cada organización adapte la implementación de la gestión de la seguridad operacional a su entorno específico.

Nota 1.— En el presente manual, el término "organización" se utiliza con referencia a los Estados y los proveedores de servicios.

Nota 2.— En este manual, el término "proveedor de servicios" hace referencia a cualquier organización de la industria de la aviación que implemente SMS, ya sea con carácter obligatorio o voluntario, a diferencia del Anexo 19, donde se utiliza el término para referirse a una lista muy específica de organizaciones que figura en el Capítulo 3 y que excluye a los explotadores de la aviación general internacional.

Esta cuarta edición se divide en nueve capítulos que van creando en forma progresiva una comprensión de la gestión de la seguridad operacional por parte del lector. Estos capítulos pueden agruparse según los siguientes tres temas:

1) *Fundamentos de la gestión de la seguridad operacional* – Los Capítulos 1 a 3 se dirigen a crear la comprensión de los principios fundamentales de la gestión de la seguridad operacional por parte del lector.

2) *Desarrollo de inteligencia de la seguridad operacional* – En los Capítulos 4 a 7 se refuerzan dichos fundamentos. Estos capítulos comprenden cuatro tópicos interrelacionados que abordan el aprovechamiento de los datos de seguridad operacional y de la información sobre seguridad operacional para elaborar una percepción viable que pueda ser utilizada por la dirección de una organización para tomar decisiones basadas en datos, incluyendo las relacionadas con la forma más eficaz y eficiente de utilizar sus recursos.

3) *Implementación de la gestión de la seguridad operacional* – En los Capítulos 8 y 9 se explica cómo aplicar los conceptos presentados en los capítulos precedentes a efectos de institucionalizar la gestión de la seguridad operacional a nivel del Estado y del proveedor de servicios.

En el presente manual no se presenta orientación para apoyar los SARPS sobre gestión de la seguridad operacional específicos de cada sector que figuran fuera del Anexo 19 (p. ej., programas de análisis de datos de vuelo). En el *Manual de investigación de accidentes e incidentes de aviación* (Doc 9756) figura orientación sobre la realización de investigaciones independientes de accidentes e incidentes por parte de los Estados con arreglo al Anexo 13 — *Investigación de accidentes e incidentes de aviación*.

La OACI agradece las contribuciones del Grupo de expertos sobre gestión de la seguridad operacional (SMP) y del Grupo para la aplicación de la protección de la información sobre seguridad operacional (SIP-IG) así como de otros grupos de expertos y expertos individuales que proporcionaron apoyo, asesoramiento y otros aportes para este manual. El contenido del mismo se elaboró durante un período de dos años y posteriormente se presentó a un extenso proceso de examen paritario para recoger y tomar en cuenta comentarios de la comunidad de expertos, teniendo en consideración que se espera que el manual constituya la orientación general sobre gestión de la seguridad operacional para una amplia comunidad.

Mucho se agradecería recibir comentarios sobre este manual, en particular con respecto a su aplicación y utilidad, de todos los Estados, misiones de auditoría de la vigilancia de la seguridad operacional y misiones de cooperación técnica de la OACI. Estos comentarios serán tenidos en cuenta en la preparación de ediciones subsiguientes. Se ruega dirigir los comentarios a:

Secretaria General
Organización de Aviación Civil Internacional
999 Robert-Bourassa Boulevard
Montréal, Quebec
Canada H3C 5H7

ÍNDICE

Página

Glosario ..... (vii)

Definiciones ..... (vii)

Abreviaturas y acrónimos ..... (ix)

Publicaciones ..... (xi)

Capítulo 1. Introducción 1-1

1.1 Concepto de seguridad operacional 1-1
1.2 Aplicabilidad de la gestión de la seguridad operacional 1-3
1.3 Implementación de la gestión de la seguridad operacional 1-5
1.4 Gestión integrada de los riesgos 1-7

Capítulo 2. Fundamentos de la gestión de la seguridad operacional 2-1

2.1 El concepto de seguridad operacional y su evolución 2-1
2.2 Los seres humanos en el sistema 2-3
2.3 Causalidad de accidentes 2-6
2.4 El dilema de la gestión 2-9
2.5 Gestión de riesgos de seguridad operacional 2-11

Capítulo 3. Cultura de seguridad operacional 3-1

3.1 Introducción 3-1
3.2 Cultura de seguridad operacional y gestión de la seguridad operacional 3-1
3.3 Desarrollo de una cultura de seguridad operacional positiva 3-3

Capítulo 4. Gestión del rendimiento en materia de seguridad operacional 4-1

4.1 Introducción 4-1
4.2 Objetivos de seguridad operacional 4-3
4.3 Indicadores y metas de rendimiento en materia de seguridad operacional 4-4
4.4 Observación del rendimiento en materia de seguridad operacional 4-12
4.5 Actualización de los objetivos de seguridad operacional 4-17

Capítulo 5. Sistemas de recopilación y procesamiento de datos sobre seguridad operacional 5-1

5.1 Introducción 5-1
5.2 Recopilación de datos e información sobre seguridad operacional 5-2
5.3 Taxonomías 5-8
5.4 Procesamiento de datos de seguridad operacional 5-10
5.5 Gestión de datos e información sobre seguridad operacional 5-11

Página

Capítulo 6. Análisis de la seguridad operacional 6-1

6.1 Introducción 6-1
6.2 Tipos de análisis 6-2
6.3 Notificación de los resultados de los análisis 6-4
6.4 Compartición e intercambio de información sobre seguridad operacional 6-5
6.5 Toma de decisiones basada en datos 6-7

Capítulo 7. Protección de datos e información sobre seguridad operacional y fuentes conexas 7-1

7.1 Objetivos y contenido 7-1
7.2 Principios fundamentales 7-1
7.3 Alcance de la protección 7-3
7.4 Nivel de protección 7-5
7.5 Principios de protección 7-8
7.6 Principios de excepción 7-11
7.7 Divulgación al público 7-16
7.8 Protección de los datos registrados 7-18
7.9 Compartición e intercambio de información sobre seguridad operacional 7-18

Capítulo 8. Gestión estatal de la seguridad operacional 8-1

8.1 Introducción 8-1
8.2 Programa estatal de seguridad operacional (SSP) 8-3
8.3 Componente 1: Política, objetivos y recursos estatales de seguridad operacional 8-4
8.4 Componente 2: Gestión estatal de los riesgos de seguridad operacional 8-14
8.5 Componente 3: Aseguramiento estatal de la seguridad operacional 8-23
8.6 Componente 4: Promoción estatal de la seguridad operacional 8-31
8.7 Implementación del SSP 8-33

Capítulo 9. Sistemas de gestión de la seguridad operacional 9-1

9.1 Introducción 9-1
9.2 Marco para el SMS 9-1
9.3 Componente 1: Política y objetivos de seguridad operacional 9-2
9.4 Componente 2: Gestión de riesgos de seguridad operacional 9-11
9.5 Componente 3: Aseguramiento de la seguridad operacional 9-19
9.6 Componente 4: Promoción de la seguridad operacional 9-27
9.7 Planificación de la implementación 9-30

GLOSARIO

DEFINICIONES

Cuando los términos indicados a continuación se emplean en este manual, tienen los significados siguientes.

Nota.— Cuando aparece un asterisco junto a un término, eso indica que dicho término ya ha sido definido en Anexos y Procedimientos para los servicios de navegación aérea (PANS).

Activador. Nivel o valor establecido para un indicador de rendimiento en materia de seguridad operacional determinado que sirve para iniciar una acción requerida (p. ej., una evaluación, ajuste o medida correctiva).

****Datos de seguridad operacional.*** Conjunto definido de hechos o valores de seguridad operacional recogidos de diversas fuentes relacionadas con la aviación, y que se utiliza para mantener o mejorar la seguridad operacional.

Nota.— Dichos datos de seguridad operacional se recogen de actividades proactivas o reactivas relacionadas con la seguridad operacional, entre ellas las siguientes:

a) investigaciones de accidentes o incidentes;

b) notificaciones de seguridad operacional;

c) notificaciones de mantenimiento de la aeronavegabilidad;

d) observación de la performance operacional;

e) inspecciones, auditorías, encuestas; o

f) estudios y revisiones de la seguridad operacional.

Defensas. Medidas de mitigación específicas, controles preventivos o medidas de recuperación aplicadas para evitar que suceda un peligro o que aumente a una consecuencia indeseada.

Ejecutivo responsable. Persona única e identificable que es responsable del rendimiento eficaz y eficiente del SMS del proveedor de servicios.

Errores. Acción u omisión, por parte de un miembro del personal de operaciones, que da lugar a desviaciones de las intenciones o expectativas de organización o de un miembro del personal de operaciones.

Gestión del cambio. Proceso formal para gestionar los cambios dentro de una organización de forma sistemática, a fin de conocer los cambios que puede tener un impacto en las estrategias de mitigación de peligros y riesgos identificados antes de implementar tales cambios.

****Indicador de rendimiento en materia de seguridad operacional.*** Parámetro de seguridad basado en datos que se utiliza para observar y evaluar el rendimiento en materia de seguridad operacional.

****Información sobre seguridad operacional.*** Datos de seguridad operacional, organizados o analizados en un contexto determinado de modo que resulten útiles para fines de gestión de la seguridad operacional.

***Meta de rendimiento en materia de seguridad operacional.** La meta proyectada o prevista del Estado o proveedor de servicios para un indicador de rendimiento en materia de seguridad operacional, en un período de tiempo determinado, que coincide con los objetivos de seguridad operacional.

***Mitigación de riesgos.** Proceso de incorporación de defensas, controles preventivos o medidas de recuperación para reducir la gravedad o probabilidad de la consecuencia proyectada de un peligro.

***Nivel aceptable del rendimiento en materia de seguridad operacional (ALoSP).** Nivel de rendimiento en materia de seguridad operacional de la aviación civil en un Estado, como se define en su programa estatal de seguridad operacional, expresado en términos de objetivos e indicadores de rendimiento en materia de seguridad operacional.

***Objetivo de seguridad operacional.** Una declaración breve y de alto nivel del logro de seguridad operacional o resultado deseado que ha de conseguirse mediante el programa estatal de seguridad operacional o el sistema de gestión de la seguridad operacional del proveedor de servicios.

Nota.— Los objetivos de seguridad operacional se elaboran a partir de los principales riesgos de seguridad operacional de la organización y deberían tenerse en cuenta durante la subsiguiente elaboración de indicadores y metas de rendimiento en materia de seguridad operacional.

***Peligro.** Condición u objeto que podría provocar un incidente o accidente de aviación o contribuir al mismo.

***Programa estatal de seguridad operacional (SSP).** Conjunto integrado de reglamentos y actividades destinado a mejorar la seguridad operacional.

***Rendimiento en materia de seguridad operacional.** Logro de un Estado o un proveedor de servicios en lo que respecta a la seguridad operacional, de conformidad con lo definido mediante sus metas e indicadores de rendimiento en materia de seguridad operacional.

***Riesgo de seguridad operacional.** La probabilidad y la severidad previstas de las consecuencias o resultados de un peligro.

***Seguridad operacional.** Estado en el que los riesgos asociados a las actividades de aviación relativas a la operación de aeronaves, o que apoyan directamente dicha operación, se reducen y controlan a un nivel aceptable.

***Sistema.** Una estructura organizada, con un propósito definido, integrada por elementos y componentes interrelacionados e interdependientes, así como políticas, procedimientos y prácticas conexos creados para llevar a cabo una actividad específica o resolver un problema.

***Sistema de gestión de la seguridad operacional (SMS).** Enfoque sistemático para la gestión de la seguridad operacional que incluye las estructuras orgánicas, la rendición de cuentas, las responsabilidades, las políticas y los procedimientos necesarios.

***Supervisión.** Actividades mediante las cuales el Estado se asegura activamente, mediante inspecciones, auditorías y otras actividades, de que los titulares de licencias, certificados, autorizaciones o aprobaciones de aviación sigan satisfaciendo los requisitos establecidos y operen con el nivel de competencia y seguridad operacional requeridos por el Estado.

***Vigilancia de la seguridad operacional.** Función realizada por un Estado para asegurar que las personas y organismos que desempeñan actividades de aviación cumplan las leyes y reglamentos nacionales relativos a la seguridad operacional.

ABREVIATURAS Y ACRÓNIMOS

ADREP	Notificación de datos sobre accidentes/incidentes
AIA	Autoridad de investigación de accidentes
ALoSP	Nivel aceptable del rendimiento en materia de seguridad operacional
AOC	Certificado de explotador de servicios aéreos
ATS	Servicios de tránsito aéreo
CAA	Autoridad de aviación civil
CVR	Registrador de la voz en el puesto de pilotaje
D3M	Toma de decisiones basada en datos
Doc	Documento
ERP	Plan de respuesta ante emergencias
FDA	Análisis de datos de vuelo
FDR	Registrador de datos de vuelo
FMS	Sistema de gestión financiera
FRMS	Sistema de gestión de riesgos asociados a la fatiga
GASP	Plan global para la seguridad operacional de la aviación
iSTARS	Sistema integrado de análisis y notificación de tendencias de seguridad operacional
LOSA	Auditoría de la seguridad de las operaciones de línea
OACI	Organización de Aviación Civil Internacional
OHSMS	Sistema de gestión sobre cuestiones de salud y seguridad en el trabajo
OSHE	Seguridad, salud y ambiente en el trabajo
PIRG	Grupo regional de planificación y ejecución
QMS	Sistema de gestión de la calidad
RASG	Grupo regional de seguridad operacional de la aviación
RSOO	Organización regional de vigilancia de la seguridad operacional
SAG	Grupo de acción de seguridad operacional
SARPS	Normas y métodos recomendados
SD	Desviación estándar
SDCPS	Sistema de recopilación y procesamiento de datos sobre seguridad operacional
SeMS	Sistema de gestión de la seguridad de la aviación
SMM	Manual de gestión de la seguridad operacional
SMP	Grupo de expertos sobre gestión de la seguridad operacional
SMS	Sistema de gestión de la seguridad operacional
SPI	Indicador de rendimiento en materia de seguridad operacional
SPT	Meta de rendimiento en materia de seguridad operacional
SRB	Consejo de revisión de seguridad operacional
SRBS	Supervisión de la seguridad operacional basada en riesgos
SRM	Gestión de riesgos de seguridad operacional
SSO	Vigilancia de la seguridad operacional
SSP	Programa estatal de seguridad operacional
STDEVP	Desviación estándar de la población
TNA	Evaluación de las necesidades de instrucción
USOAP	Programa universal de auditoría de la vigilancia de la seguridad operacional

PUBLICACIONES

(citadas en este manual)

Los documentos siguientes son citados en este manual o pueden proporcionar textos de orientación adicionales.

DOCUMENTOS DE LA OACI

Anexes al Convenio sobre Aviación Civil Internacional

Anexo 1 — *Licencias al personal*

Anexo 6 — *Operación de aeronaves*
Parte I — *Transporte aéreo comercial internacional — Aviones*
Parte II — *Aviación general internacional — Aviones*

Anexo 8 — *Aeronavegabilidad*

Anexo 13 — *Investigación de accidentes e incidentes de aviación*

Anexo 14 — *Aeródromos*
Volumen I — *Diseño y operaciones de aeródromos*

Anexo 18 — *Transporte sin riesgos de mercancías peligrosas por vía aérea*

Anexo 19 — *Gestión de la seguridad operacional*

PANS

Procedimientos para los servicios de navegación aérea (PANS) — Aeródromos (Doc 9981)

Procedimientos para los servicios de navegación aérea — Gestión del tránsito aéreo (PANS-ATM, Doc 4444)

Manuales

Manual de servicios de aeropuertos (Doc 9137), Parte 3 — *Control y reducción del peligro que representa la fauna silvestre*

Manual de planificación de servicios de tránsito aéreo (Doc 9426)

Manual de aeronavegabilidad (Doc 9760)

Manual de seguridad de la aviación (Doc 8973 — distribución limitada)

Plan global para la seguridad operacional de la aviación (GASP) (Doc 10004)

Manual de investigación de accidentes e incidentes de aviación (Doc 9756)
Parte I — *Organización y planificación*
Parte II — *Procedimientos y listas de verificación*
Parte III — *Investigación*
Parte IV — *Redacción de informes*

Manual para la supervisión de los enfoques de gestión de la fatiga (Doc 9966)

Manual sobre emisores laser y seguridad de vuelo (Doc 9815)

Manual sobre sistemas de aeronaves pilotadas a distancia (RPAS) (Doc 10019)

Manual sobre las competencias de los inspectores de seguridad operacional en la aviación civil (Doc 10070)

Manual sobre el sistema de notificación de la OACI de los choques con aves (IBIS) (Doc 9332)

Manual sobre protección de la información de seguridad operacional (Doc 10053)
Parte I — *Protección de registros de investigación de accidentes e incidentes*

Manual de vigilancia de la seguridad operacional (Doc 9734)
Parte A — *Establecimiento y gestión de un sistema estatal de vigilancia de la seguridad operacional*
Parte B — *Establecimiento y gestión de una organización regional de vigilancia de la seguridad operacional*

Instrucciones Técnicas para el transporte sin riesgos de mercancías peligrosas por vía aérea (Doc 9284)

———————————

Capítulo 1

INTRODUCCIÓN

1.1 CONCEPTO DE SEGURIDAD OPERACIONAL

1.1.1 La seguridad operacional procura mitigar en forma proactiva los riesgos de seguridad operacional antes de que resulten en accidentes e incidentes de aviación. Mediante la implementación de la gestión de la seguridad operacional, los Estados pueden manejar sus actividades de seguridad operacional en forma más disciplinada, integradora y concentrada. La clara comprensión de su función y contribución respecto de la seguridad de las operaciones permite que el Estado y su industria de aviación prioricen medidas para enfrentar los riesgos de seguridad operacional y gestionar en forma más eficaz sus recursos para alcanzar el beneficio óptimo de la seguridad operacional de la aviación.

1.1.2 La eficacia de las actividades de gestión de la seguridad operacional del Estado se fortalece cuando se implementan en forma oficial e institucionalizada mediante un programa estatal de seguridad operacional (SSP) y sistemas de gestión de la seguridad operacional (SMS) para sus proveedores de servicios. El programa estatal de seguridad operacional, combinado con los SMS de sus proveedores de servicios, trata sistemáticamente los riesgos de seguridad operacional, mejora el rendimiento en materia de seguridad operacional de cada proveedor de servicios y, en forma colectiva, mejora el rendimiento en materia de seguridad operacional del Estado.

1.1.3 Cada Estado elabora y mantiene su SSP como enfoque estructurado para contribuir a la gestión de su rendimiento en materia de seguridad operacional de la aviación. El historial actual de seguridad operacional de la aviación se ha logrado mediante un enfoque tradicional basado en el cumplimiento y debería continuar tratándose como el fundamento del SSP. Como tal, los Estados deberían asegurar que cuentan con sistemas eficaces de vigilancia de la seguridad operacional. En el Capítulo 8 figura más información sobre el SSP.

1.1.4 Los Estados exigirán que los proveedores de servicios bajo su autoridad elaboren y mantengan un SMS, según se establece en el Anexo 19 — *Gestión de la seguridad operacional*, para mejorar en forma continua su rendimiento en materia de seguridad operacional mediante la identificación de peligros, acopio y análisis de datos, y evaluación y gestión continuas de los riesgos de seguridad operacional (véase el párrafo 1.2 por detalles sobre aplicabilidad del SMS). En el Capítulo 9 figura más información sobre la implementación de SMS.

1.1.5 Los objetivos del *Plan global para la seguridad operacional de la aviación* (GASP, Doc 10004) de la OACI estipulan que los Estados establezcan sistemas robustos y sostenibles de vigilancia de la seguridad operacional y que desarrollen los mismos en forma progresiva para alcanzar medios más perfeccionados de gestionar el rendimiento en materia de seguridad operacional. Estos objetivos corresponden a los requisitos de la OACI para la implementación de SSP por los Estados y de SMS por los proveedores de servicios.

1.1.6 Este enfoque de la seguridad operacional basado en el rendimiento ofrece mejoras dado que se concentra en el logro de resultados deseados en vez de concentrarse únicamente en determinar si el Estado cumple o no las disposiciones correspondientes. No obstante, es importante señalar que la aplicación de un enfoque del rendimiento en materia de seguridad operacional requiere colaboración puesto que requiere esfuerzos de parte de la industria de la aviación para elaborar medios apropiados de alcanzar los resultados especificados y, con respecto a los Estados, para evaluar el enfoque de cada proveedor de servicio.

1.1.7 BENEFICIOS DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

La implementación de la gestión de la seguridad operacional tiene muchos beneficios, entre ellos los siguientes:

a) *Fortalecimiento de la cultura de seguridad operacional* – La cultura de seguridad operacional de una organización puede fortalecerse poniendo en evidencia el compromiso de la administración y haciendo que el personal participe activamente en la gestión de los riesgos de seguridad operacional. Cuando la administración otorga activamente carácter prioritario a la seguridad operacional ello es normalmente bien recibido por el personal y pasa a constituir parte de las operaciones normales.

b) *Enfoque documentado y basado en procesos para garantizar la seguridad operacional* – Establece un enfoque claro y documentado para lograr operaciones seguras y que es comprendido por el personal y puede explicarse fácilmente a terceros. Además, una definición clara de un rendimiento básico permite introducir cambios controlados cuando se mejora continuamente el programa o sistema de seguridad operacional, lo que ayuda a la organización a optimizar los recursos necesarios para implantar cambios.

c) *Mejor comprensión de interfaces y relaciones de seguridad operacional* – El proceso de documentar y definir interfaces en la gestión de la seguridad operacional puede beneficiar la comprensión por la organización de las relaciones entre procesos, lo que conduce a una mejor comprensión del proceso completo y a la presentación de oportunidades para aumentar la eficiencia.

d) *Detección temprana mejorada de los peligros de seguridad operacional* – Mejora la capacidad del Estado o proveedor de servicios de detectar problemas de seguridad operacional emergentes, lo que puede prevenir accidentes e incidentes mediante la identificación proactiva de peligros y la gestión de los riesgos de seguridad operacional.

e) *Toma de decisiones de seguridad operacional basada en datos* – Mejora la capacidad del Estado o proveedor de servicios de reunir datos de seguridad operacional con fines de análisis de ésta. Si se piensa en forma estratégica para determinar las preguntas que deben responderse, la información sobre seguridad operacional resultante puede ayudar a los encargados de tomar decisiones, en tiempo casi real, a adoptar decisiones válidas y mejor fundamentadas. Un aspecto importante de esta toma de decisiones es la asignación de recursos a las áreas de mayor preocupación o necesidad.

f) *Comunicación mejorada sobre seguridad operacional* – Proporciona un lenguaje de seguridad operacional común a través de una organización y de la industria. Un lenguaje de seguridad operacional común es una herramienta fundamental para el desarrollo de una comprensión común de los objetivos y logros de la organización en materia de seguridad operacional. En particular, proporciona un reconocimiento de los objetivos de seguridad operacional de la organización y de sus indicadores de rendimiento en materia de seguridad operacional (SPI) y de las metas de rendimiento en materia de seguridad operacional (SPT), que establecen la orientación y la motivación para ésta. El personal será más consciente del rendimiento de la organización y de los progresos alcanzados hacia el logro de los objetivos de seguridad operacional definidos, así como de la forma en que contribuyen al éxito de la organización. El lenguaje de seguridad operacional común permite que los proveedores de servicios con múltiples actividades aeronáuticas reúnan información sobre seguridad operacional a través de entidades orgánicas. Esto es necesario para apoyar la gestión de interfaces a través de todo el sistema aeronáutico.

g) *Pruebas de que la seguridad operacional constituye una prioridad* – Demuestran la forma en que la administración apoya y habilita la seguridad operacional, la forma en que se identifican y gestionan los riesgos de seguridad y la forma en que se mejora continuamente el rendimiento de la seguridad operacional, resultando en una mayor confianza de parte de la comunidad aeronáutica, tanto interna como externa a la organización. Esto también resulta en una confianza del personal respecto del

rendimiento en materia de seguridad operacional de la organización, que puede llevar a una creciente atracción y retención de personal de elevado calibre. También permite que los Estados y organizaciones regionales de vigilancia de la seguridad operacional (RSOO) desarrollen confianza en el rendimiento de los proveedores de servicios en materia de seguridad operacional.

h) *Posibles ahorros financieros* – Puede permitir que algunos proveedores de servicios estén en condiciones de obtener descuentos en sus primas de seguros o una reducción de las primas de seguro de indemnización de sus empleados sobre la base de los resultados de sus SMS.

i) *Aumento de la eficiencia* – Posible reducción del costo de las operaciones mediante la exposición de las ineficiencias en procesos y sistemas existentes. La integración con otros sistemas de gestión internos o externos puede también aportar economías sobre costos adicionales.

j) *Posibilidad de evitar costos* – Mediante la identificación proactiva de peligros y la gestión de riesgos de seguridad operacional (SRM), pueden evitarse los costos en que se incurre debido a accidentes e incidentes. En tales casos, los costos directos pueden comprender: lesiones corporales, daños a la propiedad, reparación de equipo y retrasos. Los costos indirectos pueden comprender: acciones judiciales, lucro cesante y reputación dañada, excedentes de repuestos, herramientas e instrucción, aumento de las primas de seguro, disminución de productividad del personal, recuperación y limpieza de equipo, pérdida de uso de equipo que lleve a sustitución de equipo a corto plazo e investigaciones internas.

1.2 APLICABILIDAD DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

En el Capítulo 3 del Anexo 19 se esbozan las responsabilidades del Estado en materia de gestión de la seguridad operacional que incluyen exigir a los proveedores de servicios identificados en los SARPS que implementen SMS. Las disposiciones relativas a la implementación de SMS por proveedores de servicios figuran en el Capítulo 4 y en el Apéndice 2 del Anexo 19.

1.2.1 Aplicabilidad del SMS

1.2.1.1 La evaluación para determinar la aplicabilidad del SMS para la Enmienda 1 del Anexo 19 se basó en un conjunto de criterios. Se prevé que estos mismos criterios sean utilizados periódicamente por la OACI y por el Grupo de expertos sobre gestión de la seguridad operacional (SMP) para revaluar la necesidad de extender la aplicabilidad a otras organizaciones aeronáuticas.

Enfoque de sistema total para la seguridad operacional

1.2.1.2 El enfoque de sistema total para la seguridad operacional considera a la industria de la aviación en su totalidad como un sistema. Todos los proveedores de servicios y sus sistemas para la gestión de la seguridad operacional se consideran como subsistemas. Esto permite que el Estado considere las interacciones y las relaciones causa-efecto en la totalidad del sistema. A menudo resulta imposible o poco práctico construir todos los sistemas de seguridad operacional en la misma forma. Por lo tanto, una preocupación principal para Estados y proveedores de servicios es la mejor forma de gestionar las interfaces entre sistemas diferentes en interacción.

1.2.1.3 Al examinar la aplicabilidad de los SMS, se tuvo en cuenta la relación entre los proveedores de servicios que ya cuentan con un SMS con arreglo al Anexo 19 y otras organizaciones con actividades aeronáuticas. La aplicación del SMS debería reducir el riesgo de que existan brechas o superposiciones de seguridad operacional, y no aumentar los riesgos de seguridad operacional mediante un interfuncionamiento disminuido.

Consecuencias de la subcontratación

1.2.1.4 Para que la SRM sea eficaz en el ámbito de los proveedores de servicios es importante definir con claridad las responsabilidades para la identificación de peligros y la gestión de los riesgos de seguridad operacional conexos en la totalidad de la cadena de servicios dentro del sistema, sin brechas ni superposiciones. Cuando un proveedor de servicios con SMS contrata una organización no sujeta a un SMS, los peligros y riesgos de seguridad operacional que podrían introducirse por el contratista son tratados por el SMS del proveedor de servicios. Esto impone responsabilidades SRM adicionales en el proveedor de servicios para asegurar que se tiene conocimiento de los riesgos de seguridad operacional inducidos por las actividades de sus contratistas. En el Capítulo 2 figura más información sobre la SRM.

Control normativo de los riesgos de seguridad operacional

1.2.1.5 Los Estados deberían evaluar si la legislación y reglamentos existentes tratan eficazmente los peligros que la actividad entraña. Podría ocurrir que los requisitos existentes proporcionen suficiente mitigación de riesgos de seguridad operacional y la imposición del requisito de contar con SMS a las organizaciones a las que no se aplica el Anexo 19 puede no resultar en importantes beneficios en materia de seguridad operacional.

1.2.2 Ampliación de la aplicabilidad discrecional de SMS

1.2.2.1 Los criterios de aplicabilidad mencionados anteriormente también pueden servir de orientación a los Estados cuando consideren una ampliación de la aplicabilidad del SMS más allá de la definición del Anexo 19 o la promoción de una implementación voluntaria. La aplicabilidad discrecional del SMS debería considerarse seriamente. La decisión de ampliar la aplicabilidad del SMS a sectores o proveedores de servicios debería tener en cuenta los riesgos de seguridad operacional identificados en el Estado y, si se toma la decisión de hacerlo, la implementación del SMS debería observarse como parte del SSP. Antes de exigir SMS, los Estados deben considerar si:

a) existen otras opciones viables para alcanzar las mejoras deseadas en el rendimiento en materia de seguridad operacional; y

b) se dispone de recursos suficientes para que el Estado y el sector industrial implementen y observen el SMS. En particular, debe considerarse las posibles consecuencias para el personal y el reto potencial de adquirir e integrar las habilidades y conocimientos necesarios.

1.2.2.2 Cada Estado debería considerar el nivel aceptable del rendimiento en materia de seguridad operacional (ALoSP) en toda su industria e instituir un plan de aplicabilidad del SMS que tenga la mayor probabilidad de alcanzar los objetivos de seguridad operacional del Estado. Es probable que el plan de aplicabilidad del SMS evolucione en forma paralela a los del Estado.

1.2.3 Responsabilidad de la gestión de la seguridad operacional

No existen en el Anexo 19 disposiciones dirigidas a transferir al Estado las responsabilidades del proveedor o explotador de servicios de aviación. Los Estados cuentan con muchas herramientas para gestionar la seguridad operacional dentro de su sistema. Como parte de su SSP, cada Estado debería considerar las mejores opciones para la vigilancia de las actividades aeronáuticas que puedan no corresponder a la órbita de los actuales Anexos de la OACI así como la vigilancia de actividades nuevas o emergentes.

1.2.4 Aplicabilidad de los proveedores de servicios estatales o militares

1.2.4.1 En algunos Estados, la función de proveedor de servicios es proporcionada por la administración pública civil o por el sector militar. Algunos proveedores de servicios civiles proporcionan servicios al sector militar bajo contrato, y algunas organizaciones militares proporcionan servicios civiles. Independientemente del arreglo en cuestión, debería

exigirse al proveedor de servicios para el sector civil del Estado que cumpla con todos los SARPS aplicables de la OACI, incluyendo los requisitos SMS del Anexo 19 sin importar el carácter específico de dicha organización. La descripción del sistema estatal o del proveedor de servicios debería tener en cuenta las funciones de esas organizaciones y sus relaciones mutuas. El ejecutivo responsable del proveedor de servicios, ya sea civil o militar, debería estar en condiciones de explicar los arreglos en cuestión y la forma en que se gestionan los riesgos de seguridad operacional. En pocas palabras, los proveedores de servicios deberían gestionar la seguridad operacional sin importar los arreglos organizativos.

1.2.4.2 Donde el Estado funciona como proveedor de servicios debería existir una clara separación entre sus funciones como proveedor de servicios y las correspondientes a la autoridad normativa estatal. Esto se logra mediante una clara definición de funciones y responsabilidades del personal de la autoridad estatal y de provisión de servicios para evitar posibles conflictos de intereses.

1.2.5 Seguridad, salud y ambiente en el trabajo y seguridad operacional de la aviación

La seguridad, salud y ambiente en el trabajo (OSHE) [también denominada salud y seguridad laboral (OHS) o salud y seguridad en el lugar de trabajo (WHS)] es un campo que abarca la seguridad, la salud y el bienestar de los trabajadores. La diferencia principal entre el sistema de gestión de la seguridad operacional de la aviación y el sistema OSHE es la intención de cada uno. En muchos Estados los empleadores tienen la obligación jurídica de ocuparse en forma razonable de la salud y seguridad de sus empleados. La intención de los programas OSHE es cumplir las obligaciones jurídicas y éticas de los empleadores mediante el fomento de un ambiente laboral seguro y saludable. Estos aspectos se tratan normalmente por un órgano gubernamental diferente del que se ocupa de los asuntos aeronáuticos. Por ello, el Anexo 19, Capítulo 2, *Aplicación*, se concentra intencionalmente en las "funciones de gestión de la seguridad operacional que atañen, o sirven de apoyo directo, a la operación segura de las aeronaves".

1.3 IMPLEMENTACIÓN DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

1.3.1 El establecimiento de una base sólida es fundamental para el logro de una implementación eficaz de la gestión de la seguridad operacional. Los aspectos siguientes deberían tratarse como primeros pasos para la implantación de SSP o SMS:

a) *Compromiso de la administración superior*: Es fundamental que la administración superior de todos los órganos aeronáuticos del Estado se comprometa a implementar la gestión de la seguridad operacional en forma eficaz.

b) *Cumplimiento de los requisitos prescriptivos*: El Estado debería asegurar que cuenta con un sistema de vigilancia de la seguridad operacional bien desarrollado para el otorgamiento de licencias, certificación, autorización y aprobación de individuos y organizaciones que realizan actividades aeronáuticas en el Estado, incluyendo personal técnico cualificado. Los proveedores de servicios deberían asegurar que cuentan con procesos para garantizar el continuo cumplimiento de los requisitos prescriptivos establecidos.

c) *Régimen de cumplimiento*: El Estado debería establecer una política y marcos para imponer el cumplimiento a efectos de permitir que las partes gestionen y resuelvan desviaciones y transgresiones menores.

d) *Protección de la información sobre seguridad operacional*: Es fundamental que los Estados instituyan un marco jurídico de protección para asegurar la disponibilidad continua de datos de seguridad operacional e información sobre seguridad operacional.

1.3.2 Descripción del sistema

La descripción del sistema consiste en un resumen de los procesos, actividades e interfaces de la organización (Estado o proveedor de servicios) que deben abordarse para la identificación de peligros y evaluación de riesgos de seguridad operacional abarcadas en sus sistemas de seguridad operacional. En ella se describe el sistema de aviación dentro del que funciona la organización asi como las diversas entidades y autoridades involucradas. También comprende las interfaces dentro de la organización, así como aquellas con organizaciones externas que contribuyen a la prestación segura de los servicios. La descripción del sistema proporciona un punto de partida para la implementación del SSP/SMS. En los Capítulos 8 y 9, respectivamente, figura más información sobre la descripción del sistema para los Estados y los proveedores de servicios.

1.3.3 Interfaces

1.3.3.1 Cuando los Estados y los proveedores de servicios consideren la implementación de la gestión de la seguridad operacional es importante tener en cuenta los riesgos de seguridad operacional inducidos por las entidades interrelacionadas. Las interfaces pueden ser internas (p. ej., entre los departamentos de operaciones y de mantenimiento o los departamentos de finanzas, recursos humanos o asuntos jurídicos), o pueden ser externas (p. ej., otro Estado, proveedores de servicios o servicios contratados). Los Estados y los proveedores de servicios tienen mayor control sobre los riesgos de seguridad operacional conexos cuando se identifican y gestionan las interfaces. Estas se definen como parte de la descripción del sistema.

Evaluación de las consecuencias de las interfaces para la seguridad operacional

1.3.3.2 Una vez que el Estado o el proveedor de servicios ha identificado sus interfaces, el riesgo de seguridad operacional planteado por cada interfaz se evalúa aplicando los procesos de evaluación de riesgos de seguridad operacional existentes en la organización (véanse detalles en el Capítulo 2). Sobre la base de los riesgos de seguridad operacional identificados, el Estado o el proveedor de servicios puede tener en cuenta trabajar con otras organizaciones para determinar una estrategia apropiada de control de riesgos de seguridad operacional. Las organizaciones que trabajan en colaboración pueden estar en condiciones de identificar más peligros de las interfaces, evaluar los riesgos de seguridad operacional conexos y determinar controles mutuamente apropiados. La colaboración es muy conveniente porque la percepción de los riesgos de seguridad operacional puede ser diferente entre diferentes organizaciones.

1.3.3.3 También es importante reconocer que cada organización involucrada es responsable de identificar y gestionar los peligros que puedan afectarla. El carácter crítico de la interfaz puede ser diferente para cada organización. Cada organización puede aplicar razonablemente diferentes clasificaciones del riesgo de seguridad operacional y tener diferentes prioridades en la materia (en términos de rendimiento de seguridad operacional, recursos, tiempo).

Observación y gestión de las interfaces

1.3.3.4 Los Estados y los proveedores de servicios son responsables de la observación continua y la gestión de sus interfaces para asegurar que los servicios de proporcionan en forma segura. Un enfoque eficaz para las interfaces de la SRM es establecer acuerdos formales entre las organizaciones interrelacionadas con responsabilidades claramente definidas en cuanto a la observación y la gestión. Si se documentan y comparten todos los problemas de seguridad operacional de las interfaces, los informes de seguridad operacional y las enseñanzas obtenidas, así como los riesgos de seguridad operacional entre las organizaciones en cuestión se asegurará una comprensión clara de la gestión. La compartición permite transferir conocimientos y prácticas laborales que podrían mejorar la eficacia de cada organización en la materia.

1.3.4 Planificación de la implementación

1.3.4.1 La realización de un análisis de brechas antes de emprender la implementación de SSP/SMS permitirá a la organización identificar la brecha entre las estructuras y procesos organizativos actuales y los necesarios para el

funcionamiento eficaz del SSP o SMS. Para el SSP, es importante incluir un examen de las preguntas del protocolo del Programa universal de auditoría de la vigilancia de la seguridad operacional (USOAP) que se consideran como la base de dicho programa.

1.3.4.2 El plan de implementación del SSP o SMS es, como su nombre lo indica, un plan para la instrumentación del SSP/SMS. Proporciona una clara descripción de los recursos, tareas y procesos necesarios, y un cronograma y una secuencia indicativos de las tareas y responsabilidades fundamentales. En los Capítulos 8 y 9, respectivamente, figura más información sobre la implementación de la gestión de la seguridad operacional para los Estados y los proveedores de servicios.

Evaluación del grado de desarrollo

1.3.4.3 Poco después de implementar los componentes y elementos fundamentales del SSP o SMS, deberían realizarse evaluaciones periódicas para observar cuán eficazmente está funcionando. A medida que se desarrolla el sistema, la organización debería procurar garantías de que está funcionando según lo previsto y que resulta eficaz para alcanzar sus objetivos y metas de seguridad operacional declarados. La gestión de la seguridad operacional lleva tiempo para alcanzar la madurez necesaria y el objetivo final debería ser el mantenimiento o la mejora continua del rendimiento de la organización en materia de seguridad operacional.

1.3.5 Consideraciones de tamaño y complejidad

1.3.5.1 Cada Estado y cada proveedor de servicios es diferente de los demás. Los SSP y SMS están diseñados para adaptarse a las necesidades específicas de cada Estado o proveedor de servicios. Todos los componentes y todos los elementos de los SSP y SMS están interconectados y son interdependientes y son necesarios para un funcionamiento eficaz. Es importante de que los requisitos de SSP y SMS no se implementen solamente en forma prescriptiva. Los requisitos tradicionales de carácter prescriptivo deben complementarse con un enfoque basado en el rendimiento.

1.3.5.2 El programa o sistema está diseñado para producir los resultados deseados de cada organización sin cargas indebidas. Los SSP y SMS, si están bien implementados, tienen por objeto complementar y mejorar los sistemas y procesos existentes en la organización. La gestión efectiva de la seguridad operacional se alcanzará mediante una cuidadosa planificación e implantación, asegurando que cada requisito se enfoca de manera que corresponda a la cultura y entorno operacional de la organización. En los Capítulos 8 y 9, respectivamente, figura más información sobre los aspectos que han de considerarse al implementar SSP/SMS para Estados y proveedores de servicios.

1.3.6 Integración de los elementos básicos

Es importante señalar que todos los sistemas están compuestos de tres elementos básicos: personas, procesos y tecnología. La gestión de la seguridad operacional no constituye una excepción. Al establecer o mantener los diferentes procesos, actividades y funciones, todos los Estados y proveedores de servicios deberían cerciorarse de que han tenido en cuenta la intención de cada requisito y, lo que es más importante, la forma en que trabajan conjuntamente para permitir que la organización satisfaga sus objetivos de seguridad operacional. Todos y cada uno de estos elementos de la gestión de la seguridad operacional, así como sus interrelaciones, se abarcarán a lo largo del presente manual.

1.4 GESTIÓN INTEGRADA DE LOS RIESGOS

1.4.1 El sistema de aviación en su totalidad comprende muchos y diferentes sistemas funcionales como los financieros, ambientales, de seguridad operacional y de seguridad de la aviación. Estos dos últimos son los principales dominios operacionales del sistema de aviación global. Como conceptos comparten importantes características en tanto ambos se ocupan de los riesgos de que ocurran sucesos con consecuencias de diversa magnitud. No obstante, difieren respecto del importante elemento de la intencionalidad. La seguridad de la aviación se ocupa de actos maliciosos y

voluntarios para perturbar el funcionamiento de un sistema. La seguridad operacional se concentra en el impacto negativo para el funcionamiento de los sistemas en cuestión provocado por consecuencias no intencionales de una combinación de factores.

1.4.2 En el contexto operacional, todos los sistemas funcionales producen algún tipo de riesgo que debe gestionarse en forma apropiada para disminuir posibles consecuencias adversas. Tradicionalmente, cada sistema ha desarrollado marcos y prácticas de gestión de riesgos específicas de cada sector dirigidas a abordar las características propias de cada sistema. La mayoría de estas prácticas de gestión de riesgos comprenden análisis completos de las consecuencias dentro del sistema, a menudo conocidos como gestión de consecuencias imprevistas. Otro aspecto son las consecuencias entre sistemas que resultan de procesos de gestión de riesgos específicos del sistema. Esto se relaciona con el hecho de que una estrategia eficaz de gestión de riesgos de un sector específico puede tener consecuencias negativas sobre otro sector operacional de la aviación. En el contexto aeronáutico, la dependencia entre sistemas que se destaca con mayor frecuencia es el dilema entre seguridad operacional y seguridad de la aviación. Las medidas de seguridad de la aviación eficaces pueden tener consecuencias negativas para la seguridad operacional y a la inversa. Los dominios de seguridad operacional y seguridad de la aviación pueden diferir en la intención subyacente, pero convergen en el objetivo común de proteger a las personas y los bienes (p. ej., el tratamiento de las ciberamenazas y riesgos requiere coordinación a través de los dominios de seguridad operacional y seguridad de la aviación). En algunos casos, la gestión del riesgo inherente de un dominio puede afectar al otro en formas imprevistas, como en los ejemplos siguientes:

a) el reforzamiento de las puertas del puesto de pilotaje, necesario por los riesgos de seguridad de la aviación, puede tener consecuencias de seguridad operacional en el funcionamiento de la aeronave;

b) las restricciones impuestas al transporte en la cabina de dispositivos electrónicos personales puede desplazar el riesgo de seguridad de la aviación de la cabina a la bodega de carga, lo que aumentaría los riesgos de seguridad operacional; y

c) el cambio de ruta para evitar el vuelo sobre zonas de conflicto puede provocar una congestión de los corredores aéreos, lo que constituiría un problema de seguridad operacional.

1.4.3 Una exitosa gestión de riesgos en la aviación debería apuntar a la reducción general de los riesgos en el sistema, incluyendo todos los sistemas funcionales involucrados. Este proceso requiere una evaluación analítica del sistema en su totalidad al más alto nivel de la entidad correspondiente (Estado, organizaciones regionales, proveedores de servicios). La evaluación e integración de las necesidades e interdependencias del sistema funcional se conoce como gestión integrada de los riesgos (IRM). La IRM se concentra en la reducción global de los riesgos de la organización. Esto se consigue mediante un análisis cuantitativo y cualitativo de los riesgos inherentes y de la eficacia y consecuencias de los procesos de gestión de riesgos específicos de cada sector. La IRM tiene la responsabilidad sistémica de coordinar, armonizar y optimizar los procesos de gestión de riesgos con el único objetivo de reducir el riesgo. La IRM no puede remplazar las gestiones de riesgos específicas de los sistemas funcionales, y no pretende delegar funciones y responsabilidades adicionales a estos. La IRM es un concepto de alto nivel dirigido a aprovechar el asesoramiento de expertos en gestión de riesgos específicos de cada sector y proporcionar información holística para alcanzar el más alto nivel de rendimiento del sistema a un nivel socialmente aceptable. Más amplia información sobre gestión de riesgos de seguridad operacional, dentro del alcance del presente manual, figura en los Capítulos 2, 8 (para Estados) y 9 (para proveedores de servicios).

Nota.— La estructura y las áreas de responsabilidad del gobierno dentro del Estado pueden afectar la vigilancia de cada área. Por ejemplo, la autoridad de aviación civil (CAA) es responsable de la seguridad operacional de la aviación, mientras que el órgano de protección del medio ambiente es responsable de la vigilancia ambiental. Cada entidad de vigilancia puede tener diferentes requisitos y metodologías.

———————

Capítulo 2

FUNDAMENTOS DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

2.1 EL CONCEPTO DE SEGURIDAD OPERACIONAL Y SU EVOLUCIÓN

2.1.1 Este capítulo proporciona una descripción general de los conceptos y prácticas fundamentales de la gestión de la seguridad operacional. Es importante comprender estos fundamentos antes de concentrarse en los aspectos específicos de la gestión de la seguridad operacional que figuran en los capítulos posteriores.

2.1.2 Dentro del contexto de la aviación, la seguridad operacional es “el estado en el que los riesgos asociados a las actividades de aviación relativas a la operación de aeronaves, o que apoyan directamente dicha operación, se reducen y controlan a un nivel aceptable”.

2.1.3 La seguridad operacional de la aviación tiene carácter dinámico. Continuamente surgen nuevos peligros y riesgos de seguridad operacional que deben mitigarse. Siempre y cuando los riesgos de seguridad operacional se mantengan en un nivel de control adecuado, un sistema tan abierto y dinámico como la aviación podrá seguir manteniéndose seguro. Es importante señalar que el nivel aceptable del rendimiento en materia de seguridad operacional está a menudo definido e influenciado por las normas y la cultura, tanto nacionales como internacionales.

2.1.4 El progreso en materia de seguridad operacional de la aviación puede describirse mediante cuatro enfoques, que a grandes rasgos corresponden a épocas de actividad. Dichos enfoques se indican a continuación y se ilustran en la Figura 2-1.

a) *Técnico* — Desde principios de la década de 1900 hasta fines de la década de 1960, la aviación surgió con una forma de transporte en masa, en la cual las deficiencias identificadas se relacionaban inicialmente con factores técnicos y fallas tecnológicas. El enfoque de las actividades de seguridad operacional fue, por tanto, orientado a la investigación y mejora de los factores técnicos (por ejemplo, las aeronaves). Para la década de 1950, las mejoras tecnológicas generaron una reducción gradual de la frecuencia de accidentes y los progresos de seguridad operacional se ampliaron para abarcar el cumplimiento reglamentario y la vigilancia.

b) *Factores humanos* — A principios de la década de 1970, la frecuencia de los accidentes de aviación se vio significativamente reducida gracias a los avances tecnológicos y a las mejoras de los reglamentos de seguridad operacional. La aviación se convirtió en un modo de transporte más seguro y el enfoque de las actividades de seguridad operacional se extendió para incluir problemas de factores humanos como la “interfaz hombre-máquina”. A pesar de la inversión de recursos en la mitigación de errores, el desempeño humano seguía citándose como el factor recurrente en los accidentes. El aspecto de factores humanos tendía a centrarse en la persona, sin considerar plenamente el contexto operacional e institucional. No fue sino hasta principios de la década de 1990 que se reconoció por primera vez que las personas operan en un entorno complejo, que incluye múltiples factores que tienen el potencial de afectar la conducta humana.

c) *Institucional* — Desde mediados de la década de 1990 hasta el fin del siglo, la seguridad operacional comenzó a verse desde una perspectiva sistémica que consistía en abordar los factores institucionales además de los factores humanos y técnicos. Se introdujo la noción de “accidente institucional”. Esta perspectiva consideraba el impacto de la cultura y las políticas institucionales

sobre la eficacia de los controles de riesgos de seguridad operacional. Además, el acopio y análisis rutinarios de datos de seguridad operacional aplicando metodologías reactivas y proactivas permitió a las organizaciones controlar los riesgos de seguridad operacional conocidos y detectar problemas de seguridad operacional emergentes. Estas mejoras proporcionaron los conocimientos y los fundamentos que permitieron avanzar hacia el enfoque actual de la gestión de la seguridad operacional.

d) *Sistema total* — Desde principios del siglo XXI, muchos Estados y proveedores de servicios habían adoptado los enfoques de seguridad operacional del pasado y evolucionado hacia niveles más elevados de desarrollo de la seguridad. Habían comenzado a implementar SSP o SMS y están ahora cosechando los beneficios de seguridad operacional. No obstante, hasta la fecha los sistemas de seguridad operacional se han concentrado principalmente en el rendimiento individual en materia de seguridad operacional y en el control local, con mínima consideración del contexto más amplio del sistema aeronáutico total. Esto ha llevado al creciente reconocimiento del carácter complejo del sistema de aviación y, por parte de las diferentes organizaciones, de que todas desempeñan un papel en la seguridad operacional de la aviación. Hay muchos ejemplos de accidentes e incidentes que indican que las interfaces entre organizaciones han contribuido a resultados negativos.

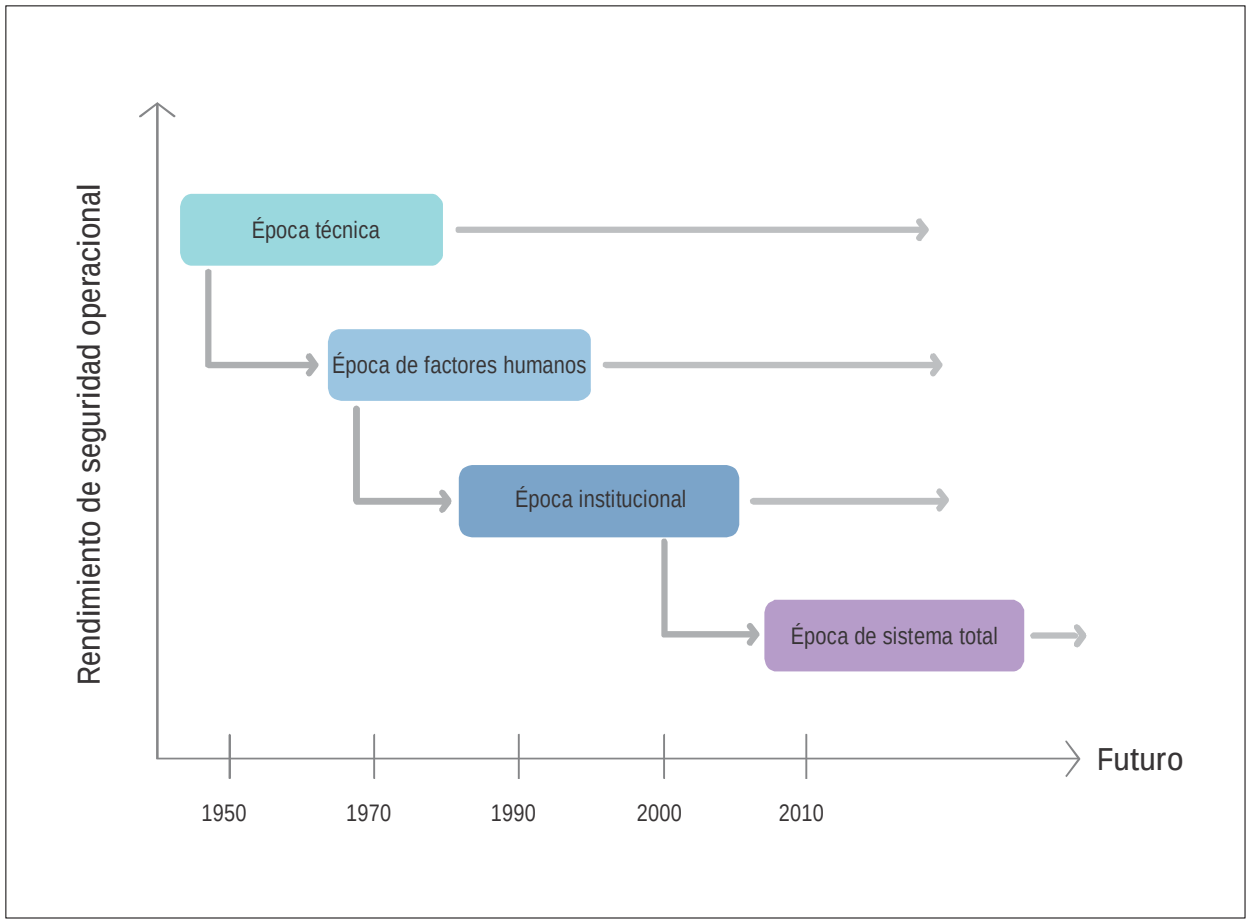


Figura 2-1. Evolución de la seguridad operacional

2.1.5 La evolución constante y complicada de la seguridad operacional ha llevado a los Estados y proveedores de servicios a un punto en el que están prestando seria consideración a las interacciones e interfaces entre los componentes del sistema: las personas, los procesos y las tecnologías. Esto ha conducido a un mayor reconocimiento de la función positiva que las personas desempeñen en el sistema. La colaboración entre los proveedores de servicios y entre éstos y los Estados trae aparejados beneficios en materia de seguridad operacional. Esta perspectiva ha alimentado a muchas iniciativas de colaboración entre proveedores de servicios y ha llevado al reconocimiento de los beneficios de la colaboración cuando se trata de problemas de seguridad operacional. Un buen ejemplo de ello es el Programa de seguridad operacional en la pista, de la OACI.

2.1.6 Para que el enfoque de sistema total en colaboración tenga éxito, deben comprenderse y gestionarse plenamente las interfaces e interacciones entre las organizaciones (incluidos los Estados). Los Estados también han comenzado a reconocer la función que puede desempeñar el enfoque de sistema total de la aviación en el desarrollo de sus SSP. Por ejemplo, dicho enfoque contribuye a gestionar los riesgos de seguridad operacional que abarcan varias actividades aeronáuticas.

2.2 LOS SERES HUMANOS EN EL SISTEMA

2.2.1 La forma en que las personas piensan acerca de sus responsabilidades con respecto a la seguridad operacional y la forma en que interactúan mutuamente para realizar sus tareas afectan considerablemente el rendimiento de la organización en materia de seguridad operacional. La gestión de la seguridad operacional debe abordar la forma en que las personas contribuyen, tanto positiva como negativamente, a la seguridad operacional de la organización. El aspecto factores humanos se refiere a comprender las formas en que las personas interactúan con el mundo, sus capacidades y limitaciones, e influir en la actividad humana para mejorar la forma en que las personas trabajan. Como resultado, la consideración de los factores humanos es parte integral de la gestión de la seguridad operacional, necesaria para comprender, identificar y mitigar riesgos así como para optimizar las contribuciones humanas a la seguridad operacional de la organización.

2.2.2 Las siguientes son maneras fundamentales en las que los procesos de gestión de la seguridad operacional consideran a los factores humanos:

a) compromiso de la administración superior para crear un entorno laboral que optimice el desempeño humano y aliente al personal a participar activamente y contribuir en los procesos de gestión de la seguridad operacional de la organización;

b) las responsabilidades del personal con respecto a la gestión de la seguridad operacional se aclaran para asegurar una comprensión y expectativas comunes;

c) la organización proporciona al personal información que:

   1) describe los comportamientos esperados con respecto a los procesos y procedimientos institucionales;

   2) describe las medidas que ha de adoptar la organización en respuesta a los comportamientos individuales;

d) los niveles de recursos humanos se vigilan y ajustan para asegurar que se cuenta con personal suficiente para satisfacer las demandas operacionales;

e) se establecen políticas, procesos y procedimientos para fomentar las notificaciones de seguridad operacional;

f) se analizan los datos de seguridad operacional y la información sobre seguridad operacional para permitir la consideración de los riesgos relacionados con el variable desempeño humano y las limitaciones humanas, con atención particular a los factores institucionales y operacionales conexos;

g) se elaboran políticas, procesos y procedimientos claros, concisos y viables, con miras a:

1) optimizar el desempeño humano;

2) prevenir errores involuntarios;

3) reducir las consecuencias no deseadas del variable desempeño humano; la eficacia de esto se vigila continuamente durante las operaciones normales;

h) la observación continua de las operaciones normales comprende la evaluación de si se aplican procesos y procedimientos y, cuando estos no se siguen, se realizan investigaciones para determinar la causa de ello;

i) las investigaciones de seguridad operacional comprenden la evaluación de los factores humanos contribuyentes, examinando no solamente comportamientos sino las razones de los mismos (contexto), en el entendido de que en la mayoría de los casos las personas tratan al máximo de realizar su trabajo;

j) el proceso de gestión de cambios incluye la consideración de la evolución de tareas y funciones de los seres humanos en el sistema;

k) el personal se capacita para asegurar su competencia en la ejecución de sus funciones, se examina la eficacia de la instrucción y se adaptan los programas de instrucción para satisfacer las necesidades cambiantes.

2.2.3 La eficacia de la gestión de la seguridad operacional depende en gran medida del grado de apoyo y del compromiso de la administración superior en cuanto a la creación de un entorno laboral que optimice el desempeño humano y aliente al personal a participar activamente y contribuir en los procesos de gestión de la seguridad operacional de la organización.

2.2.4 Para abordar la forma en que la organización influye en el desempeño humano debe existir un apoyo de alto nivel para implementar una gestión eficaz de la seguridad operacional. Esto comprende el compromiso de la administración para crear un entorno laboral correcto y una cultura de seguridad operacional correcta que tenga en cuenta los factores humanos. Esto también influirá en las actitudes y comportamientos de todas las personas en la organización. En el Capítulo 3 figura más información sobre la cultura de seguridad operacional.

2.2.5 Se han creado varios modelos para apoyar la evaluación de los factores humanos respecto del rendimiento de la seguridad operacional. El modelo SHELL es bien conocido y resulta útil para ilustrar el impacto y la interacción de los diferentes componentes del sistema con respecto a los seres humanos y hace hincapié en la necesidad de considerar a los factores humanos como parte integral de la SRM.

2.2.6 En la Figura 2-2 se ilustra la relación entre las personas (en el centro del modelo) y los componentes del lugar de trabajo. El modelo SHELL contiene los siguientes cuatro componentes:

a) soporte lógico (software-S): procedimientos, capacitación, asistencia técnica, etc.;

b) soporte físico (hardware-H): máquinas y equipo;

c) entorno (environment-E): el entorno laboral donde debe funcionar el resto del sistema L-H-S; y

d) elemento humano (liveware-L): otras personas en el lugar de trabajo.



Figura 2-2. Modelo SHELL

2.2.7 *Elemento humano*. En el centro del modelo SHELL se encuentran las personas en la primera línea de operaciones. No obstante, de todas las dimensiones del modelo, esta es la menos predecible y más susceptible a los efectos de influencias internas (hambre, fatiga, motivación, etc.) y externas (temperatura, iluminación, ruido, etc.). Aunque las personas son increíblemente adaptables, están sujetas a importantes variaciones del rendimiento. Los seres humanos no están estandarizados al mismo grado que el soporte físico, así que los bordes de este bloque no son simples ni rectos. Los efectos de las irregularidades en las interfaces entre los diversos bloques SHELL y el bloque central Elemento humano se deben entender para evitar tensiones que puedan comprometer el desempeño humano. Los bordes irregulares de los módulos representan el acoplamiento imperfecto de cada módulo. Esto resulta útil para visualizar las siguientes interfaces entre los diversos componentes del sistema de aviación:

a) *Elemento humano-soporte físico (L-H)*. La interfaz L-H hace referencia a la relación entre la persona y los atributos físicos del equipo, máquinas e instalaciones. Esto considera los aspectos ergonómicos de la operación del equipo por el personal, la forma en que se presenta la información de seguridad operacional y la forma en que se indican y operan los conmutadores y las palancas para que su funcionamiento resulte lógico e intuitivo.

b) *Elemento humano-soporte lógico (L-S)*. La interfaz L-S es la relación entre la persona y los sistemas de apoyo que se encuentran en el lugar de trabajo, por ejemplo, reglamentos, manuales, listas de verificación, publicaciones, procesos y procedimientos, y soporte lógico de computadora. Incluye temas tales como la experiencia reciente, precisión, formato y presentación, vocabulario, claridad y simbología. La interfaz L-S considera los procesos y procedimientos y la facilidad de comprenderlos y aplicarlos.

c) *Elemento humano-elemento humano (L-L)*. La interfaz L-L es la relación entre personas en el mismo entorno de trabajo. Algunas de estas interacciones corresponden al interior de la organización (colegas, supervisores, administradores), muchas otras se dan entre individuos de diferentes organizaciones con diferentes funciones (controladores de tránsito aéreo con pilotos, pilotos con mecánicos, etc.). En ella se considera la importancia de la comunicación y las habilidades interpersonales, así como la dinámica de grupo, para determinar la actuación humana.

El advenimiento de la gestión de recursos de tripulación y su ampliación a los servicios de tránsito aéreo (ATS) y operaciones de mantenimiento ha permitido a las organizaciones considerar el desempeño en equipo en la gestión de errores. También dentro del alcance de esta interfaz están las relaciones entre personal y administración así como la cultura institucional general.

d) *Elemento humano-entorno (L-E)*. Esta interfaz involucra la relación entre las personas y el entorno físico. Esto comprende aspectos como la temperatura, la luz ambiental, el ruido, las vibraciones y la calidad del aire. También considera factores del entorno externo, como las condiciones meteorológicas, la infraestructura y el terreno.

2.3 CAUSALIDAD DE ACCIDENTES

2.3.1 El modelo de “queso suizo” (o modelo de Reason), desarrollado por el profesor James Reason y bien conocido en la industria de la aviación, ilustra que los accidentes entrañan penetraciones sucesivas de múltiples defensas del sistema. Estas penetraciones o brtechas pueden generarse por muchos factores como fallas de los equipos o errores operacionales. El modelo de queso suizo sostiene que los sistemas complejos, como los de la aviación, están muy bien protegidos con capas de defensas (conocidas también como “barreras”). Las fallas de un solo punto rara vez traen consecuencias. Las brechas en las defensas de seguridad pueden ser una consecuencia atrasada de las decisiones tomadas en los niveles más altos de la organización, las que pueden permanecer latentes hasta que sus efectos o potencial de daño se activen por determinadas condiciones operacionales (conocidas como condiciones latentes). Bajo dichas circunstancias, las fallas humanas (o “fallas activas”), a nivel operacional actúan para violar las capas finales de la defensa de seguridad. El modelo de Reason propone que todos los accidentes incluyen una combinación de fallas activas y condiciones latentes.

2.3.2 Las fallas activas son medidas tomadas o no tomadas, como errores e infracciones, que tienen efectos adversos inmediatos. Por lo general, gracias a la retrospectiva, se consideran medidas inseguras. Las fallas activas se asocian normalmente con el personal de primera línea (pilotos, controladores de tránsito aéreo, mecánicos de mantenimiento de aeronaves, etc.) y pueden producir resultados perjudiciales.

2.3.3 Las condiciones latentes pueden existir mucho antes de que se experimente un resultado dañino. Las consecuencias de las condiciones latentes pueden permanecer ocultas por mucho tiempo. Inicialmente, estas condiciones latentes no se perciben como perjudiciales, pero serán evidentes luego de la violación de las defensas del sistema. Personas muy lejanas en tiempo y espacio del suceso pueden crear dichas condiciones. Las condiciones latentes en el sistema pueden incluir aquellas generadas por la falta de cultura de seguridad operacional, elecciones en cuanto a equipo o diseño de procedimientos, metas institucionales en conflicto, sistemas institucionales defectuosos o decisiones de la administración.

2.3.4 El paradigma de “accidente institucional” ayuda a minimizar fallas activas de individuos mediante la identificación de estas condiciones latentes en todo el sistema en vez de la realización de esfuerzos localizados. Es importante destacar que las condiciones latentes, cuando son creadas, normalmente tienen buenas intenciones. Los encargados de tomar decisiones en la organización a menudo tienen que equilibrar recursos finitos y prioridades y costos potencialmente conflictivos. Las decisiones adoptadas, normalmente a diario en las grandes organizaciones, podría, en circunstancias particulares, conducir involuntariamente a resultados perjudiciales.

2.3.5 En la Figura 2-3 se ilustra como el modelo del queso suizo ayuda a comprender la interacción de los factores institucionales y de gestión en la causalidad de accidentes. Allí se ilustra que varias defensas están incorporadas en el sistema de aviación para protegerlo contra variaciones en las decisiones o rendimientos humanos en todos los niveles del sistema. Pero normalmente cada capa de defensa presenta puntos débiles, indicados por los agujeros de las rebanadas de “queso suizo”. A veces todos los puntos débiles están alineados (representados por los agujeros alineados) conduciendo a una ruptura o brecha que penetra todas las barreras defensivas y puede provocar un resultado catastrófico. El modelo de queso suizo representa la forma en que las condiciones latentes siempre están presentes dentro del sistema y pueden manifestarse mediante factores activadores locales.

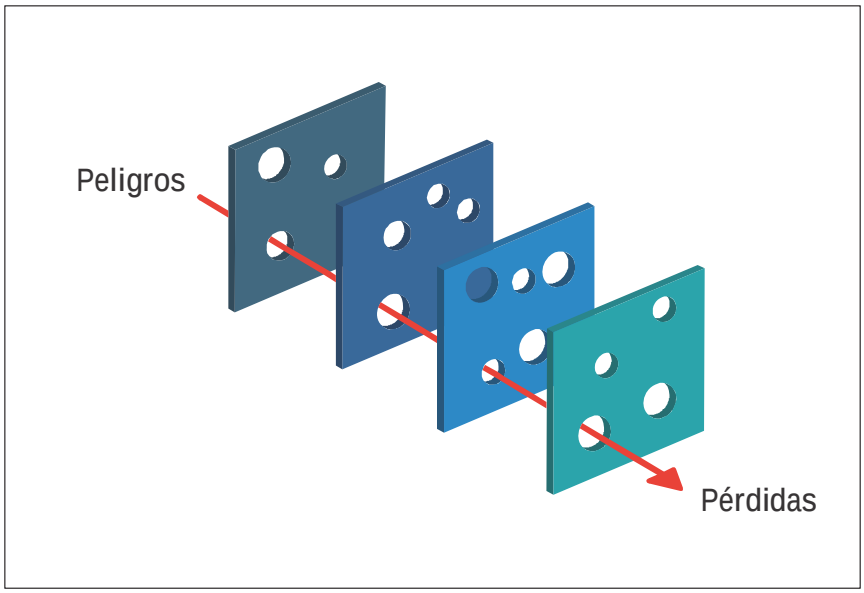


Figura 2-3. Concepto de causalidad de accidentes

2.3.6 Es importante reconocer que algunas de las defensas, o de las brechas, pueden estar influenciadas por una organización interactuante (en interfaz). Por lo tanto, es muy importante que los proveedores de servicios evalúen y gestionen dichas interfaces.

2.3.7 Aplicaciones del modelo "queso suizo" a la gestión de la seguridad operacional

2.3.7.1 El modelo de "queso suizo" puede utilizarse como guía de análisis tanto por los Estados como por los proveedores de servicios examinando más allá de los individuos involucrados en un incidente o peligro identificado, para determinar las circunstancias institucionales que pueden haber permitido que se manifestara la situación en cuestión. Puede aplicarse durante la SRM, la supervisión de la seguridad operacional, auditorías internas, gestión de cambios e investigaciones de seguridad operacional. En cada caso, el modelo puede aplicarse para considerar cuáles de las defensas de la organización son en verdad eficaces, cuáles podrían penetrarse o haberse penetrado y cómo podría beneficiarse el sistema mediante defensas adicionales. Una vez identificadas, cualesquiera debilidades en las defensas podrían reforzarse para proteger contra futuros accidentes a incidentes.

2.3.7.2 En la práctica, el suceso de que se trate penetrará las defensas en la dirección de la flecha (peligros a pérdida) según se muestra en la Figura 2-3. Las evaluaciones de la situación se realizarán en sentido opuesto, en este caso de pérdidas a peligros. Los accidentes de aviación reales normalmente comprenderán un cierto grado de complejidad adicional. Hay modelos más perfeccionados que pueden ayudar a Estados y proveedores de servicios a comprender cómo y por qué suceden los accidentes.

2.3.8 La desviación de la práctica

2.3.8.1 La teoría de Scott A. Snook sobre la desviación de la práctica se utiliza para comprender cómo la actuación de cualquier sistema se "desvía" respecto de su diseño original. Con frecuencia, las tareas, procedimientos y equipo se diseñan y planifican inicialmente en un entorno teórico, en condiciones ideales, con la hipótesis implícita de que casi todo puede predecirse y controlarse y que todo funciona según lo previsto. Normalmente esto se basa en tres suposiciones fundamentales, a saber:

a) está disponible la tecnología necesaria para lograr las metas de producción del sistema;

b) las personas están capacitadas, son competentes y están motivadas para operar correctamente la tecnología, según lo previsto; y

c) reglamentos y procedimientos indicarán el comportamiento humano y del sistema.

Estas suposiciones son el trasfondo del rendimiento del sistema base (o ideal), y pueden representarse gráficamente como una línea recta a partir de la fecha de implantación operacional, como se muestra en la Figura 2-4.

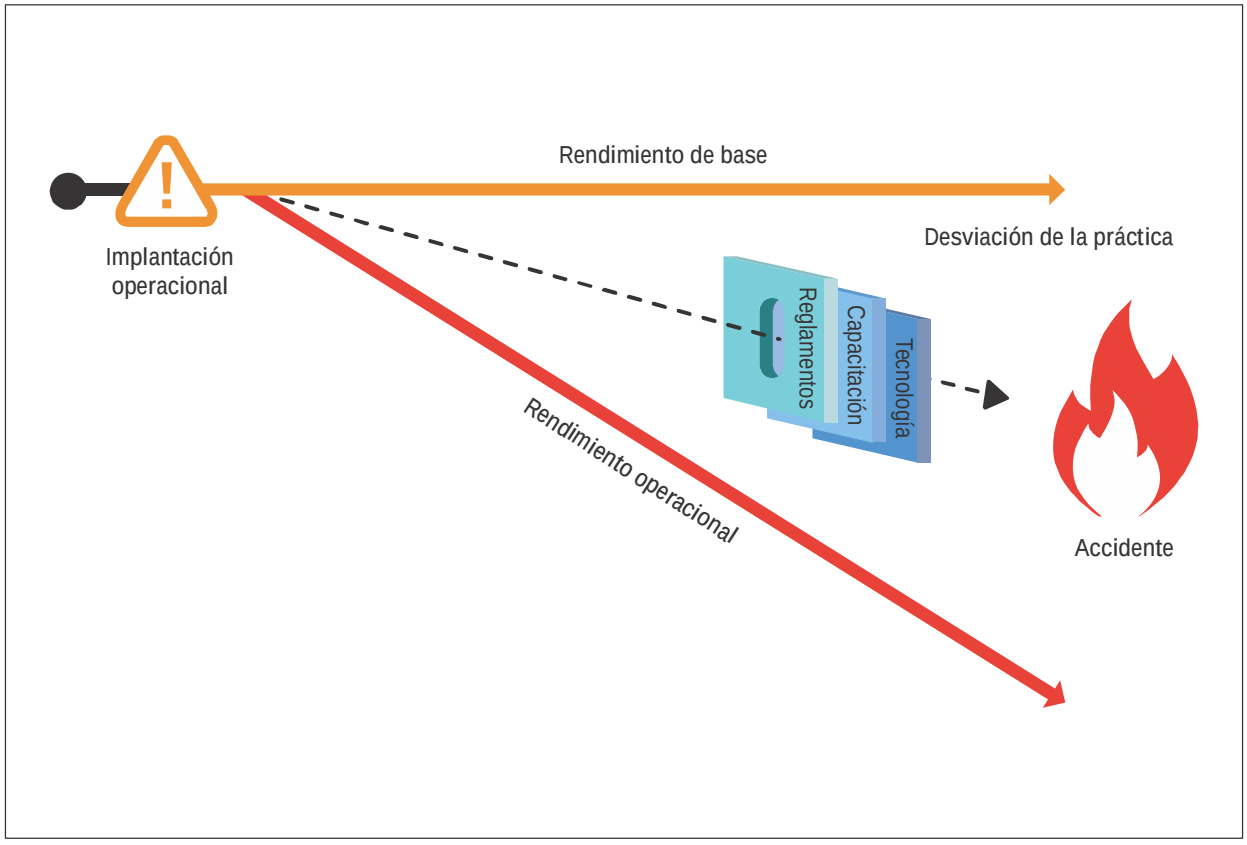


Figura 2-4. Concepto de desviación de la práctica

2.3.8.2 Una vez implantado operacionalmente, el sistema debería actuar idealmente según el diseño, siguiendo el rendimiento de base (línea naranja) la mayor parte del tiempo. En realidad, el rendimiento operacional es diferente del rendimiento de base, como consecuencia de las operaciones en un entorno complejo, siempre cambiante y normalmente exigente (línea roja). Dado que la desviación es una consecuencia de la práctica diaria, se le conoce como "desviación de la práctica". El término "desviación" se refiere en este contexto al alejamiento gradual desde un curso definido debido a influencias externas.

2.3.8.3 Snook afirma que la desviación de la práctica es inevitable en cualquier sistema, sin importar cuan cuidadosa y bien pensada haya sido la planificación del diseño. Los siguientes son algunos de los motivos de la desviación de la práctica:

a) tecnología que no siempre funciona como se predice;

b) procedimientos que no pueden ejecutarse según lo planificado bajo ciertas condiciones operacionales;

c) introducción de cambios al sistema, como la adición de nuevos componentes;

d) interacciones con otros sistemas;

e) cultura de seguridad operacional;

f) adecuación (o inadecuación) de los recursos (p. ej., equipo de apoyo);

g) enseñanzas obtenidas de éxitos y fallas para mejorar las operaciones, y así sucesivamente.

2.3.8.4 En realidad, a pesar de las deficiencias del sistema, las personas harán que el sistema funcione diariamente, aplicando adaptaciones (o soluciones) locales y estrategias personales. Estas soluciones pueden sortear o circunvalar la protección de controles de riesgo de seguridad operacional y defensas correspondientes existentes.

2.3.8.5 Las actividades de aseguramiento de la seguridad operacional, como auditorías, observaciones y vigilancia de los SPI pueden contribuir a revelar comportamientos que se desvían de la práctica. El análisis de la información sobre seguridad operacional para determinar las razones de dicha desviación contribuye a mitigar los riesgos de seguridad operacional. Cuanto más cerca del inicio de la implantación operacional se identifique la desviación de la práctica, más fácil será para la organización llevar a cabo una intervención. En los Capítulos 8 y 9, respectivamente, figura más información sobre aseguramiento de la seguridad operacional para Estados y proveedores de servicios.

2.4 EL DILEMA DE LA GESTIÓN

2.4.1 En una organización comprometida con el suministro de servicios, los riesgos de producción/rentabilidad y seguridad operacional están vinculados. Una organización debe mantener su rentabilidad para continuar funcionando mediante el equilibrio de la producción con riesgos de seguridad operacional aceptables (y los costos involucrados en la aplicación de controles de riesgos de seguridad operacional). Los controles de riesgos de seguridad operacional típicos son la tecnología, la instrucción, los procesos y los procedimientos. Para el Estado, los controles de riesgos de seguridad operacional son similares, es decir, la instrucción del personal, el uso adecuado de la tecnología, la vigilancia eficaz y los procesos y procedimientos internos que respaldan la vigilancia. La implementación de los controles de riesgos de seguridad operacional tiene un precio – dinero, tiempo, recursos – y el objetivo de los controles de riesgos de seguridad operacional es normalmente el mejoramiento del rendimiento en materia de seguridad operacional, y no el rendimiento en cuanto a la producción. No obstante, algunas inversiones en "protección" también pueden mejorar la "producción" mediante la reducción de accidentes e incidentes y, con ello, sus costos conexos.

2.4.2 El espacio de seguridad operacional es una metáfora para la zona donde una organización equilibra la producción y la rentabilidad deseadas manteniendo al mismo tiempo la protección de la seguridad operacional necesaria mediante controles de riesgos de seguridad operacional. Por ejemplo, un proveedor de servicios puede querer invertir en equipo nuevo. Este nuevo equipo puede proporcionar simultáneamente las necesarias mejoras de eficiencia así como mayor fiabilidad y rendimiento de seguridad operacional. Esta toma de decisiones entraña una evaluación de las ventajas para la organización así como de los riesgos de seguridad operacional involucrados. La asignación de recursos excesivos para la protección o los controles de riesgos puede causar que la actividad sea poco rentable, lo que pone en peligro la viabilidad de la organización.

2.4.3 Por otro lado, la asignación excesiva de recursos para la producción a expensas de la protección puede tener consecuencias sobre el producto o servicio y, en última instancia, puede producir un accidente. Por lo tanto, es fundamental que se defina un límite de seguridad operacional que proporcione la alerta temprana de la existencia o el desarrollo de una asignación de recursos desequilibrada. Las organizaciones utilizan sistemas de gestión financiera para reconocer cuando se están acercando demasiado a la bancarrota y aplican la misma lógica y herramientas empleadas en la gestión de la seguridad operacional para observar su rendimiento en materia de seguridad operacional. Esto permite que la organización funcione en forma rentable y segura dentro del espacio de seguridad operacional. En la Figura 2-5 se presenta una ilustración de los límites del espacio de seguridad operacional de una organización. Las organizaciones deben observar y gestionar continuamente su espacio de seguridad operacional dado que los riesgos de seguridad y las influencias externas cambian con el tiempo.

2.4.4 La necesidad de equilibrar la rentabilidad y la seguridad operacional (o la producción y protección) se ha convertido en un requisito fácilmente comprendido y aceptado desde la perspectiva del proveedor de servicios. Este equilibrio es igualmente aplicable a la gestión de la seguridad operacional por el Estado, dado que el requisito de equilibrar los recursos necesarios para las funciones de protección del Estado que incluyen la certificación y la supervisión.

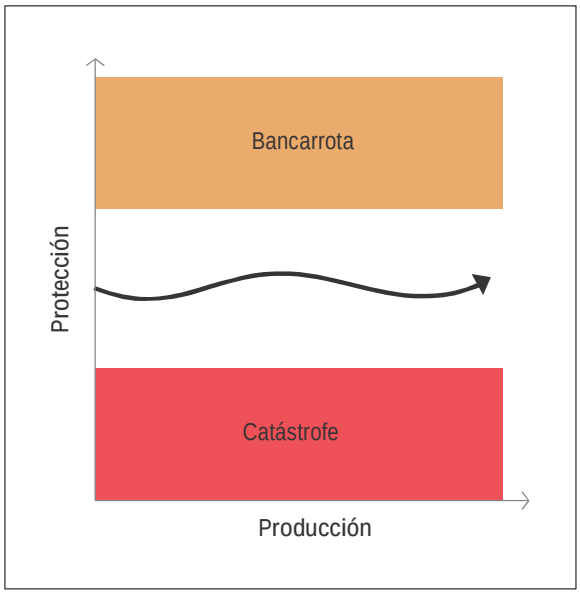


Figura 2-5. Concepto de espacio de seguridad operacional

2.5 GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

La gestión de riesgos de seguridad operacional (SRM) es un componente fundamental de la gestión de la seguridad operacional y comprende la identificación de peligros, la evaluación de riesgos de seguridad operacional, la mitigación de dichos riesgos y la aceptación de los mismos. La SRM es una actividad continua debido a que el sistema de aviación cambia constantemente, pueden introducirse nuevos peligros y algunos peligros y riesgos de seguridad operacional conexos pueden cambiar con el tiempo. Además, la eficacia de las estrategias de mitigación de riesgos de seguridad operacional implementadas debe vigilarse para determinar si se requieren ulteriores medidas.

2.5.1 Introducción a los peligros

2.5.1.1 En la aviación, los peligros pueden considerarse como la posibilidad latente de que ocurran daños que está siempre presente en una forma u otra en el sistema o su entorno. Este potencial de daño puede aparecer en formas diferentes, por ejemplo como una condición natural (p. ej., terreno) o un aspecto técnico (p. ej., señalización de las pistas).

2.5.1.2 Los peligros constituyen una parte inevitable de las actividades aeronáuticas, pero su manifestación y posibles consecuencias adversas pueden abordarse mediante estrategias de mitigación que apuntan a contener la posibilidad de que el peligro conduzca a una condición insegura. La aviación puede coexistir con los peligros en la medida en que estos estén controlados. La identificación de peligros es el primer paso en el proceso SRM. Precede a la evaluación de los riesgos de seguridad operacional y requiere una clara comprensión de los peligros y sus consecuencias conexas.

2.5.2 Comprensión de los peligros y sus consecuencias

2.5.2.1 La identificación de los peligros se centra en las condiciones u objetos que podrían provocar o contribuir a la operación insegura de las aeronaves o del equipo relacionado con la seguridad operacional de la aviación, así como sus productos y servicios (en los párrafos siguientes se presenta orientación sobre la distinción de peligros directamente pertinentes a la seguridad operacional de la aviación respecto de otros peligros generales o industriales).

2.5.2.2 Por ejemplo, considérese un viento de quince kt, lo que no es necesariamente una condición peligrosa. De hecho, un viento de 15 kt que sopla directamente a lo largo de la pista mejora el despegue de la aeronave y la performance de aterrizaje. Pero si el viento de 15 kt sopla en una dirección perpendicular a la pista, se genera una condición de viento de costado o transversal que puede resultar peligrosa para las operaciones. Esto se debe a su potencial de contribuir a la inestabilidad de la aeronave. La reducción del control podría conducir a un incidente, como una salida de pista lateral.

2.5.2.3 Existe una tendencia común de confundir los peligros con sus consecuencias. Una consecuencia es un resultado que puede ser activado por un peligro. Por ejemplo, una salida de pista (aterrizaje largo) es una consecuencia posible relacionada con el peligro de una pista contaminada. Al definir claramente el peligro primero, se puede identificar más prontamente las posibles consecuencias.

2.5.2.4 En el ejemplo de viento de costado anterior, un resultado inmediato del peligro sería la pérdida de control lateral seguida de una posterior salida de la pista. La consecuencia final podría ser un accidente. El potencial de daño de un peligro se materializa mediante una o muchas consecuencias. Es importante que las evaluaciones de los riesgos de seguridad operacional identifiquen todas las consecuencias posibles. Las consecuencias más extremas, como la pérdida de vidas humanas, deberían diferenciarse de las que tienen carácter más leve, como los incidentes de aeronaves, el aumento de la carga de trabajo de la tripulación de vuelo o la incomodidad de los pasajeros. La descripción de las consecuencias facilita la evaluación de los riesgos y el ulterior desarrollo e implementación de estrategias de mitigación mediante la priorización y asignación de recursos. Una identificación de peligros adecuada genera una evaluación más precisa de los riesgos de seguridad operacional.

Identificación y priorización de peligros

2.5.2.5 Los peligros existen en todos los niveles de la organización y son detectables a partir de muchas fuentes como los sistemas de notificación, inspecciones, auditorías, reuniones de intercambio de ideas y opiniones de expertos. El objetivo es identificar en forma proactiva los peligros antes de que produzcan accidentes, incidentes u otros sucesos relacionados con la seguridad operacional. Un mecanismo importante para la identificación proactiva de peligros es un sistema de notificación voluntaria de seguridad operacional. En el Capítulo 5 figura orientación adicional sobre los sistemas de notificación voluntaria. La información recogida mediante tales sistemas puede complementarse con las observaciones o constataciones registradas durante inspecciones de rutina en el sitio o las auditorías de la organización.

2.5.2.6 Los peligros también pueden identificarse a partir de la revisión o el estudio de los informes de investigaciones tanto internas como externas. La consideración de los peligros al examinar informes de investigaciones de accidentes o incidentes es una buena manera de mejorar el sistema de identificación de peligros de la organización. Esto es particularmente importante cuando la cultura de seguridad operacional de la organización no está lo suficientemente madura como para respaldar un sistema de notificación voluntaria de peligros eficaz o en pequeñas organizaciones con sucesos o informes limitados. Una forma importante de obtener información sobre peligros específicos relacionados con operaciones y actividades es recurrir a fuentes externas como la OACI, asociaciones comerciales u otros órganos internacionales.

2.5.2.7 La identificación de peligros también puede considerar peligros generados fuera de la organización y peligros que escapan al control directo de la organización, como las condiciones meteorológicas extremas o las cenizas volcánicas. El conocimiento de peligros relacionados con los riesgos de seguridad operacional emergentes constituye también un aspecto importante para que las organizaciones puedan prepararse a fin de enfrentar situaciones que puedan ocurrir.

2.5.2.8 Al identificar peligros debería tenerse en cuenta lo siguiente:

a) descripción del sistema;

b) factores de diseño, incluyendo diseño de equipo y tareas;

c) limitaciones de la actuación humana (p. ej., fisiológicas, sicológicas, físicas y cognitivas);

d) procedimientos y prácticas operacionales, incluyendo documentación y listas de verificación y su validación en condiciones de operación reales;

e) factores de comunicación, incluyendo los medios de difusión, terminología e idioma;

f) factores institucionales, como los relacionados con la contratación, instrucción y retención de personal, compatibilidad de los objetivos de producción y de seguridad operacional, asignación de recursos, presiones de operación y cultura de seguridad operacional corporativa;

g) factores relacionados con el entorno operacional (p. ej., condiciones meteorológicas, ruido y vibraciones ambientales, temperatura e iluminación);

h) factores de vigilancia normativa, incluyendo la aplicación e imposición del cumplimiento de reglamentos así como la certificación de equipo, personal y procedimientos;

i) sistemas de observación del rendimiento que puedan detectar desviaciones de la práctica, desviaciones operacionales o un deterioro de la fiabilidad del producto;

j) factores de la interfaz humano-máquina; y

k) factores relacionados con las interfaces SSP/SMS con otras organizaciones.

Peligros de seguridad, salud y ambiente en el trabajo (OSHE)

2.5.2.9 Los riesgos de seguridad operacional asociados con peligros combinados, que tienen un impacto simultáneo en la seguridad operacional de la aviación, además de OSHE, pueden gestionarse en forma separada (paralela) mediante procesos de mitigación de riesgos con el fin de abordar las consecuencias separadas de la aviación y OSHE, respectivamente. O bien, se puede usar un sistema integrado de mitigación de riesgos de aviación y OSHE para abordar tales peligros combinados. Un ejemplo de peligro combinado es un rayo que impacta en una aeronave en la puerta de tránsito de un aeropuerto. Un inspector de OSHE podría considerar este peligro como "peligro en el lugar de trabajo" (seguridad operacional del personal de tierra/lugar de trabajo). Para un inspector de la seguridad operacional de la aviación, es también un peligro de aviación con el riesgo de dañar la aeronave y la seguridad de los pasajeros. Es importante considerar tanto las consecuencias para OSHE y para la seguridad operacional de la aviación de tales peligros combinados, dado que no son siempre las mismas. El propósito y enfoque de los controles preventivos para OSHE y para las consecuencias de seguridad operacional de la aviación pueden ser diferentes.

Metodologías de identificación de peligros

2.5.2.10 Las dos metodologías principales para identificar peligros son:

a) *Reactiva*. Esta metodología involucra el análisis de resultados o sucesos pasados. Los peligros se identifican mediante la investigación de sucesos de seguridad operacional. Los incidentes y accidentes son indicadores de deficiencias del sistema y, por lo tanto, pueden usarse para determinar los peligros que contribuyeron al suceso.

b) *Proactiva*. Esta metodología involucra el acopio de datos de seguridad de sucesos de consecuencias más leves o de rendimiento de procesos y el análisis de la información de seguridad operacional o de la frecuencia de los sucesos para determinar si un peligro podría conducir a un accidente o incidente. La información sobre seguridad operacional para la identificación proactiva de peligros procede principalmente de programas de análisis de datos de vuelo (FDA), sistemas de notificación de seguridad operacional y de la función de aseguramiento de la seguridad operacional.

2.5.2.11 Los peligros también pueden identificarse mediante análisis de datos de seguridad operacional que identifiquen tendencias adversas y permitan predecir posibles peligros emergentes, etc.

Peligros relacionados con interfaces del SMS con organizaciones externas

2.5.2.12 Las organizaciones deberían también identificar peligros relacionados con sus interfaces de gestión de la seguridad operacional. Siempre que sea posible, esto debería llevarse a cabo como actividad conjunta con las organizaciones interconectadas (en interfaz). La identificación de peligros debería considerar el entorno operacional y las diversas capacidades institucionales (personas, procesos, tecnologías) que podrían contribuir a la prestación segura del servicio o a la disponibilidad, funcionalidad o rendimiento del producto.

2.5.2.13 Como ejemplo, un servicio de escala para una aeronave involucra muchas organizaciones y personal de operaciones que trabajan en la aeronave o en torno a la misma. Probablemente existan peligros relacionados con las interfaces entre el personal de operaciones, su equipo y la coordinación de la actividad del servicio de escala.

2.5.3 Probabilidad del riesgo de seguridad operacional

2.5.3.1 La probabilidad del riesgo de seguridad operacional se define como la probabilidad de que pueda suceder una consecuencia o un resultado de seguridad operacional. Con las siguientes preguntas se puede ayudar a determinar dicha probabilidad:

a) ¿Existe un historial de sucesos similares al que se considera o es este un suceso aislado?

b) ¿Qué otros equipos o componentes del mismo tipo presentan problemas similares?

c) ¿Cuántos miembros del personal siguen los procedimientos en cuestión, o están sujetos a ellos?

d) ¿Cuál es la exposición del peligro que se considera? Por ejemplo, ¿durante qué porcentaje de la operación se utiliza el equipo o se realiza la actividad?

2.5.3.2 Tener en cuenta los posibles factores subyacentes a estas preguntas contribuirá a evaluar la probabilidad de las consecuencias del peligro en cualquier escenario previsible.

2.5.3.3 Un suceso se considera previsible si cualquier persona razonable podría haber esperado que sucediera dicho tipo de suceso en las mismas circunstancias. Es imposible identificar todos los peligros concebibles o teóricamente probables. Por lo tanto, se requiere un buen juicio para determinar un nivel de detalle apropiado en la identificación de los peligros. Los proveedores de servicios deberían actuar con la debida diligencia al identificar peligros importantes y razonablemente previsibles en relación con su producto o servicio.

Nota.— Con respecto al diseño de productos, se tiene la intención de que el término "previsible" corresponda a su uso en los reglamentos, políticas y orientaciones sobre aeronavegabilidad.

2.5.3.4 La Tabla 1 presenta una clasificación típica de la probabilidad de riesgos de seguridad operacional. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un evento o condición inseguros, la descripción de cada categoría y una asignación de valor a cada una. Este ejemplo utiliza términos cualitativos; también pueden definirse términos cuantitativos a efectos de una evaluación más precisa. Esto dependerá de la disponibilidad de datos de seguridad operacional apropiados y del grado de desarrollo de la organización y la operación.

Tabla 1. Tabla de probabilidad de riesgos de seguridad operacional

Probabilidad	*Significado*	*Valor*
Frecuente	Es probable que suceda muchas veces (ha ocurrido frecuentemente)	5
Ocasional	Es probable que suceda algunas veces (ha ocurrido con poca frecuencia)	4
Remoto	Es poco probable que ocurra, pero no imposible (rara vez ha ocurrido)	3
Improbable	Es muy poco probable que ocurra (no se sabe que haya ocurrido)	2
Sumamente improbable	Es casi inconcebible que el suceso ocurra	1

Nota.— Este es solo un ejemplo. El nivel de detalle y complejidad de las tablas y matrices debe adaptarse a las necesidades y complejidades particulares de cada organización. También se debe tener presente que las organizaciones pueden incluir criterios tanto cualitativos como cuantitativos.

2.5.4 Gravedad del riesgo de seguridad operacional

2.5.4.1 Una vez completada la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional teniendo en cuenta las posibles consecuencias relacionadas con el peligro. La gravedad del

riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La clasificación de la gravedad debería tener en cuenta:

a) muertes o lesiones graves que podrían ocurrir como resultado de:

1) encontrarse en la aeronave;

2) tener contacto directo con cualquier parte de la aeronave, incluyendo las que se hayan desprendido de la misma; o

3) exposición directa al chorro de los reactores; y

b) daños:

1) daños o fallas estructurales sufridos por la aeronave que:

i) afecten adversamente la resistencia estructural, performance o características de vuelo de la aeronave;

ii) requerirían normalmente importantes reparaciones o sustituciones del componente afectado;

2) daños sufridos por el equipo de ATS o aeródromo que:

i) afecten adversamente la gestión de la separación de aeronaves; o

ii) afecten adversamente la capacidad de aterrizaje.

2.5.4.2 La evaluación de la gravedad debería considerar todas las posibles consecuencias relacionadas con un peligro, teniendo en cuenta la peor condición previsible. En la Tabla 2 se presenta una clasificación típica de la gravedad del riesgo de seguridad operacional. Comprende cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada una de ellas. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla es solo un ejemplo.

Tabla 2. Ejemplo de gravedad del riesgo de seguridad operacional

Gravedad	*Significado*	*Valor*
Catastrófico	• Aeronave o equipo destruidos • Varias muertes	A
Peligroso	• Gran reducción de los márgenes de seguridad operacional, estrés físico o una carga de trabajo tal que ya no se pueda confiar en que el personal de operaciones realice sus tareas con precisión o por completo • Lesiones graves • Daños importantes al equipo	B
Grave	• Reducción importante de los márgenes de seguridad operacional, reducción en la capacidad del personal de operaciones para tolerar condiciones de operación adversas, como resultado de un aumento en la carga de trabajo o como resultado de condiciones que afecten su eficiencia	C

Gravedad	*Significado*	*Valor*
	• Incidente grave • Lesiones a las personas	
Leve	• Molestias • Limitaciones operacionales • Uso de procedimientos de emergencia • Incidente leve	D
Insignificante	• Pocas consecuencias	E

2.5.5 Tolerabilidad del riesgo de seguridad operacional

2.5.5.1 El índice de riesgo de seguridad operacional se crea mediante la combinación de resultados de las evaluaciones de probabilidad y gravedad. En el ejemplo anterior, se trata de un designador alfanumérico. Las respectivas combinaciones de gravedad/probabilidad se presentan en la matriz de evaluación de riesgos de seguridad operacional de la Tabla 3. Dicha matriz se aplica para determinar la tolerabilidad del riesgo de seguridad operacional. Considérese, por ejemplo, una situación en que la probabilidad del riesgo de seguridad operacional se ha evaluado como ocasional (4), y la gravedad del riesgo de seguridad operacional se ha evaluado como peligrosa (B), la combinación de ambas es el índice de riesgo de seguridad operacional (4B).

Tabla 3. Ejemplo de matriz de riesgos de seguridad operacional

Probabilidad del riesgo de seguridad operacional		*Gravedad del riesgo*				
Probabilidad		*Catastrófico A*	*Peligroso B*	*Importante C*	*Leve D*	*Insignificante E*
Frecuente	5	5A	5B	5C	5D	5E
Ocasional	4	4A	4B	4C	4D	4E
Remoto	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Sumamente improbable	1	1A	1B	1C	1D	1E

Nota.— En la determinación de la tolerabilidad del riesgo de seguridad operacional, deberían tenerse en cuenta la calidad y la fiabilidad de los datos utilizados para la identificación del peligro y la probabilidad del riesgo de seguridad operacional.

2.5.5.2 El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a la matriz de tolerabilidad del riesgo de seguridad operacional que describe — en forma narrativa — los criterios de tolerabilidad para la organización particular. La Tabla 4 es un ejemplo de tabla de tolerabilidad del riesgo de seguridad

operacional. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B corresponde a la categoría de “intolerable”. En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por lo tanto, la organización debería tomar medidas de control de riesgos para reducir:

a) la exposición de la organización a un riesgo en particular, es decir reducir el componente de probabilidad del índice de riesgo a un nivel aceptable;

b) la gravedad de las consecuencias relacionadas con el peligro, es decir, reducir el componente de gravedad del índice de riesgo a un nivel aceptable; o

c) tanto la gravedad como la probabilidad para que el riesgo pueda gestionarse a un nivel aceptable.

2.5.5.3 Los riesgos de seguridad operacional son evaluados en concepto como aceptables, tolerables o intolerables. Los riesgos evaluados que desde un principio estaban identificados en la región intolerable resultan inaceptables bajo todo punto de vista. La probabilidad o gravedad de las consecuencias de los peligros tienen tal magnitud, y sus posibles daños representan tal amenaza para la seguridad operacional, que se requiere una medida de mitigación inmediata o la cancelación de la operación.

Tabla 4. Ejemplo de tabla de tolerabilidad del riesgo de seguridad operacional

Rango del índice de riesgo de seguridad operacional	*Descripción del riesgo*	*Medida recomendada*
5A, 5B, 5C, 4A, 4B, 3A	INTOLERABLE	Tomar medidas inmediatas para mitigar el riesgo o suspender la actividad. Realizar la mitigación de riesgos de seguridad operacional prioritaria para garantizar que haya controles preventivos o adicionales o mejorados para reducir el índice de riesgos al rango tolerable.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1ª	TOLERABLE	Puede tolerarse sobre la base de la mitigación de riesgos de seguridad operacional. Puede necesitar una decisión de gestión para aceptar el riesgo.
3E, 2D, 2E, 1B, 1C, 1D, 1E	ACEPTABLE	Aceptable tal cual. No se necesita una mitigación de riesgos posterior.

2.5.6 Evaluación de riesgos relacionados con factores humanos

2.5.6.1 La consideración de los factores humanos tiene particular importancia en la SRM puesto que las personas pueden ser tanto una fuente como una solución de los riesgos de seguridad operacional, a saber:

a) contribuyendo a un accidente o incidente mediante una actuación variable debido a limitaciones humanas;

b) previendo y adoptando medidas apropiadas para evitar una situación peligrosa: y

c) resolviendo problemas, tomando decisiones y adoptando medidas para mitigar los riesgos.

2.5.6.2 Por consiguiente, es importante involucrar a personas con adecuada experiencia en factores humanos en la identificación, evaluación y mitigación de los riesgos.

2.5.6.3 La SRM requiere que se aborden todos los aspectos de los riesgos de seguridad operacional, incluyendo los relacionados con las personas. La evaluación de los riesgos asociados con el desempeño humano es más compleja que la de los factores de riesgo relacionados con la tecnología y el entorno dado que:

a) el desempeño humano es muy variable, con una amplia gama de influencias interactuantes tanto internas como externas al individuo. Muchos de los efectos de la interacción entre estas influencias son difíciles o imposibles de predecir; y

b) las consecuencias del variable desempeño humano serán diferentes según la tarea que se realice y el contexto de la misma.

2.5.6.4 Lo señalado anteriormente complica la forma en que se determina la probabilidad y la gravedad del riesgo. Por consiguiente, la experiencia en factores humanos es muy valiosa para identificar y evaluar los riesgos de seguridad operacional. [La gestión de la fatiga aplicando procesos SMS se aborda en el *Manual para la supervisión de los enfoques de gestión de la fatiga* (Doc 9966)].

2.5.7 Estrategias de mitigación de riesgos de seguridad operacional

2.5.7.1 La mitigación de riesgos de seguridad operacional se conoce a menudo como control de riesgos de seguridad operacional. Los riesgos de seguridad operacional deberían gestionarse a un nivel aceptable mitigándolos mediante la aplicación de adecuados controles de riesgos de seguridad operacional. Esto debería equilibrarse con respecto al tiempo, costos y dificultades de adoptar medidas para reducir o eliminar el riesgo. El nivel de riesgo de seguridad operacional puede disminuirse mediante la reducción de la gravedad de las posibles consecuencias, la probabilidad de que el suceso ocurra o la reducción de la exposición a ese riesgo de seguridad operacional. Es más sencillo y más común reducir dicha probabilidad que reducir la gravedad.

2.5.7.2 Las mitigaciones de riesgos de seguridad operacional son medidas que resultan a menudo en cambios de los procedimientos operacionales, equipo o infraestructura. Las estrategias de mitigación de riesgo de seguridad operacional corresponden a tres categorías:

a) *Evitar*: Se cancela o evita la operación o actividad debido a que los riesgos de seguridad operacional superan los beneficios de continuarla, eliminado así el riesgo de seguridad operacional en su totalidad.

b) *Reducir*: Se reduce la frecuencia de la operación o actividad o se adoptan medidas para reducir la magnitud de las consecuencias del riesgo.

c) *Segregar*: Se toman medidas para aislar los efectos de las consecuencias del riesgo o se introduce capas redundantes de protección contra los riesgos.

2.5.7.3 La consideración de los factores humanos es parte integral de la identificación de mitigaciones eficaces porque se requiere que las personas apliquen la mitigación o las medidas correctivas o contribuyan a las mismas. Por ejemplo, las mitigaciones pueden incluir el uso de procesos o procedimientos. Sin aportes de las personas que los utilizarán en situaciones del “mundo real” o de individuos con experiencia en factores humanos, los procesos o procedimientos elaborados pueden no ser adecuados al propósito en cuestión y resultar en consecuencias imprevistas. Además, deberían considerarse las limitaciones de la actuación humana como parte de toda mitigación de riesgos de seguridad operacional, desarrollando estrategias de captación de errores para tener en cuenta la variabilidad de dicha actuación. En última instancia, esta importante perspectiva de factores humanos tendrá como resultado mitigaciones más completas y eficaces.

2.5.7.4 Una estrategia de mitigación de riesgos de seguridad operacional puede involucrar uno de los enfoques descritos anteriormente o puede incluir múltiples enfoques. Es importante considerar la gama completa de posibles medidas de control para encontrar una solución óptima. La eficacia de cada estrategia alternativa debe evaluarse antes de adoptar decisiones. Cada alternativa de mitigación de riesgos de seguridad operacional propuesta debería examinarse a partir de las perspectivas siguientes:

a) *Eficacia*. El grado en que las alternativas reducen o eliminan los riesgos de seguridad operacional. La eficacia puede determinarse en términos de las defensas técnicas, de instrucción y normativas que puedan reducir o eliminar los riesgos.

b) *Costo/beneficio*. El grado en que las ventajas percibidas de la mitigación superan los costos.

c) *Practicidad*. El grado en que la mitigación puede implementarse y cuán apropiada resulta en términos de recursos tecnológicos, financieros y administrativos disponibles así como de legislación, voluntad política, realidades operacionales, etc.

d) *Aceptabilidad*. El grado en que la alternativa resulta aceptable para las personas que se espera la apliquen.

e) *Cumplimiento*. El grado en que pueda vigilarse el cumplimiento de nuevas reglas, reglamentos o procedimientos operacionales.

f) *Duración*. El grado en que la mitigación pueda ser sostenible y eficaz.

g) *Riesgos de seguridad operacional residuales*. El grado de riesgo de seguridad operacional que permanece después de la implementación de la mitigación inicial y que pueda requerir medidas adicionales de control de riesgos.

h) *Consecuencias involuntarias*. La introducción de nuevos peligros y riesgos de seguridad operacional conexos relacionados con la implementación de una alternativa de mitigación.

i) *Tiempo*. El tiempo requerido para implantar la alternativa de mitigación de riesgo de seguridad operacional.

2.5.7.5 Las medidas correctivas deberían tener en cuenta las defensas que existan y su capacidad o incapacidad de alcanzar un nivel aceptable de riesgo de seguridad operacional. Esto puede resultar en una revisión de evaluaciones de riesgos anteriores que puedan haber sido afectadas por la medida correctiva. Las mitigaciones y controles de riesgos de seguridad operacional deberán verificarse o auditarse para asegurar que son eficaces. Otra forma de observar la eficacia de las mitigaciones es aplicando los SPI. En el Capítulo 4 figura más información sobre la gestión del rendimiento en materia de seguridad operacional y los SPI.

2.5.8 Documentación de la gestión de riesgos de la seguridad operacional

2.5.8.1 Las actividades de gestión de riesgos de seguridad operacional deberían documentarse, incluyendo toda su posición subyacente a la evaluación de la probabilidad y la gravedad, las decisiones adoptadas, y toda medida de mitigación de riesgos emprendidas. Esto puede realizarse utilizando una hoja de cálculo o una tabla. Algunas organizaciones pueden utilizar una base de datos u otro soporte lógico donde puedan almacenarse y analizarse grandes volúmenes de datos de seguridad operacional o de información sobre seguridad operacional.

2.5.8.2 El mantenimiento de un registro de peligros identificados minimiza la probabilidad de que la organización pierda de vista sus peligros conocidos. Cuando se identifican nuevos peligros, pueden compararse con los peligros conocidos que figuran en el registro para ver si ya han sido registrados y qué medidas se adoptaron para mitigarlos. Los registros de peligros se presentan normalmente en forma de tablas y típicamente incluyen lo siguiente: el peligro, posibles consecuencias, evaluación de riesgos conexos, fecha de identificación, categoría del peligro, breve descripción, cuándo y dónde se aplica, quién o quiénes lo han identificado y qué medidas se adoptaron para mitigar los riesgos.

2.5.8.3 Las herramientas y procesos de toma de decisiones sobre riesgos de seguridad operacional pueden utilizarse para mejorar la repetición y justificación de las decisiones tomadas por los encargados de adoptar decisiones de seguridad operacional en la organización. En la Figura 2-6 se proporciona un ejemplo de ayuda para tomar decisiones sobre riesgos de seguridad operacional.

2.5.9 Análisis de costo-beneficios

El análisis de costo-beneficios o rentabilidad se realiza normalmente durante las actividades de mitigación de riesgos de seguridad operacional. Se asocia comúnmente con la gestión empresarial, como una evaluación de impactos normativos o procesos de gestión de proyectos. No obstante, puede que haya situaciones donde una evaluación de riesgos de seguridad operacional tenga consecuencias financieras de importancia. En tales situaciones, puede justificarse un análisis de costo-beneficios o un proceso de rentabilidad complementarios para respaldar la evaluación de los riesgos de seguridad operacional. Esto asegurará que el análisis de rentabilidad o la justificación de medidas de control de riesgos recomendadas han tenido en cuenta las repercusiones financieras conexas.

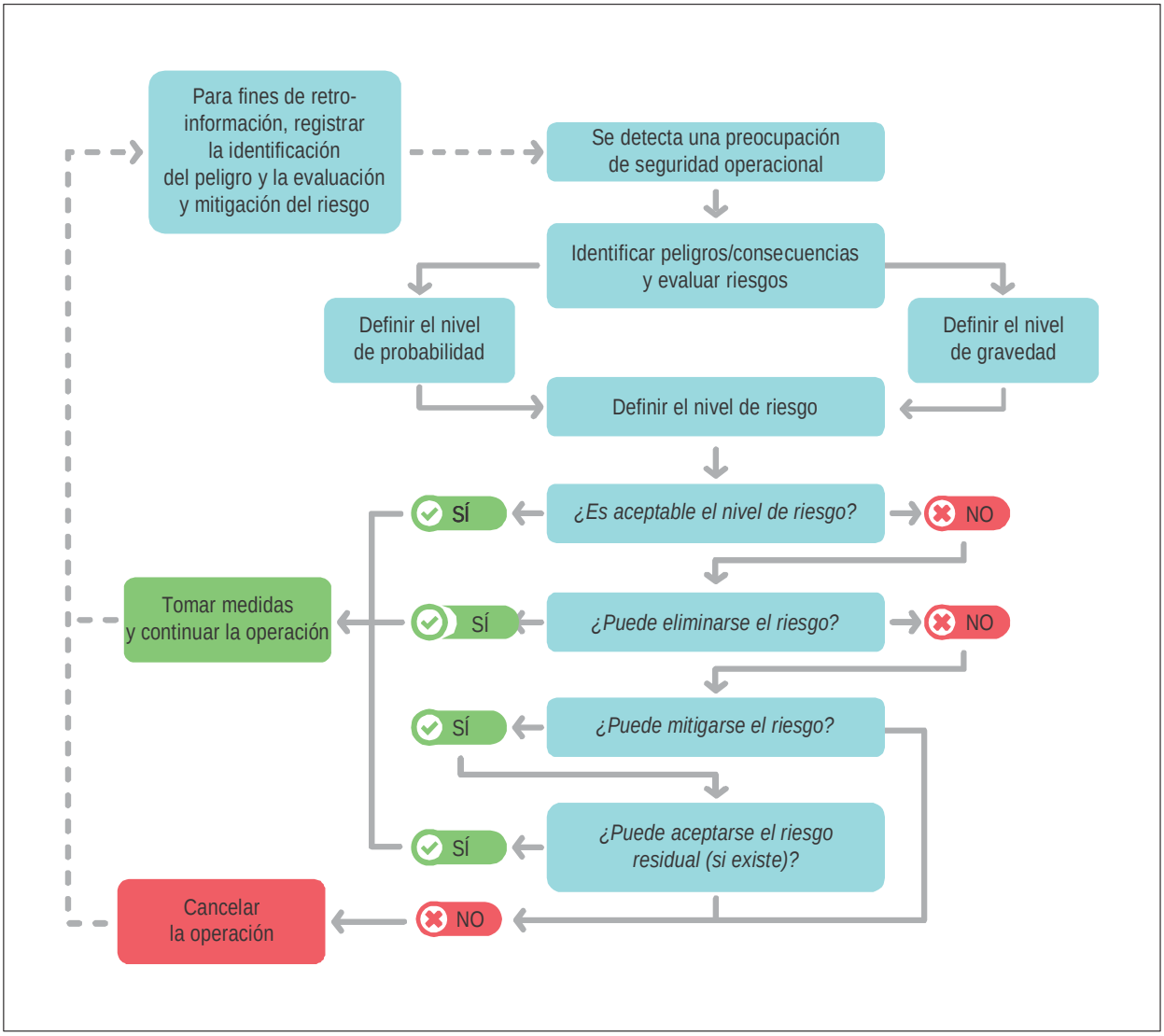


Figura 2-6. Ayuda para tomar decisiones sobre riesgos de seguridad operacional

Capítulo 3

CULTURA DE SEGURIDAD OPERACIONAL

3.1 INTRODUCCIÓN

3.1.1 Una cultura de seguridad operacional es la consecuencia natural de la presencia de seres humanos en el sistema de aviación. La cultura de seguridad se ha descrito como “la forma en que las personas se comportan en relación con la seguridad operacional y los riesgos cuando nadie está mirando”. Es una expresión de la forma en que la administración y los empleados de una organización perciben, valoran y priorizan la seguridad operacional y se refleja en la medida en que los individuos y grupos:

a) son conscientes de los riesgos y peligros conocidos que enfrentan la organización y sus actividades;

b) se comportan continuamente para mantener y mejorar la seguridad operacional;

c) pueden acceder a los recursos requeridos para las operaciones seguras;

d) están dispuestos y son capaces de adaptarse cuando enfrentan problemas de seguridad operacional;

e) están dispuestos a comunicar problemas de seguridad operacional; y

f) evalúan continuamente los comportamientos relacionados con la seguridad operacional en toda la organización.

3.1.2 En el Anexo 19 se exige que los Estados y los proveedores de servicios promuevan una cultura de seguridad operacional positiva con miras a fomentar una eficaz implementación de la gestión de la seguridad operacional mediante los SSP o SMS. En este capítulo se brinda orientación para la promoción de una cultura de seguridad operacional positiva.

3.2 CULTURA DE SEGURIDAD OPERACIONAL Y GESTIÓN DE LA SEGURIDAD OPERACIONAL

3.2.1 Se dé cuenta de ello o no, una organización tendrá varias “culturas de seguridad” diferentes que reflejan actitudes y comportamientos a nivel de grupos. No existen dos organizaciones idénticas e incluso dentro de la misma organización diferentes grupos pueden tener diferentes formas de pensar la seguridad operacional, hablar de la seguridad operacional y actuar frente a problemas de seguridad operacional. Esta variedad puede corresponder a diferentes actividades.

3.2.2 La forma en que los valores de seguridad operacional se incorporan en prácticas por la administración y el personal afecta directamente la forma en que se establecen y mantienen los elementos principales de los SSP y SMS. Como consecuencia, la cultura de seguridad operacional tiene impacto directo en el rendimiento en materia de seguridad operacional. Si se piensa que la seguridad operacional no es tan importante, eso daría lugar a la aplicación de soluciones alternativas, reducciones y simplificaciones o toma de decisiones o valoraciones inseguras, especialmente cuando el riesgo se percibe como bajo y no hay consecuencias o peligros aparentes. Por consiguiente, la cultura de seguridad operacional de una organización influye considerablemente en el desarrollo y eficacia de su SSP o SMS. La cultura de seguridad operacional constituye la influencia individual más importante en la gestión de la seguridad operacional. Si una organización ha instituido todos los requisitos de gestión de la seguridad operacional pero no cuenta con una cultura de seguridad operacional positiva, es probable que no funcione bien.

3.2.3 Cuando la organización tiene una cultura de seguridad operacional positiva, y la misma es visiblemente apoyada por la administración superior y media, el personal de primera línea tiende a experimentar un sentido de responsabilidad compartida con respecto al logro de los objetivos de seguridad operacional de la organización. Una gestión de la seguridad operacional eficaz también apoya los esfuerzos tendientes a la creación de una cultura de seguridad operacional cada vez más positiva mediante el aumento de la visibilidad del apoyo de la administración y la mejora de la participación activa del personal en la gestión de los riesgos de seguridad operacional.

3.2.4 Una cultura de seguridad operacional positiva se basa en un alto nivel de confianza y respeto entre el personal y la administración. Se requiere tiempo y esfuerzo para construir una cultura de seguridad operacional positiva, que puede ser fácilmente dañada por decisiones y acciones, acciones u omisiones de la administración. Se necesita un esfuerzo y un reforzamiento continuo. Cuando la dirección apoya activamente las prácticas de seguridad operacional, ello pasa a ser la forma normal de actuar. La situación ideal es contar con una implantación completa y efectiva de SSP/SMS y una cultura de seguridad operacional positiva. Por consiguiente, la cultura de seguridad operacional de una organización se considera a menudo como reflejo del grado de madurez de sus SSP/SMS. La gestión eficaz de la seguridad operacional facilita una cultura de seguridad operacional positiva y una cultura de seguridad operacional positiva facilita la gestión eficaz de la seguridad operacional.

3.2.5 La cultura de seguridad operacional y su influencia en las notificaciones de seguridad operacional

3.2.5.1 Los SSP y SMS están apoyados por los datos de seguridad operacional y la información sobre seguridad operacional necesarios para abordar deficiencias y peligros de seguridad operacional existentes y posibles, incluyendo problemas identificados por el personal. El éxito de un sistema de notificación depende enteramente del flujo continuo de información desde y hacia organizaciones e individuos. La protección de los datos de seguridad operacional, información sobre seguridad operacional y fuentes conexas resulta fundamental para asegurar la continua disponibilidad de la información. Por ejemplo, en los sistemas de notificación voluntaria de seguridad operacional, esto puede lograrse mediante un sistema de carácter confidencial y no utilizado para fines diferentes del mantenimiento o mejoramiento de la seguridad operacional. Los beneficios son dobles. A menudo el personal está en más estrecho contacto con los peligros de seguridad operacional, de modo que un sistema de notificación voluntaria le permite identificar activamente esos peligros y sugerir soluciones viables. Al mismo tiempo, el reglamentador o la administración pueden reunir información importante sobre seguridad operacional y crear confianza con las organizaciones o el personal de operaciones que notifica la información. En el Capítulo 7 figura más información sobre la protección de los datos y la información sobre seguridad operacional.

3.2.5.2 Si las organizaciones o individuos están dispuestos o no a notificar sus experiencias y errores depende en gran medida de los beneficios y desventajas percibidos relacionados con la notificación en sí. Los sistemas de notificación de seguridad operacional pueden ser anónimos o confidenciales. En general, en un sistema de notificación anónimo un informante no revela su identidad. En este caso, no hay oportunidades para una aclaración ulterior del contenido del informe, ni posibilidad de retroinformación. En un sistema de notificación confidencial, la información de identificación sobre el informante solo es conocida por un custodio designado. Si las organizaciones e individuos que notifican problemas de seguridad operacional están protegidos y son tratados en forma justa y coherente, es más probable que divulguen dicha información y trabajen con los reglamentadores o administradores para gestionar eficazmente los riesgos de seguridad operacional conexos.

3.2.5.3 Se espera que los Estados adopten leyes para cumplir las disposiciones del Anexo 19 relativas a la protección de datos de seguridad operacional, información sobre seguridad operacional y fuentes conexas. En el caso de los sistemas de notificación voluntaria, debería garantizarse la confidencialidad y el sistema de notificación debería funcionar con arreglo a las leyes de protección de la seguridad operacional. Además, las organizaciones deben contar con una política disciplinaria apropiada, al alcance de todos y ampliamente comprendida. La política disciplinaria debería indicar claramente los comportamientos que se consideran inaceptables y la forma en que la organización responderá en tales casos. La política disciplinaria debe aplicarse en forma justa, razonable y continua. Finalmente, es más probable que las organizaciones e individuos notifiquen sus experiencias y errores en un entorno en el que no se les juzgue o trate injustamente por parte de sus colegas o sus empleadores.

3.2.5.4 En general, las organizaciones e individuos deben creer que se les apoyará cuando presenten informes en interés de la seguridad operacional. Esto comprende errores y equivocaciones institucionales y personales. Un aumento en el número de notificaciones confidenciales y una disminución de los informes anónimos indica normalmente que la organización avanza hacia una cultura de seguridad operacional positiva.

3.2.6 La cultura de seguridad operacional y la diversidad cultural

3.2.6.1 La cultura nacional diferencia las características de naciones particulares, como el papel de cada persona dentro de la sociedad, la forma en que se distribuye la autoridad y las prioridades nacionales con respecto a los recursos, las responsabilidades, la moralidad, los objetivos y los diferentes sistemas jurídicos.

3.2.6.2 Desde una perspectiva de gestión de la seguridad operacional, la cultura nacional influye en la cultura institucional y desempeña un gran papel en la determinación del carácter y el alcance de las políticas de cumplimiento reglamentarias, incluyendo las relaciones entre el personal de la autoridad normativa y el personal de la industria, así como la medida en que se protege la información relacionada con la seguridad operacional. Esto, a su vez, gravitará en la disposición de las personas a notificar problemas de seguridad operacional.

3.2.6.3 La mayoría de las organizaciones emplean actualmente personas de diversas extracciones culturales, que pueden definirse por su nacionalidad, origen étnico, religión o género. Las operaciones de aviación y la seguridad operacional se basan en la eficaz interacción entre diferentes grupos profesionales, cada uno de ellos con su propia cultura profesional. Por ello, la cultura de seguridad operacional de la organización puede también verse afectada considerablemente por la variedad de entornos culturales de los miembros de su personal.

3.2.6.4 Por consiguiente, la gestión de la seguridad operacional en el sistema de aviación requiere interacción con un personal culturalmente diverso y la gestión del mismo. No obstante, cuando implementen la gestión de la seguridad operacional, los administradores deberían poder moldear su personal diverso en equipos eficaces. Es fundamental eliminar las diferencias en las percepciones de los riesgos de seguridad operacional que pueden deberse a diferentes interpretaciones culturales y mejorar otros aspectos de seguridad operacional, como las comunicaciones, los estilos de liderazgo y la interacción entre supervisores y subordinados. El éxito dependerá en la capacidad de la administración de promover una comprensión común de la seguridad operacional y de la función de cada individuo en su eficacia. Independientemente de los antecedentes culturales del individuo, la gestión eficaz de la seguridad operacional se basa en una cultura de seguridad operacional compartida, en la que todos los miembros de la organización comprenden lo que se espera de ellos en relación con la seguridad operacional y los riesgos “aunque nadie esté mirando”.

3.2.7 La cultura de seguridad operacional y los cambios en la organización

La gestión de la seguridad operacional exige que las organizaciones gestionen los riesgos de seguridad operacional relacionados con los cambios institucionales y operacionales. Las preocupaciones del personal respecto de la carga de trabajo, seguridad laboral y acceso a la instrucción se relacionan con cambios importantes en las organizaciones y pueden tener consecuencias negativas sobre la cultura de seguridad operacional. El grado en que el personal se siente involucrado en el desarrollo de los cambios y comprende su función en el proceso también influirá en la cultura de seguridad operacional.

3.3 DESARROLLO DE UNA CULTURA DE SEGURIDAD OPERACIONAL POSITIVA

3.3.1 Una cultura de seguridad operacional positiva tiene las características siguientes:

a) los administradores y los empleados, individual y colectivamente, quieren tomar decisiones y aplicar medidas que promuevan la seguridad operacional;

b) los individuos y grupos critican en forma continua sus comportamientos y procesos y ven con agrado las críticas de otros que buscan tener oportunidades para cambiar y mejorar a medida que el entorno cambia;

c) la administración y el personal comparten el conocimiento de los peligros y riesgos enfrentados por la organización y sus actividades, y la necesidad de gestionar los riesgos;

d) los individuos actúan y toman decisiones con arreglo a una creencia común de que la seguridad operacional es parte de la forma en que trabajan;

e) los individuos valoran recibir información e informar a otros, sobre la seguridad operacional; y

f) las personas brindan a sus colegas y administradores información sobre sus experiencias y se fomenta la notificación de errores y equivocaciones para mejorar la forma de actuar en el futuro.

3.3.2 Las medidas adoptadas por la administración y los empleados pueden llevar a que su cultura de seguridad operacional sea más positiva. En la Tabla 5 se brindan ejemplos de los tipos de acciones de la administración y el personal que habilitarán o inhabilitarán la cultura de seguridad operacional positiva en una organización. Las organizaciones deberían concentrarse en proporcionar elementos habilitadores que eliminen los inhabilitadores que existan para promover y alcanzar una cultura de seguridad operacional positiva.

Tabla 5. Ejemplos de acciones que habilitarán o inhabilitarán una cultura de seguridad operacional positiva

Elemento	*Descripción general*	*Habilitadores*	*Inhabilitadores*
Compromiso con la seguridad operacional			
El compromiso con la seguridad operacional refleja el grado en que la administración superior de la organización tiene una actitud positiva respecto de la seguridad operacional y reconoce su importancia. La administración superior debería estar genuinamente comprometida con el logro y mantenimiento de un alto nivel de seguridad operacional y motivar a sus empleados dándoles los medios para hacerlo.		• La administración conduce una cultura de seguridad operacional y motiva activamente a sus empleados para que se preocupen por la misma, no sólo con palabras sino actuando como ejemplo • La administración proporciona recursos para muchas tareas relacionadas con la seguridad operacional (p. ej., instrucción) • Se establece una vigilancia continua de la gestión de la seguridad operacional y gobernanza conexa	• La administración demuestra claramente que el lucro, la reducción de costos y la eficiencia son lo primero • Las inversiones para mejorar la seguridad operacional se efectúan a menudo solo cuando lo exigen los reglamentos o después de accidentes • No hay vigilancia ni gobernanza establecidas con respecto a la gestión de la seguridad operacional

Elemento	*Descripción general*	*Habilitadores*	*Inhabilitadores*
Adaptabilidad			
La adaptabilidad refleja el grado en que los empleados y la administración están dispuestos a aprender de experiencias pasadas y en condiciones de tomar las medidas necesarias para mejorar el nivel de seguridad operacional de la organización		• Se fomenta activamente la contribución de los empleados al tratar problemas de seguridad operacional • Todos los incidentes y constataciones de auditorías se investigan y se actúa en consecuencia • Los procesos y procedimientos institucionales se cuestionan en cuanto a su impacto en la seguridad operacional (alto grado de autocrítica) • Se demuestra y aplica un enfoque proactivo claro de la seguridad operacional	• No se fomenta la contribución de los empleados en problemas de seguridad operacional a todos los niveles del personal • A menudo las medidas se adoptan solo después de accidentes o cuando lo exigen los reglamentos • Los procesos y procedimientos institucionales se consideran adecuados en la medida en que no ocurren accidentes (complacencia o falta de autocrítica) • Aun cuando ocurre un accidente la organización no se autocuestiona • Se demuestra y aplica un enfoque reactivo de la seguridad operacional
Conciencia/sensibilización			
La conciencia refleja el grado en que empleados y administradores son conscientes de los riesgos de aviación que enfrentan la organización y sus actividades Desde la perspectiva del Estado el personal es consciente de los riesgos de seguridad operacional inducidos por sus propias actividades y las organizaciones que supervisan. Los empleados y la administración deberían mantener constantemente un alto grado de vigilancia con respecto a la seguridad operacional		• Se ha establecido una forma eficaz de identificar peligros • Las investigaciones procuran establecer las causas básicas • La organización está siempre al tanto de importantes mejoras de la seguridad operacional y se adapta a las mismas según sea necesario	• No se realizan esfuerzos para identificar peligros • Las investigaciones se detienen en la primer causa viable sin procurar determinar la causa básica • La organización no está al tanto de importantes mejoras de seguridad operacional • La organización no evalúa si se implantan adecuadamente las mejoras de seguridad

Elemento	*Descripción general*	*Habilitadores*	*Inhabilitadores*
		• La organización evalúa sistemáticamente si se aplican y funcionan según lo previsto las mejoras de la seguridad operacional • Los miembros apropiados de la organización están bien conscientes de los riesgos de seguridad operacional inducidos por sus acciones individuales y las operaciones o actividades de la compañía	• Cuando corresponde, los miembros de la organización no están conscientes de los riesgos de seguridad operacional inducidos por sus acciones individuales y operaciones de la compañía • Los datos de seguridad operacional se recopilan pero no se analizan ni se toman medidas al respecto
Comportamiento con respecto a la seguridad operacional			
El comportamiento con respecto a la seguridad operacional refleja el grado en que todos los niveles de la organización se comportan para mantener y mejorar el nivel de seguridad. La importancia de la seguridad operacional debería reconocerse y se deberían instituir procesos y procedimientos necesarios para mantenerla		• Los empleados se automotivan para actuar en forma segura y como ejemplos • Se practica la observación continua del comportamiento de seguridad • El comportamiento inseguro intencional no es tolerado por la administración y los colegas • Las condiciones de trabajo apoyan la seguridad operacional de la aviación en todo momento	• Los empleados no son castigados por el comportamiento inseguro intencional en beneficio de sus propios intereses o los de terceros • Las condiciones de trabajo provocan comportamientos y acciones alternativas que van en detrimento de la seguridad operacional de la aviación • No se vigila la seguridad operacional de la aviación dentro de los productos al servicio de la organización • No se ven con agrado las críticas constructivas para beneficiar la seguridad operacional de la aviación

Elemento	*Descripción general*	*Habilitadores*	*Inhabilitadores*
Información			
La información refleja el grado en que se distribuyen los conocimientos y datos a todas las personas necesarias dentro de la organización. Debería permitirse y fomentarse que los empleados notifiquen preocupaciones de seguridad operacional de la aviación y reciban comentarios sobre sus informes. La información laboral relacionada con la seguridad operacional de la aviación debe comunicarse correctamente a las personas adecuadas para evitar malas interpretaciones que podrían contribuir a situaciones y consecuencias peligrosas para el sistema aeronáutico El Estado se muestra abierto a compartir información relacionada con la seguridad operacional de la aviación con todos los proveedores de servicios		• Existe un entorno abierto y justo para notificar problemas de seguridad operacional • Se brinda a los empleados información sobre seguridad operacional en forma oportuna para permitir la realización de operaciones o la toma de decisiones seguras • La administración y los supervisores verifican regularmente si la información de seguridad operacional es comprendida y se actúa sobre la misma • Se practica activamente la transferencia de conocimientos y la instrucción con respecto a la seguridad operacional de la aviación (p. ej., se comparten las experiencias adquiridas)	• Es evidente un entorno de notificación de seguridad operacional con asignación de culpas • Se retiene la información sobre seguridad operacional • No se vigila la eficacia de las comunicaciones de seguridad operacional • No se proporciona transferencia de conocimientos o instrucción
Confianza			
La contribución de los empleados a la seguridad operacional es favorecida por un entorno de notificación que fomente la confianza de que sus acciones u omisiones, acordes con su instrucción y experiencia, no serán castigadas. Un enfoque viable es aplicar una prueba de sensatez – es decir, si es razonable que una persona con el mismo nivel de experiencia e instrucción podría hacer la misma cosa. Un entorno de este tipo es fundamental para la notificación eficaz y eficiente de la seguridad operacional		• Hay una diferencia entre el comportamiento aceptable e inaceptable, conocida por todos los empleados • Las investigaciones de sucesos (incluyendo accidentes e incidentes) consideran factores individuales así como institucionales • Se reconoce y recompensa con carácter continuo el buen rendimiento en materia de seguridad operacional de la aviación	• No hay diferencias identificables entre comportamiento aceptable e inaceptable • Los empleados son sistemática y rigurosamente castigados por los errores humanos • Las investigaciones de accidentes e incidentes se concentran solamente en factores individuales

Elemento	*Descripción general*	*Habilitadores*	*Inhabilitadores*
Los sistemas eficaces de notificación de seguridad operacional contribuyen a asegurar que las personas están dispuestas a notificar sus errores y experiencias, de modo que los Estados y los proveedores del servicio tengan acceso a datos e información pertinentes necesarios para tratar deficiencias y peligros de seguridad operacional tanto existentes como posibles. Estos sistemas crean un entorno en el que las personas pueden confiar en que su información y datos de seguridad operacional se utilizarán exclusivamente para mejorar la misma.		• Hay buena disposición de los empleados y personal de operaciones para notificar sucesos en los que han estado involucrados	• Se da por descontado un buen rendimiento y un buen desempeño en materia de seguridad operacional

3.3.3 Observación de la cultura de seguridad operacional

3.3.3.1 La cultura de seguridad operacional está sujeta a muchas influencias y las organizaciones pueden optar por evaluar su cultura de seguridad operacional para:

a) comprender cómo las personas se sienten respecto de la organización y cuán importante se percibe que es la seguridad operacional;

b) identificar puntos fuertes y débiles;

c) identificar diferencias entre diversos grupos (subculturas) dentro de la organización; y

d) examinar los cambios con el tiempo (p. ej., en respuesta a cambios institucionales importantes como a consecuencia de un accidente, un cambio en la administración superior o la modificación de un arreglo de relaciones industriales).

3.3.3.2 Hay varias herramientas que se utilizan para evaluar el grado de madurez de la cultura de seguridad operacional, normalmente en combinación:

a) cuestionarios;

b) entrevistas y grupos de discusión;

c) observaciones; y

d) exámenes de documentos.

3.3.3.3 La evaluación del grado de madurez de la cultura de seguridad operacional puede proporcionar valiosos conocimientos que conduzcan a medidas de la administración para fomentar los comportamientos deseados en materia de seguridad operacional. Cabe señalar que existe un cierto grado de subjetividad en dichas evaluaciones y que éstas pueden reflejar opiniones y percepciones de las personas involucradas en un momento particular solamente. Además, la calificación de la madurez de la cultura de seguridad operacional puede tener consecuencias imprevistas alentando involuntariamente a la organización a que procure lograr la calificación “correcta”, en vez de trabajar en conjunto para comprender y mejorar la cultura de seguridad operacional.

Capítulo 4

GESTIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL

4.1 INTRODUCCIÓN

4.1.1 La gestión del rendimiento en materia de seguridad operacional es crucial para el funcionamiento de los SSP y SMS. Si está bien implementada, proporcionará a la organización los medios para determinar si sus actividades y procesos funcionan eficazmente para alcanzar sus objetivos de seguridad operacional. Esto se logra mediante la identificación de indicadores de rendimiento en materia de seguridad operacional (SPI), que se utilizan para vigilar y medir dicho rendimiento. Mediante la identificación de los SPI, la información obtenida permitirá que la administración superior tenga conocimiento de la situación actual y apoye la toma de decisiones, incluso la determinación de si hay que adoptar medidas para mitigar en mayor grado los riesgos de seguridad operacional a efectos de asegurar que la organización alcanza sus objetivos de seguridad operacional.

4.1.2 En la siguiente Figura 4-1 se muestra el proceso genérico de gestión del rendimiento en materia de seguridad operacional y la forma en que se relaciona con los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) y los análisis de dicha seguridad, que se analizan en los Capítulos 5 y 6, respectivamente. La relación con la promoción de la seguridad operacional se muestra para destacar la importancia de comunicar dicha información a toda la organización. En los Capítulos 8 y 9, respectivamente, se presenta más información sobre la promoción de la seguridad operacional, un componente importante de los SSP y SMS que a menudo no se aprecia debidamente.

4.1.3 La gestión de rendimiento en materia de seguridad operacional ayuda a la organización a plantearse y responder las cuatro más importantes preguntas con respecto a la gestión de la seguridad operacional:

a) ¿Cuáles son los principales riesgos de seguridad operacional de la organización? *Se obtiene de un examen de datos de accidentes e incidentes de aviación así como de análisis predictivo para identificar y definir riesgos emergentes.*

b) ¿Qué desea lograr la organización en términos de seguridad operacional y cuáles son los principales riesgos de seguridad operacional que deben tratarse? *Los objetivos de seguridad operacional de la organización.*

c) ¿Cómo conocerá la organización que está avanzando hacia sus objetivos de seguridad operacional? *Mediante SPI, SPT y, si es posible, activadores de seguridad operacional.*

d) ¿Qué datos e información sobre seguridad operacional se necesitan para tomar decisiones de seguridad operacional bien fundadas, incluyendo la asignación de recursos de la organización? *Mediante un SDCPS evolutivo y análisis de datos de seguridad operacional.*

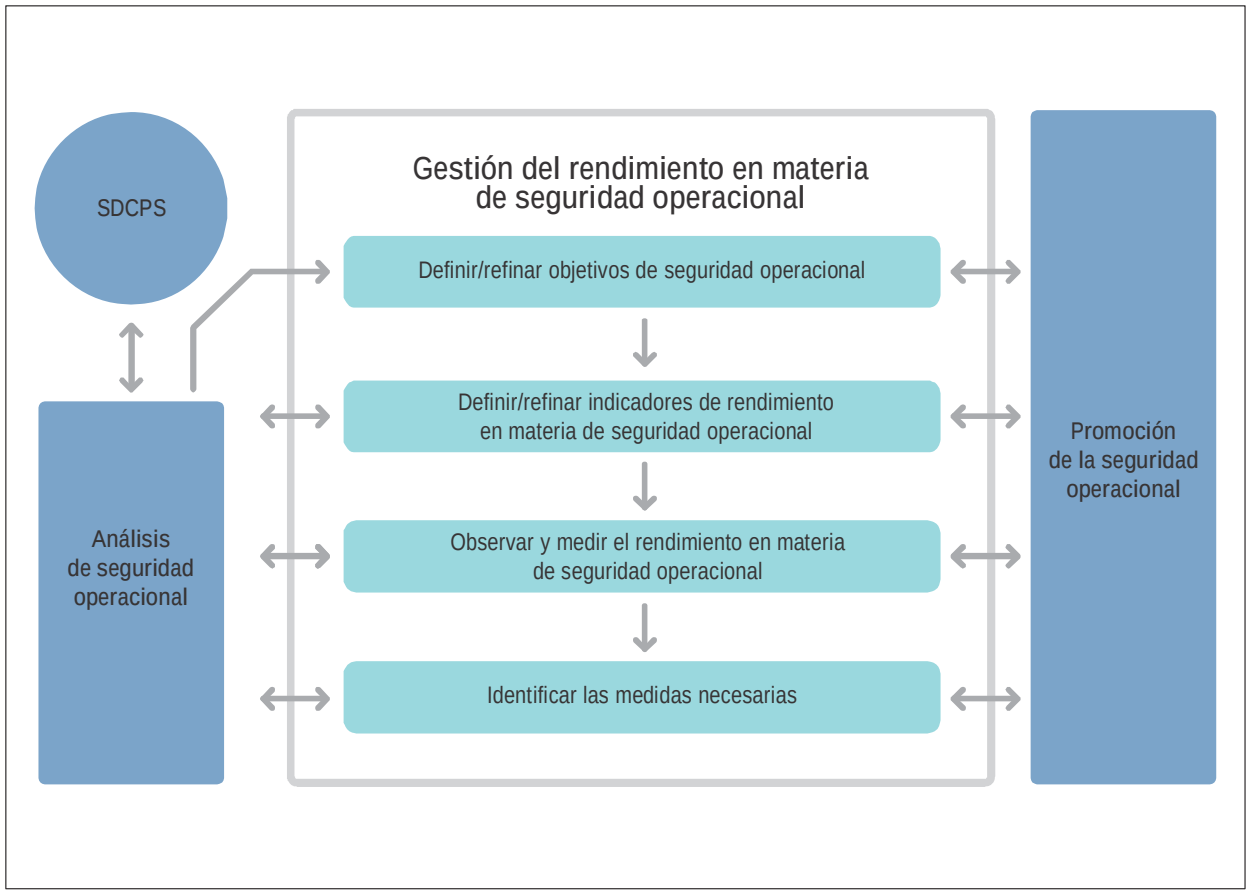


Figura 4-1. Proceso de gestión del rendimiento en materia de seguridad operacional

4.1.4 El proceso de gestión del rendimiento de la seguridad operacional también puede aplicarse al establecimiento de un nivel aceptable del rendimiento en materia de seguridad operacional (ALoSP). En el Capítulo 8 figuran más detalles sobre el establecimiento de un ALoSP.

4.1.5 Relaciones entre los Estados y los proveedores de servicios

4.1.5.1 Hay similitudes entre el Estado y los proveedores de servicios en cuanto al uso y aplicación de técnicas de rendimiento de la seguridad operacional. Si bien la orientación presentada en este capítulo se ha elaborado tanto para los Estados como para los proveedores de servicios, en esta sección se identifican algunas diferencias en la materia.

4.1.5.2 El desarrollo del rendimiento en materia de seguridad operacional por parte del Estado debería concentrarse en lo que el Estado en cuestión considera como sus aspectos más importantes para gestionar la seguridad operacional. Para el Estado, un SSP implementado eficazmente se utiliza como una herramienta de adopción de decisiones para la gestión del rendimiento en materia de seguridad operacional, que debería incluir: el rendimiento en materia de seguridad operacional de sus proveedores de servicios, la capacidad de vigilancia del Estado y el apoyo proporcionado a los proveedores de servicios mediante el establecimiento de directrices. Los Estados deberían considerar la medición de sus capacidades para:

a) mantener su sistema de vigilancia de la seguridad operacional;

b) aplicar medidas de seguridad operacional específicas e introducir iniciativas de seguridad; y

c) adaptar los controles de riesgos de seguridad operacional existentes para cerciorarse de que siguen siendo eficaces.

4.1.5.3 Para los proveedores de servicios, la función principal de la gestión de rendimiento en materia de seguridad operacional consiste en observar y medir la forma en que se están gestionando los riesgos de seguridad operacional. Esto se logra mediante la implantación eficaz de un SMS que genere información que se utilizará para formular decisiones respecto de la gestión de la seguridad operacional, incluyendo la implementación de controles de riesgos de seguridad y la asignación de recursos.

4.1.5.4 El éxito de la gestión de la seguridad operacional depende del compromiso entre el Estado y sus proveedores de servicios. Pueden haber beneficios en el Estado que identifique SPI adecuados que puedan ser observados por los proveedores de servicios y luego compartidos con el Estado, en particular para el establecimiento del ALoSP (véase el Capítulo 8 por más información). La información recibida de los proveedores de servicios ayudará al Estado en su evaluación de rendimiento en materia de seguridad operacional de su industria aeronáutica y de su propia capacidad para proporcionar una vigilancia eficaz y apoyar a los proveedores de servicios. No obstante, estos deberían asegurar que sus SPI son apropiados a su contexto operacional, historial de actuación y expectativas.

4.1.6 La gestión del rendimiento en materia de seguridad operacional y las interfaces

4.1.6.1 Cuando los Estados y proveedores de servicios consideren implantar la gestión de la seguridad operacional, es importante considerar los riesgos de seguridad operacional inducidos por las entidades interconectadas. Las interfaces pueden ser internas (p. ej., entre los departamentos de operaciones y mantenimiento o los de finanzas, recursos humanos o asuntos jurídicos), o pueden ser externas (p. ej., otro Estado, proveedores de servicios o servicios contratados). Los peligros y los riesgos conexos en los puntos de interfaz se cuentan entre los factores contribuyentes más comunes a los sucesos de seguridad operacional. Los Estados y los proveedores de servicios tienen mayor control sobre los riesgos relacionados con las interfaces cuando éstas se identifican y gestionan bien. Las interfaces deberían definirse en la descripción del sistema de la organización.

4.1.6.2 Los Estados y proveedores de servicios son responsables de la continua vigilancia, observación y gestión de sus interfaces para garantizar resultados seguros. El riesgo de seguridad operacional planteado por cada interfaz debería, en condiciones ideales, ser evaluados en colaboración por las entidades interconectadas. La colaboración es muy conveniente debido a que la percepción de los riesgos de seguridad operacional y su tolerabilidad puede variar según las organizaciones interrelacionadas. La compartición de la gestión de los riesgos de la interfaz, mediante el establecimiento y vigilancia de los SPI, fomenta la conciencia mutua sobre los riesgos de seguridad operacional en vez de la ignorancia de los mismos o una gestión de riesgos posiblemente unilateral. También crea una oportunidad para transferir conocimientos y prácticas laborales que podrían mejorar la eficacia de ambas organizaciones en materia de seguridad operacional.

4.1.6.3 Por este motivo, deberían convenirse y establecerse SPI para observar y medir los riesgos y la eficacia de las medidas de mitigación. Un ejemplo de enfoque eficaz sería un acuerdo formal de gestión de interfaces entre las organizaciones interconectadas, con responsabilidades claramente definidas en cuanto a la observación y la gestión.

4.2 OBJETIVOS DE SEGURIDAD OPERACIONAL

4.2.1 Los objetivos de seguridad operacional son declaraciones breves, de alto nivel, de logros en materia de seguridad operacional o resultados deseados que han de alcanzarse. Los objetivos de seguridad operacional proporcionan dirección a las actividades de la organización, y por ello, deberían ser coherentes con la política de seguridad operacional que establece el compromiso de seguridad operacional de alto nivel de la organización. También resultan útiles para comunicar al personal y a la comunidad aeronáutica en su totalidad las prioridades en materia de

seguridad operacional. El establecimiento de objetivos de seguridad operacional proporciona una dirección estratégica para el proceso de gestión del rendimiento en materia de seguridad operacional así como una base sólida para la toma de decisiones relacionadas con la misma. La gestión del rendimiento en materia de seguridad operacional debería ser una consideración principal cuando se enmiendan políticas o procesos o se asignan recursos de la organización con el fin de mejorar dicho rendimiento.

4.2.2 Los objetivos de seguridad operacional pueden ser:

a) *orientados a procesos*: declarados en términos de comportamientos seguros que se esperan del personal operacional o el rendimiento de medidas implementadas por la organización para gestionar los riesgos de seguridad operacional; o

b) *orientados a resultados*: engloba medidas y tendencias relativas a la contención de accidentes o pérdidas operacionales.

4.2.3 El conjunto de objetivos de seguridad operacional debería comprender una mezcla de objetivos orientados a procesos y orientados a resultados para proporcionar suficiente cobertura y dirección para los SPI y las SPT. Los objetivos de seguridad operacional por sí mismos no tienen por qué ser específicos, medibles, alcanzables, pertinentes y oportunos (SMART) (George T. Doran, 1981), en la medida en que dichos objetivos y SPI y SPT acompañantes formen un paquete que permita a la organización demostrar si está manteniendo o mejorando su rendimiento en materia de seguridad operacional.

Tabla 6. Ejemplos de objetivos de seguridad operacional

Ejemplos de objetivos de seguridad operacional		
Orientados a procesos	Estado o proveedor de servicios	Aumentan los niveles de notificación de seguridad operacional
Orientados a resultados	Proveedor de servicios	Reducen la tasa de sucesos de seguridad operacional adversos en la plataforma. (alto nivel) o Reducen el número anual de sucesos de seguridad operacional adversos en la plataforma respecto del año anterior.
Orientados a resultados	Estado	Reducen el número anual de sucesos de seguridad operacional en el sector X.

4.2.4 Una organización también puede optar por identificar objetivos de seguridad operacional a nivel táctico u operacional así como aplicarlos a proyectos, productos y procesos específicos. Un objetivo de seguridad operacional también puede expresarse mediante el uso de otros términos con significado similar (p. ej., finalidad o meta).

4.3 INDICADORES Y METAS DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL

4.3.1 Tipos de indicadores de rendimiento en materia de seguridad operacional

Indicadores cualitativos y cuantitativos

4.3.1.1 Los SPI se utilizan para ayudar a la administración a saber si es probable o no que la organización logre su objetivo de seguridad operacional; pueden ser cualitativos o cuantitativos. Los indicadores cuantitativos se refieren a la medición por cantidades, más que por calidades, mientras que los indicadores cualitativos son descriptivos y miden

por calidad. Los indicadores cuantitativos son preferibles a los cualitativos porque se los puede contar y comparar más fácilmente. La elección del indicador depende de la disponibilidad de datos confiables que se puedan medir cuantitativamente. Importa plantearse si la evidencia necesaria debe estar en forma de datos comparables y generalizables (cuantitativos) o en forma de imágenes descriptivas de la situación de seguridad operacional (cualitativa). Cada opción, cualitativa o cuantitativa, entraña diferentes tipos de SPI que pueden lograrse de mejor manera mediante un proceso reflectivo de selección de SPI. Una combinación de enfoques resulta útil en muchas situaciones y puede resolver muchos de los problemas que pueden surgir de la adopción de un enfoque único. Un ejemplo de indicador cualitativo para un Estado podría ser el grado de madurez de los SMS de sus proveedores de servicios en un sector particular, o la evaluación de la cultura de seguridad operacional para un proveedor de servicios.

4.3.1.2 Los indicadores cuantitativos pueden expresarse como un número (x incursiones) o como una tasa (x incursiones por n movimientos). En algunos casos, una expresión numérica será suficiente. No obstante, el solo uso de números puede crear una impresión distorsionada de la situación real de la seguridad operacional si el nivel de actividad fluctúa. Por ejemplo, si el control del tránsito aéreo registra tres fallas de altitud en julio y seis en agosto, puede haber una gran preocupación por el deterioro significativo del rendimiento en materia de seguridad operacional. Pero agosto puede haber tenido el doble de movimientos que julio, lo que significa que el incumplimiento de la altitud por movimiento, o sea la tasa, ha disminuido y no aumentado. Esto puede o no cambiar el nivel de escrutinio, pero provee otra información valiosa que puede ser vital para la toma de decisiones de seguridad operacional basadas en datos.

4.3.1.3 Por este motivo, cuando corresponda, los SPI deberían reflejarse en términos de una tasa relativa para medir el nivel de rendimiento, independientemente del nivel de actividad. Esto proporciona una medida del rendimiento normalizada, es decir, si la actividad aumenta o disminuye. En otro ejemplo, un SPI podría medir el número de incursiones en las pistas. Pero si hubo menos salidas en el periodo considerado, el resultado podía ser engañoso. Una medida más precisa y valiosa del rendimiento sería la cantidad de incursiones en las pistas en relación con el número de movimientos, p. ej., x incursiones por 1 000 movimientos.

Indicadores de resultados (lagging, en inglés) y avanzados (leading, en inglés)

4.3.1.4 Las dos categorías más comunes utilizados por los Estados y proveedores de servicios para clasificar sus SPI son los indicadores de resultados y los indicadores avanzados. Los SPI de resultados miden sucesos que ya han ocurrido. También se les conoce como “SPI basados en resultados” y normalmente (pero no siempre) son los resultados negativos que la organización intenta evitar. Los indicadores avanzados miden procesos e insumos que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como “SPI de actividad o proceso”, ya que observan y miden las condiciones que tienen el potencial de convertirse en un resultado específico, o contribuir a éste.

4.3.1.5 Los SPI de resultados ayudan a la organización a comprender lo que ha sucedido en el pasado y son útiles para determinar tendencias a largo plazo. Se pueden utilizar como indicadores de alto nivel o como una indicación de tipos específicos de sucesos o ubicaciones, como “tipos de accidentes por tipo de aeronave” o “tipos de incidentes específicos por región”. Debido a que los indicadores de resultados miden los resultados de seguridad operacional, pueden medir la efectividad de las medidas de mitigación de la seguridad operacional. También resultan eficaces para validar el rendimiento de seguridad operacional general del sistema. Por ejemplo, la vigilancia del “número de colisiones en rampa por número de movimientos entre vehículos después de un rediseño de las marcas de la rampa” se obtiene una medida de la eficacia de las nuevas marcas (suponiendo que nada más haya cambiado). La reducción en las colisiones valida una mejora en el rendimiento en materia de seguridad operacional general del sistema de rampa, que puede atribuirse al cambio en cuestión.

4.3.1.6 Las tendencias en los SPI de resultados pueden analizarse para determinar las condiciones existentes en el sistema que deberían abordarse. Utilizando el ejemplo anterior, una tendencia creciente en el número de colisiones de rampa por cantidad de movimientos pudo haber sido lo que llevó a la identificación de marcas de rampa por debajo de la norma como una mitigación.

4.3.1.7 Los SPI de resultados se dividen en dos tipos:

a) *Baja probabilidad/alta gravedad*: resultados tales como accidentes o incidentes graves. La baja frecuencia de los resultados de alta gravedad significa que la agregación de datos (a nivel de segmento industrial o nivel regional) puede dar como resultado un análisis más significativo. Un ejemplo de este tipo de SPI de resultados serían los daños a los aviones y al motor debidos a choques con aves.

b) *Alta probabilidad/baja gravedad*: resultados que no se manifestaron necesariamente en un accidente o incidente grave. A veces también se los denomina indicadores de sucesos precursores. Los SPI para resultados de alta probabilidad/baja gravedad se utilizan principalmente para vigilar problemas de seguridad específicos y medir la eficacia de las mitigaciones de riesgos de seguridad existentes. Un ejemplo de este tipo de SPI precursor sería “detecciones de aves en el radar”, que indica el nivel de actividad de las aves en lugar de la cantidad real de choques con las mismas.

4.3.1.8 Las medidas de seguridad operacional de la aviación han estado históricamente sesgadas hacia los SPI que reflejan resultados de “baja probabilidad/alta gravedad”. Esto es comprensible ya que los accidentes e incidentes graves son eventos de alto perfil y son fáciles de contar. Sin embargo, desde una perspectiva de gestión de rendimiento en materia de la seguridad operacional, existen inconvenientes en una dependencia excesiva de accidentes e incidentes graves como un indicador fiable del rendimiento en materia de seguridad operacional. Por ejemplo, los accidentes e incidentes graves son poco frecuentes (puede haber un solo accidente en un año, o ninguno) lo que hace difícil la realización de análisis estadísticos para identificar tendencias. Esto no indica necesariamente que el sistema es seguro. Una consecuencia de confiar en este tipo de datos es un falso sentido de confianza potencial en que el rendimiento en materia de seguridad operacional de una organización o sistema es eficaz, cuando de hecho puede estar peligrosamente cerca de un accidente.

4.3.1.9 Los indicadores avanzados son medidas que se centran en los procesos y aportes que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como “SPI de actividad o proceso” dado que vigilan y miden las condiciones que tienen el potencial de convertirse en un resultado específico o contribuir al mismo.

4.3.1.10 Los ejemplos de SPI avanzados que impulsan al desarrollo de capacidades organizativas para la gestión proactivo del rendimiento en materia de seguridad operacional comprenden cosas tales como “porcentaje del personal que ha completado con éxito la instrucción de seguridad operacional a tiempo” o “la frecuencia de las actividades de ahuyentamiento de aves”.

4.3.1.11 Los SPI avanzados también pueden informar a la organización sobre cómo su operación se enfrenta al cambio, incluyendo los cambios en su entorno operacional. La atención se centrará en anticipar puntos débiles y vulnerabilidades como resultado del cambio o la supervisión del rendimiento después de un cambio. Un ejemplo de SPI para vigilar un cambio en las operaciones sería “el porcentaje de sitios que han implementado el procedimiento X”.

4.3.1.12 Para una indicación más precisa y útil del rendimiento en materia de la seguridad operacional, los SPI de resultados, que miden tanto eventos de “baja probabilidad/alta gravedad” como eventos de “alta probabilidad/baja gravedad”, deben combinarse con los SPI avanzados. En la Figura 4-2 se ilustra el concepto de indicadores avanzados y de resultados que proporciona una imagen más completa y realista del rendimiento de la organización en materia de seguridad operacional.

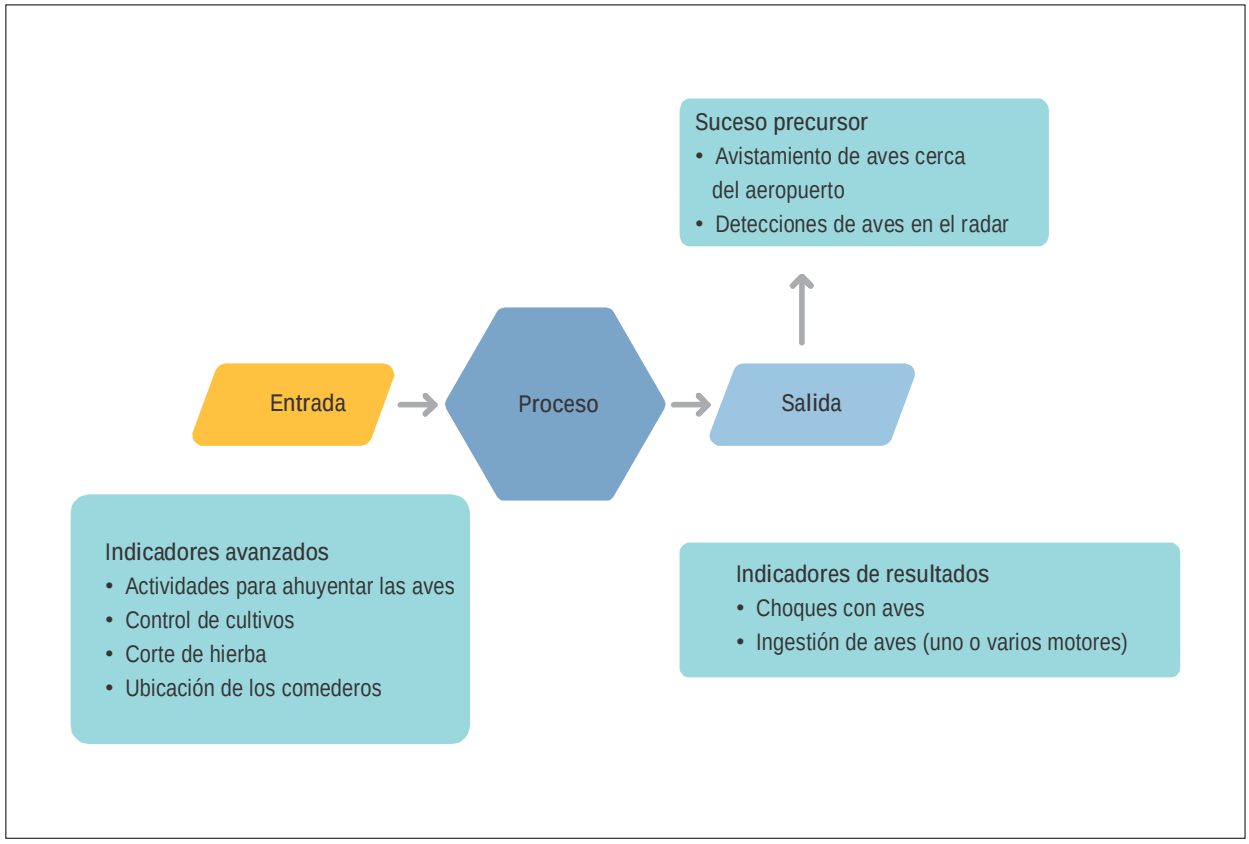


Figura 4-2. Fases del concepto de indicador avanzado y de indicador de resultados

4.3.2 Selección y definición de los SPI

4.3.2.1 Los SPI son los parámetros que le proporcionan a la organización una visión de su desempeño de seguridad operacional: dónde ha estado, dónde está ahora y hacia dónde se dirige, en relación con la seguridad operacional. Esta imagen actúa como una base sólida y defendible sobre la cual se toman decisiones de seguridad operacional basadas en datos de la organización. Estas decisiones, a su vez, afectan positivamente el rendimiento en materia de seguridad operacional de la organización. Por lo tanto, la identificación de los SPI debe ser realista, pertinente y estar vinculada a los objetivos de seguridad operacional, independientemente de su carácter simple o complejo.

4.3.2.2 Es probable que la selección inicial de los SPI se limite a la observación y medición de parámetros que representan sucesos o procesos que son fáciles o convenientes de captar (datos de seguridad operacional que pueden estar fácilmente disponibles). Idealmente, los SPI deberían enfocarse en parámetros que son indicadores importantes del rendimiento en materia de seguridad operacional, en lugar de aquellos que son fáciles de alcanzar.

4.3.2.3 Los SPI deberían ser:

a) relacionados con el objetivo de seguridad operacional que pretenden indicar;

b) seleccionados o desarrollados en base a datos disponibles y mediciones fiables;

c) apropiadamente específicos y cuantificables; y

d) realistas, teniendo en cuenta las posibilidades y limitaciones de la organización.

4.3.2.4 Normalmente, se requiere una combinación de SPI para proporcionar una indicación clara del rendimiento en materia de seguridad operacional. Debería haber un vínculo claro entre los SPI de resultados y los avanzados. Lo ideal sería definir los SPI de resultados antes de determinar los SPI avanzados. La definición de un SPI precursor vinculado a un suceso o condición más grave (SPI de resultados) asegura que existe una clara correlación entre ambos. Todos los SPI, tanto de resultados como avanzados, son igualmente válidos y valiosos. En la Figura 4-3 se ilustra un ejemplo de estos enlaces.

4.3.2.5 Es importante seleccionar los SPI que se relacionan con los objetivos de seguridad operacional de la organización. Tener SPI que estén bien definidos y alineados facilitará la identificación de las metas de rendimiento en materia de seguridad operacional (SPT), lo que mostrará el progreso hacia el logro de los objetivos de seguridad operacional. Esto le permite a la organización asignar recursos con el mayor efecto de seguridad operacional al saber exactamente lo que se requiere y cuándo y cómo actuar para lograr el rendimiento en materia de seguridad operacional previsto. Por ejemplo, un Estado tiene el objetivo de seguridad operacional de “reducir el número de salidas de pista en un 50% en tres años” y un SPI bien alineado de “número de salidas de pista por millón de salidas en todos los aeródromos”. Si el número de salidas de pista disminuye inicialmente cuando comienza la observación, pero empieza a subir nuevamente después de doce meses, el Estado podría optar por reasignar recursos fuera de un área donde, de acuerdo con los SPI, el objetivo de seguridad operacional se está logrando fácilmente y hacia la reducción de las salidas de pista para aliviar la tendencia no deseada.

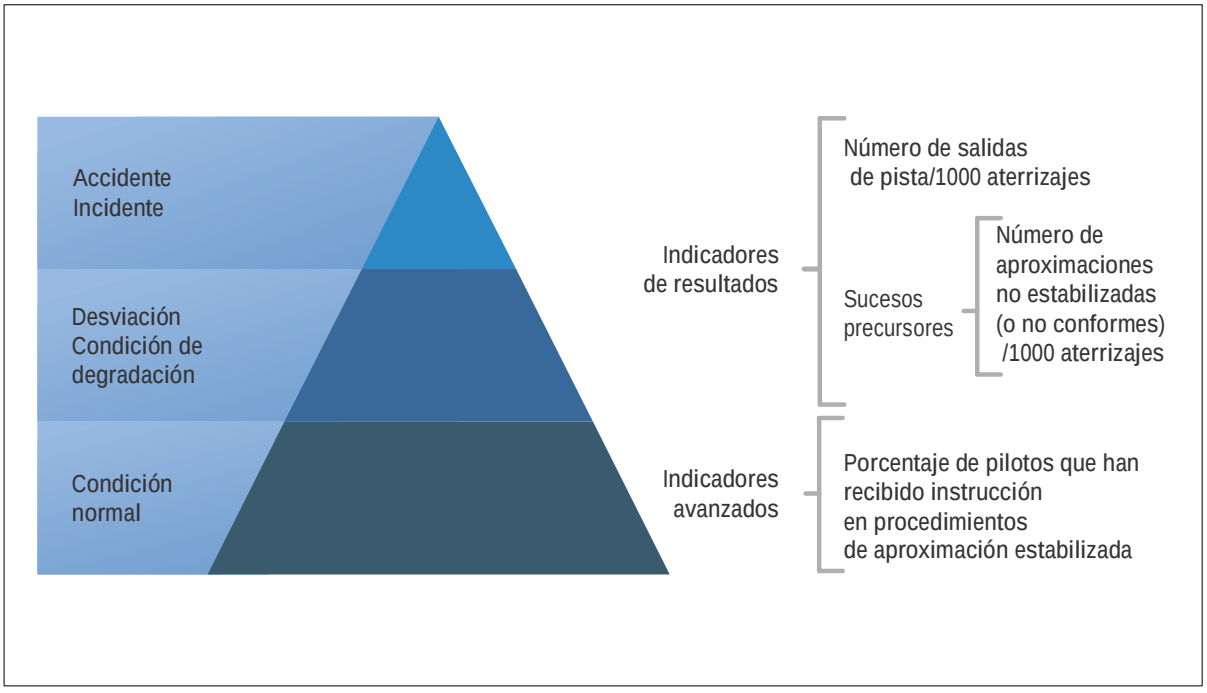


Figura 4-3. Ejemplos de enlaces entre los indicadores de resultados y los avanzados

Definición de los SPI

4.3.2.6 El contenido de cada SPI debería incluir:

a) una descripción de lo que mide el SPI;

b) el propósito del SPI (lo que se pretende gestionar y a quién se desea informar);

c) las unidades de medida y cualquier requisito para su cálculo;

d) quién es responsable de recopilar, validar, controlar, informar y actuar sobre el SPI (puede tratarse de personal de diferentes partes de la organización);

e) dónde o cómo deben recopilarse los datos; y

f) las frecuencias de las notificaciones, la recopilación, la observación y el análisis de los datos del SPI.

Los SPI y las notificaciones de seguridad operacional

4.3.2.7 Los cambios en las prácticas operacionales pueden llevar a notificaciones insuficientes hasta que su impacto sea totalmente aceptado por los posibles notificadores. Esto se conoce como “sesgo de la notificación”. Los cambios en las disposiciones relacionadas con la protección de la información de seguridad operacional, y las fuentes relacionadas, también podrían llevar a un exceso de notificaciones. En ambos casos, el sesgo de las notificaciones puede distorsionar la intención y la precisión de los datos utilizados para el SPI. Si se emplean juiciosamente, las notificaciones de seguridad operacional aún pueden proporcionar datos valiosos para la gestión del rendimiento en materia de seguridad operacional.

4.3.3 Establecimiento de metas de rendimiento en materia de seguridad operacional

4.3.3.1 Las metas de rendimiento en materia de seguridad operacional (SPT) definen los logros deseados de rendimiento en la materia a corto y mediano plazo. Actúan como “hitos” que proporcionan la confianza de que la organización está en el camino correcto para lograr sus objetivos de seguridad operacional y proporcionan una forma mensurable de verificar la eficacia de las actividades de gestión del rendimiento en materia de seguridad operacional. La configuración de las SPT debe tener en cuenta factores como el nivel predominante del riesgo de seguridad operacional, la tolerabilidad de los riesgos de seguridad operacional y las expectativas con respecto a la seguridad operacional del sector de la aviación en particular. La configuración de las SPT debería determinarse después de considerar lo que puede lograrse realmente para el sector de aviación conexo y el rendimiento reciente de la SPI en particular, cuando se dispone de datos históricos de tendencia.

4.3.3.2 Si la combinación de los objetivos de seguridad operacional, los SPI y las SPT es de tipo SMART (específica, medible, alcanzable, realista y oportuna), permitirá a la organización demostrar de manera más efectiva su desempeño de seguridad operacional. Hay múltiples enfoques para lograr los objetivos de la gestión del rendimiento en materia de seguridad operacional, especialmente la configuración de las SPT. Un enfoque entraña el establecimiento general de objetivos de seguridad operacional de alto nivel con SPI alineados para luego identificar niveles razonables de mejoras después de haberse establecido una línea base de rendimiento de seguridad operacional. Estos niveles de mejoras pueden basarse en objetivos específicos (p. ej., porcentaje de disminución) o en el logro de una tendencia positiva. Otro enfoque que se puede utilizar cuando los objetivos de seguridad operacional son SMART es hacer que las metas de seguridad operacional actúen como hitos para lograr los objetivos de seguridad operacional. Cualquiera de estos enfoques es válido y puede haber otros que la organización encuentre efectivos para demostrar su rendimiento en materia de seguridad operacional. Se pueden aplicar diferentes enfoques en combinación según corresponda a las circunstancias específicas.

Establecimiento de metas con objetivos de seguridad operacional de alto nivel

4.3.3.3 Las metas se establecen con el acuerdo de la administración superior respecto de los objetivos de seguridad operacional de alto nivel. Luego, la organización identifica los SPI apropiados que mostrarán una mejora en el rendimiento en materia de seguridad operacional con respecto a los objetivos de seguridad operacional acordados. Los SPI se medirán utilizando fuentes de datos existentes, pero también pueden requerir la recopilación de datos adicionales. Luego, la organización comienza a reunir, analizar y presentar los SPI. Las tendencias comenzarán a surgir, proporcionando una visión general de los resultados de seguridad operacional de la organización y si se dirige hacia sus objetivos de seguridad operacional o se aparta de los mismos. En este punto, la organización puede identificar SPT razonables y alcanzables para cada SPI.

Establecimiento de metas con objetivos de seguridad SMART

4.3.3.4 Los objetivos de seguridad operacional pueden ser difíciles de comunicar y de alcanzar; al dividirlos en objetivos de seguridad operacional concretos más pequeños, el proceso de alcanzarlos es más fácil de administrar. De esta forma, las metas forman un vínculo crucial entre la estrategia y las operaciones cotidianas. Las organizaciones deberían identificar áreas claves que impulsen el desempeño de seguridad operacional y establezcan una forma de medirlas. Una vez que la organización tiene una idea de cuál es su nivel de rendimiento actual mediante el establecimiento de una línea base de rendimiento en materia de seguridad operacional, puede comenzar a configurar las SPT para proporcionar a todos en el Estado un claro sentido de lo que deberían aspirar a lograr. La organización también puede utilizar la evaluación comparativa para ayudar a establecer metas de rendimiento. Esto implica usar información de rendimiento de organizaciones similares que ya han estado midiendo su desempeño para tener una idea de cómo les está yendo a otros en la comunidad.

4.3.3.5 En la Figura 4-4 se ilustra un ejemplo de la relación entre los objetivos de seguridad operacional, los SPI y las SPT. En este ejemplo, la organización registró 100 salidas de pista por millón de movimientos en 2018. Se ha determinado que esto es demasiado y se ha establecido un objetivo para reducir el número de salidas de pista en un 50% para 2022. Para observar, medir e informar sus progresos, la organización ha elegido como SPI las “salidas de pista por millón de movimientos por año”. La organización es consciente de que el progreso será más inmediato y eficaz si se establecen metas específicas que se correspondan con el objetivo de seguridad operacional. Por lo tanto, ha establecido un objetivo de seguridad operacional que equivale a una reducción promedio de 12,5% anual durante el período de notificación (cuatro años). Como se muestra en la representación gráfica, se espera que el progreso sea mayor en los primeros años y menor en los años posteriores. Esto está representado por una proyección curva hacia su objetivo. En la Figura 4-4:

a) el objetivo de seguridad operacional SMART es “una reducción del 50% en la tasa de salidas de pista para 2022”;

b) el SPI seleccionado es el “número de salidas de pista por millón de movimientos por año”; y

c) las metas de seguridad operacional relacionadas con este objetivo representan los hitos para alcanzar el objetivo de seguridad operacional SMART y corresponde a una reducción de alrededor del 12% anual hasta 2022;

    1) la SPT 1a es “inferior a 78 salidas de pistas por millón de movimientos en 2019”;

    2) la SPT 1b es “inferior a 64 salidas de pista por millón de movimientos en 2020”;

    3) la SPT 1c es “inferior a 55 salidas de pista por millón de movimientos en 2021”.

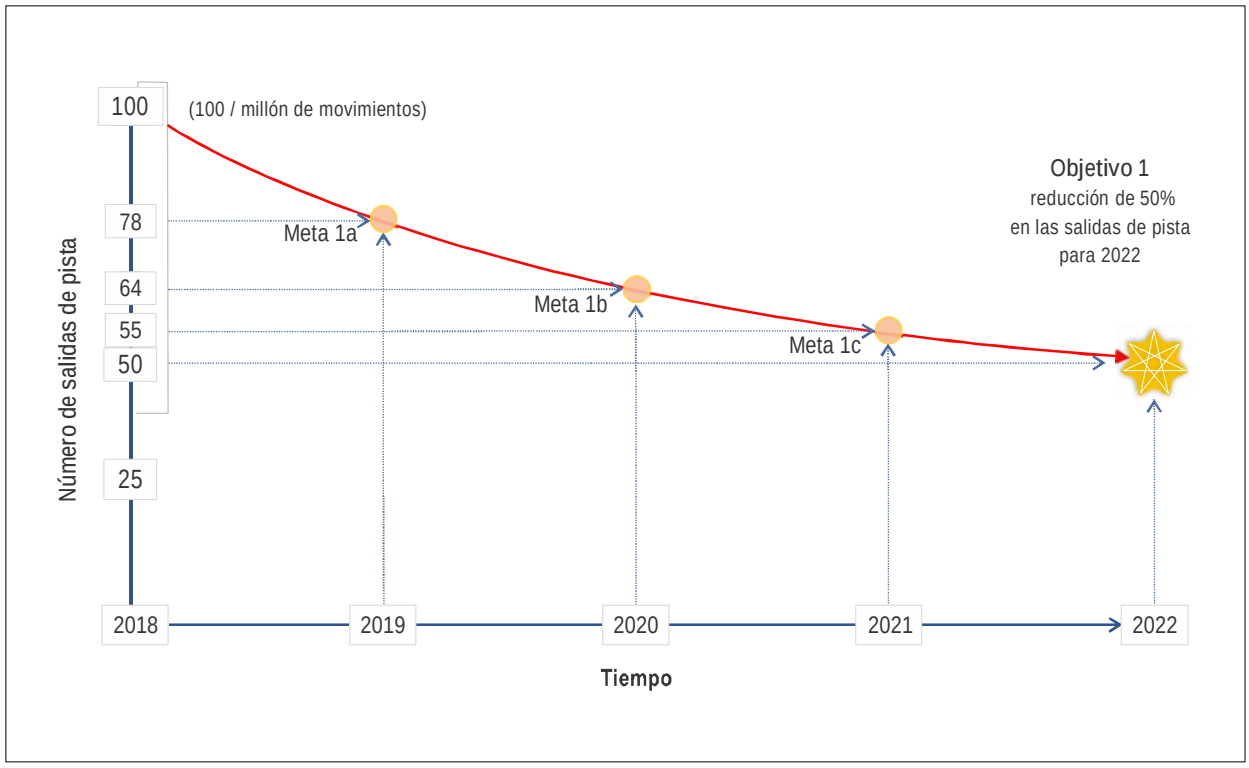


Figura 4-4. Ejemplo de SPT con objetivos de seguridad operacional SMART

Consideraciones adicionales para la selección de SPI y SPT

4.3.3.6 Al seleccionar SPI y SPT, debería también considerarse lo siguiente:

a) *Gestión de la carga de trabajo*. La creación de una cantidad viable de SPI puede ayudar al personal a gestionar su carga de trabajo de control y notificación. Lo mismo es cierto respecto de la complejidad de los SPI o la disponibilidad de los datos necesarios. Es mejor ponerse de acuerdo sobre lo que es factible, y luego priorizar la selección de los SPI sobre esta base. Si un SPI deja de contribuir al rendimiento de seguridad operacional, o ha recibido una prioridad menor, debería considerarse la interrupción de su aplicación en favor de un indicador más útil o de mayor prioridad.

b) *Extensión óptima de los SPI*. Una combinación de SPI que abarque las áreas de interés ayudará a obtener una visión más profunda del rendimiento general de la organización en materia de seguridad operacional y a tomar decisiones basadas en datos.

c) *Claridad de los SPI*. Al seleccionar un SPI, debería quedar en claro lo que se está midiendo y cuan a menudo se hace. Los SPI con definiciones claras ayudan a comprender los resultados, evitar mal entendidos y permitir comparaciones valiosas con el tiempo.

d) *Fomento de comportamientos deseados*. Las SPT pueden modificar comportamientos y contribuir a resultados deseados. Esto es especialmente importante si el logro de la meta se relaciona con recompensas institucionales, como la remuneración de la administración. Las SPT deberían fomentar comportamientos institucionales e individuales positivos que resulten deliberadamente en decisiones justificables y mejoras del rendimiento en materia de seguridad operacional. Al seleccionar SPI y SPT es igualmente importante tener en cuenta posibles comportamientos no deseados.

e) *Elección de medidas valiosas*. Es fundamental seleccionar SPI útiles, y no solo aquellos cuya medición sea fácil. La organización debería decidir cuáles son los parámetros de seguridad operacional más útiles, o sea los que orienten a la organización a la mejora de sus decisiones, gestión del rendimiento en materia de seguridad operacional, y logro de sus objetivos de seguridad operacional.

f) *Logro de las SPT*. Esta es una consideración particularmente importante y está relacionada con los comportamientos de seguridad operacional deseados. El logro de las SPT convenidas no siempre indicaría mejoras del rendimiento. La organización debería distinguir entre el mero logro de las SPT y su mejoramiento real y demostrable del rendimiento. Es imperativo que la organización considere el contexto en el que se alcanzó la meta, en vez de considerarla aisladamente. El reconocimiento de la mejora general del rendimiento, más que un logro individual de SPT fomentará comportamientos institucionales deseables y el intercambio de información de seguridad operacional que está en el centro de la SRM y del aseguramiento de la seguridad operacional. Esto podría mejorar las relaciones entre el Estado y el proveedor de servicios y su disposición a compartir datos e ideas de seguridad operacional.

Advertencias para el establecimiento de SPT

4.3.3.7 No siempre es necesario o apropiado definir las SPT dado que podrían haber SPI más fáciles de controlar en canto a tendencias que el uso de una meta determinada. Las notificaciones de la seguridad operacional son un ejemplo de cuándo una meta podría llevar a que las personas no notificaran (si la meta es no superar un número) o notificaran asuntos triviales a efectos de satisfacerla (si la meta consiste en alcanzar un determinado número). También podrían haber SPI que se utilizaran mejor para definir bien una dirección hacia la mejora continua del rendimiento en materia de seguridad operacional (es decir reducir el número de sucesos) en vez de utilizarse para definir una meta absoluta, que puede resultar difícil de determinar. En la determinación de SPT apropiadas debería también considerarse lo siguiente:

a) Posibilidad de comportamiento indeseable; si los administradores o las organizaciones se concentran demasiado en alcanzar valores numéricos como indicadores de éxito podrían no lograr la mejora prevista del rendimiento en materia de seguridad operacional.

b) Objetivos operacionales; concentrarse demasiado en el logro de objetivos operacionales (salidas en hora, reducción de costos generales, etc.) sin equilibrar las SPT puede llevar al “logro de metas operaciones” aunque no necesariamente a una mejora del rendimiento en materia de seguridad operacional.

c) Concentración en la cantidad más que en la calidad; esto puede alentar al personal o a los departamentos a alcanzar la meta pero, al hacerlo, podría entregarse un producto o servicio de baja calidad.

d) Limitación de innovaciones; aunque no se haya previsto, el haber alcanzado una meta puede llevar al relajamiento y a pensar que no se necesitan más mejoras, cayéndose así en complacencia.

e) Conflicto institucional; las metas pueden crear conflictos entre departamentos y organizaciones cuando discuten sobre quién recae la responsabilidad en vez de tratar de trabajar en conjunto.

4.3.4 Medición del rendimiento en materia de seguridad operacional

La medición correcta del rendimiento en materia de seguridad operacional involucra decidir la mejor forma de medir el logro de los objetivos en la materia. Esto variará de Estado en Estado y de proveedor de servicios en proveedor de servicios. Las organizaciones deberían tomarse el tiempo de elaborar su conciencia estratégica de lo que impulsa la mejora de la seguridad operacional para alcanzar los objetivos.

4.3.5 Uso de SPI y SPT

Los SPI y las SPT pueden utilizarse en diferentes formas para demostrar el rendimiento en materia de seguridad operacional. Es fundamental que las organizaciones adapten, seleccionen y apliquen varias herramientas y enfoques de medición dependiendo de sus circunstancias específicas y del carácter de lo que se está midiendo. Por ejemplo, en algunos casos, las organizaciones podrían adoptar SPI que tengan SPT conexas. En otras situaciones, puede ser preferible concentrarse en el logro de una tendencia positiva en los SPI, sin valores específicos para metas. El paquete de las métricas de rendimiento seleccionadas normalmente incluirá una combinación de ambos enfoques.

4.4 OBSERVACIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL

4.4.1 Una vez que la organización ha identificado las metas basadas en los SPI que en su opinión producirán los resultados previstos, debe cerciorarse de que las partes interesadas actúan en consecuencia mediante la asignación de claras responsabilidades para su realización. La definición de SPT para cada autoridad aeronáutica, sector y proveedor de servicios contribuye al logro del ALoSP para el Estado mediante la asignación de un claro proceso de rendición de cuentas.

4.4.2 Deberían establecerse mecanismos para la observación y medición del rendimiento de la organización en materia de seguridad operacional a efectos de identificar los cambios que puedan ser necesarios si el progreso alcanzado no es el esperado y reforzar el compromiso de la organización para satisfacer sus objetivos de seguridad operacional.

4.4.3 Rendimiento básico en materia de seguridad operacional

La comprensión de la forma en que los planes de la organización avanzan hacia sus objetivos de seguridad operacional exige saber dónde se encuentra en relación con la misma. Una vez establecida y funcionando la estructura de rendimiento en materia de seguridad operacional de la organización (objetivos, indicadores, metas, activadores de seguridad operacional), es posible conocer su rendimiento básico en la materia a través de un período de control y observación. El rendimiento básico en materia de seguridad operacional es el desempeño de seguridad operacional al inicio del proceso de medición de dicho rendimiento, el punto de referencia a partir del cual pueda medirse el progreso. En el ejemplo de las Figuras 4-3 y 4-4, el rendimiento básico en materia de seguridad operacional para ese objetivo determinado “100 salidas de pistas por millón de movimientos durante el año (2018)”. A partir de esta base sólida, pueden registrarse indicadores y metas precisas y significativas.

4.4.4 Perfeccionamiento de los SPI y lasSPT

4.4.4.1 Los SPI y las SPT conexas deberán revisarse para determinar si están proporcionando la información necesaria para el seguimiento de los progresos alcanzados hacia los objetivos de seguridad operacional y garantizar que las metas son realistas y pueden alcanzarse.

4.4.4.2 La gestión de rendimiento en materia de seguridad operacional es una actividad continua. Los riesgos de seguridad operacional o la disponibilidad de datos cambian con el tiempo. Los SPI iniciales pueden elaborarse utilizando recursos limitados de información de seguridad operacional. Más Adelante, pueden establecerse más canales de notificación, puede disponerse de más datos de seguridad operacional y las capacidades de análisis de seguridad de la organización probablemente alcancen mayor madurez. Puede resultar apropiado para las organizaciones elaborar SPI iniciales sencillos (más amplios). A medida que acopian más datos y logran una mayor capacidad de gestión de la seguridad operacional, las organizaciones pueden considerar el perfeccionamiento del alcance de los SPI y las SPT para corresponder mejor a los objetivos de seguridad operacional deseados. Las organizaciones pequeñas y de poca complejidad pueden optar por refinar sus SPI y SPT o seleccionar indicadores genéricos (pero específicos) que se apliquen a la mayoría de los sistemas aeronáuticos. Algunos ejemplos de indicadores genéricos serían:

a) sucesos que incluyan daño estructural al equipo;

b) sucesos que indiquen circunstancias en que casi haya ocurrido un accidente;

c) sucesos en que personal de operaciones o miembros de la comunidad aeronáutica experimentaron lesiones mortales o graves;

d) sucesos en que miembros del personal de operaciones resultaron incapacitados o no pudieron realizar sus tareas en condiciones de seguridad;

e) proporción de notificaciones voluntarias de sucesos; y

f) proporción de notificaciones obligatorias de sucesos.

4.4.4.3 Las organizaciones más grandes y complejas pueden optar por instituir una gama más amplia o profunda de SPI y SPT e integrar indicadores genéricos como los indicados anteriormente con otros específicos de cada actividad. Por ejemplo, un gran aeropuerto que preste servicios a importantes líneas aéreas y esté situado bajo un espacio aéreo complejo podría considerar la combinación de algunos de los SPI genéricos con SPI de mayor alcance para representar aspectos específicos de su operación. La observaciónj de éstos puede exigir mayores esfuerzos pero probablemente producirá resultados superiores en materia de seguridad operacional. Existe una clara correlación entre la complejidad relativa de los SPI y SPT y la escala y complejidad de las operaciones del Estado o de los proveedores de servicios. Esta complejidad relativa debería reflejarse en el indicador y en la meta establecidos. Los responsables del establecimiento de la gestión del rendimiento en materia de seguridad operacional deberían tener conciencia de esto.

4.4.4.4 El conjunto de SPI y SPT seleccionados por una organización debería realizarse periódicamente para asegurar su validez continua como indicaciones del rendimiento de la organización en materia de seguridad operacional. Entre las razones para continuar, suspender o modificar SPI y SPT figuran las siguientes:

a) los SPI notifican continuamente el mismo valor (como 0% ó 100%); es improbable que estos SPI proporcionen información útil para la toma de decisiones por la administración superior;

b) SPI con comportamientos similares se consideran como duplicados;

c) la SPT para un SPI implantada para medir la introducción de un programa o mejoras previstas se ha alcanzado;

d) otra preocupación de seguridad operacional pasa a tener mayor prioridad en cuanto a control y medición;

e) obtener una mejor comprensión de una preocupación determinada de seguridad operacional afinando las características específicas de un SPI (es decir reducir el “ruido” para aclarar la “señal”); y

f) los objetivos de seguridad operacional han cambiado y, en consecuencia, los SPI deben actualizarse para seguir siendo pertinentes.

4.4.5 Activadores de seguridad operacional

4.4.5.1 Corresponde presentar una breve perspectiva de las funciones de activadores para ayudar su posible función en el contexto de la gestión del rendimiento en materia de seguridad operacional por parte de una organización.

4.4.5.2 Un elemento activador es un nivel establecido o valor de criterio que activa (inicia) una evaluación, decisión, ajuste o medida correctiva relacionada con el indicador en cuestión. Un método para establecer criterios de activadores fuera de límites para las SPT es el uso del principio de desviación estándar de la población (STDEVP). Este método permite obtener el valor de desviación estándar (SD) sobre la base de los datos históricos precedentes de un determinado indicador de la seguridad operacional. El valor SD más el valor promedio (media) del conjunto de datos históricos constituye el valor básico de activación para el siguiente período de control. El principio de SD (función estadística básica) establece los criterios de nivel de los activadores sobre la base del desempeño histórico real del

indicador determinado (conjunto de datos), incluyendo su carácter volátil (fluctuaciones de los puntos de datos). Un conjunto de datos históricos más volátiles resultará normalmente en un mayor valor de nivel de activador (más generoso) para el siguiente período de control. Los activadores proporcionan advertencias tempranas que permiten que los encargados de tomar decisiones de seguridad operacional lo hagan sobre la base de una mayor información mejorando, así, el rendimiento en materia de seguridad operacional. En la Figura 4-5 se presenta un ejemplo de niveles de activadores basados en desviaciones estándar (SD). En el ejemplo, podría ser necesario adoptar decisiones basadas en datos y medidas de mitigación de seguridad operacional cuando la tendencia va más allá de +1SD o +2SD a partir de la media del período precedente. A menudo los niveles de activadores (en este caso +1SD, +2SD o mayores que +2SD) corresponderán los niveles de la gestión de decisiones y a la urgencia de tomar medidas.

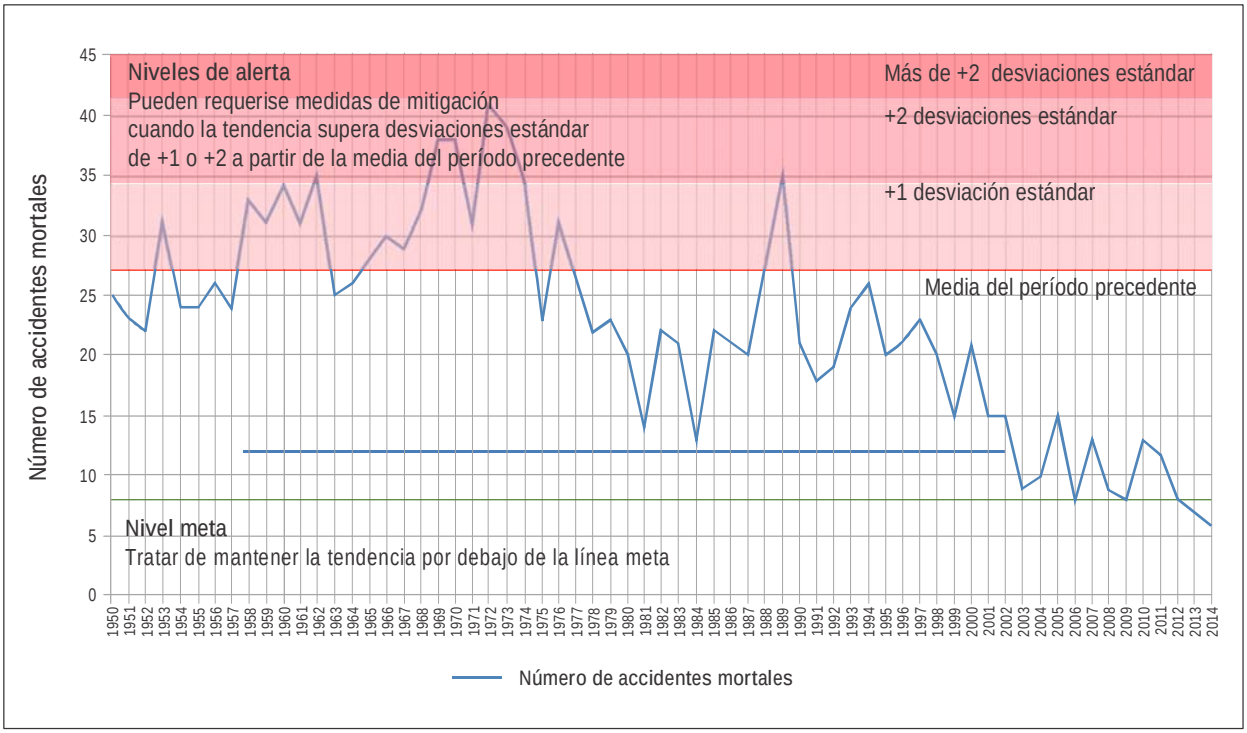


Figura 4-5. Ejemplo de representación de niveles de activadores (alertas) de seguridad operacional

4.4.5.3 Una vez definidos las SPT y los valores de activadores (si se utilizan), podrá hacerse el seguimiento de su SPI conexo para determinar sus respectivos estados de rendimiento. También podría compilarse o combinarse un resumen consolidado del resultado general del comportamiento de las SPT y activadores en el paquete total de SPI para un período de control determinado. Pueden asignarse valores cualitativos (satisfactorio/insatisfactorio) a cada logro de SPT y cada nivel de activador que no se haya traspasado. Alternativamente, pueden utilizarse valores numéricos (puntos) para obtener una medición cuantitativa del rendimiento general del paquete de SPI.

4.4.5.4 Cabe señalar que los valores de activación sirven para activar (iniciar) una evaluación, decisión, ajuste o medida correctiva relativa a un indicador particular. La activación de un SPI no es necesariamente catastrófica ni indicativa de falla. Constituye meramente un signo de que la actividad ha ido más allá del límite predeterminado. El activador tiene por objeto llamar la atención de quienes adoptan decisiones para que ahora puedan tomar, o no, medidas correctivas dependiendo de las circunstancias.

4.4.6 Advertencia sobre los activadores

4.4.6.1 La identificación de niveles fiables para activadores presenta retos. Los activadores y sus niveles conexos funcionan mejor cuando se dispone de amplios datos de seguridad operacional y de capacidades de gestión de los mismos. Esto puede imponer una carga de trabajo adicional en la organización. La noción de activador se diseñó para la SRM de sistemas puramente técnicos (p. ej., vigilancia de los motores de aeronave). En este caso, grandes volúmenes de datos cuantitativos apoyan la identificación de activadores precisos y niveles de activación. La noción de activadores es menos pertinente a la SRM de sistemas sociotécnicos. Los sistemas sociotécnicos son sistemas en los que las personas interactúan activamente con procesos y tecnologías para alcanzar los objetivos de prestación de servicios o de producción del sistema. Tanto los SSP como SMS son sistemas sociotécnicos. La utilización de activadores menos fiables y significativos en los sistemas sociotécnicos se debe a las limitaciones de las medidas fiables cuando hay seres humanos involucrados.

4.4.6.2 Por lo tanto, se necesita un enfoque más flexible para que los activadores tengan sentido. En el Anexo 19 no se requiere que los Estados o proveedores de servicios definan niveles de activadores para cada SPI. No obstante, hay beneficios para aquellas organizaciones en que los datos para un SPI son muy específicos, hay datos suficientes y estos son suficientemente fiables.

4.4.6.3 La Figura 4-6 es una ampliación del ejemplo anterior, “reducción del 50% en las salidas de pista para 2022”. En este escenario, se trata ahora del año 2020. La organización ha estado acopiando datos de seguridad operacional (SPI – “ninguna salida de pista/millón de movimientos/año”) y ha trabajado con las partes interesadas para reducir esos casos. La SPT para 2019 (<78 salidas de pista/millón de movimientos en el año) ha sido alcanzada. No obstante, el SPI muestra que, no solo no se ha alcanzado la SPT para 2020 (<64 salidas de pista/millón de movimientos en el año), sino que el número de salidas de pista ha superado el nivel de activación en dos períodos de notificación consecutivos. Los encargados de tomar decisiones han sido alertados respecto al deterioro del rendimiento en materia de seguridad operacional y ahora pueden tomar decisiones sobre la base de los datos en cuanto a la adopción de ulteriores medidas. Estas decisiones basadas en datos estarán dirigidas a devolver al rendimiento en materia de seguridad operacional a la zona aceptable y dirigirlo hacia el logro de su objetivo de seguridad.

4.4.7 Identificación de medidas requeridas

4.4.7.1 De hecho el resultado más importante de establecer una estructura de gestión del rendimiento en materia de seguridad operacional es la presentación de información a los encargados de tomar decisiones en la organización para que puedan hacerlo sobre la base de datos e información de seguridad operacional actuales y fiables. La finalidad debería ser siempre la adopción de decisiones con arreglo a la política de seguridad operacional y tendientes al logro de objetivos en esa materia.

4.4.7.2 En relación con la gestión del rendimiento en materia de seguridad operacional, la toma de decisiones basada en datos se dirige a adoptar decisiones eficaces bien fundamentadas sobre la base de los resultados de los SPI controlados y medidos, o de otras notificaciones y análisis de datos e información de seguridad operacional. El uso de datos de seguridad operacional válidos y pertinentes combinados con información que proporcione contexto apoya la toma de decisiones en la organización acorde con sus objetivos y metas de seguridad operacional. La información de contexto también puede comprender otras prioridades de partes interesadas, deficiencias conocidas en los datos y otros datos complementarios para evaluar los aspectos a favor y en contra, las oportunidades, limitaciones y riesgos relacionados con la decisión. El contar con información rápidamente disponible y de fácil interpretación contribuye a mitigar sesgos, influencias y errores humanos en el proceso de toma de decisiones.

4.4.7.3 La toma de decisiones basada en datos también apoya la evaluación de decisiones adoptadas en el pasado en apoyo de lograr la correspondencia con los objetivos de seguridad operacional. En el Capítulo 6 figura más orientación sobre la toma de decisiones basada en datos.

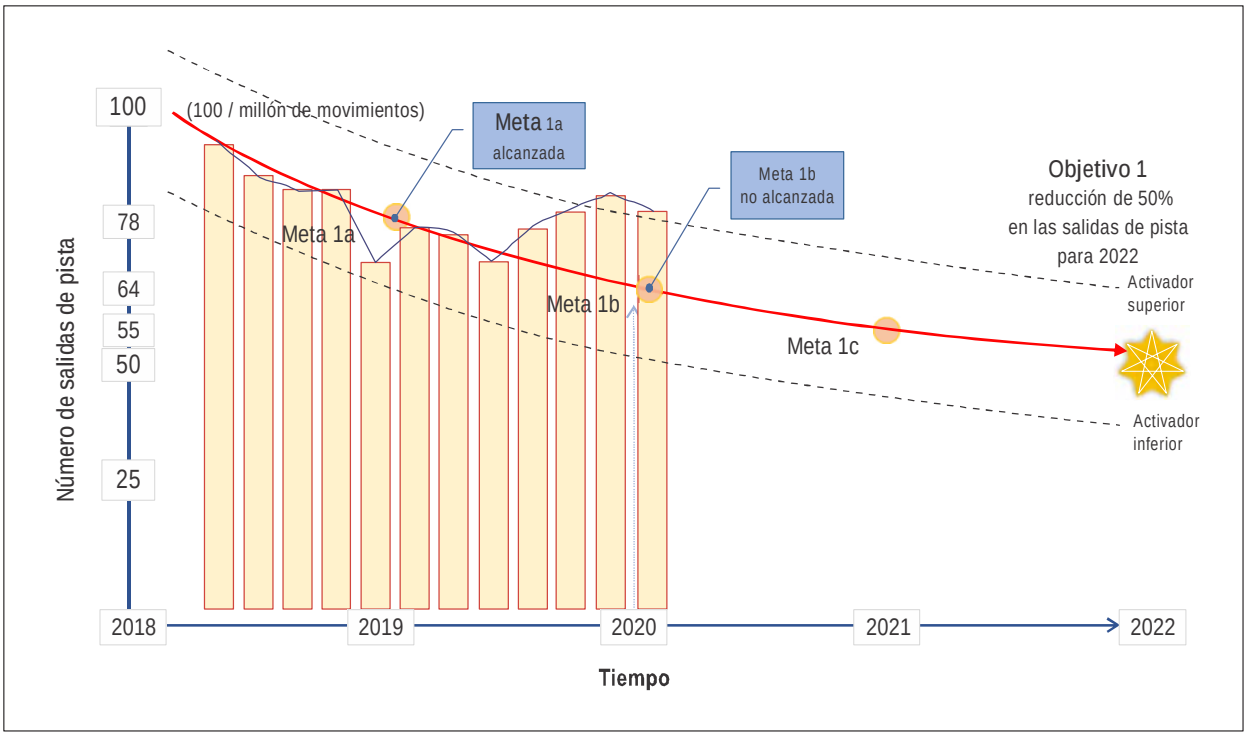


Figura 4-6. Ejemplo de establecimiento de activadores de seguridad operacional

4.5 ACTUALIZACIÓN DE LOS OBJETIVOS DE SEGURIDAD OPERACIONAL

La gestión del rendimiento en materia de seguridad operacional no pretende ser del tipo “establecer y olvidar”. La gestión de rendimiento en materia de seguridad operacional tiene carácter dinámico y es fundamental para el funcionamiento de cada Estado y de cada proveedor de servicios, y debería revisarse y actualizarse:

a) periódicamente, con arreglo al ciclo periódico establecido y convenido por el Comité de seguridad operacional de alto nivel;

b) sobre la base de insumos de los análisis de seguridad operacional (véanse detalles en el Capítulo 6); y

c) en respuesta a cambios importantes en la operación, los riesgos principales o el entorno.

Capítulo 5

SISTEMAS DE RECOPILACIÓN Y PROCESAMIENTO DE DATOS SOBRE SEGURIDAD OPERACIONAL

5.1 INTRODUCCIÓN

5.1.1 La distinción entre datos de seguridad operacional e información sobre seguridad operacional figura en las definiciones del Anexo 19. Los datos de seguridad operacional son lo que se informa o registra inicialmente como resultado de una observación o medición. Se transforman en información sobre seguridad operacional cuando son procesados, organizados, integrados o analizados en un determinado contexto a fin de que sean de utilidad para fines de gestión de la seguridad operacional. La información sobre seguridad operacional puede continuar procesándose en diferentes formas para extraer significados diferentes.

5.1.2 La gestión eficaz de la seguridad operacional depende mucho de la eficacia de la recopilación, análisis y capacidades de gestión general de los datos de seguridad operacional. El tener una sólida base de datos de seguridad operacional y de información de seguridad operacional es fundamental para la gestión de dicha seguridad, dado que constituye el fundamento para la toma de decisiones basada en datos. Los datos y la información sobre seguridad operacional fiables son necesarios para identificar tendencias, tomar decisiones y evaluar el rendimiento en materia de seguridad operacional en relación con las metas y objetivos de seguridad operacional así como para evaluar los riesgos pertinentes.

5.1.3 En el Anexo 19 se exige que los proveedores de servicios definan y mantengan un proceso formal para recopilar, registrar, actuar en consecuencia y generar información sobre peligros asociados a sus actividades, sobre la base de una combinación de métodos reactivos y proactivos de recolección de datos de seguridad operacional.

5.1.4 Análogamente, en el Capítulo 8 del Anexo 13 — *Investigación de accidentes e incidentes de aviación,* se exige que los Estados establezcan y mantengan una base de datos de accidentes e incidentes para facilitar el análisis eficaz de la información sobre deficiencias de seguridad operacional reales o posibles y para determinar las medidas preventivas necesarias.

5.1.5 En el Anexo 19 también se exige que los Estados establezcan sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) para captar, almacenar, agregar y permitir el análisis de datos e información sobre seguridad operacional a efectos de apoyar sus actividades de gestión del rendimiento en materia de seguridad operacional. El SDCPS es un término genérico utilizado para referirse a los sistemas de procesamiento y notificación, las bases de datos y esquemas para intercambio de información sobre seguridad operacional así como la información registrada. El término “base de datos de seguridad operacional” puede referirse a una base de datos o a varias de ellas. Las autoridades estatales con responsabilidades para la implementación del SSP deberían tener acceso al SDCPS para apoyar sus responsabilidades de seguridad operacional.

5.1.6 Los proveedores de servicios también deben elaborar y mantener los medios para verificar su rendimiento en materia de seguridad operacional con referencia a sus SPI y SPT en apoyo de sus objetivos de seguridad operacional mediante los SDCPS. Estos pueden basarse en métodos reactivos y proactivos de recopilación de datos e información sobre seguridad operacional.

5.1.7 La orientación que figura en este capítulo es igualmente válida para Estados y proveedores de servicios a efectos de garantizar que los datos y la información sobre seguridad operacional recopilados permitirán tomar decisiones en forma eficaz y válida.

5.1.8 Las organizaciones deberían asegurar que cuentan con personal cualificado para recopilar y almacenar datos de seguridad operacional así como con las competencias necesarias para procesarlos. Esto normalmente requiere individuos con sólidas habilidades en tecnología de la información así como conocimiento de requisitos, normalización, recopilación y almacenamiento de datos y la gobernanza conexa además de la capacidad para entender posibles cuestiones pueden ser necesarias para análisis. Además, la organización debería garantizar que cada SDCPS tiene un custodio designado para aplicar la protección de los datos e información sobre seguridad operacional así como fuentes conexas con arreglo al Apéndice 3 del Anexo 19. En el Capítulo 7 figuran más detalles al respecto.

5.2 RECOPILACIÓN DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

5.2.1 Objetivos en los diferentes niveles del sistema de aviación

5.2.1.1 Desde la década de 1970 la OACI ha venido introduciendo disposiciones en sus Anexos, Procedimientos para los servicios de navegación aérea (PANS) y otros documentos por las que se exige a los Estados que establezcan sistemas de notificación para recopilar datos e información sobre seguridad operacional. La mayoría de estas disposiciones se relacionan con sistemas de notificación de seguridad operacional específicos de cada sector, con la excepción del Anexo 13 que se concentra específicamente en la notificación de accidentes e incidentes graves. Las disposiciones sobre sistemas de notificación obligatoria y voluntaria de seguridad operacional que figuran en el Anexo 19 se originaron en el Anexo 13.

5.2.1.2 Muchos proveedores de servicios han recopilado un considerable volumen de datos e información sobre seguridad operacional, incluyendo sistemas de notificación obligatoria y voluntaria de seguridad operacional así como sistemas automáticos de captación de datos. Estos datos e información sobre seguridad operacional permite que los proveedores de servicios identifiquen peligros y apoyan las actividades de gestión del rendimiento en materia de seguridad operacional a nivel de proveedor de servicios. Existen varias ventajas en la compartición de información sobre seguridad operacional, estando entre las más importantes la identificación de peligros que van más allá de la percepción de un proveedor de servicios individual. En el Capítulo 6 figura información sobre la compartición e intercambio de información sobre seguridad operacional.

5.2.1.3 En el Anexo 19 se exige que los Estados establezcan SDCPS para captar, almacenar, agregar y permitir el análisis de datos e información sobre seguridad operacional para apoyar la identificación de peligros a través de todo el sistema de aviación. Esto implica mucho más que el mero acceso a la visualización de los datos con fines de vigilar el rendimiento en materia de seguridad operacional de los proveedores de servicios. Además, la implantación de sistemas de notificación y bases de datos para la recopilación de datos e información sobre seguridad operacional no es suficiente para asegurar la disponibilidad de dichos datos a efectos de permitir su análisis. Los Estados también deben implantar leyes, reglamentos, procesos y procedimientos para garantizar que se obtienen, notifican y recopilan los datos e información sobre seguridad operacional identificados en el Anexo 19 a efectos de ingresarlos en el SDCPS. Esto requiere la implantación de medios de protección, según el Anexo 19, Apéndice 3, para asegurar el uso de datos e información sobre seguridad operacional para fines de mantener y mejorar dicha seguridad. También pueden instituirse arreglos para que terceras partes recopilen, almacenen y analicen los datos y la información sobre seguridad operacional en nombre del Estado. En el Capítulo 7 figura información sobre la protección de los datos y la información sobre seguridad operacional.

5.2.1.4 Además, los datos y la información sobre seguridad operacional deben recopilarse, almacenarse y analizarse a nivel regional por los grupos regionales de seguridad operacional de la aviación (RASG) a efectos de facilitar la identificación de peligros que trascienden las fronteras estatales y promover actividades en colaboración para mitigar los riesgos de seguridad operacional.

5.2.2 Determinación de los datos que han de recopilarse

5.2.2.1 Cada organización debe determinar cuáles son los datos y la información sobre seguridad operacional que debe recopilar para apoyar el proceso de gestión del rendimiento en materia de seguridad operacional y tomar decisiones en esa materia. Los requisitos de datos e información sobre seguridad operacional pueden determinarse aplicando un enfoque de arriba abajo o de abajo a arriba. El enfoque escogido puede estar influenciado por diferentes consideraciones, como las condiciones y prioridades nacionales y locales, o por la necesidad de proporcionar los datos para apoyar el control de los SPI.

5.2.2.2 La identificación y recopilación de datos de seguridad operacional debería corresponder a la necesidad de la organización de gestionar eficazmente la seguridad operacional. En algunos casos, el proceso de la SRM destacará la necesidad de contar con datos de seguridad operacional adicionales para evaluar en mejor forma las consecuencias (nivel de probabilidad y gravedad) y determinar los riesgos conexos. Análogamente, el proceso de gestión del rendimiento en materia de seguridad operacional puede subrayar la necesidad de contar con información adicional para una comprensión más completa de un problema particular de seguridad operacional o para facilitar el establecimiento o perfeccionamiento de los SPI.

5.2.2.3 Deben tenerse en cuenta los posibles sesgos que hubiere en la recolección y utilización de datos e información sobre seguridad operacional. Por ejemplo, el lenguaje utilizado en las notificaciones voluntarias puede a veces ser emocional o estar dirigido al logro de los objetivos de un individuo en particular, lo que no necesariamente correspondería a los mejores intereses de la organización en su totalidad. En estos casos, la información debería utilizarse con prudencia y sensatez.

5.2.2.4 Los Estados y proveedores de servicios deberían considerar la adopción de un enfoque integrado de la recopilación de datos de seguridad operacional procedentes de diferentes fuentes, tanto internas como externas. La integración permite a las organizaciones obtener una visión más exacta de sus riesgos de seguridad operacional y de los logros de sus objetivos en la materia. Cabe señalar que los datos y la información sobre seguridad operacional que inicialmente parecen no estar relacionados, más adelante podrían resultar críticos para identificar problemas de seguridad operacional y apoyar la toma de decisiones basada en datos.

5.2.2.5 Es aconsejable racionalizar el volumen de datos e información sobre seguridad operacional mediante la identificación de los aspectos que específicamente apoyan la gestión eficaz de la seguridad operacional dentro de la organización. Los datos y la información sobre seguridad operacional recopilados deberían apoyar la medición razonable del rendimiento de un sistema y la evaluación de los riesgos conocidos, así como la identificación de riesgos emergentes, dentro del alcance de las actividades de la organización. Los datos y la información sobre seguridad operacional requeridos serán influenciados por el volumen y la complejidad de las actividades de la organización.

5.2.2.6 En la Figura 5-1 se brindan ejemplos de datos e información sobre seguridad operacional típicos, que en muchos casos ya están disponibles. La coordinación entre departamentos o divisiones es necesaria para racionalizar las actividades de notificación y recopilación de datos de seguridad operacional a efectos de evitar la duplicación.

5.2.3 Investigaciones de accidentes e incidentes

En el Anexo 13 se exige que los Estados establezcan y mantengan una base de datos de accidentes e incidentes para facilitar el análisis eficaz de la información sobre deficiencias de la seguridad operacional reales o posibles y para determinar las medidas preventivas necesarias. Las autoridades estatales encargadas de la aplicación del SSP deberían tener acceso a la base de datos de accidentes e incidentes en apoyo de sus responsabilidades funcionales en materia de seguridad operacional. La información adicional para fundamentar medidas preventivas puede figurar en los informes finales sobre accidentes e incidentes que hayan sido objeto de investigación.

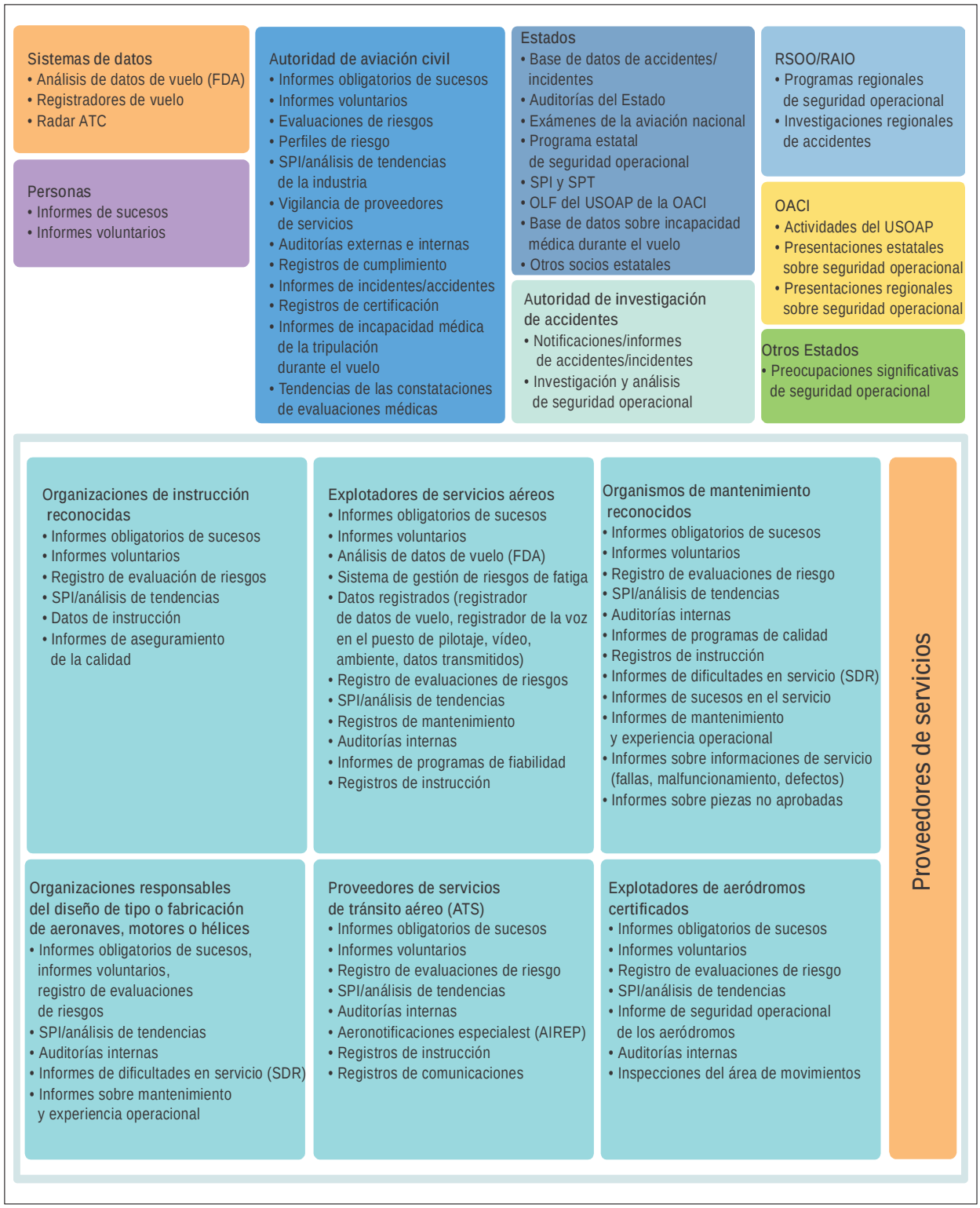


Figura 5-1. Fuentes típicas de datos e información sobre seguridad operacional

5.2.4 Investigaciones de seguridad operacional por autoridades estatales o proveedores de servicios de aviación

5.2.4.1 Con arreglo a las disposiciones del Anexo 13, los Estados deben investigar los accidentes, así como los incidentes graves, de aeronaves con una masa máxima superior a 2 250 kg que hayan ocurrido en su territorio. Estas investigaciones son realizadas por la autoridad de investigación de accidentes (AIA) del Estado en cumplimiento del Anexo 13. La realización de tales investigaciones puede delegarse en otro Estado u organización regional de investigación de accidentes e incidentes (RAIO), por acuerdo y consentimiento mutuos.

5.2.4.2 Se fomenta la realización de investigaciones de seguridad operacional, aparte de las obligadas por el Anexo 13, dado que producen información de seguridad operacional útil para apoyar la mejora del rendimiento en esa materia. En el Capítulo 9 figura información adicional sobre investigaciones de seguridad operacional por parte de los proveedores de servicios.

5.2.5 Sistemas de notificación obligatoria de seguridad operacional

5.2.5.1 En el Anexo 19 se exige que los Estados establezcan un sistema de notificación obligatoria de seguridad operacional que incluya, pero no se limite, a la notificación de incidentes. Los sistemas de notificación elaborados por los Estados y proveedores de servicios deberían ser lo más sencillos posibles en cuanto al acceso, generación y presentación de notificaciones obligatorias. Los sistemas de notificación obligatoria de seguridad operacional deberían dirigirse a la captación de toda la información valiosa sobre un suceso, incluyendo lo que sucedió, dónde y cuándo y cuál es el destinatario de la notificación. Además, los sistemas de notificación obligatoria de seguridad operacional deberían poder captar algunos peligros específicos que se sabe contribuyen a accidentes y cuya oportuna identificación y comunicación se considera valiosa (p. ej., condiciones meteorológicas rutinarias, actividad volcánica, etc.).

5.2.5.2 Independientemente del alcance de los sistemas de notificación obligatoria, se recomienda que todas las notificaciones recopiladas con carácter obligatorio estén protegidas con arreglo a los principios que se detallan en el Capítulo 7.

5.2.5.3 Los sistemas de notificación obligatoria de sucesos tienden a recopilar más información de carácter técnico (p. ej., fallas de equipo) que aspectos de actuación humana. Para abordar la necesidad de una mayor gama de notificaciones de seguridad operacional, los Estados también deberían implementar un sistema de notificación voluntaria de seguridad operacional. Esto se dirige a adquirir más información, como la relativa a aspectos relacionados con los factores humanos, y mejorar la seguridad operacional de la aviación.

Notificación de accidentes e incidentes

5.2.5.4 La notificación de accidentes e incidentes es pertinente a todas las partes interesadas en la aviación. Se requiere que el personal de operaciones notifique a la AIA del Estado los accidentes y ciertos tipos de incidentes, tan pronto como sea posible y por los medios más rápidos disponibles. Los incidentes graves deben notificarse y en el Adjunto C del Anexo 13 figura una lista de ejemplos de incidentes que podrían ser graves.

5.2.5.5 Los siguientes son los aspectos principales que habrán de considerarse al decidir si un incidente debería clasificarse como grave:

a) ¿Indicaban las circunstancias que era muy probable que ocurriera un accidente?

b) ¿Se evitó el accidente solo gracias a la buena suerte?

5.2.6 Sistemas de notificación voluntaria de seguridad operacional

5.2.6.1 Deberían establecerse sistemas de notificación voluntaria de seguridad operacional para recopilar datos e información sobre seguridad operacional no captados por el sistema de notificación obligatoria de seguridad operacional. Estas notificaciones van más allá de la notificación típica de incidentes. Los informes voluntarios tienden a destacar condiciones latentes, como procedimientos o reglamentos de seguridad inapropiados, errores humanos, etc. La notificación voluntaria constituye una forma de identificar peligros.

5.2.6.2 Los Estados deberían brindar protección a los datos de seguridad operacional captados por los sistemas de notificación voluntaria y fuentes conexas, así como a la información sobre seguridad operacional obtenida de los mismos. Se aconseja a los Estados y proveedores de servicios que se remitan al Capítulo 7 donde figura orientación sobre cómo aplicar la protección de los datos y la información sobre seguridad operacional y fuentes conexas. La aplicación apropiada de la protección asegurará la continua disponibilidad de datos e información sobre seguridad operacional. Los Estados también deberían considerar medios para promover la notificación voluntaria.

5.2.7 Disposiciones sobre notificación de seguridad operacional específica de cada sector

Las disposiciones sobre sistemas de notificación de seguridad operacional continúan evolucionando. Se han introducido recientemente nuevos requisitos de notificación específicos de cada sector, como la fatiga y los sistemas de aeronaves pilotadas a distancia (RPAS), a efectos de abordar preocupaciones de seguridad operacional específicas y actividades aeronáuticas emergentes. En la Tabla 7 se presentan algunos ejemplos de sistemas de notificación específicos de sectores incluidos en diversos Anexos, PANS y otros documentos.

Tabla 7. Ejemplos de sistemas de notificación específicos de sectores en diversos Anexos, PANS y otros documentos

Sistema de notificación	*Referencia*	*Para Estado/ proveedor de servicios*	*Año de adopción/ aprobación inicial*
Notificación de investigaciones de accidentes e incidentes de aviación	Anexo 13 — *Investigación de accidentes e incidentes de aviación*	Estado	1951
Notificación de incidentes de tránsito aéreo	PANS-ATM (Doc 4444), *Procedimientos para los servicios de navegación aérea — Gestión del tránsito aéreo*	Estado y proveedor de servicios	1970
Notificación de accidentes e incidentes de mercancías peligrosas	Anexo 18 — *Transporte sin riesgo de mercancías peligrosas por vía aérea*	Estado	1981
Notificación de dificultades en servicio	Anexo 8 — *Aeronavegabilidad*	Estado	1982
Notificación de incidentes de tránsito aéreo	Doc 9426, *Manual de planificación de servicios de tránsito aéreo*, Parte 2	Proveedor de servicios	1984
Notificación de choques con fauna silvestre/aves	Doc 9332, *Manual sobre el sistema de información de la OACI de los choques con aves (IBIS)*	Proveedor de servicios	1989

Sistema de notificación	*Referencia*	*Para Estado/ proveedor de servicios*	*Año de adopción/ aprobación inicial*
	Anexo 14 — *Aeródromos*, Volumen I — *Diseño y operaciones de aeródromos*	Estado y proveedor de servicios	1990
	Doc 9137, *Manual de servicios de aeropuertos*, Parte 3 — *Control y reducción del peligro que representa la fauna silvestre*	Estado y proveedor de servicios	1991
Notificación de emisiones láser	Doc 9815, *Manual sobre emisores láser y seguridad de vuelo*	Estado	2003
Notificación de casos de fatiga	Anexo 6 — *Operación de aeronaves*, Parte I — *Transporte aéreo comercial internacional — Aviones*	Proveedor de servicios	2011
	Doc 9966, *Manual para la supervisión de los enfoques de gestión de la fatiga*	Proveedor de servicios	2012
Notificación de dificultades en servicio	Doc 9760, *Manual de aeronavegabilidad*	Estado	2014
Notificación de seguridad operacional en el aeródromo	Doc 9981, *Procedimientos para los servicios de navegación aérea (PANS) – Aeródromos*	Proveedor de servicios	2014
Sistemas de aeronaves pilotadas a distancia (RPAS)	Doc 10019, *Manual sobre sistemas de aeronaves pilotadas a distancia (RPAS)*	Proveedor de servicios	2015
Sucesos de incapacitación durante el vuelo y constataciones de evaluaciones médicas	Anexo 1 — *Licencias al personal*	Estado	2016
Notificación de accidentes e incidentes de mercancías peligrosas	Doc 9284, *Instrucciones Técnicas para el transporte sin riesgos de mercancías peligrosas por vía aérea*	Estado y proveedor de servicios	2017

5.2.8 Sistemas de notificación de autodivulgación

Los sistemas de los proveedores de servicios para la recopilación de datos de seguridad operacional mediante sistemas de notificación de autodivulgación, incluyendo la captación automática de datos como el programa de acción de seguridad operacional de la aviación (ASAP) y los programas FDA [programa de aseguramiento de la calidad de las operaciones de vuelo (FOQA), auditorías de la seguridad operacional de las operaciones de línea (LOSA) y el estudio de la seguridad de las operaciones normales (NOSS)], constituyen ejemplos de sistemas que captan datos de seguridad operacional mediante observaciones directas de las tripulaciones de vuelo o controladores de tránsito aéreo, respectivamente. Todos estos sistemas permiten registrar el desempeño satisfactorio de sistemas y personas. En el Capítulo 7 figura más información sobre la protección de los datos y la información sobre seguridad operacional captados por sistemas de notificación de autodivulgación y sus fuentes.

5.2.9 Resultados de inspecciones, auditorías o estudios

Los resultados de las interacciones entre representantes del Estado y proveedores de servicios, como las inspecciones, auditorías o estudios, pueden también resultar útiles para la reunión de datos e información sobre seguridad operacional. Los datos y la información sobre seguridad operacional procedentes de estas interacciones pueden utilizarse como pruebas de la eficacia del propio programa de supervisión.

5.2.10 Recopilación óptima de datos e información sobre seguridad operacional

Gran parte de los datos y la información sobre seguridad operacional utilizados como base para la toma de decisiones basada en datos procede de operaciones rutinarias y cotidianas que están disponibles dentro de la organización. La organización debería identificar, en primer lugar, la cuestión específica a la que los datos y la información sobre seguridad operacional pretenden responder o el problema que debe abordarse. Esto ayudará a determinar la fuente apropiada y aclarar el volumen de datos o información necesarios.

5.3 TAXONOMÍAS

5.3.1 Los datos de seguridad operacional deberían categorizarse idealmente mediante taxonomías y definiciones de apoyo de modo que puedan captarse y almacenarse usando términos significativos. Las taxonomías y definiciones comunes establecen un lenguaje estándar, mejorando la calidad de la información y la comunicación. La capacidad de la comunidad de aviación para concentrarse en problemas de seguridad operacional mejora considerablemente si se comparte un lenguaje común. Estas clasificaciones permiten la realización de análisis y facilitan la compartición y el intercambio de información. Algunos ejemplos de taxonomías son los siguientes:

a) Modelo de aeronave: la organización puede construir una base de datos con todos los modelos certificados para operar.

b) Aeropuerto: la organización puede utilizar los códigos de la OACI o de la Asociación del Transporte Aéreo Internacional (IATA) para identificar los aeropuertos.

c) Tipo de suceso: la organización puede utilizar taxonomías elaboradas por la OACI y otras organizaciones internacionales para clasificar los sucesos.

5.3.2 Existen varias taxonomías aeronáuticas comunes en la industria. He aquí algunos ejemplos:

a) ADREP: taxonomía de categorías de sucesos que integra el sistema de notificación de accidentes de incidentes de la OACI. Constituye una recopilación de atributos y valores conexos que permiten realizar análisis de tendencias de seguridad operacional en esas categorías.

b) Equipo de taxonomía común del Equipo de seguridad operacional de la aviación comercial (CAST) y la Organización de Aviación Civil Internacional (OACI) (CICTT): encargado de elaborar taxonomías y definiciones comunes para los sistemas de notificación de accidentes e incidentes de aviación.

c) Equipo especial sobre indicadores del rendimiento en materia de seguridad operacional (SPI-TF): encargado de elaborar métricas armonizadas mundialmente para los SPI de los proveedores de servicios como parte de sus SMS, a efectos de asegurar la uniformidad en la recopilación de información y comparación de resultados de análisis.

5.3.3 En la Tabla 8 figura, a título de ejemplo solamente, un extracto de la taxonomía elaborada por el CICTT.

Tabla 8. Ejemplo de taxonomía típica

Tipo de operación	*Actividad/ infraestructura/sistema*	*Valor*
Aeródromo, proveedor de servicios de navegación aérea, explotador de servicios aéreos, organismo de mantenimiento, organización de diseño y fabricación	Reglamentador	Legislación o reglamentos ausentes, deficientes o ineficaces
		Capacidad de investigación de accidentes ausente o ineficaz
		Capacidad de vigilancia inadecuada
	Administración	Compromiso de la administración limitado o ausente – la administración no muestra apoyo a la actividad
		Descripción ausente o incompleta de funciones, obligaciones de rendir cuentas y responsabilidades
		Disponibilidad de recursos o planificación, incluso personal, limitada o ausente
		Ausencia o ineficacia de políticas
		Procedimientos, incluso instrucciones, incorrectos o incompletos
		Ausencia o deficiencia de relaciones entre administración y personal
		Estructura de organización ausente o ineficiente
		Deficiente cultura de seguridad operacional en la organización
		Ausencia o ineficiencia de procedimientos de auditoría
		Ausencia o limitación de la asignación de recursos

5.3.4 Las taxonomías sobre peligros son especialmente importantes. A menudo la identificación de un peligro es la primera etapa en el proceso de gestión de riesgos. Comenzar con un lenguaje reconocido en común hace que los datos de seguridad tengan más significado, sean más fáciles de clasificar y de procesamiento más sencillo. La estructura de una taxonomía de peligros puede comprender un componente genérico y uno específico.

5.3.5 El componente genérico permite a los usuarios captar el carácter de un peligro con miras a ayudar a su identificación, análisis y codificación. El CICTT ha establecido una taxonomía de peligros de alto nivel que clasifica los mismos en familias de tipos de peligro (ambientales, técnicos, institucionales y humanos).

5.3.6 El componente específico añade precisión a la definición y contexto del peligro. Esto permite realizar un procesamiento más detallado de la gestión de riesgos. Los criterios siguientes pueden resultar útiles al formular las definiciones de peligros. Cuando se designe un peligro, este debería ser:

a) claramente identificable;

b) descrito en el estado deseado (controlado); y

c) identificado por medio de nombres aceptados.

5.3.7 Las taxonomías comunes pueden no siempre estar disponibles entre bases de datos. En tales casos, debería utilizarse un mapeo (correspondencia) de datos para permitir la normalización de los datos y la información sobre seguridad operacional basada en la equivalencia. Utilizando un ejemplo de tipo de aeronave, un mapeo de los datos podría mostrar que “Boeing 787-8” en una base de datos equivale a “788” en otra. Este puede no ser un proceso directo puesto que el nivel de detalle durante la captación de los datos y la información sobre seguridad operacional puede ser diferente. La mayoría de los SDCPS estarán configurados para ayudar a la normalización de la captación de datos, lo que aliviaría la carga del mapeo de los mismos.

5.4 PROCESAMIENTO DE DATOS DE SEGURIDAD OPERACIONAL

El procesamiento de datos de seguridad operacional se refiere a la manipulación de éstos para producir información sobre seguridad operacional significativa en formularios útiles como diagramas, informes o tablas. Existen varias consideraciones de importancia respecto del procesamiento de datos de seguridad operacional, incluyendo la calidad, agregación, fusión y filtrado de los mismos.

5.4.1 Calidad de los datos

5.4.1.1 La calidad de los datos se relaciona con los datos limpios y adecuados a la finalidad. La calidad de los datos entraña los aspectos siguientes:

a) limpieza;

b) pertinencia;

c) oportunidad; y

d) exactitud y corrección.

5.4.1.2 La limpieza de los datos es el proceso de detectar y corregir (o eliminar) registros corruptos o inexactos de un conjunto, tabla o base de datos y se refiere a la identificación de partes incompletas, incorrectas, inexactas o irrelevantes de los datos para posteriormente sustituir, modificar o suprimir los datos sucios o burdos.

5.4.1.3 Los datos pertinentes son aquellos que satisfacen las necesidades de la organización y representan sus aspectos más importantes. Una organización debería evaluar la pertinencia de los datos sobre la base de sus necesidades y actividades.

5.4.1.4 La oportunidad de los datos y la información sobre seguridad operacional es una función de su actualidad. Los datos utilizados para tomar decisiones deberían reflejar lo que está sucediendo tan cerca del tiempo real como sea posible. A menudo se requiere buen juicio sobre la base de la volatilidad de la situación. Por ejemplo, los datos recopilados dos años atrás sobre un tipo de aeronave que todavía funciona en la misma ruta, sin cambios significativos, pueden proporcionar una reflexión oportuna de la situación mientras que los datos recopilados hace una semana sobre un tipo de aeronave que no está más en servicio pueden no reflejar en forma significativa y oportuna la realidad actual.

5.4.1.5 La exactitud de los datos se refiere a valores que son correctos y reflejan el escenario determinado según se ha descrito. La inexactitud de los datos ocurre normalmente cuando los usuarios ingresan un valor equivocado o introducen un error tipográfico. Este problema puede solucionarse si se cuenta con personal cualificado e instruido para el ingreso de datos o si existen componente en la aplicación como el corrector ortográfico. Con el tiempo, los valores de los datos pueden perder exactitud, lo que se conoce también como “deterioro de los datos”. El movimiento es otra causa de la inexactitud de los datos. A medida que los datos se extraen, transforman y trasladan de una base de datos a otra, pueden alterarse en alguna medida, especialmente si el soporte lógico no es robusto.

5.4.2 Agregación de datos e información sobre seguridad operacional

La agregación de datos es la reunión o acopio de datos e información sobre seguridad operacional y su almacenamiento en el SDCPS de la organización expresándose en forma de resumen apto para análisis. Agregar datos e información sobre seguridad operacional es recopilarlos para obtener un conjunto de datos mayor. En el caso del SDCPS, los elementos individuales de los datos de seguridad operacional se agregan en una base de datos sin dar más importancia a unos que a otros. Una finalidad común de la agregación es obtener información sobre un grupo o tipo particular de actividad sobre la base de variables específicas como la ubicación, el tipo de flota o el grupo

profesional. La agregación de datos puede a veces resultar útil para múltiples organizaciones o regiones que no cuentan con suficientes datos como para asegurar la no identificación adecuada a efectos de proteger las fuentes de los datos y la información sobre seguridad operacional así como para apoyar los análisis.

5.4.3 Fusión de datos

La fusión de datos es el proceso de integrar varios conjuntos de datos de seguridad operacional para producir datos que resulten más coherentes, enlazados y útiles que los proporcionados por cada conjunto individual de datos. La integración de los conjuntos de datos de seguridad operacional seguida por su reducción o sustitución mejora la fiabilidad y utilidad de dichos datos. Por ejemplo, datos de los sistemas FDA de los explotadores de servicios aéreos pueden integrarse con datos meteorológicos y datos radar para obtener un conjunto de datos más útil a efectos de procesamiento ulterior.

5.4.4 Filtrado de datos e información sobre seguridad operacional

El filtrado de datos de seguridad operacional se refiere a una amplia gama de estrategias o soluciones para refinar los conjuntos de datos. Esto significa que los conjuntos de datos se refinan sencillamente al grado necesario para los encargados de adoptar decisiones, sin incluir otros datos que puedan ser repetitivos, irrelevantes o incluso confidenciales o delicados. Pueden utilizarse diferentes tipos de filtros de datos para generar informes o presentar los datos en formas que faciliten la comunicación.

5.5 GESTIÓN DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

5.5.1 La gestión de datos e información sobre seguridad operacional puede definirse como la elaboración, ejecución y supervisión de planes, políticas, programas y prácticas que aseguren la integridad, disponibilidad, utilidad y protección generales de dichos datos e información utilizados por la organización.

5.5.2 La gestión de datos e información sobre seguridad operacional que aborda las funciones necesarias garantizará que los datos y la información sobre seguridad operacional de la organización se recopilan, almacenan, analizan, conservan y archivan así como también se gobiernan, protegen y comparten, según se prevé. Específicamente, se debería identificar lo siguiente:

a) el tipo de datos que se ha de recopilar;

b) definiciones, taxonomía y formatos de los datos;

c) la forma en que los datos se recopilarán, cotejarán e integrarán con otras fuentes de datos e información sobre seguridad operacional;

d) la forma en que los datos y la información sobre seguridad operacional se almacenarán, archivarán y apoyarán; por ejemplo, la estructura de la base de datos y, si se trata de un sistema IT, la arquitectura de apoyo;

e) la forma en que se utilizarán los datos y la información sobre seguridad operacional;

f) el modo en que la información se compartirá e intercambiará con otras partes;

g) la forma en que se protegerán los datos y la información sobre seguridad operacional, específica del tipo y fuente de los datos y la información sobre seguridad operacional; y

h) la forma en que se medirá y mantendrá la calidad.

5.5.3 Sin procesos claramente definidos para producir información sobre seguridad operacional, una organización no puede lograr información justificable, fiable y coherente sobre la cual tomar con confianza decisiones basadas en datos.

5.5.4 Gobernanza de los datos

La gobernanza de los datos es la autoridad, control y toma de decisiones respecto de procedimientos y procesos que apoyen las actividades de gestión de datos de una organización, la gobernanza establece la forma en que se recopilan, analizan, utilizan, comparten y protegen los datos y la información sobre seguridad operacional. La gobernanza de los datos asegura que los sistemas de gestión de datos tienen el efecto deseado mediante las características fundamentales de integridad, disponibilidad, usabilidad y protección, que se describen a continuación.

Integridad — La integridad de los datos se refiere a la fiabilidad de las fuentes, información y sucesos que contienen. No obstante, la integridad de los datos comprende el mantenimiento y aseguramiento de la exactitud y coherencia de los datos durante toda su vida útil. Este es un aspecto crítico del diseño, implementación y utilización del SDCPS cuando se almacenan, procesan o recuperan los datos.

Disponibilidad — Debería aclararse quién tiene autorización para utilizar o compartir los datos y la información sobre seguridad operacional almacenados. Esto debe tener en cuenta el acuerdo entre el propietario de los datos o la información y su custodio. Para las entidades autorizadas a utilizar los datos, debería estar bien claro cómo obtener acceso a los mismos y cómo procesarlos. Existen varias técnicas para maximizar la disponibilidad de los datos, incluyendo la redundancia de los lugares de almacenamiento y de los métodos y herramientas de acceso a los datos.

Usabilidad — A efectos de maximizar el aprovechamiento de los datos y la innovación sobre seguridad operacional, es también importante considerar normas de usabilidad. Las personas están continuamente interactuando y comprometiéndose con los datos y la información de seguridad operacional a medida que los adquieren. Las organizaciones deberían minimizar los errores humanos al aplicar medios automáticos. Las herramientas que pueden aumentar la usabilidad comprenden diccionarios de datos y repositorios de metadatos. A medida que la interacción humana evoluciona hacia mayores aplicaciones de datos y procesos de aprendizaje de máquina, será cada vez más importante comprender mejor la usabilidad humana aplicada a máquinas para minimizar errores de cálculos de datos e información de seguridad operacional en el futuro.

Protección — Los Estados deberían garantizar que los datos y la información sobre seguridad operacional así como las fuentes conexas reciben adecuada protección. En el Capítulo 7 figura más información al respecto.

5.5.5 Gestión de metadatos

5.5.5.1 Los metadatos se definen como un conjunto de datos que describe y brinda información sobre otros datos, en otras palabras, datos sobre los datos. El uso de normas sobre metadatos proporciona un significado común o definición de los mismos. Asegura el uso y la interpretación adecuada por propietarios y usuarios, así como la fácil recuperación de los datos para su análisis.

5.5.5.2 Es importante que las organizaciones cataloguen sus datos sobre la base de sus propiedades, entre otras:

a) carácter de los datos;

b) procedencia de los datos (fuente original);

c) quién creó los datos;

d) cuándo fueron creados;

e) quién utilizó los datos;

f) para qué se utilizaron;

g) frecuencia de la recopilación; y

h) todo procesamiento o transformación de los datos.

5.5.5.3 Los metadatos proporcionan una comprensión común del carácter de los datos y aseguran el uso e interpretación correctos por parte de propietarios y usuarios de los mismos. Esto también puede identificar errores en la recolección de los datos, lo que conduce a la continua mejora del programa.

Capítulo 6

ANÁLISIS DE LA SEGURIDAD OPERACIONAL

6.1 INTRODUCCIÓN

6.1.1 El análisis de la seguridad operacional es el proceso de aplicar técnicas estadísticas o analíticas de otro tipo para verificar, examinar, describir, transformar, condensar, evaluar y visualizar los datos y la información sobre seguridad operacional a efectos de descubrir información útil, sugerir conclusiones y apoyar la toma de decisiones basada en datos. Los análisis ayudan a las organizaciones a generar información sobre seguridad operacional viable en forma de estadísticas, gráficos, mapas, paneles y presentaciones. El análisis de la seguridad operacional es especialmente valioso para las organizaciones grandes o con mucha madurez que manejan grandes volúmenes de datos de seguridad operacional. El análisis de seguridad operacional se basa en la aplicación simultánea de técnicas de estadística, computación e investigación operativa. El resultado de un análisis de seguridad operacional debería presentar la situación en esa materia en una forma que permita la toma de decisiones de seguridad operacional basadas en datos.

6.1.2 Los Estados deben establecer y mantener un proceso para analizar los datos y la información sobre seguridad operacional del SDCPS y bases de datos de seguridad operacional conexas. Uno de los objetivos del análisis de datos e información de seguridad operacional a nivel estatal es la identificación de peligros sistémicos e intersectoriales que de otra manera podrían no ser identificados por los procesos de análisis de datos de seguridad operacional de los proveedores de servicios.

6.1.3 El análisis de la seguridad operacional puede ser una nueva función que el Estado o el proveedor de servicios puede tener que establecer. Cabe señalar que las competencias requeridas para realizar análisis de la seguridad operacional efectivos pueden estar fuera del alcance de los inspectores de seguridad operacional tradicionales. Los Estados y los proveedores de servicios deberían considerar cuáles son las cualificaciones necesarias para analizar la información de seguridad operacional y decidir si esta función, con instrucción apropiada, debería ser una extensión del puesto de trabajo actual o si sería más eficaz establecer un nuevo puesto, externalizar la función o aplicar una combinación de esos enfoques. La decisión deberá basarse en los planes y circunstancias de cada Estado o proveedor de servicios.

6.1.4 Paralelamente a las consideraciones en materia de recursos humanos, debería existir un análisis del soporte lógico actual y de las políticas y procesos operacionales y de toma de decisiones. Para que sea eficaz, el análisis de la seguridad operacional debería integrarse con las herramientas, políticas y procesos básicos existentes en la organización. Una vez integrado, el desarrollo continuo de la inteligencia en materia de seguridad operacional debería ser fluido y formar parte de las prácticas empresariales normales de la organización.

6.1.5 Los análisis de datos e información de seguridad operacional pueden realizarse de varias formas, algunas de las cuales requieren capacidades analíticas más robustas que otras. El uso de herramientas apropiadas para el análisis de los datos y la información sobre seguridad operacional proporciona una comprensión más precisa de la situación general mediante el examen de los datos en formas que revelan las relaciones, conexiones, patrones y tendencias existentes en la misma.

6.1.6 Una organización con capacidades maduras de análisis está en óptimas condiciones para:

a) establecer métricas de seguridad operacional eficaces;

b) establecer capacidades de presentación de la seguridad operacional (p. ej., panel de seguridad operacional) para la rápida interpretación de información sobre seguridad operacional por los encargados de tomar decisiones;

c) observar el rendimiento en materia de seguridad operacional de un determinado sector, organización, sistema o proceso;

d) destacar tendencias y metas en materia de seguridad operacional;

e) alertar a los encargados de tomar decisiones de seguridad operacional, sobre la base de elementos activadores;

f) identificar factores que provoquen cambios;

g) identificar conexiones o“correlaciones” entre diversos factores;

h) comprobar hipótesis; y

i) elaborar capacidades de modelización predictiva.

6.1.7 Las organizaciones deberían incluir una buena gama de fuentes de información apropiadas en sus análisis de seguridad operacional, y no solo de “datos de seguridad operacional”. Ejemplos de adiciones útiles al conjunto de datos son: condiciones meteorológicas, terreno, tránsito, aspectos demográficos, geografía, etc. El acceso y la explotación de una gama más amplia de fuentes de datos permitirán asegurar que los analistas y los encargados de tomar decisiones de seguridad operacional son conscientes del contexto más amplio, dentro del cual se toman las decisiones en la materia.

6.1.8 Los Estados, en particular, deberían interesarse especialmente en tener información que identifique tendencias y peligros de seguridad operacional que afectan a todo el sistema de aviación.

6.2 TIPOS DE ANÁLISIS

El análisis de los datos y la información sobre seguridad operacional también permite a los encargados de tomar decisiones comparar información con otros grupos (es decir, un grupo de control o comparación) para ayudar a extraer conclusiones de los datos en cuestión. Los enfoques comunes comprenden análisis descriptivos (descripciones), análisis inferenciales (deducción) y análisis predictivo (predicción), según se ilustra en la Figura 6-1.

6.2.1 Análisis descriptivo

6.2.1.1 La estadística descriptiva se aplica para describir o resumir datos de manera que resulten significativos y útiles. Contribuye a describir, mostrar o resumir datos de modo que surjan patrones a partir de los datos y contribuyan a definir claramente estudios de casos, oportunidades y retos. Las técnicas descriptivas proporcionan información sobre los datos; no obstante, no permiten que los usuarios formulen conclusiones más allá de los datos analizados o que lleguen a conclusiones respecto de hipótesis sobre los mismos. Son solamente una forma de describir los datos.

6.2.1.2 La estadística descriptiva resulta útil debido a que si solamente se presentan los datos brutos, particularmente en grandes cantidades, sería difícil visualizar lo que los datos muestran. La estadística descriptiva permite a los usuarios presentar y visualizar los datos en una forma que tiene más sentido, permitiendo una interpretación más sencilla de los mismos. Entre las herramientas utilizadas para resumir los datos figuran las tablas y matrices, gráficas y cartas, e incluso mapas. La estadística descriptiva incluye medidas de la tendencia central como la media (promedio), la mediana y el modo, así como también medidas de la variabilidad como el rango, los cuartiles, mínimos y máximos, distribuciones de frecuencia, varianza y desviación estándar (SD). Estos resúmenes pueden ser la base inicial para describir los datos como parte de un análisis estadístico más amplio o pueden resultar suficientes por sí mismos para una investigación particular.

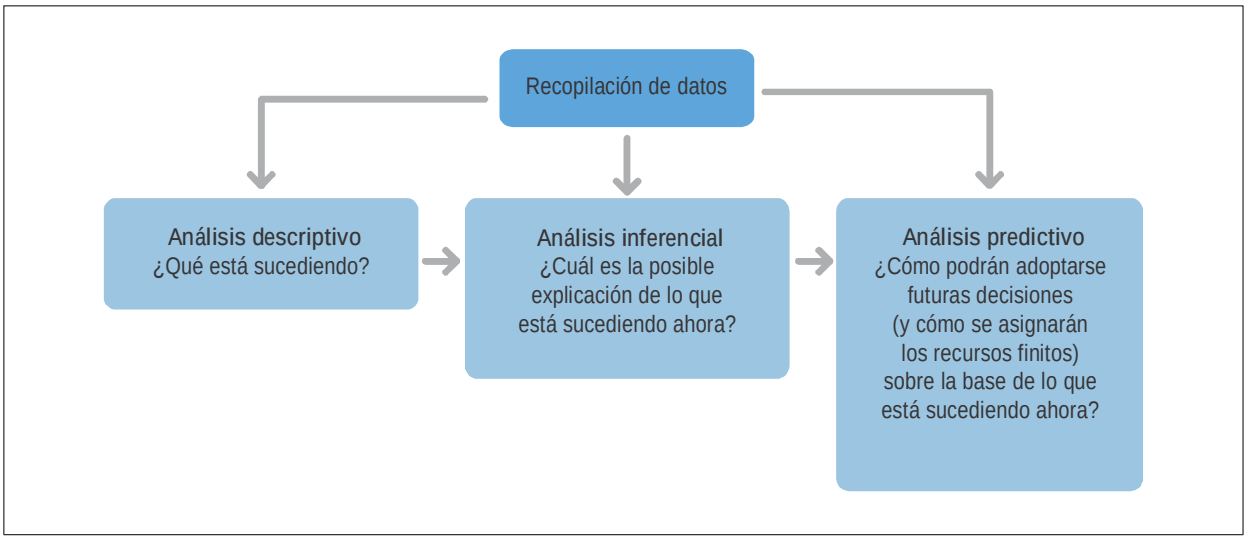


Figura 6-1. Tipos comunes de análisis estadísticos

6.2.2 Análisis inferencial

La estadística inferencial (o inductiva) tiene por objeto utilizar los datos para entender la población más amplia que la muestra de datos representa. No siempre es conveniente o posible examinar cada elemento de una población entera y tener acceso a la misma. La estadística inferencial incluye técnicas que permiten a los usuarios de datos disponibles hacer generalizaciones e inferencias, así como llegar a conclusiones sobre la población de la cual se han tomado las muestras para describir tendencias. Estas técnicas comprenden métodos para estimar parámetros, ensayar hipótesis estadísticas, comparar el desempeño promedio de dos grupos de la misma medida para identificar diferencias o similitudes, e identificar posibles correlaciones y correspondencias entre variables.

6.2.3 Análisis predictivo

Otros tipos de análisis comprenden análisis de probabilidad o predictivos que extraen información a partir de datos históricos y actuales a efectos de predecir tendencias y patrones de comportamiento. Los patrones encontrados en los datos contribuyen a identificar riesgos emergentes y oportunidades. A menudo, el suceso de interés desconocido se encuentra en el futuro, pero el análisis predictivo puede aplicarse a cualquier tipo de elemento desconocido en el pasado, presente o futuro. El aspecto central del análisis predictivo se basa en captar relaciones entre variables de sucesos pasados y explotarlas para predecir el resultado desconocido. Algunos sistemas permiten a los usuarios modelar escenarios diferentes de riesgos u oportunidades con diferentes resultados. Esto permite a los encargados de tomar decisiones evaluar las que puedan adoptar teniendo en cuenta las circunstancias desconocidas diferentes y evaluar la forma en que pueden asignar eficazmente los recursos limitados a sectores donde existen los mayores riesgos o las mejores oportunidades.

6.2.4 Análisis combinado

6.2.4.1 Los diversos tipos de análisis estadísticos están interconectados y a menudo se realizan en conjunto. Por ejemplo, una técnica inferencial puede ser la herramienta principal aplicada a la extracción de conclusiones respecto de un conjunto de datos, pero también normalmente se aplican y presentan estadísticas descriptivas. Además, los resultados de las estadísticas inferenciales se utilizan a menudo como base para los análisis predictivos.

6.2.4.2 Las técnicas analíticas pueden aplicarse a los análisis de la seguridad operacional a efectos de:

a) identificar las causas y los factores contribuyentes relacionados con peligros y elementos que afectan negativamente la mejora continua de la seguridad operacional de la aviación;

b) examinar áreas que puedan mejorar y aumentar la eficacia de los controles de seguridad operacional; y

c) apoyar la observación continua del rendimiento y tendencias en materia de seguridad operacional.

6.3 NOTIFICACIÓN DE LOS RESULTADOS DE LOS ANÁLISIS

6.3.1 Los resultados de los análisis de datos de seguridad operacional pueden destacar áreas de alto riesgo y ayudar a los encargados de tomar decisiones y a los administradores a:

a) adoptar medidas correctivas inmediatas;

b) implementar supervisión de la seguridad operacional basada en riesgos;

c) definir o refinar políticas de seguridad operacional u objetivos en la materia;

d) definir o refinar los SPI;

e) definir o refinar las SPT;

f) establecer activadores de SPI;

g) promover la seguridad operacional; y

h) realizar ulteriores evaluaciones de riesgos de seguridad operacional.

6.3.2 Los resultados de los análisis de seguridad operacional deberían ponerse a disposición de todas las partes interesadas en la seguridad operacional de la aviación en la forma en que puedan comprenderse fácilmente. Los resultados deberían presentarse teniendo presente a quienes están dirigidos, como los encargados de tomar decisiones institucionales, proveedores de servicios externos, CAA y otros Estados. Los resultados de los análisis de seguridad operacional deberían presentarse en varias formas, entre ellas las siguientes:

a) Alertas de seguridad operacional inminentes: para transmitir a otros Estados o proveedores de servicios los peligros de seguridad operacional con posibles resultados que podrían resultar catastróficos y que requieren medidas inmediatas.

b) Informes de análisis de seguridad operacional: normalmente en ellos se presenta información cuantitativa y cualitativa con una clara descripción del grado y fuente de las incertidumbres involucradas en las constataciones de los análisis. Estos informes también pueden incluir recomendaciones de seguridad operacional pertinentes.

c) Conferencias sobre seguridad operacional: para que los Estados y proveedores de servicios puedan compartir información sobre seguridad operacional y resultados de análisis de seguridad operacional que puedan promover iniciativas de colaboración.

6.3.3 Resulta útil traducir las recomendaciones en planes de acción, decisiones y prioridades que los encargados de tomar decisiones en la organización deben considerar y, si es posible, señalar quiénes deben hacer qué con respecto a los resultados de los análisis y cuándo.

6.3.4 Herramientas de visualización como cartas, gráficos, imágenes y paneles son medios sencillos pero eficaces de presentar los resultados de análisis de datos. Varios ejemplos de informes visuales de análisis de datos pueden encontrarse en el sistema integrado de análisis y notificación de tendencias de seguridad operacional (iSTARS) de la OACI en https://icao.int/safety/iSTARS.

6.3.5 Paneles y tableros de control sobre seguridad operacional

6.3.5.1 El rendimiento de la organización en materia de seguridad operacional debería ser demostrable e indicar claramente a todas las partes interesadas que dicha seguridad se está gestionando en forma eficaz. Un enfoque de dicha demostración es a través de un “panel o tablero de control sobre seguridad operacional”, que consiste en una representación visual que permite a los ejecutivos principales, administradores y profesionales de seguridad operacional contar con una manera rápida y fácil de visualizar el rendimiento de la organización en materia de seguridad operacional.

6.3.5.2 Además de una presentación en tiempo real de los SPI y SPT de la organización, estos paneles de control también pueden incluir información sobre la categoría, causas y gravedad de peligros específicos. Idealmente, la información presentada en el tablero o panel puede adaptarse para mostrar la información requerida a efectos de apoyar la toma de decisiones en diversos niveles de la organización. El uso de activadores resulta útil para proporcionar aspectos visuales básicos a fin de subrayar si hay problemas que deben tratarse para un indicador específico. Los analistas y los encargados de tomar decisiones querrán tener la capacidad de configurar el panel o tablero de control para que presente sus principales indicadores así como una característica que les permita abordar en mayor profundidad los aspectos de las métricas.

6.3.5.3 La recopilación y análisis de los datos que se requieren para la gestión y la toma de decisiones eficaz constituyen un proceso continuo. Los resultados de los análisis de datos pueden revelar que se deben recopilar y analizar más y mejores datos para apoyar las medidas y decisiones que la organización debe adoptar. En la Figura 6-2 se presenta la forma en que la notificación de resultados de análisis puede determinar ulteriores necesidades de recopilar datos.

6.4 COMPARTICIÓN E INTERCAMBIO DE INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

La seguridad operacional puede mejorarse aún más cuando se comparte o intercambia información en la materia. Asegura una respuesta coherente, basada en datos y transparente respecto de preocupaciones de seguridad operacional a nivel mundial, estatal e institucional. Compartir información sobre seguridad operacional corresponde a dar, mientras que intercambiar corresponde a dar y recibir a cambio.

6.4.1 Compartición dentro del Estado

6.4.1.1 Los Estados deberían promover el establecimiento de redes para compartir o intercambiar información sobre seguridad operacional entre usuarios del sistema de aviación y facilitar la compartición y el intercambio de dicha información, a menos que sus leyes nacionales establezcan otra cosa. En los Capítulos 8 y 9, respectivamente, figura orientación sobre promoción de la seguridad operacional para Estados y proveedores de servicios.

6.4.1.2 El nivel de protección y las condiciones en las cuales se compartirá o intercambiará la información sobre seguridad operacional entre autoridades estatales y proveedores de servicios debe ser compatible con las leyes nacionales. En el Capítulo 7 figura más información sobre la protección de datos e información sobre seguridad operacional.

6.4.2 Compartición entre Estados

Los Estados deberían compartir la información sobre seguridad operacional con otros Estados tan pronto como sea posible si, en los análisis de la información contenida en su SDCPS, se identifican asuntos de seguridad operacional que puedan ser de interés para otro Estado. También se alienta a los Estados a compartir información sobre seguridad operacional con sus RASG. Antes de compartir la información sobre seguridad operacional, los Estados deberían asegurar que el nivel de protección en las condiciones bajo las cuales se compartirá dicha información corresponde a lo expuesto en el Anexo 19, Apéndice 3. En el Capítulo 7 figura orientación más detallada en la materia.

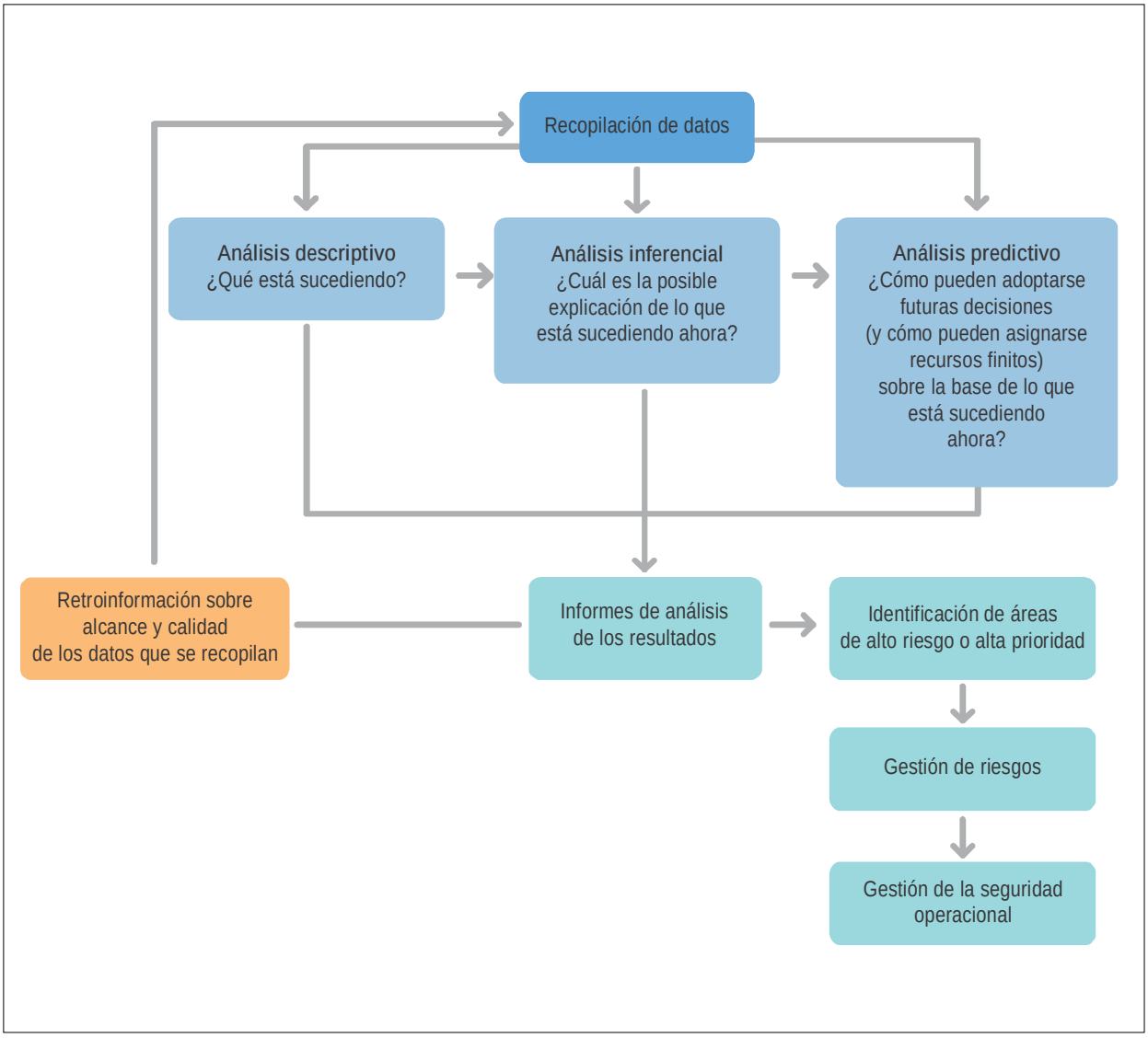


Figura 6-2. Integración de D3M con la gestión de la seguridad operacional

6.5 TOMA DE DECISIONES BASADA EN DATOS

6.5.1 El propósito principal del análisis y la notificación de seguridad operacional es presentar a los encargados de tomar decisiones un panorama de la situación en la materia que les permita adoptar decisiones sobre la base de los datos presentados. Esto se conoce como toma de decisiones basada en datos (denominada también DDDM ó D3M), un enfoque basado en procesos para la toma de decisiones.

6.5.2 Muchos incidentes de aviación se han debido, por lo menos parcialmente, a decisiones de gestión deficientes, que pueden resultar en una dilapidación de dinero, trabajo y recursos. El objetivo de los encargados de tomar decisiones de seguridad operacional consiste, a corto plazo, en minimizar resultados deficientes y alcanzar resultados eficaces y, a largo plazo, contribuir al logro de los objetivos de seguridad operacional de la organización.

6.5.3 No es fácil tomar buenas decisiones. Las decisiones se toman a menudo sin que puedan considerarse todos los factores pertinentes. Los encargados de tomar decisiones también están sujetos a sesgos o inclinaciones que, en forma consciente o no, afectan las decisiones tomadas.

6.5.4 El propósito de la D3M no es necesariamente tomar la decisión “perfecta” o ideal, sino tomar una buena decisión que alcance el objetivo a corto plazo (respecto del cual se está tomando la decisión en cuestión) y contribuya a alcanzar el objetivo a largo plazo (un mejor rendimiento de la organización en materia de seguridad operacional). Las buenas decisiones deben ser:

a) *Transparentes*: la comunidad de aviación debería conocer todos los factores que influyeron en una decisión, incluyendo el proceso utilizado para alcanzarla.

b) *Responsables y sujetas a rendición de cuentas*: el encargado de tomar una decisión se hace cargo de la misma y de los resultados conexos. La claridad y la transparencia también entrañan la obligación de rendir cuentas – no es fácil ocultarse tras una decisión cuando las funciones y responsabilidades están definidas en forma detallada y las expectativas relacionadas con la nueva decisión se han presentado claramente.

c) *Justas y objetivas*: el encargado de la decisión no está influenciado por consideraciones que no son pertinentes (p. ej., lucro o relaciones personales).

d) *Justificables y defendibles*: puede demostrarse que la decisión es razonable considerando las contribuciones a la misma y el procedimiento seguido.

e) *Reproducibles*: dada la misma información disponible a quien adoptó la decisión y aplicando el mismo procedimiento, otra persona alcanzaría la misma decisión.

f) *Ejecutables*: la decisión es suficientemente clara y dicha claridad minimiza las incertidumbres.

g) *Pragmáticas*: los seres humanos son criaturas emotivas, lo que significa que es imposible eliminar el aspecto emocional de una decisión. No obstante, pueden eliminarse los sesgos emocionales egoístas o interesados. Una pregunta saludable a formularse frente a decisiones difíciles es: ¿a quién sirve o beneficia la decisión?

6.5.5 Ventajas de la toma de decisiones basada en datos

6.5.5.1 La D3M permite a los encargados de tomar decisiones concentrarse en los resultados de seguridad operacional deseados que correspondan a la política y objetivos de seguridad operacional y abordar diversos aspectos relativos a la gestión de cambios, evaluaciones de riesgo de seguridad operacional, etc. La D3M puede ayudar a tomar decisiones respecto de:

a) cambios que pueden esperarse en los requisitos estatutarios y normativos, tecnologías emergentes o recursos que puedan afectar a la organización;

b) posibles cambios en las necesidades y expectativas de la comunidad de aviación y partes interesadas;

c) diversas prioridades que deben establecerse y gestionarse (p. ej., estratégicas, operacionales, recursos);

d) nuevas habilidades, competencias, herramientas e incluso procesos de gestión de cambios que puedan ser necesarios para implementar nuevas decisiones;

e) riesgos que deben evaluarse, gestionarse o minimizarse;

f) servicios, productos y procesos existentes que actualmente proporcionan el valor más elevado para las partes interesadas; y

g) evolución de las demandas de nuevos servicios, productos y procesos.

6.5.5.2 Un enfoque estructurado como el D3M conduce a decisiones que se correspondan con lo indicado por los datos de seguridad operacional. Esto exige tener confianza en el marco de gestión del rendimiento en materia de seguridad operacional; si hay confianza en los SDCPS, habrá confianza en las decisiones obtenidas de los mismos.

6.5.6 Retos comunes en la toma de decisiones basada en datos

6.5.6.1 Los procesos de implementación de la recopilación y análisis de datos insumen tiempo y dinero, e involucran también conocimientos expertos y habilidades que pueden no estar rápidamente disponibles en la organización. El volumen apropiado de tiempo y recursos invertidos en el proceso de toma de decisiones debe considerarse cuidadosamente. Los factores que han de tenerse en cuenta incluyen las sumas de dinero involucradas en la decisión, el grado de influencia de la misma y su permanencia en cuanto a la seguridad operacional. Si la organización no comprende de qué se trata, el proceso de D3M puede transformarse en una fuente de frustraciones para los encargados de tomar decisiones, haciendo que afecten negativamente o abandonen el proceso. Al igual que los SSP y SMS, la D3M y la gestión del rendimiento en materia de seguridad operacional requieren el compromiso de construir y mantener las estructuras y habilidades necesarias para maximizar las oportunidades que dicha toma de decisiones presenta.

6.5.6.2 Es más difícil crear confianza en los datos que confiar en contribuciones y opiniones de expertos. La adopción del enfoque de D3M exige un cambio en la cultura y en la mentalidad de la organización cuando las decisiones se basan en SPI fiables y en los resultados de otros análisis de datos de seguridad operacional.

6.5.6.3 En algunos casos, el proceso de toma de decisiones puede atascarse en un intento de encontrar la “mejor solución posible”, lo que también se conoce como “parálisis analítica”. Entre las estrategias que pueden aplicarse para evitar este empantanamiento figuran las siguientes:

a) establecer un plazo máximo;

b) contar con alcance y objetivos bien definidos; y

c) no tratar de alcanzar una decisión o solución “perfecta” la primera vez, sino más bien lograr una decisión “adecuada” y “práctica” y mejorar luego decisiones ulteriores.

6.5.7 Proceso de toma de decisiones basada en datos

6.5.7.1 El proceso D3M puede ser una herramienta crítica que aumenta el valor y la eficacia del SSP y el SMS. La gestión eficaz de la seguridad operacional depende de la adopción de decisiones defendibles y bien basadas. A su vez, la D3M eficaz se basa en la claridad de las definiciones de los requisitos de datos e información sobre seguridad operacional, normas, métodos de recopilación, gestión, análisis y compartición de los datos, todos los cuales son componentes del proceso D3M. En la Figura 6-3 se ilustra dicho proceso.

Etapa 1 — Definición del problema u objetivo

6.5.7.2 La primera etapa de la planificación y establecimiento del proceso de D3M es definir el problema que debe resolverse o el objetivo de seguridad operacional que ha de alcanzarse. ¿Cuál es la pregunta que debe responderse? ¿Qué decisión de seguridad operacional deben alcanzar los encargados de hacerlo? ¿Qué formas se corresponden con los objetivos más estratégicos de la organización? En el proceso de definir el problema, los encargados de tomar decisiones deben plantearse las preguntas siguientes:

a) ¿La recopilación y el análisis de los datos apoyan y se relacionan con los objetivos o metas de seguridad operacional de la organización?

b) ¿Se dispone de los datos necesarios? o ¿pueden obtenerse en forma razonable?

c) ¿Resulta práctico y viable recopilar y analizar los datos?

d) ¿Se dispone de los recursos necesarios (personas, equipo, soporte lógico, fondos)?

6.5.7.3 En el contexto de la gestión de la seguridad operacional, los principales problemas de la organización se relacionan con la evaluación y selección de prioridades de seguridad operacional que se correspondan con los objetivos de dicha seguridad y establecer medidas para la mitigación de riesgos de seguridad operacional.

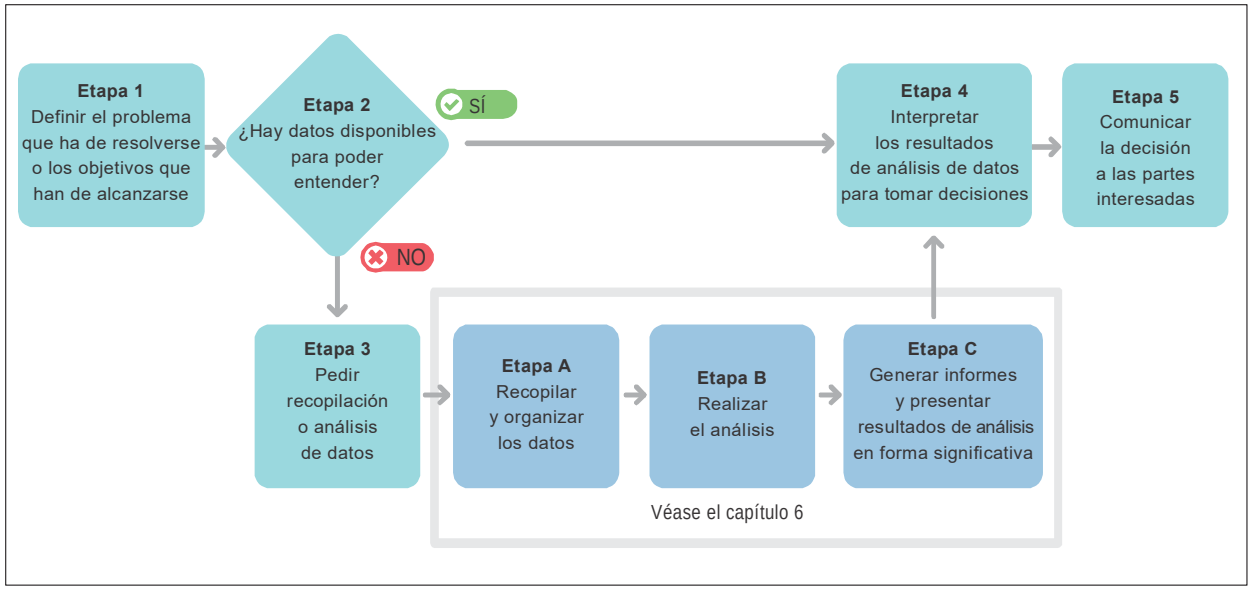


Figura 6-3. Fases de la toma de decisiones basada en datos

Etapa 2 — Acceso a los datos para apoyar la toma de decisiones

6.5.7.4 La siguiente etapa consiste en identificar los datos necesarios para responder al problema (teniendo en cuenta las disposiciones sobre protección de la información). No hay datos más valiosos que otros. El énfasis debería estar en la determinación de si los datos disponibles resultan apropiados para responder y resolver al problema. Si los datos necesarios están disponibles, seguir a la etapa 4. Si los datos correctos no están disponibles, la organización deberá recopilar, almacenar, analizar y presentar nuevos datos e información sobre seguridad operacional en forma significativa.

Etapa 3 — Solicitar datos para apoyar la toma de decisiones

6.5.7.5 Si los datos no están fácilmente disponibles, la organización debe encontrar maneras de recopilarlos. Esto puede significar el establecimiento de otros SPI y quizás SPT correspondientes. El establecimiento de indicadores adicionales puede insumir costos. Una vez conocidos éstos, la organización debería estimar si las ventajas superan dichos costos. El énfasis debería estar principalmente en la identificación, observación y medición de los datos de seguridad operacional necesarios para tomar decisiones efectivas de seguridad operacional basada en datos. Si los costos superan los beneficios, habrá que considerar fuentes de datos o indicadores de alternativa.

6.5.7.6 En la fase de planificación del proceso D3M, la organización debe definir el objetivo que desea alcanzar mediante el establecimiento de las SPT y los SPI y el análisis de los datos. ¿Por qué la organización necesita abordar el problema identificado? ¿Cuál es la meta razonable? ¿Cómo y dónde utilizarán los encargados de las decisiones los resultados de la recopilación y análisis de los datos? Tener una comprensión clara de las razones por las que la organización necesita recopilar, analizar, compartir e intercambiar datos e información sobre seguridad operacional resulta fundamental para cualquier SDCPS.

6.5.7.7 Los elementos siguientes se combinan para permitir que la organización identifique tendencias, formule decisiones bien informadas, evalúe el rendimiento en materia de seguridad operacional en relación con los objetivos definidos, evalúe riesgos o cumpla sus requisitos:

a) gestión del rendimiento en materia de seguridad operacional – constituye el marco de gobernanza de los datos e información sobre seguridad operacional;

b) SDCPS – constituye la función de recopilación y procesamiento de datos de seguridad operacional; y

c) D3M como proceso de toma de decisiones confiable.

Etapa 4 — Interpretación de los resultados de análisis de datos y toma de decisiones basada en datos

6.5.7.8 Los datos recopilados deben presentarse a los encargados de tomar decisiones en el momento oportuno y en forma significativa. La adecuación y el volumen de los conjuntos de datos, el grado de perfeccionamiento de las técnicas analíticas y las habilidades de los analistas solo serán eficaces si los datos se presentan cuando son necesarios y en formatos que faciliten su comprensión por parte de los encargados de las decisiones. Los conocimientos obtenidos de los datos deberían apoyar la toma de decisiones y, en última instancia, contribuir a mejorar el rendimiento en materia de seguridad operacional.

6.5.7.9 Hay varios modelos de toma de decisiones disponibles. La aplicación de un enfoque convenido y normalizado podrá maximizar la coherencia y la eficacia de las decisiones de la organización basadas en datos. La mayoría de esos modelos comprenden las etapas siguientes:

a) reunir un equipo o grupo con las habilidades y experiencia necesarias [p. ej., grupo de acción de seguridad operacional (SAG)];

b) definir claramente el problema u objetivo de seguridad operacional y su contexto;

c) examinar las SPT y los objetivos de seguridad operacional de la organización para garantizar una correspondencia continua;

d) examinar e interpretar los datos de seguridad operacional para comprender lo que éstos indican;

e) considerar y analizar las alternativas viables;

f) considerar el riesgo de acciones (o inacciones) factibles;

g) obtener consenso dentro del grupo de toma de decisiones;

h) comprometerse con la decisión basada en datos y actuar al respecto (transformar datos en acciones); y

i) vigilar y evaluar los resultados.

Etapa 5 — Comunicar la decisión

6.5.7.10 Para que una decisión de seguridad operacional resulte eficaz, debe comunicarse a las partes interesadas, a saber:

a) personal que deberá aplicar las medidas necesarias;

b) persona que notificó la situación (si es necesario);

c) todo el personal, para asegurar que se mantiene informado sobre las mejoras de seguridad operacional (promoción de la seguridad operacional; para los Estados véase el Capítulo 8; para proveedores de servicios véase el Capítulo 9); y

d) los administradores de conocimientos de la organización para asegurar que la decisión se incorpora al acervo de conocimientos de la misma.

6.5.7.11 Por más información sobre comunicaciones de seguridad operacional, véanse los párrafos 8.6 para los Estados y 9.6 para los proveedores de servicios.

———————————

Capítulo 7

PROTECCIÓN DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL Y FUENTES CONEXAS

7.1 OBJETIVOS Y CONTENIDO

7.1.1 En este capítulo se describen los principios básicos que rigen la protección de los datos y la información sobre seguridad operacional captados por los sistemas de notificación de seguridad operacional u obtenidos de éstos, así como las fuentes de tales datos e información.[1] También se proporciona orientación y asesoramiento sobre la aplicación de estos principios por las autoridades normativas de aviación de los Estados, los proveedores de servicios, legisladores, abogados, fiscales, funcionarios judiciales y otras autoridades competentes con responsabilidades para la toma de decisiones sobre el uso y protección de datos de seguridad operacional, información sobre seguridad operacional y sus fuentes conexas. Este capítulo puede resultar útil para otras personas que procuren acceder a los datos o información sobre seguridad operacional o difundir los mismos.

7.1.2 El capítulo comprende los temas siguientes:

a) principios fundamentales;

b) alcance y nivel de la protección;

c) principios de protección;

d) principios de excepción;

e) divulgación al público;

f) protección de los datos registrados; y

g) intercambio y compartición de información sobre seguridad operacional.

7.2 PRINCIPIOS FUNDAMENTALES

7.2.1 El objetivo de la protección de los datos y la información sobre seguridad operacional así como de sus fuentes conexas es asegurar su continua disponibilidad con miras a utilizarlos para mantener o mejorar la seguridad operacional de la aviación, alentando al mismo tiempo a individuos y organizaciones a que notifiquen datos e información sobre seguridad operacional. En este contexto, la importancia de implementar formas de protección resulta fundamental. Las formas de protección no tienen por objeto eximir a las fuentes de sus obligaciones relacionadas con la seguridad o interferir con la adecuada administración de justicia.

1. Con arreglo al Anexo 19, las fuentes de datos e información sobre seguridad operacional comprenden tanto individuos como organizaciones.

7.2.2 La seguridad operacional de la aviación no es sólo responsabilidad de los Estados o proveedores de servicios. Es una responsabilidad compartida a la cual todas las partes interesadas deberían contribuir, entre otras cosas, mediante el suministro de datos e información pertinentes a través de notificaciones de seguridad operacional.

7.2.3 Aunque los datos y la información pueden proceder de diversas fuentes, la notificación de datos e información sobre seguridad operacional por individuos y organizaciones del sistema aeronáutico resulta fundamental para la gestión de la seguridad operacional. Los sistemas de notificación de seguridad operacional eficaces contribuyen a asegurar que las personas están, y permanecen, dispuestas a notificar sus errores y experiencias, de modo que los Estados y los proveedores de servicios tengan acceso a los datos e información pertinentes necesarios para abordar deficiencias y peligros de seguridad operacional existentes y potenciales. Esta garantía se proporciona mediante la creación de un entorno en el que las personas pueden confiar en que los datos y la información sobre seguridad operacional se utilizarán exclusivamente para mantener y mejorar la misma, a menos que se aplique uno de los principios de excepción.

7.2.4 En el Anexo 19 no se proporciona protección a los individuos u organizaciones mencionados en la notificación. No obstante, los Estados pueden extender la protección a dichos individuos u organizaciones.

7.2.5 Es importante que tanto los individuos como las organizaciones estén protegidos, así como los datos e información sobre seguridad operacional que estos notifican. Los individuos y las organizaciones están protegidos por:

a) seguridades de que no serán objeto de sanciones sobre la base de sus notificaciones; y

b) limitación del uso de los datos e información sobre seguridad operacional notificados a fines destinados a mantener o mejorar la seguridad operacional.

Estas protecciones son válidas a menos que sea aplicable uno de los principios de excepción que se analizan a continuación.

7.2.6 En el Anexo 19 se exige que los Estados se aseguren de que los datos y la información sobre seguridad operacional no se utilicen para fines distintos de los establecidos en los ***principios de protección*** a menos que se aplique un principio de excepción. Los ***principios de excepción*** establecen las circunstancias en las cuales podría permitirse una desviación respecto de esos principios de protección.

7.2.7 Los Estados y los proveedores de servicios pueden adoptar medidas preventivas, correctivas o de rectificación que sean necesarias, sobre la base de los datos e información sobre seguridad operacional notificados con el fin de mantener o mejorar la seguridad operacional — es decir, permitir que los Estados y los proveedores de servicios adopten medidas apropiadas para:

a) protegerse contra la posibilidad de daño o lesiones inmediatas como resultado de un riesgo de seguridad operacional hasta que dicho riesgo pueda identificarse y mitigarse;

b) asegurar que se adoptan medidas apropiadas para minimizar la probabilidad de que dicho riesgo pueda ocurrir nuevamente en el futuro;

c) prevenir la exposición a un riesgo de seguridad operacional no mitigado; o

d) asegurar la integridad del propio sistema de notificación y del sistema más amplio del que forma parte.

7.2.8 Debido a que tales medidas son fundamentales para los objetivos y la eficacia de todo sistema de gestión de la seguridad operacional, el Anexo 19 establece expresamente que no se impedirá que se tomen medidas de carácter preventivo, correctivo o de rectificación a efectos de mantener o mejorar la seguridad operacional de la aviación. Dichas medidas pueden tomarse en función de los procesos de gestión de la seguridad operacional aplicables y, por ello, no están sujetas a los principios de excepción establecidos en el Anexo.

7.2.9 Las medidas preventivas, correctivas o de rectificación pueden implicar la restricción, limitación o prevención[2] del ejercicio de ciertos privilegios [3], la prestación de servicios o la operación de aeronaves, hasta que se hayan abordado eficazmente los riesgos de seguridad identificados. Cuando se adoptan para esos fines, en el marco de protocolos establecidos, las medidas de protección o precaución no deben considerarse como punitivas o disciplinarias. El propósito de tales medidas es prevenir o minimizar la exposición a riesgos de seguridad operacional no mitigados.

7.2.10 Los principios relativos a la protección de los datos y la información de seguridad operacional así como de sus fuentes, que figuran en el Anexo 19, proporcionan más claridad y transparencia, así como una igualdad de condiciones, con miras a facilitar el intercambio de datos e información sobre seguridad operacional entre los Estados, como lo requiere el Anexo.

7.3 ALCANCE DE LA PROTECCIÓN

7.3.1 Alcance de los datos e información sobre seguridad operacional abarcados por los principios de protección

7.3.1.1 La protección se aplica a los datos de seguridad operacional captados por los sistemas de notificación voluntaria de seguridad operacional y fuentes conexas, así como a la información sobre seguridad operacional obtenida de los mismos. Esto puede aplicarse también a los sistemas de notificación obligatoria de seguridad operacional cuando corresponda (véase 7.4.3). Las fuentes de los datos y la información sobre seguridad operacional pueden ser individuos u organizaciones.

7.3.1.2 En algunos Estados, los sistemas de notificación de seguridad operacional pueden incluir la notificación de datos para investigaciones de seguridad operacional realizadas por autoridades estatales o proveedores de servicios aeronáuticos, datos e información captados por los sistemas de autodivulgación de notificaciones (incluyendo sistemas automáticos y sistemas manuales de captación de datos) u otros datos e información pertinente. Los principios de protección y excepción, por consiguiente, pueden hacerse extensivos también a los datos e información sobre seguridad operacional captados por dichos sistemas.

7.3.1.3 Los principios de protección y de excepción se aplicarán también a otros casos. Por ejemplo, en el Anexo 6 — *Operación de aeronaves*, Parte I — *Transporte aéreo comercial internacional — Aviones* se establece que las fuentes de los programas de análisis de datos de vuelo (FDA) deberían protegerse con arreglo a los principios que figuran en el Anexo 19.

7.3.1.4 El tipo de datos e información sobre seguridad operacional que pueden captarse por los sistemas de notificación de seguridad operacional, así como las clases de sistemas que pueden ser parte de los mismos, pueden evolucionar con el tiempo paralelamente a la evolución de los propios sistemas de gestión de la seguridad operacional. Los datos y la información sobre seguridad operacional así como los sistemas de notificación de la misma que no están expresamente identificados en el Anexo 19 en la actualidad, podrían estar gobernados por futuras versiones del Anexo 19.

2. La prevención del ejercicio de privilegios puede comprender la suspensión o revocación de licencias.
3. Los privilegios del titular de una autorización están especificados en la licencia o certificado expedido por las autoridades normativas del Estado en el ámbito de la aviación.

7.3.2 Interacción con los principios de protección que figuran en otros Anexos

7.3.2.1 Ciertos tipos de datos e información sobre seguridad operacional que están protegidos en el marco del Anexo 19 pueden, en ciertas circunstancias, estar sujetos a otros requisitos de protección.

7.3.2.2 En particular, en el Anexo 19 se especifica que cuando se ha instituido una investigación en el marco del Anexo 13, los registros de investigaciones de accidentes e incidentes enumerados en el Anexo 13 están sujetos a las protecciones acordadas en dicho Anexo, y no a las del Anexo 19.

7.3.2.3 Este principio se aplica a partir del momento en que ocurre un accidente o incidente que corresponde al Anexo 13 y permanece aplicable aún después de la publicación del informe final. En el *Manual sobre protección de la información de seguridad operacional* (Doc 10053) figura orientación sobre la protección de los registros de investigaciones de accidentes e incidentes.

7.3.2.4 Análogamente, aunque el Anexo 19 proporciona protección a los datos registrados cuando se utilizan para fines de gestión de la seguridad operacional, el Anexo 6 brinda protección a las grabaciones de los registradores de vuelo en operaciones normales, que no corresponden a investigaciones del tipo abarcado por el Anexo 13.

7.3.2.5 En el Anexo 6 se aborda el uso de registradores de la voz en el puesto de pilotaje (CVR) y registradores de imágenes de a bordo (AIR) que debería limitarse a fines relacionados con la seguridad operacional con las salvaguardias apropiadas para inspecciones de los sistemas de registradores de vuelo, o cuando los registros o transcripciones conexas se procuran para procesos penales. Dichos procesos penales se han introducido en la enmienda como una excepción de las protecciones acordadas a los CVR y AIR a fines de permitir que las autoridades competentes tengan acceso a estos tipos de registros y sus transcripciones y los utilicen sin restricciones en casos en que se han cometido delitos y los miembros de la tripulación involucrados puedan no haber consentido a dicho uso (p. ej., casos de apoderamiento ilícito).

7.3.2.6 Análogamente, el uso de registradores de datos de vuelo (FDR), sistemas registradores de datos de aeronave (ADRS), así como AIR de Clases B y C y sistemas registradores de imágenes de a bordo (AIRS) debería limitarse a fines de aeronavegabilidad o mantenimiento, incluyendo los programas FDA, con las protecciones apropiadas acordadas por el Anexo 19.

7.3.2.7 En la Figura 7-1 se proporcionan directrices generales respecto de la interacción entre los marcos de protección de los Anexos 6, 13 y 19, para utilizar en consulta con las disposiciones aplicables.

7.3.2.8 Con respecto a los programas FDA, las fuentes permanecen, en todas las situaciones, protegidas por los principios que figuran en el Anexo 19.

7.3.3 Aplicación de los principios del Anexo 19 a los proveedores de servicios

7.3.3.1 En el Anexo 19 se describe un entorno de notificación que fomente la confianza como aquel “en el que los empleados y el personal operacional puedan tener la confianza de que las acciones u omisiones que correspondan a su formación y experiencia no serán objeto de sanciones”. Una acción u omisión corresponde a la formación y experiencia de una persona cuando es razonable prever que otra persona con el mismo nivel de experiencia y formación podría hacer, o no hacer, la misma cosa. Dicho entorno es fundamental para la notificación de seguridad operacional eficaz y eficiente.

7.3.3.2 Alentar a las personas a que notifiquen datos o información sobre seguridad operacional pertinentes requiere que las fuentes de dichas notificaciones estén protegidas respecto de medidas adoptadas por un Estado con arreglo al Anexo 19, así como respecto a acciones tomadas en su entorno laboral.

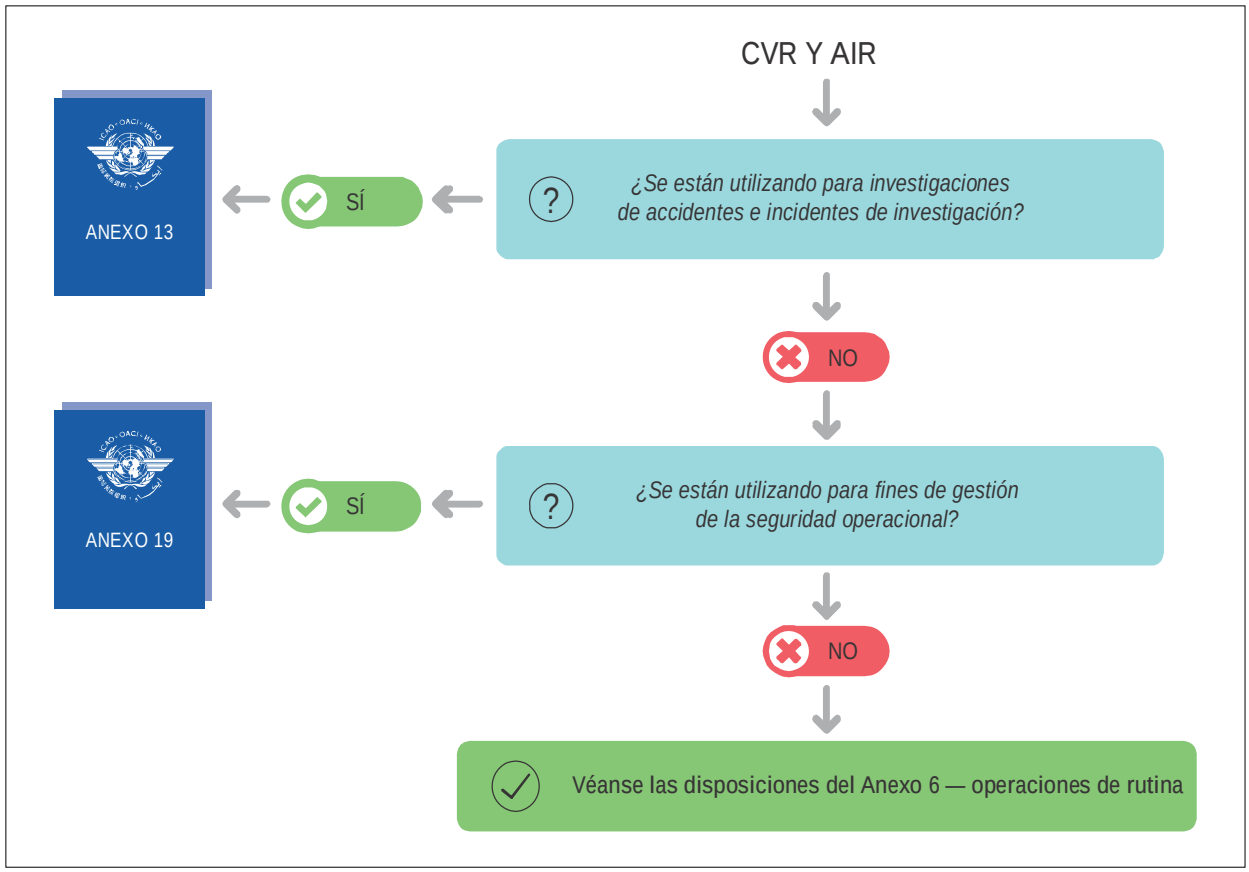


Figura 7-1. Directrices sobre la interacción de disposiciones de protección

7.3.3.3 Las disposiciones del Anexo se dirigen a proporcionar los requisitos mínimos que han de satisfacer todos los Estados, independientemente del volumen y complejidad de sus actividades de aviación civil. Cada Estado es responsable de elaborar requisitos suficientes para asegurar el cumplimiento satisfactorio por parte del Estado y sus proveedores de servicios.

7.3.3.4 Los principios de protección y excepción que se aplican a los datos de seguridad operacional, información sobre seguridad operacional y fuentes conexas en el marco del Anexo 19 deberían ser implementados por los Estados y los proveedores de servicios por igual. Para asegurar el logro de este objetivo, se espera que los Estados adopten leyes, reglamentos y políticas nacionales pertinentes para asegurar que sus proveedores de servicios apliquen las disposiciones que figuran en el Anexo 19.

7.4 NIVEL DE PROTECCIÓN

7.4.1 Condiciones para la protección en el marco del Anexo 19

7.4.1.1 En el Anexo 19 se requiere que los Estados especifiquen las condiciones bajo las cuales los datos, la información sobre seguridad operacional y las fuentes conexas reúnen los requisitos para ser protegidos. Al hacerlo, se espera que los Estados consideren si:

a) los datos o la información sobre seguridad operacional están abarcados en el ámbito del Anexo 19;

b) hay circunstancias bajo las cuales el Anexo 6 o el Anexo 13 tendrían precedencia respecto del Anexo 19; y

c) se aplica un principio de excepción.

7.4.2 Medidas necesarias para mantener o mejorar la seguridad operacional de la aviación

7.4.2.1 En el Anexo 19 se asegura que no se impedirá que los Estados y proveedores de servicios utilicen los datos e información sobre seguridad operacional para tomar medidas de carácter preventivo, correctivo o de rectificación que sean necesarias para mantener o mejorar la seguridad operacional de la aviación. De acuerdo con dicho objetivo, dichas medidas, si se adoptan, deberían evitar en lo posible que tengan consecuencias adversas, financieras, para la reputación o de otros tipos para la fuente de dichos datos o información sobre seguridad operacional.

7.4.2.2 Las medidas de carácter preventivo, correctivo o de rectificación se dirigen a abordar circunstancias o condiciones que presenten riesgos inaceptables para la seguridad operacional de la aviación.

7.4.2.3 Las *medidas preventivas* son aquellas adoptadas para prevenir que ocurran o vuelvan a ocurrir sucesos o peligros que planteen riesgos para la seguridad operacional.

7.4.2.4 Las *medidas correctivas* son aquellas adoptadas para abordar carencias o deficiencias particulares relacionadas con la seguridad operacional, como el caso en que un titular de autorización no pueda demostrar el cumplimiento de las normas aplicables de seguridad operacional o competencia. Las medidas correctivas pueden ser necesarias para hacer que el titular de una autorización cumpla dichas normas.

7.4.2.5 Las *medidas de rectificación* son aquellas adoptadas para abordar las causas subyacentes de carencias o deficiencias particulares relacionadas con la seguridad operacional, como en la instrucción. Las medidas de rectificación también pueden involucrar la restricción, limitación, suspensión o revocación de los privilegios de un titular de autorización, certificado o licencia que no continúe satisfaciendo las cualificaciones necesarias para ejercer dichos privilegios.

7.4.2.6 Aunque pueden especificarse para uno u otro fin, dichas medidas pueden aplicarse a más de un propósito. Por ejemplo, un reglamentador o proveedor de servicios puede adoptar medidas que exijan que el titular de una licencia o certificado reciba instrucción adicional y que se abstenga de ejercer los privilegios de dicha licencia o certificado hasta haber completado satisfactoriamente dicha instrucción. Un reglamentador también puede adoptar medidas para revocar, retirar o suspender determinados privilegios del certificado de una organización. Tales medidas, si bien son de rectificación porque abordan las causas subyacentes de un problema de seguridad operacional, pueden considerarse también como correctivas debido a que tratan una deficiencia particular. Cualquiera sea la caracterización de la medida adoptada, debería existir una relación clara y demostrable entre la medida particular adoptada y el mantenimiento o mejora de la seguridad operacional.

7.4.2.7 Los datos o información sobre seguridad operacional pueden revelar peligros o deficiencias que requieran medidas de rectificación o correctivas para mantener la seguridad operacional o identificar sectores en los que la adopción de medidas preventivas mejorarían la seguridad operacional abordando riesgos posibles o emergentes. Para poner en evidencia la condición o peligro subyacente que justifique la adopción de medidas preventivas, correctivas o de rectificación, los Estados pueden tener que utilizar datos o información sobre seguridad operacional. Por ejemplo, los datos y la información sobre seguridad operacional pueden ser necesarios para establecer la base de una medida administrativa relativa a licencias o para satisfacer el requisito de carga de la prueba. También, los datos y la información sobre seguridad operacional pueden ser necesarios para establecer la necesidad de instrucción adicional de un titular de licencia o de cambios en los sistemas de un explotador. También pueden ser necesarios para asegurar la integridad y el funcionamiento adecuado del sistema de notificación así como del sistema más amplio del que éste forma parte.

7.4.2.8 Dependiendo de las circunstancias, las medidas preventivas, correctivas o de rectificación, si bien no es su propósito, pueden percibirse como punitivas por el individuo o el proveedor de servicios objeto de las mismas. En efecto, algunas personas pueden considerar que las medidas sobre licencias adoptadas para abordar deficiencias en la competencia tienen carácter punitivo, en vez de ser medidas necesarias para corregir o remediar un riesgo de seguridad operacional.

7.4.2.9 A pesar de estas percepciones, en el Anexo 19 no se impide que los Estados utilicen los datos e información sobre seguridad operacional para tomar medidas que sean necesarias para mantener o mejorar la seguridad operacional de la aviación. Cuando sea necesario adoptar medidas para mantener o mejorar el nivel de seguridad operacional de la aviación o para impedir el deterioro a corto o largo plazo de la seguridad del sistema de aviación, los Estados pueden utilizar datos o información sobre seguridad operacional en apoyo de dichas medidas, siempre que tengan un objetivo y un efecto de carácter preventivo, correctivo o de rectificación demostrables. En tales casos, los Estados deberían considerar la adopción de disposiciones necesarias para comunicar claramente el fundamento de cada medida tomada, a fin de demostrar su propósito de seguridad operacional y minimizar cualquier consecuencia adversa sobre las notificaciones futuras. Por otra parte, debería prohibirse, a menos que se aplique algunos de los principios de excepción, el uso de datos e información sobre seguridad operacional para adoptar medidas cuyos propósitos en la materia no puedan demostrarse, y que, por el contrario, muestren un objetivo y consecuencias de carácter puramente punitivo o disciplinario.

7.4.3 Protección de los sistemas de notificación obligatoria

7.4.3.1 En el Anexo 19 se especifican diferentes requisitos para la protección de los datos y la información sobre seguridad operacional, así como de sus fuentes conexas, captados por los sistemas de notificación voluntaria y obligatoria de seguridad operacional. La protección de los datos e información sobre seguridad operacional captados por los sistemas de notificación voluntaria de seguridad operacional constituye una Norma, a fin de garantizar la continua disponibilidad y una mayor uniformidad entre los Estados, mientras que para los sistemas de notificación obligatoria de seguridad operacional el suministro de dicha protección constituye un Método recomendado.

7.4.3.2 En algunas jurisdicciones, los datos y la información sobre seguridad operacional captados por los sistemas de notificación obligatoria y voluntaria de seguridad operacional están sujetos a diferentes niveles de protección, ofreciéndose a los datos e información sobre seguridad operacional obtenidos de sistemas de notificación voluntaria una protección mayor que a los obtenidos de los sistemas obligatorios. Esta distinción puede justificarse por la necesidad de incentivar el suministro voluntario de datos e información sobre seguridad operacional en formas que no se consideran necesarias en el caso de los sistemas de notificación obligatoria.

7.4.3.3 Otros Estados ofrecen el mismo alto nivel de protección a los datos y la información de seguridad operacional de ambos tipos de sistema. Esto puede justificarse por el reconocimiento de que la exigencia jurídica de notificar puede por sí misma no ser suficiente para asegurar que se notifiquen los datos y la información sobre seguridad operacional pertinentes y que el valor de un entorno de confianza en fundamental para cualquier tipo de notificación. El extender las protecciones a los sistemas de notificación obligatoria también puede alentar a las personas a proporcionar detalles adicionales que, de otra forma, podrían no proporcionar si no existiera dicha protección.

7.4.3.4 Si un Estado hace extensiva a los sistemas de notificación obligatoria la protección brindada a los datos y la información sobre seguridad operacional captados por los sistemas de notificación voluntaria, los principios de protección y excepción que figuran en el Anexo 19 deberían aplicarse a dichos datos e información captados por ambos sistemas así como a sus fuentes respectivas.

7.4.4 Protección de datos e información en el dominio público

7.4.4.1 Puede haber casos en los que los datos o información sobre seguridad operacional estén disponibles en el dominio público. En algunos casos, puede ser que tales datos o información no tengan carácter delicado y que su

ulterior divulgación no afecte adversamente la continua disponibilidad de datos o información sobre seguridad operacional. Un ejemplo de dichos datos e información que no tienen carácter delicado son los relacionados con las condiciones meteorológicas.

7.4.4.2 En otros casos, los datos y la información sobre seguridad operacional normalmente sujetos a los principios de protección pueden de alguna manera llegar al dominio público, por ejemplo, a través de filtraciones a los medios de difusión. En tales casos, los Estados deberían abstenerse de continuar divulgando los datos y la información que hayan transcendido, puesto que los principios de protección no serán suspendidos automáticamente.

7.5 PRINCIPIOS DE PROTECCIÓN

7.5.1 Aplicación de los principios de protección

7.5.1.1 La protección de datos e información sobre seguridad operacional y sus fuentes conexas debería ser la conducta normal para el Estado. El Estado puede proporcionar protección eficaz por medios jurídicos, apoyados por procedimientos amplios y claros.

7.5.1.2 El propósito básico de brindar protección es asegurar la continua disponibilidad de los datos y la información sobre seguridad operacional alentando a individuos y organizaciones a que identifiquen, notifiquen, analicen y corrijan las deficiencias que hubiere. Esto exige que todos los involucrados conozcan por adelantado las reglas y procesos que rigen dicha protección. Esas reglas y procesos deberían formalizarse y no estar sujetos a aplicaciones arbitrarias si se quiere que sirvan de fundamento de un sistema basado en la confianza.

7.5.1.3 Al proteger los datos o información sobre seguridad operacional, debería considerarse el objetivo que dicha protección se dirige a alcanzar. El objetivo puede ser evidente a partir del tipo de datos e información que han de protegerse. En muchos casos, la protección tiene por objeto prevenir que se utilicen datos e información sobre seguridad operacional contra el individuo o la organización que notificó dichos datos o información. En otros casos, puede ser importante proteger los datos o la información sobre seguridad operacional respecto de su publicación general o su utilización en contextos no relacionados con la seguridad operacional, como controversias locales sobre utilización de terrenos que involucren operaciones aeroportuarias y aspectos de atenuación del ruido.

7.5.1.4 La acción del Estado es fundamental en la creación de disposiciones de protección. En procedimientos formales donde existen reglas que rigen el tipo de evidencia o pruebas que se pueden presentar, solo la acción del Estado puede proporcionar la protección necesaria mediante la institución de legislación o reglamentos apropiados que prohíban o limiten estrictamente la admisibilidad de la información protegida. Por ejemplo, en procedimientos penales contra un individuo, debería prohibirse el uso de un informe voluntario presentado por el acusado si no se relaciona directamente con el supuesto delito.

7.5.1.5 En los procedimientos civiles contra un proveedor de servicios debería existir una regla que, como mínimo, requiera la presunción[4] refutable de que puede no utilizarse información protegida. En un procedimiento contra una línea aérea por daños sufridos como resultado de un suceso, un demandante puede procurar acceso general a los archivos del SMS del explotador en un intento por descubrir información general que puede no estar directamente relacionada con el incidente, pero que podría resultar desfavorable para el explotador. El procedimiento establecido para determinar dichas cuestiones debería llevar a la autoridad competente (en este caso muy probablemente un tribunal) encargada de aplicar los principios de excepción (ver 7.6 por más detalles) a exigir al demandante que indique precisamente que tipo de información debería descubrirse y demostrar la pertinencia de la misma respecto del procedimiento, así como demostrar la no disponibilidad de fuentes alternativas para la misma o similar información. La

4. Una presunción refutable es una suposición que se considera verdadera salvo prueba en contrario.

autoridad competente también podría preguntar al demandante como éste se vería perjudicado si no tiene acceso a la información en cuestión. Si se decide permitir dicho acceso, la autoridad competente debería imponer salvaguardias formales con arreglo a los requisitos procesales aplicables, como una medida cautelar para impedir la publicación en general y restringir el acceso a las partes pertinentes de las actas procesales.

7.5.1.6 En los procesos administrativos donde se cuestionan determinadas cualificaciones operacionales o técnicas, competencias y capacidades de un individuo o una organización, la seguridad operacional será casi invariablemente un aspecto importante. En tales casos, podría requerirse el uso de datos o información sobre seguridad operacional, pero deberían proporcionarse disposiciones ejecutables para el uso controlado y limitado de dichos datos e información. Cuando los datos o la información sobre seguridad operacional proporcionan la base para adoptar decisiones en dichos casos relacionados con la seguridad operacional, debería exigirse una extraordinaria cautela a efectos de prevenir consecuencias adversas o perjudiciales para la fuente de la información como resultado del uso de dichos datos. En general, los individuos y organizaciones a quienes se alienta a notificar información en el marco de un plan de notificación protegida reconocerán que hay circunstancias en las cuales deben adoptarse medidas en interés de la seguridad operacional basadas, total o parcialmente en un informe protegido. La institución de requisitos ejecutables debería asegurar que dichas medidas son fundamentalmente imparciales para la consecución del objetivo de mantener o mejorar la seguridad operacional.

7.5.1.7 Un ejemplo de tal situación podría ser una notificación de un controlador de tránsito aéreo que perdió el conocimiento durante un breve período de tiempo en su trabajo. No se vio afectada la separación y la única prueba de que ocurrió el suceso fue el propio informe del controlador. Para fines relacionados con la seguridad operacional, el análisis de dicha notificación requirió más investigación, lo que a su vez exigió que el individuo en cuestión fuera identificado de alguna manera. La corrección inmediata podría involucrar la separación del controlador del servicio activo (sin desventajas financieras o para su reputación) mientras se realizara un examen y revisión médicos completos. Una vez llevado a cabo dicho examen, el resultado puede ser o bien la autorización médica, un tratamiento médico o un retiro de servicio por orden médica (nuevamente, sin desventajas financieras o para la reputación). Si el controlador fuera sencillamente despedido, es muy improbable que en el futuro sea tan fácil obtener informes similares de otros individuos.

7.5.1.8 Hasta este momento, la cuestión se ha centralizado en la acción directa del Estado para proporcionar protección necesaria y apropiada. En la práctica, gran parte de los datos y la información sobre seguridad operacional para los que se requiere protección pertenecen al entorno operacional de un proveedor de servicios e involucra relaciones entre empleadores y empleados. En estas situaciones, la protección no siempre estaría abarcada en la legislación o en otras formas de requisitos estatales ejecutables. Incluso en tales casos, no obstante, los Estados podrían estar en condiciones de exigir protección efectiva mediante sus procesos de certificación, aprobación y supervisión continua. En el Anexo 19 se exige que determinados proveedores de servicios implementen un SMS eficaz. La gestión eficaz de la seguridad operacional se basa en la recopilación, análisis y protección de los datos. Sin datos el sistema perdería eficacia. El SSP debería permitir que los Estados instruyan a las organizaciones a que implanten políticas que brinden protección a sus empleados como un elemento de sus SMS.

7.5.1.9 Una forma de proporcionar dicha protección podría involucrar la no identificación del informante. Si bien la confidencialidad de las notificaciones es una estrategia útil, el anonimato completo, cuando es posible, elimina la posibilidad de seguimiento durante la fase de análisis. Las políticas deberían concentrarse en el tipo de uso que la autoridad competente podría hacer, o permitir, de los datos e información sobre seguridad operacional en cuestión. El análisis presentado en 7.5.1.6 en relación con los procedimientos administrativos se aplica igualmente al contexto empleador/empleado. Nuevamente, las personas que deberían presentar notificaciones necesarias estarían remisas a proporcionarlas si dichos informes, u otros datos o captación de los mismos, se utilizan para apoyar una suspensión o un despido de carácter punitivo o disciplinario.

7.5.1.10 La captación de datos e información sobre seguridad operacional por medios automáticos, como los FDR, registradores de la voz o vídeo, o registradores en el entorno de control del tránsito aéreo, debería ser parte de toda política o reglamento de protección. El uso de estos dispositivos como parte de la captura de datos del SMS, cuando los reglamentos o las políticas lo permiten, debería respetar plenamente los principios de protección en la misma forma en

que se respetan las notificaciones presentadas en forma voluntaria. La confianza de la población notificadora resulta fundamental para la gestión eficaz de la seguridad operacional.

7.5.2 Procedimientos

7.5.2.1 En el Anexo 19 se exige que los Estados se aseguren de que los datos y la información sobre seguridad operacional no se utilicen para procedimientos disciplinarios, civiles, administrativos y penales contra empleados, personal de operaciones u organizaciones, a menos que se aplique un principio de excepción.

7.5.2.2 El término “procedimientos” puede tener un alcance más completo y más amplio que el término “acciones”. Puede también referirse en términos más estrechos a los procesos de un órgano particular para examinar o imponer “acciones” que han sido adoptadas por otras autoridades (o por un organismo dentro de la misma autoridad). En un sentido general, los términos “procedimientos” y “acciones” pueden considerarse como que abarcan todas las etapas o medidas adoptadas para iniciar, dar efecto o revisar una decisión de una autoridad que afecte los derechos, privilegios, intereses legítimos o expectativas razonables de una persona (según se identifiquen en las leyes aplicables). Habida cuenta de los diferentes sistemas jurídicos, el carácter y alcance de las acciones o procedimientos particulares pueden variar. Por ejemplo, en algunos Estados:

a) Las *acciones o procedimientos penales y civiles* normalmente involucran autoridades judiciales. Estos procedimientos pueden incluir el inicio de la acción, la comparecencia del acusado, todas las etapas auxiliares o provisionales, los alegatos, los procesos de descubrimiento legal y otras consultas formales. Como consecuencia de tales acciones o procedimientos, una persona puede verse expuesta a daños monetarios, multas o en algunos casos encarcelamiento.

b) Las *acciones o procedimientos administrativos* pueden involucrar una consulta, investigación o audiencia frente a un reglamentador o a un tribunal que se relacione con medidas para variar, suspender, revocar o cancelar una autorización (con fines cuya relación con la seguridad operacional puede demostrarse en algunos casos, y con fines punitivos en otros).

c) Las *acciones o procedimientos disciplinarios* pueden referirse al proceso por el cual un empleador responda a violaciones o infracciones reales o aparentes de reglas y procedimientos por parte de un empleado. El resultado de tales acciones o procedimientos puede ser la absolución del empleado respecto de las infracciones supuestas, o la sanción o despido del empleado si las acusaciones son corroboradas.

7.5.2.3 Otras autoridades pueden estar involucradas en las acciones y procedimientos mencionados, como tribunales administrativos, órganos profesionales o éticos u otros órganos examinadores dentro de una organización.

7.5.2.4 Es importante recordar que los principios de protección no se aplican cuando los Estados adoptan una medida preventiva, correctiva o de rectificación necesaria para mantener o mejorar la seguridad operacional de la aviación (véase 7.4.2). Esto también se aplica a todo procedimiento, acción o medida relacionada con una decisión de carácter preventivo o de rectificación tomada con el fin de mantener o mejorar la seguridad operacional. Por ejemplo, el uso de datos o información sobre seguridad operacional para justificar la adopción de una medida preventiva, correctiva o de rectificación está permitido en los procedimientos iniciados por un individuo o una organización tendientes a impugnar la medida en cuestión.

7.5.2.5 Aunque pueden haber casos en que los datos o información sobre seguridad operacional se utilicen en litigios iniciados por una tercera parte contra la fuente de la notificación, se alienta a loso Estados a que adopten todas las medidas necesarias para asegurar que los datos y la información sobre seguridad operacional no se utilicen para fines que no sean los de mantener y mejorar la seguridad operacional de la aviación (a menos que se aplique un principio de excepción).

7.5.3 Garantías autorizadas

7.5.3.1 Algunos factores pueden mitigar las consecuencias negativas relacionadas con la divulgación o uso de datos o información sobre seguridad operacional para fines que no sean mantener o mejorar la seguridad operacional de la aviación. Puede ser posible limitar posibles daños derivados de la divulgación o uso propuestos mediante la implantación de garantías o salvaguardias para limitar el mayor grado la divulgación o uso de los datos e información sobre seguridad operacional. Los Estados pueden incluir en su legislación o reglamentos, con arreglo a los cuales se considera la aplicación de los principios de excepción, la facultad de la autoridad competente de imponer requisitos para mantener el carácter confidencial de los datos o información sobre seguridad operacional después de haberse adoptado una decisión para permitir el acceso a los mismos.

7.5.3.2 La no identificación de la fuente de los datos e información sobre seguridad operacional es otra salvaguardia que puede aplicarse antes de que la autoridad competente autorice la divulgación de los mismos para fines que no sean mantener o mejorar la seguridad operacional. No obstante, el anonimato puede resultar difícil cuando las fuentes que proporcionan los datos o información sobre seguridad operacional pueden ser fácilmente identificables a partir del contenido de los datos o información notificados. Por ejemplo, el informe de un suceso que involucró un tipo de aeronave utilizado solamente por un explotador único dentro de una jurisdicción particular puede poner inmediatamente en evidencia a dicho explotador (o incluso a un empleado en particular), sencillamente identificando el tipo de aeronave en cuestión. En tales casos, la forma y el lugar en que se propone divulgar o utilizar los datos o la información sobre seguridad operacional, así como el carácter de los mismos, tendrían especial importancia.

7.5.3.3 Si se propone utilizar datos o información sobre seguridad operacional en un foro donde el conocimiento de las personas u organizaciones relacionadas con los datos o la información es limitado, la autoridad competente puede confiar en que el anonimato proporcionaría una protección suficiente de las fuentes. Análogamente, si el carácter de la información es principalmente técnico, podría no haber en la misma mucha información de identificación que deba suprimirse u ocultarse, lo que facilitaría la labor de protección. La autoridad competente también debería considerar si el foro de la divulgación propuesta o el uso de los datos o la información y el carácter de la misma, afectarían la medida en que puedan identificarse las fuentes y si la supresión de información de identificación resultaría suficiente. Si la divulgación o uso propuestos puede afectar adversamente a una organización o a una compañía, como el explotador de aeronaves, entonces la autoridad competente debería decidir si la no identificación de los datos o la información proporcionaría protección razonable similar a la que la compañía o el explotador podrían haber obtenido si no se hubiera permitido la divulgación o el uso.

7.5.3.4 Si la autoridad competente considera que la no identificación de la fuente de los datos o información sobre seguridad operacional puede impedir el uso previsto o permisible de dichos datos o información, el anonimato no resultaría apropiado. Por consiguiente, los Estados pueden optar por implementar diversos tipos de garantías (o combinaciones de salvaguardias) para permitir la divulgación limitada para un fin específico impidiendo al mismo tiempo el uso más amplio o la divulgación al público de los datos o información sobre seguridad operacional. Ejemplos de dichas garantías son las órdenes de protección, audiencias a puerta cerrada, exámenes a puerta cerrada y resúmenes.

7.5.3.5 Los Estados y las organizaciones también pueden adoptar mejores prácticas, como el asegurar que el entorno en que se recopila, almacena, procesa y transmite la información es suficientemente seguro y que los controles de acceso y las autorizaciones son suficientes para proteger los datos y la información sobre seguridad operacional.

7.6 PRINCIPIOS DE EXCEPCIÓN

Los principios de protección se aplican a los datos y la información sobre seguridad operacional y sus fuentes conexas, a menos que una autoridad competente determine que se aplica uno de tres principios de excepción. El custodio del SDCPS debería tener conocimiento de las protecciones que se aplican a los datos y a la información sobre seguridad operacional y fuentes conexas y asegurar que los mismos se divulgan y utilizan con arreglo a las disposiciones del Anexo 19.

7.6.2 Designación de la autoridad competente

7.6.2.1 Dado que los principios de excepción estarán administrados para una amplia gama de fines diferentes, la autoridad competente será también diferente dependiendo del carácter de los datos o la información en cuestión y del tipo de uso que se pretende. En cada caso particular, la tarea de la autoridad competente será decidir si se aplica un principio de excepción en particular. La autoridad competente deberá ser capaz de sopesar intereses conflictivos o contrapuestos, como las leyes relativas al derecho de saber, reglamentos no relacionados con la seguridad operacional de la aviación, reglas para divulgación en litigios y otros aspectos a efectos de que el público pueda tener confianza en sus capacidades de toma de decisiones. Las autoridades competentes podrían incluir a las autoridades judiciales, autoridades normativas u otras partes con responsabilidades en la aviación designadas con arreglo a las leyes nacionales y otros requisitos ejecutables.

7.6.2.2 Los Estados y las organizaciones deberán identificar autoridades competentes apropiadas a la tarea de aplicar los principios de excepción para fines diferentes. En la siguiente Tabla 9 se proporcionan ejemplos de posibles autoridades competentes y situaciones.

Tabla 9. Ejemplos de situaciones y posibles autoridades competentes

Situación	*Posible autoridad competente*
La divulgación o el uso de datos o información sobre seguridad operacional son solicitados por un miembro del público con arreglo a las leyes relativas al derecho de saber[5].	Departamento gubernamental u órgano administrativo
La cuestión de la divulgación o uso de los datos o información pasa a ser objeto de litigio en el marco de las mismas leyes sobre el derecho de saber, o los datos o información sobre seguridad operacional se solicitan para utilizar en procedimientos judiciales.	Corte de justicia o tribunal administrativo
Una autoridad normativa debe adoptar medidas para mantener o mejorar la seguridad operacional.	CAA
En el caso de divulgación o uso de datos o información sobre seguridad operacional en custodia de una organización.	Persona en la organización responsable de la seguridad operacional de la aviación, como un gerente o un grupo integrado por la administración, un representante de los empleados y, en algunos Estados, un representante del reglamentador

7.6.2.3 Cuando una organización identifica a su autoridad competente, el ejercicio responsable de discreción por parte de ésta sobre la aplicación de los principios de la excepción y de protección puede muy bien proporcionar suficiente autocontrol dentro de la organización. La determinación final de la autoridad competente para cada propósito específico corresponde a cada Estado y organización, dependiendo de las leyes y políticas aplicables.

7.6.2.4 La designación permanente de la oficina y jurisdicción de la autoridad competente (p. ej., autoridades judiciales para asuntos que involucren litigios, la CAA para medidas de reglamentación) puede considerarse para facilitar la rápida toma de decisiones. Una designación permanente también proporcionará la certeza de que la autoridad competente cuenta con atribuciones y experiencia para tratar estos asuntos. Además, resulta crítico que la autoridad competente cuente con reglas y procedimientos que rijan el proceso de toma de decisiones. Estas reglas y

5. En la sección 7.7 de este capítulo figura más información sobre las leyes relativas al derecho de saber.

procedimientos deberían basarse en las leyes nacionales aplicables. Esto solo puede lograrse si la designación de la autoridad competente en un sector determinado permanece constante.

7.6.3 Aplicación de los principios de excepción

7.6.3.1 El primer caso en que una autoridad competente puede hacer excepciones respecto de la protección es cuando "determine que los hechos y circunstancias indican de manera razonable que el suceso pudo haber sido causado por un acto u omisión que, de acuerdo con las leyes nacionales, se considere que constituye una conducta de negligencia grave, un acto doloso o una actividad criminal". En la mayoría de los casos, la autoridad competente apropiada para tomar dicha determinación será una autoridad judicial, administrativa o de fiscalía.

7.6.3.2 Debido a que una evaluación del carácter de los datos o la información sobre seguridad operacional en cuestión determinará a menudo si la conducta en cuestión satisface una u otra de las condiciones para uso excepcional, no es necesario que los hechos y circunstancias del caso hagan inequívocamente claro que dicha conducta excepcional ha ocurrido. En vez de ello, solo es necesario que de esos hechos y circunstancias proporcionen una base razonable sobre la cual podría determinarse que el suceso pudo haber sido causado por dicha conducta. Cuando la autoridad competente determine que, sobre la base de los hechos y circunstancias de un caso, el suceso pudo haber sido resultado de negligencia grave, acto doloso o actividad criminal, en el sentido que dichos términos tienen en las leyes nacionales — se aplica un principio de excepción y los datos o la información sobre seguridad operacional así como sus fuentes conexas pueden divulgarse.

7.6.3.3 Diferentes sistemas jurídicos pueden presentar diferentes interpretaciones en el marco de las leyes nacionales sobre el significado de esos términos. En general, la negligencia grave se refiere a un acto u omisión cometido con grave desconsideración o indiferencia frente a un riesgo evidente, independientemente de si dicho riesgo ha sido plenamente tenido en cuenta por el actor. Esto se describe a veces como conducta imprudente. Un acto doloso es una acción u omisión ilícitas cuyo actor sabe que lo son o es conscientemente indiferente frente a la cuestión de si lo es o no. El conocimiento y la intención en tales casos pueden también a veces relacionarse con las consecuencias de la conducta, y no solo a su descripción oficial como ilícita. En todo caso, el examen de pruebas y las medidas aplicables para tomar una determinación sobre el carácter de la conducta en cuestión deberían ajustarse a las leyes de la jurisdicción pertinente. Además, debido a que el principio de excepción establece una diferencia entre conducta de "negligencia grave" o "acto doloso", por una parte y "actividad criminal" por la otra, resulta claro que la conducta que pueda constituir ya sea "negligencia grave" o "acto doloso" (aunque dicha conducta pueda estar descrita en el derecho nacional aplicable) deberá evaluarse sobre la base de una norma civil y no penal.

7.6.3.4 El segundo caso en que la autoridad competente puede determinar que se aplica una excepción a las reglas de protección es cuando habiendo efectuado un examen de los datos o la información sobre seguridad operacional en cuestión, la autoridad competente determine que su divulgación es "necesaria para la administración apropiada de la justicia" y que las "ventajas de su divulgación pesan más que las repercusiones adversas que a escala nacional e internacional dicha divulgación tendrá en la futura recopilación y disponibilidad de los datos y la información sobre seguridad operacional".

7.6.3.5 Esto involucra un proceso de evaluación en dos etapas, en el cual la autoridad competente debe considerar en primer lugar si los datos o la información son "necesarios para la administración apropiada de la justicia", que puede no ser el caso si se dispone de fuentes alternativas para la misma información, y en segundo lugar, si determina que la divulgación es necesaria para la administración apropiada de la justicia si, en comparación, la divulgación de dichos datos o información pesa más que las repercusiones adversas que su divulgación tendría en la futura recopilación y disponibilidad de los datos y la información sobre seguridad operacional para fines de mantener o mejorar dicha seguridad.

7.6.3.6 Si se prevé el uso de datos o información sobre seguridad operacional en una acción o procedimiento (civil, administrativo, penal o disciplinario), entonces el posible impacto negativo de dicho uso puede relacionarse con la fuente de tales datos o información. Aun si pueden imponerse garantías para prevenir que los datos o información

sobre seguridad operacional se divulguen fuera de los límites de la acción o procedimiento, toda consecuencia negativa del uso de tales datos o información durante un procedimiento podría desalentar futuras notificaciones o divulgaciones de datos e información sobre seguridad operacional para fines de mantener o mejorar dicha seguridad. Si el uso propuesto de los datos o la información involucra la difusión al público o publicación de tales datos o información más allá de los límites del procedimiento, la autoridad competente también debería considerar las posibles consecuencias perjudiciales sobre la comunidad más amplia (nacional e internacional).

7.6.3.7 A nivel del individuo, hacer pública la información puede ir en perjuicio o detrimento de la persona involucrada, como vergüenza, bochorno o posible pérdida de sustento. A nivel más amplio, la publicación o difusión de datos o información sobre la seguridad operacional en un caso particular puede crear un factor de disuasión general para personas en situaciones similares, aunque no estén involucradas en la acción o procedimiento particular, en cuanto a notificar o contribuir a la recopilación de tales datos e información.

7.6.3.8 Al tomar la determinación respecto de los dos primeros principios de excepción, la autoridad competente deberá cerciorarse de que:

a) en el primer caso, el contenido de los datos o información sobre seguridad operacional que se pretende divulgar o utilizar es necesario para decidir si el acto u omisión constituye negligencia grave, acto doloso o actividad criminal; o

b) en el segundo caso, dichos datos, información o fuente conexa son necesarios para la administración apropiada de la justicia.

7.6.3.9 La autoridad competente determinará si los datos o la información sobre seguridad operacional o la identidad de la fuente de dichos datos sobre información son necesarios para el caso. Si la autoridad competente puede tomar una decisión en forma razonable sin referirse a los datos, información o fuentes protegidos, entonces deberá darse mayor peso al mantenimiento de la protección de los mismos. No es necesario suponer por adelantado la recopilación y la disponibilidad de los datos, información sobre seguridad operacional y fuentes conexas cuando la autoridad competente puede tomar una decisión sin requerir la divulgación (o uso) de dichos datos e información. Esto ayudará a asegurar la continua disponibilidad de datos e información sobre seguridad operacional para mantener o mejorar la seguridad operacional de la aviación.

7.6.3.10 Pueden surgir consecuencias adversas de la divulgación o uso de datos e información sobre seguridad operacional y fuentes conexas, como la reticencia del personal operacional aeronáutico a cooperar voluntariamente con los inspectores. Si tales datos, información o detalles sobre sus fuentes no son necesarios para probar un hecho fundamental en un procedimiento, entonces la futura recopilación y disponibilidad de datos e información sobre seguridad operacional así como sus fuentes conexas no debería ponerse en peligro mediante su divulgación innecesaria según cualquiera de estos principios de excepción. Además, si la información requerida puede obtenerse prácticamente de otras fuentes, la autoridad competente puede decidir no otorgar acceso a los datos o información hasta que se hayan agotado todas las posibilidades razonables de adquirir dicha información.

7.6.3.11 Análogamente, si se pide a una autoridad competente de un Estado que no dispone de leyes relativas al derecho de saber que decida si los datos o información sobre seguridad operacional deberían divulgarse al público (p. ej., respondiendo a solicitudes de los medios), dicha autoridad competente muy probablemente desearía saber cuán importante es que el público conozca el contenido de tal información. En esa situación, la autoridad competente podría plantear preguntas como, “Sin conocer el contenido de los datos o la información, ¿comprendería adecuadamente el público el carácter del suceso o tendría el mismo consecuencias para la seguridad del público viajero?”. Si se puede apoyar la opinión de que el conocimiento del público se vería comprometido por la falta de acceso a los datos o información sobre seguridad operacional ello podría apoyar el pedido de divulgación. No obstante, estos datos o información no deberían divulgarse solo porque sucede lo anterior. Si la divulgación comprometiera gravemente la continua disponibilidad de datos e información sobre seguridad operacional desalentando futuras notificaciones en la materia, la balanza no se inclinaría necesariamente a favor de la divulgación.

7.6.3.12 La tercera excepción involucra casos en los cuales, “después de efectuar un examen de los datos o información sobre seguridad operacional”, la autoridad competente determina “que su divulgación es necesaria para mantener o mejorar la seguridad operacional, y que las ventajas de su divulgación pesan más que las repercusiones adversas que a escala nacional e internacional dicha divulgación tendrá en la futura recopilación y disponibilidad de datos e información sobre seguridad operacional”. Esta excepción se aplica a la divulgación de datos o información sobre seguridad operacional necesarios para mantener o mejorar dicha seguridad. No se aplica al uso de esos datos o información en relación con medidas preventivas, correctivas o de rectificación adoptadas por una autoridad normativa que sean necesarias para mantener o mejorar la seguridad operacional de la aviación.

7.6.3.13 Las circunstancias contempladas por el Anexo 19 involucran la consideración por una autoridad competente de las ventajas de divulgar datos o información sobre seguridad operacional para fines más generales relativos al mantenimiento o mejora de la seguridad operacional, incluyendo, por ejemplo, fines de instrucción y educación o la publicación de información y asesoramiento sobre seguridad operacional para beneficio de la comunidad más amplia. El análisis de esta situación involucra el mismo tipo de proceso en dos etapas descrito en 7.6.3.5: en primer lugar, pedir que la autoridad competente decida si la “divulgación es necesaria para mantener o mejorar la seguridad operacional”, y, en segundo lugar, pedir a la autoridad competente que determine que las ventajas de divulgar dichos datos o información pesan más que las posibles repercusiones adversas que dicha divulgación tendrá en la futura recopilación y disponibilidad de tales datos e información.

7.6.3.14 Al considerar la segunda etapa de este análisis, en el Anexo 19 se alienta a las autoridades competentes a que tengan en cuenta “el consentimiento de la fuente de los datos y la información sobre seguridad operacional”. La importancia de este reconocimiento pone de relieve la distinción crítica planteada en 7.4.2, diferenciando entre la divulgación de datos e información sobre seguridad operacional para fines relacionados en general con el mantenimiento o mejora de la seguridad operacional (en cuyo caso este principio de excepción se aplicará), y el uso de dichos datos e información para fines particulares de carácter preventivo, correctivo y de rectificación para apoyar el mantenimiento o mejora de la seguridad operacional (en cuyo caso no será necesario satisfacer los requisitos de ningún principio de excepción dado que su uso ya está permitido dentro de los principios de protección).

7.6.3.15 Ajustándose al espíritu de los principios de protección, al considerar el uso de datos o información sobre seguridad operacional en apoyo de medidas preventivas, correctivas o de rectificación adoptadas para mantener o mejorar la seguridad operacional, puede ser posible que la autoridad competente evalúe si puede disponerse prácticamente de otra fuente apropiada de dichos datos o de información. En ese caso, podría evitarse incluso este uso no excepcional de datos o información sobre seguridad operacional protegidos.

7.6.3.16 No obstante, dicha consideración de factibilidad no exige ni sugiere la aplicación de uno de los principios de excepción enumerados en el Anexo 19. Esto se debe a que el principio de excepción se aplica cuando el interés de mantener o mejorar la seguridad operacional se compara con algún otro interés público conflictivo (p. ej., la administración adecuada de la justicia, el otorgamiento de acceso público a los datos o información, o la facilitación de procesos de instrucción o educación mediante la inclusión de datos o información protegidos). Las medidas preventivas, correctivas o de rectificación adoptadas para mantener o mejorar la seguridad operacional corresponde al ámbito de los principios de protección y no hay intereses opuestos no relacionados con la seguridad respecto de los cuales deba compararse dicho uso.

7.6.4 Consideraciones adicionales para aplicar un principio de excepción

7.6.4.1 Al decidir si un principio de excepción se aplica en un caso determinado, la autoridad competente debería siempre tener en cuenta el consentimiento de la fuente de los datos o información sobre seguridad operacional. Si una persona ha recibido garantías de confidencialidad con respecto a datos o información sobre seguridad operacional de los cuales es la fuente, el uso, divulgación o publicación de tales datos o información en una forma que contradiga dichas garantías probablemente tenga consecuencias adversas sobre los datos e información de ese tipo que pueda proporcionar dicha persona en el futuro. Además, si los datos o información sobre seguridad operacional se divulgaran o utilizaran a pesar de las garantías de confidencialidad de la fuente, ello podría tener consecuencias adversas análogas para toda persona que pueda tener conocimiento de ese hecho.

7.6.4.2 Para evitar situaciones no deseadas del tipo mencionado en 7.6.4.1, será prudente asegurar que los individuos y organizaciones comprendan claramente por adelantado cómo, cuándo, dónde y con qué fin podrían utilizarse los datos e información que proporcionan, con arreglo a la aplicación de los principios de excepción. Dicha comprensión es fundamental para establecer y mantener un entorno de notificación predecible basado en la confianza.

7.6.4.3 En la Figura 7-2[6] se ilustran directrices generales respecto de la aplicación de los principios de excepción por la autoridad competente con arreglo a las disposiciones del Anexo 19.

7.7 DIVULGACIÓN AL PÚBLICO

7.7.1 El público tiene un interés general en los datos o la información sobre seguridad operacional. El interés del público está en la apertura, transparencia y rendición de cuentas de modo de tener un conocimiento general de la seguridad operacional del sistema y garantías de que se está haciendo todo lo necesario para abordar dicha seguridad. Individuos o grupos de interés específicos también pueden estar interesados en los datos o la información sobre seguridad operacional por motivos que no estén directamente relacionados con dicha seguridad. La divulgación puede ser voluntaria, como resultado de un pedido de información al gobierno, o a través de procesos de carácter judicial. El hecho de que la divulgación al público de datos o de información sobre seguridad operacional sea apropiada o no depende del carácter de dichos datos e información. Esa determinación corresponde a la autoridad competente según se estableció anteriormente.

7.7.2 Si se divulgan al público datos o información sobre seguridad operacional, no siempre es posible limitar la forma en que se utilizaría dicha información. Por cierto, la apertura y la transparencia deberían fomentarse pero, al mismo tiempo, deben tenerse en cuenta los derechos y expectativas legítimas de las personas involucradas en notificar y analizar los datos y la información sobre seguridad operacional así como la necesidad de protegerles de daños inapropiados a sus intereses o reputación. No obstante, esto puede no siempre aplicarse a los Estados que no disponen de leyes relativas al derecho de saber.

7.7.3 Muchos Estados tienen legislación que en efecto obliga a que se divulgue toda la información en poder de las instituciones estatales. Dichas leyes se conocen a veces como leyes relativas al derecho de saber. En el marco de estas leyes, a menos que exista una exención para un tipo particular de información, la misma debe divulgarse por el gobierno si se le solicita. Entre los ejemplos de exenciones figurarían la información confidencial, la información comercial delicada o la información de tipo registros médicos que están protegidas por leyes de privacidad. Normalmente, los datos o la información sobre seguridad operacional no están exentos. Con arreglo al Anexo 19, los Estados pueden optar por crear exenciones o reglas respecto a la divulgación al público en sus leyes relativas al derecho de saber o en cualquier otro tipo de leyes, incluyendo la legislación aeronáutica.

7.7.4 Las leyes relativas al derecho de saber se aplican por lo general a información en poder del gobierno. Puesto que la mayoría de los datos y la información sobre seguridad operacional que requieren protección respecto de su divulgación se obtienen del personal operacional o de un proveedor de servicios, un enfoque práctico sería permitir que dichos datos e información permanezcan dentro de la organización en vez de depositarlos en una autoridad gubernamental. De esta forma, la cuestión de la divulgación al público no se plantea a menos que alguna medida adicional del gobierno, como un procedimiento administrativo, la haga necesaria. Cuando la cuestión de la divulgación a público se presenta en un procedimiento administrativo o judicial, la autoridad competente debería aplicar los principios básicos de protección analizados anteriormente. Este enfoque puede no funcionar si los proveedores de servicios se ven obligados a notificar datos e información sobre seguridad operacional a una autoridad gubernamental, o si el proveedor de servicios es una autoridad u organismo gubernamental o parte de una entidad de ese tipo.

6. Es importante recordar que no se impedirá que los Estados utilicen los datos e información sobre seguridad operacional para tomar medidas de carácter preventivo, correctivo o de rectificación que sean necesarias para mantener o mejorar la seguridad operacional de la aviación.

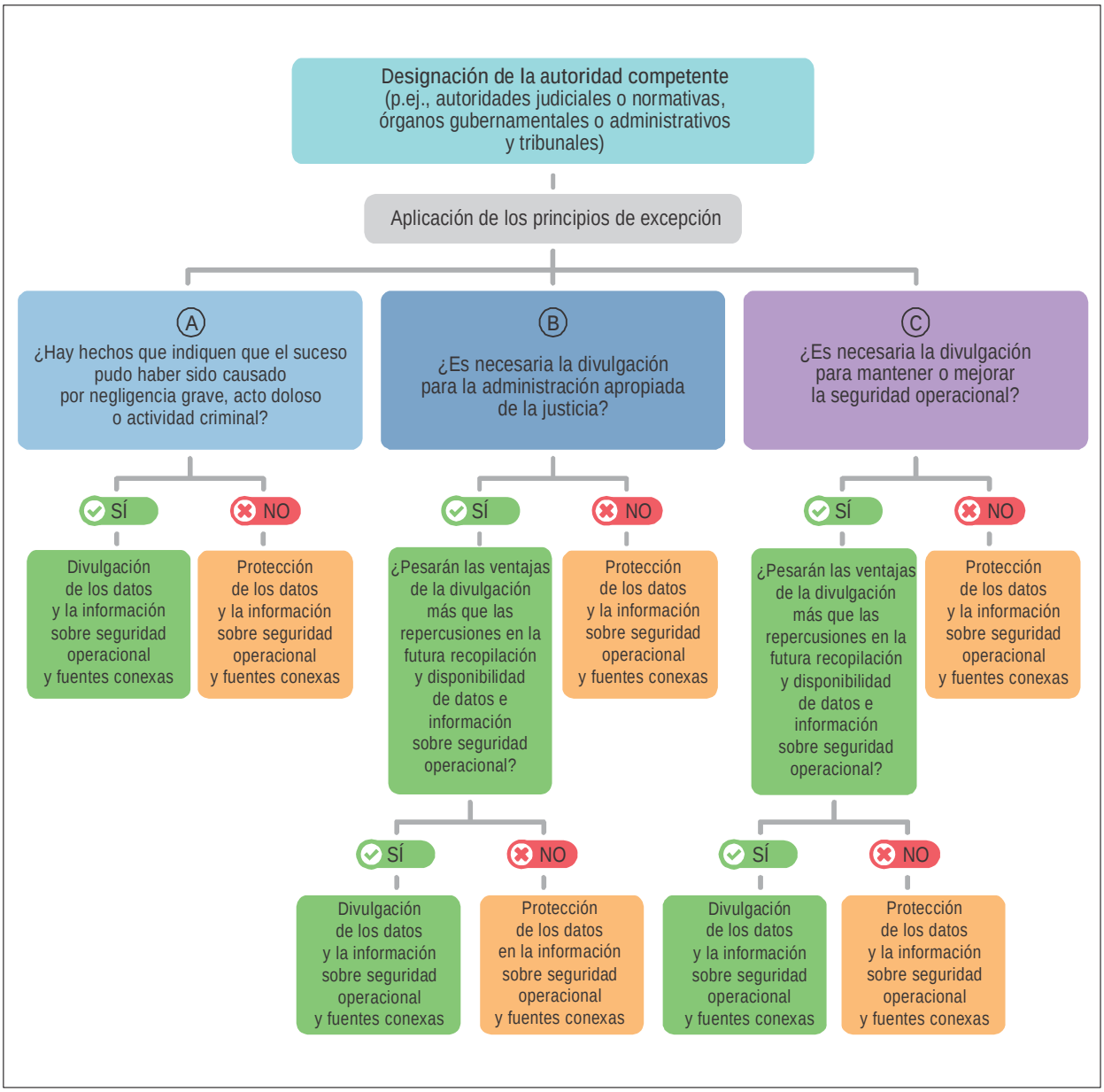


Figura 7-2. Directrices para la aplicación de los principios de excepción

7.7.5 La incorrecta evaluación de reclamaciones concurrentes para obtener acceso a datos o información sobre seguridad operacional puede tener consecuencias adversas para las actividades presentes y futuras en dos formas. La divulgación al público de ciertos datos o información puede percibirse como una violación de la privacidad de los individuos o de las expectativas de confidencialidad de organizaciones relacionadas con dichos datos e información. El uso de ciertos datos o información como parte de un argumento en apoyo de sanciones contra individuos u organizaciones involucrados puede considerarse también como una violación de principios básicos de equidad. La futura disponibilidad de datos e información sobre seguridad operacional puede verse afectada por el comportamiento humano predecible de retener información debido a la percepción de una posible amenaza basada en su divulgación o uso incriminatorio. Esto puede tener un impacto evidente en las funciones de recopilación y análisis de datos de la gestión de la seguridad operacional.

7.7.6 Si una autoridad competente determina que los datos o la información sobre seguridad operacional pueden divulgarse al público, se espera que el Estado asegure que dicha divulgación se efectúa con arreglo a las leyes de confidencialidad aplicables o que se hace sin revelar las identidades y en forma resumida o combinada. En 7.5.3 figura más información sobre garantías autorizadas.

7.8 PROTECCIÓN DE LOS DATOS REGISTRADOS

7.8.1 Protección de grabaciones ambiente en el lugar de trabajo

7.8.1.1 Las grabaciones ambiente de las conversaciones en el lugar de trabajo deberían ser parte de toda política o reglamentación sobre protección. El uso de estos registros como parte de la gestión de la seguridad operacional cuando los reglamentos o políticas lo permitan debería respetar plenamente los principios de protección y excepción. La confianza de las personas que presenten informes es fundamental para la gestión eficaz de la seguridad operacional. Dicha confianza no debería verse comprometida.

7.8.1.2 Las disposiciones del Anexo 19 se aplican a las funciones de gestión de la seguridad operacional relativas a la operación segura de las aeronaves o en apoyo directo de la misma. Las grabaciones ambiente de las conversaciones en el lugar de trabajo pueden estar regidas por leyes sobre confidencialidad nacionales que no están definidas en el Anexo 19.

7.8.1.3 Las grabaciones ambiente de las conversaciones en el lugar de trabajo pueden comprender registros de CVR, AIR u otros registradores de vuelo, así como registros de comunicaciones de fondo y del entorno acústico en los puestos de trabajo de los controladores del tránsito aéreo.

7.9 COMPARTICIÓN E INTERCAMBIO DE INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

7.9.1 Protección de la información compartida entre Estados

7.9.1.1 Teniendo en cuenta que uno de los principales objetivos de compartir e intercambiar información sobre seguridad operacional es garantizar una respuesta sistemática, basada en hechos y transparente a las preocupaciones de seguridad operacional a nivel estatal y mundial, en el proceso de compartir e intercambiar dicha información, los Estados actuarán con arreglo a los principios siguientes:

a) cumplimiento del Convenio sobre Aviación Civil Internacional (Convenio de Chicago), sus Anexos y otras obligaciones multilaterales y bilaterales de los Estados;

b) la compartición e intercambio de información sobre seguridad operacional no conducirá a una violación por parte de las autoridades estatales pertinentes de las leyes nacionales relativas a la protección de dicha información, entre ellas las leyes y reglamentos nacionales sobre protección de secretos de Estados, datos personales, secretos comerciales así como sobre violación de los derechos de individuos y entidades jurídicas;

c) la información sobre seguridad operacional compartida e intercambiada por un Estado no debería utilizarse en una forma que afecte adversamente al propio Estado, sus líneas aéreas, sus funcionarios públicos y sus ciudadanos así como para otros fines inapropiados, incluyendo los fines de lucro;

d) el único propósito de proteger la información sobre seguridad operacional respecto del uso inapropiado es garantizar su continua disponibilidad de modo que puedan adoptarse medidas preventivas adecuadas y oportunas y mejorar la seguridad operacional de la aviación; y

e) la compartición e intercambio de información sobre seguridad operacional debería ajustarse a los principios de protección que figuran en el Anexo 19.

7.9.1.2 El marco jurídico para compartir e intercambiar información puede basarse en acuerdos bilaterales entre Estados insertados, por ejemplo, en sus acuerdos sobre transporte aéreo (servicios aéreos). Para facilitar la compartición e intercambio de información, los Estados también pueden acordar que dichos arreglos bilaterales se apliquen con carácter provisional, si corresponde, pendientes de su ratificación y entrada en vigor.

7.9.1.3 Los Estados deberían promover y facilitar el establecimiento de redes para compartir e intercambiar información sobre seguridad operacional entre los usuarios del sistema aeronáutico. La compartición y el intercambio de información sobre seguridad operacional es fundamental para garantizar una respuesta sistemática, basada en hechos y transparente a las preocupaciones de seguridad operacional a los niveles estatal y mundial.

———————

Capítulo 8

GESTIÓN ESTATAL DE LA SEGURIDAD OPERACIONAL

8.1 INTRODUCCIÓN

8.1.1 En el Capítulo 3 del Anexo 19 figuran SARPS relativos a las responsabilidades funcionales estatales en materia de gestión de la seguridad operacional. Estos comprenden el establecimiento y mantenimiento de un programa estatal de seguridad operacional (SSP) dirigido a gestionar la seguridad operacional en forma integral.

8.1.2 Con la primera edición del Anexo 19, se esperaba que los Estados establecieran e implantaran dos conjuntos de disposiciones, a saber, los ocho elementos críticos (CE) del sistema estatal de supervisión de la seguridad operacional (SSO) y los cuatro componentes del SSP. El aspecto de supervisión de la seguridad operacional reflejaba la función tradicional del Estado, que consiste en asegurar la implementación eficaz por la industria de la aviación de los SARPS prescriptivos, mientras que el SSP representaba la incorporación de principios de gestión de la seguridad operacional. Los detalles de los ocho elementos críticos figuraban en el Apéndice 1 del Anexo con categoría de SARPS, y los elementos detallados de un marco para la implantación y mantenimiento del SSP figuraban en el Adjunto A del mismo como texto de orientación.

8.1.3 El sistema de supervisión de la seguridad operacional y el SSP estaban estrechamente relacionados en cuanto a los objetivos de seguridad operacional que cada uno de ellos procura alcanzar. Ambos abordaban las funciones y responsabilidades del Estado, el primero principalmente con respecto a la vigilancia de la seguridad operacional y el segundo con respecto a la gestión de la seguridad operacional y al rendimiento en materia de seguridad operacional. Existen claramente algunos aspectos de gestión de la seguridad operacional dentro de los ocho CE que reflejan la transición a un enfoque proactivo de dicha gestión. Por ejemplo, las obligaciones de vigilancia (CE-7) pueden considerarse como un elemento del aseguramiento de la seguridad operacional y la legislación de aeronáutica básica (CE-1) y los reglamentos de explotación específicos (CE-2) también se reflejaban en el marco SSP original como importantes controles de riesgos de seguridad operacional.

8.1.4 Estas responsabilidades se han integrado en la segunda edición del Anexo 19 y se presentan en forma colectiva como responsabilidades funcionales estatales en materia de gestión de la seguridad operacional. Los SARPS relacionados con las responsabilidades estatales de gestión de la seguridad operacional, que abarcan tanto la supervisión de la seguridad operacional como la gestión de ésta, son interdependientes y constituyen un enfoque integrado conducente a la gestión eficaz de la seguridad operacional. Aunque el término SSP continúa utilizándose en la segunda edición del Anexo 19, su significado ha cambiado para comprender el conjunto integrado de SARPS que figuran en el Capítulo 3. Como tal, el SSP ya no se describe como marco, sino más bien como un programa para cumplir las responsabilidades estatales en materia de gestión de la seguridad operacional, que incluyen la supervisión de dicha seguridad. Como tal, el SSP es parte del amplio concepto de gestión estatal de la seguridad operacional. Esta evolución se ilustra en la Figura 8-1.

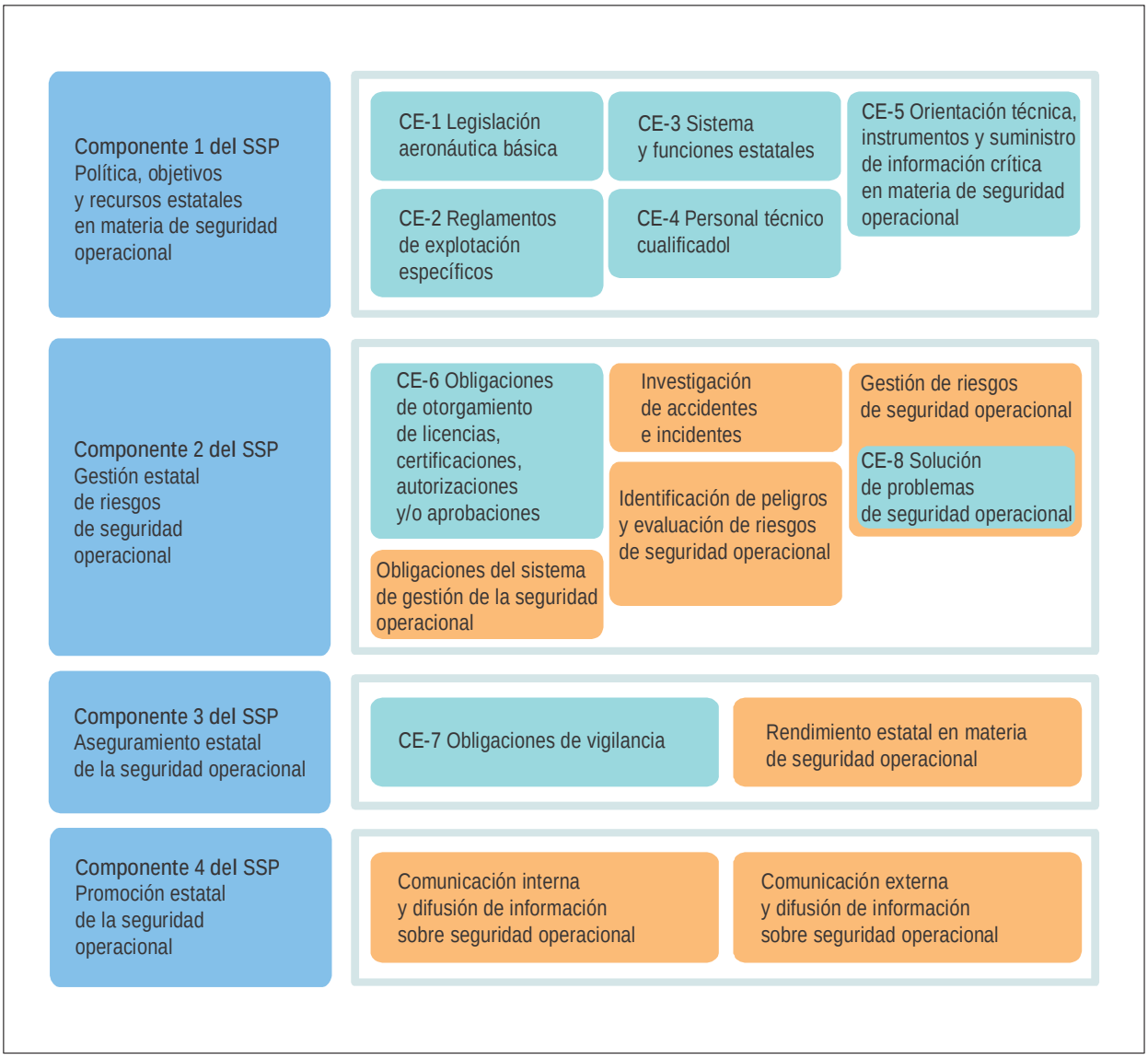


Figura 8-1. Programa estatal integrado de seguridad operacional

8.2 PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

8.2.1 Elementos críticos del sistema estatal de supervisión de la seguridad operacional

Los CE del sistema estatal de supervisión de la seguridad operacional (SSO) constituyen la base del SSP. En la segunda edición del Anexo 19 se subraya la importancia de un sistema de supervisión de la seguridad operacional mediante el mantenimiento de las disposiciones relacionadas con los ocho CE a nivel de norma. La mayoría de los requisitos del marco SSP se han elevado de categoría a métodos recomendados, con algunos de ellos elevados a categoría de norma. En el *Manual de vigilancia de la seguridad operacional*, Parte A — *Establecimiento y gestión de un sistema estatal de vigilancia de la seguridad operacional* (Doc 9734) figuran detalles sobre los CE del sistema SSO.

8.2.2 Panorama del programa estatal de seguridad operacional

8.2.2.1 El SSP es un conjunto integrado de reglamentos y actividades dirigidos a mejorar la seguridad operacional. Para el establecimiento y mantenimiento del SSP, los SARPS de la OACI están estructurados en los siguientes cuatro componentes:

a) política, objetivos y recursos estatales de seguridad operacional;

b) gestión estatal de los riesgos de seguridad operacional;

c) aseguramiento estatal de la seguridad operacional; y

d) promoción estatal de la seguridad operacional.

8.2.2.2 La implementación de un SSP requiere coordinación entre múltiples autoridades responsables de las funciones aeronáuticas del Estado. La implementación del SSP no altera las funciones respectivas de las organizaciones aeronáuticas del Estado o su informe normal de interactuar entre sí. En vez de ello, el SSP se dirige a aprovechar las funciones y capacidades colectivas en materia de seguridad operacional para continuar mejorando la misma dentro del Estado. Cuando comienzan a implantar un SSP, la mayoría de los Estados descubre que ya cuentan con procesos y actividades existentes que abarcan muchos aspectos del SSP. La implementación del SSP se dirige a mejorar estos procesos con elementos adicionales de rendimiento y basados en riesgos de seguridad operacional, así como facilitar la eficaz implementación del SMS por la industria de aviación del Estado.

8.2.2.3 El SSP se dirige a:

a) asegurar que el Estado cuenta con un marco legislativo eficaz para apoyar reglamentos de operación específicos;

b) asegurar la coordinación del SRM y el aseguramiento de la seguridad operacional y la sinergia entre las autoridades aeronáuticas estatales pertinentes;

c) apoyar la implementación efectiva y la interacción apropiada con los SMS de los proveedores de servicios;

d) facilitar la observación y la medición del rendimiento en materia de seguridad operacional de la industria aeronáutica del Estado; y

e) mantener o mejorar continuamente el rendimiento general del Estado en materia de seguridad operacional.

8.2.3 Delegación de funciones y actividades de gestión de la seguridad operacional

8.2.3.1 Algunas actividades de gestión de la seguridad operacional requieren nuevas competencias como la realización de evaluaciones de riesgos de seguridad operacional, análisis de datos de seguridad operacional o evaluación de la adecuación de los SPI.

8.2.3.2 El Estado puede optar por delegar algunas funciones o tareas específicas abarcadas por el SSP en otro Estado, organización regional de vigilancia de la seguridad operacional (RSOO) u otra organización competente, como una asociación comercial, organizaciones representativas de la industria u órganos privados. Si bien el Estado puede delegar funciones específicas, seguirá necesitando suficiente personal para interactuar con la entidad delegada y procesar la información proporcionada por dicha entidad.

8.2.3.3 Los Estados también deberían considerar el establecimiento de procesos técnicos y administrativos apropiados para asegurar que las funciones delegadas se llevan a cabo en forma satisfactoria.

8.2.3.4 Independientemente del arreglo, el Estado retiene la responsabilidad de asegurar que cualquier tarea delegada se realiza con arreglo a sus requisitos nacionales y a los SARPS.

8.2.3.5 La delegación puede permitir que los Estados con un nivel relativamente bajo de actividades aeronáuticas recopilen en forma colectiva datos sobre seguridad operacional para identificar tendencias y coordinar estrategias de mitigación.

8.2.3.6 Si el Estado opta por recibir asistencia para el desarrollo de procesos de vigilancia debería incluir la elaboración de perfiles institucionales de riesgos de seguridad operacional para proveedores de servicios, la planificación y priorización de las inspecciones, auditorías y actividades de observación de las organizaciones/ proveedores de servicios aprobados.

8.2.3.7 Si un Estado opta por delegar las actividades de vigilancia, debería asegurar que retiene el acceso a los registros de vigilancia con resultados documentados. El Estado también debería observar y examinar periódicamente el rendimiento en materia de seguridad operacional de cada proveedor de servicios y asegurar que está bien establecido quién observará y ejecutará (si es necesario) la solución de los problemas de seguridad operacional que hubiere.

8.2.3.8 La delegación es un medio para que los Estados con recursos limitados puedan asegurar su acceso a los conocimientos técnicos apropiados. En el *Manual de vigilancia de la seguridad operacional*, Parte B — *Establecimiento y gestión de una organización regional de vigilancia de la seguridad operacional* (Doc 9734) figura orientación sobre el establecimiento de una RSOO.

8.3 COMPONENTE 1: POLÍTICA, OBJETIVOS Y RECURSOS ESTATALES DE SEGURIDAD OPERACIONAL

8.3.1 El primer componente del SSP define la forma en que el Estado gestionará la seguridad operacional en todo su sistema aeronáutico. Esto incluye la determinación de los requisitos, obligaciones, funciones y actividades de las diferentes autoridades aeronáuticas del Estado con respecto al SSP, así como los objetivos de seguridad operacional amplios que han de lograrse. La política y objetivos estatales en materia de seguridad operacional deberían documentarse para proporcionar claras expectativas y mantener las actividades de gestión de la seguridad operacional de la CAA del Estado, y aquellas de otras autoridades aeronáuticas estatales, concentrándose en mantener y mejorar el rendimiento en materia de seguridad operacional. Esto permite que el Estado proporcione directrices de seguridad operacional claras en apoyo de su sistema de transporte aéreo en crecimiento continuo y cada vez más complejo.

8.3.2 El marco jurídico del Estado establece la forma en que se gestionará la seguridad operacional de la aviación. Los proveedores de servicios son jurídicamente responsables de la seguridad operacional de sus productos y

servicios. Estos deben ajustarse a los reglamentos de seguridad operacional establecidos por el Estado. El Estado debería asegurar que las autoridades aeronáuticas involucradas en la implementación y mantenimiento del SSP cuentan con los necesarios recursos para la eficaz implementación del mismo.

8.3.3 El Componente 1 del SSP, Política, objetivos y recursos estatales de seguridad operacional, está integrado por los siguientes elementos:

a) legislación aeronáutica básica;

b) reglamentos de explotación específicos;

c) sistema y funciones estatales;

d) personal técnico cualificado; y

e) orientación técnica, instrumentos y suministro de información crítica en materia de seguridad operacional.

8.3.4 Legislación aeronáutica básica

8.3.4.1 En el Doc 9734, Parte A figura orientación sobre la legislación aeronáutica básica (CE-1).

Nota.— En todo este manual, el término "legislación" se utiliza en forma genérica para incluir la legislación aeronáutica básica y los reglamentos de explotación específicos.

8.3.4.2 Puede ser necesario contar con disposiciones legislativas que faculten a las diversas autoridades aeronáuticas del Estado (p. ej., CAA o autoridad de investigación de accidentes) para ejecutar sus funciones. El hecho de si la legislación aeronáutica básica debe mencionar, o no, específicamente la implementación del SSP como función de la CAA depende del sistema jurídico del Estado. Algunos Estados pueden considerar que la implementación del SSP está implícita en las funciones ya mencionadas en su legislación aeronáutica básica. En ese caso, puede o ser necesario enmendar dicha legislación. Las pruebas de la implementación del SSP deberían estar claramente disponibles en los documentos estatales oficiales. El Estado también debería poder demostrar su compromiso para abordar sus responsabilidades de gestión de la seguridad operacional, como se presentan en el Anexo 19.

8.3.4.3 Como parte de su SSP, se espera que el Estado establezca una política de cumplimiento que:

a) apoye y fomente una cultura de seguridad operacional positiva;

b) describa la forma en que el Estado asegura la protección de los datos y la información sobre seguridad operacional y fuentes conexas, especialmente si la información proporcionada es autoincriminatoria; y

c) especifique las condiciones y circunstancias en las cuales los proveedores de servicios que cuentan con un SMS están autorizados para abordar y resolver sucesos que involucren ciertos problemas internos de seguridad operacional, dentro del contexto de sus SMS y a satisfacción de la autoridad estatal pertinente, siempre que el SMS se ajuste al marco SMS y demuestre ser eficaz y tener madurez.

8.3.4.4 Mediante la aplicación de principios de gestión de la seguridad operacional, la relación entre un Estado y sus proveedores de servicios debería evolucionar más allá del cumplimiento y la ejecución, para alcanzar una asociación dirigida a mantener o mejorar continuamente el rendimiento en materia de seguridad operacional.

8.3.5 Reglamentos de explotación específicos

8.3.5.1 En el Doc 9734, Parte A, figura orientación sobre reglamentos de explotación específicos (CE-2), incluyendo la adaptación o adopción de reglamentos de otro Estado.

Reglamentos prescriptivos y basados en el rendimiento

8.3.5.2 Los reglamentos de seguridad operacional constituyen una herramienta importante que pueden utilizar los Estados para controlar los riesgos de seguridad operacional. Con la transición a la gestión de la seguridad operacional, también se ha registrado una tendencia hacia la introducción de reglamentos basados en el rendimiento. Para comprender el carácter de esos reglamentos basados en el rendimiento, se debe comprender en primer lugar los reglamentos de carácter prescriptivo. Los reglamentos de carácter prescriptivo son aquellos que establecen explícitamente lo que debe hacerse y cómo debe hacerse. La expectativa es que el cumplimiento de estos reglamentos alcanzará el nivel de seguridad operacional deseado. Muchos reglamentos prescriptivos se elaboraron después de un accidente y se basan en lecciones aprendidas y en el deseo de evitar que ocurra un accidente en el futuro debido a las mismas causas. Desde la perspectiva del proveedor de servicios, la satisfacción de los requisitos prescriptivos significa implementar los reglamentos sin desviaciones. No se espera que el proveedor de servicios o la autoridad realicen más análisis o presenten justificaciones.

8.3.5.3 Hasta hace poco tiempo los SARPS de la OACI se habían concentrado en requisitos prescriptivos como medio de identificar normas mínimas y asegurar el interfuncionamiento. No obstante, es cada vez más necesario habilitar reglamentos basados en el rendimiento para apoyar enfoques de implementación innovadores que puedan mejorar la eficiencia y alcanzar o superar los objetivos de seguridad operacional.

8.3.5.4 Los Anexos de la OACI proporcionan ejemplos de normas que permiten la introducción de reglamentos prescriptivos y basados en el rendimiento. El siguiente es un ejemplo de una Norma del Anexo 14 — *Aeródromos*, Volumen I — *Diseño y operaciones de aeródromos*, que permite introducir reglamentos prescriptivos:

> *3.3.1 Cuando el extremo de una pista no dispone de una calle de rodaje o de una curva de viraje en la calle de rodaje y la letra de clave es D, E o F, se proporcionará una plataforma de viraje en la pista para facilitar el viraje de 180 grados de los aviones.*

8.3.5.5 El ejemplo anterior permite introducir un reglamento prescriptivo dado que identifica solamente una forma de demostrar el cumplimiento si la pista es del tipo especificado: es decir, proporcionar una plataforma de viraje en la pista. La desviación con respecto a los reglamentos prescriptivos se permite normalmente como excepción de los mismos.

8.3.5.6 En contraste, las normas que permiten la introducción de reglamentos basados en el rendimiento se expresan en términos del resultado deseado. Los reglamentos basados en el rendimiento resultantes requieren que el proveedor de servicios demuestre que su enfoque propuesto alcanzará el resultado deseado. El siguiente es un ejemplo de Norma basada en el rendimiento extraído del Anexo 6, Parte I.

> *7.2.11 El avión irá suficientemente provisto de equipo de navegación para asegurar que, en caso de falla de un elemento del equipo en cualquier fase del vuelo, el equipo restante permita que el avión navegue de conformidad con 7.2.1 y, cuando corresponda, con 7.2.2, 7.2.5 y 7.2.6.*

8.3.5.7 Obsérvese que la Norma anterior no indica el equipo de navegación específico requerido. En vez de ello, describe el resultado deseado, es decir, que en caso de falla de un elemento del equipo, el equipo restante debe permitir que el avión navegue en condiciones de seguridad. El equipo requerido dependería del diseño de la aeronave. Los reglamentos redactados de esta forma requerirían que el explotador de servicios aéreos proporcione a la autoridad los datos necesarios para demostrar la forma en que cumple dicho requisito. Esto puede hacerse mediante su propio

análisis, pero para tales tipos de reglamentos basados en el rendimiento, la información necesaria está a menudo disponible en otras fuentes. En este caso, tanto la autoridad como el explotador de servicios aéreos harían uso de los datos de fabricantes de aeronaves para orientar su decisión, y no es necesario que el explotador de servicios aéreos elabore su propia solución novedosa. Al redactar reglamentos basados en el rendimiento, los Estados deben tener en cuenta la forma en que puede demostrarse el cumplimiento. Puede ser necesario que el Estado elabore textos de orientación o medios aceptables de cumplimiento para apoyar la satisfacción del requisito por parte de la industria.

8.3.5.8 El siguiente es otro ejemplo de Norma basada en el rendimiento, extraído del Apéndice 2 del Anexo 19.

> *2.1.1 El proveedor de servicios definirá y mantendrá un proceso que garantice la identificación de los peligros asociados a sus productos o servicios de aviación.*

8.3.5.9 En el ejemplo anterior, aunque la norma exige que se implante un proceso para identificar peligros, no especifica el aspecto de dicho proceso. Los Estados pueden permitir que los proveedores de servicios diseñen su propia metodología. La función del reglamentador sería evaluar si la metodología, procesos y sistemas del proveedor de servicios resultarían en verdad en la identificación de peligros. La autoridad también debería evaluar el rendimiento del proceso de identificación de peligros del proveedor de servicios, por ejemplo, mediante la evaluación del volumen, tipos e importancia de los peligros identificados. Los reglamentos basados en el rendimiento redactados de esta forma requieren que los reglamentadores posean la pericia y la experiencia técnica para evaluar el rendimiento del sistema, en vez de evaluar solamente el cumplimiento prescriptivo de la letra de los reglamentos. También se requieren más recursos para la evaluación dado que la implementación sería diferente de un proveedor de servicios a otro.

Facilitación de opciones prescriptivas y basadas en el rendimiento

8.3.5.10 En algunos casos, los SARPS de la OACI requieren que se establezcan reglamentos de carácter prescriptivo, y al mismo tiempo ofrecen a los Estados la opción de establecer reglamentos basados en el rendimiento para apoyar otros medios de cumplimiento. Cuando los Estados establecen reglamentos prescriptivos y basados en el rendimiento, los proveedores de servicios que no cuentan con conocimientos técnicos para elaborar su propio enfoque a efectos de satisfacer los reglamentos basados en el rendimiento, pueden optar por cumplir los reglamentos prescriptivos. Para aquellos proveedores de servicios que no cuentan con tales conocimientos, los reglamentos resultantes les permitirán elaborar un medio de cumplimiento apropiado a sus propias operaciones, y pueden también ofrecer la posibilidad de una mayor flexibilidad operacional y un uso más eficaz de los recursos. Las normas de gestión de la fatiga, como las que figuran en el Anexo 6, Parte I, Enmienda 43, proporcionan un buen ejemplo de ello:

> *4.10.1 El Estado del explotador establecerá reglamentos para fines de gestión de la fatiga. Estos reglamentos estarán basados en principios, conocimientos científicos y experiencia operacional, y su propósito será garantizar que los miembros de la tripulación de vuelo y de cabina estén desempeñándose con un nivel de alerta adecuado. Por consiguiente, el Estado del explotador establecerá:*
>
> *a) reglamentos prescriptivos relativos a limitaciones del tiempo de vuelo, período de servicio de vuelo, períodos de servicio y de requisitos de períodos de descanso; y*
>
> *b) reglamentos sobre Sistemas de gestión de riesgos asociados a la fatiga (FRMS), cuando se autoriza al explotador para que utilice un FRMS con el fin de gestionar la fatiga.*
>
> *4.10.2 El Estado del explotador requerirá que el explotador, conforme a 4.10.1 y con fines de gestión de sus riesgos de seguridad operacional relacionados con la fatiga, establezca:*

a) limitaciones del tiempo de vuelo, períodos de servicio de vuelo, períodos de servicio, requisitos de períodos de descanso que estén dentro de los reglamentos prescriptivos de gestión de la fatiga establecidos por el Estado del explotador; o

b) un Sistema de gestión de riesgos asociados a la fatiga (FRMS) conforme a 4.10.6 para todas las operaciones; o

c) un FRMS que se ajuste a 4.10.6 para parte de sus operaciones y a los requisitos de 4.10.2 a) para el resto de sus operaciones.

8.3.5.11 En el ejemplo anterior, la Norma requiere que los Estados establezcan reglamentos de carácter prescriptivo para la limitación de tiempos de vuelo y períodos de servicio de vuelo, mientras que el establecimiento de reglamentos para apoyar el FRMS tiene carácter opcional. El FRMS Brinda al explotador de servicios aéreos la oportunidad de abordar de mejor manera sus riesgos específicos en materia de fatiga y al mismo tiempo ofrece la posibilidad de flexibilidad operacional fuera de los reglamentos prescriptivos de limitación de tiempos de vuelo y de servicio. El Estado debe considerar si es necesario proporcionar, alternativamente, reglamentos sobre FRMS en los reglamentos prescriptivos obligatorios de limitación de tiempos, y si cuenta con los recursos necesarios para proporcionar una supervisión apropiada del FRMS. La Norma 4.10.2 procede a aclarar que se requiere que el explotador gestione sus riesgos de seguridad operacional relacionados con la fatiga. Al establecer reglamentos sobre FRMS el explotador puede hacerlo dentro de los reglamentos prescriptivos sobre limitaciones a que se hace referencia en 4.10.2 a), o mediante la implantación de FRMS basado en el rendimiento a que se hace referencia en 4.10.2 b) y c). Los explotadores de servicios aéreos que no tienen los conocimientos técnicos para desarrollar un FRMS y satisfacer los requisitos normativos conexos deberían ajustarse a los reglamentos prescriptivos.

8.3.5.12 Cabe señalar que los reglamentos basados en el rendimiento no siempre son apropiados. Los reglamentos prescriptivos continúan siendo apropiados cuando es necesario tener un medio de cumplimiento normalizado, por ejemplo, para facilitar el interfuncionamiento. Los requisitos relativos a las señales de pista, por ejemplo, son de carácter necesariamente prescriptivo.

8.3.5.13 En la práctica, los reglamentos son rara vez totalmente prescriptivos o completamente basados en el rendimiento, sino que contienen elementos de ambos. También son basados en el rendimiento en diferentes grados. Cuando un Estado considere implementar reglamentos basados en el rendimiento, debe considerar la capacidad y grado de madurez de la industria, sectores específicos de la industria o incluso de cada proveedor de servicios y sus SMS. Los reglamentos basados en el rendimiento también exigen más de parte del reglamentador, requiriéndoles no solo verificar el cumplimiento sino también poder evaluar sistemas y rendimiento en materia de seguridad operacional teniendo en cuenta el contexto operacional específico de cada proveedor de servicios. Los Estados deben asegurar que están en condiciones de continuar supervisando gestionando la industria, observando si se requieren niveles más altos de conocimientos técnicos así como más recursos. Los SMS proporcionan las bases y los mecanismos para que los proveedores de servicios cumplan los reglamentos basados en el rendimiento, pero ello no es una garantía automática de que cada proveedor de servicios con un SMS pueda hacerlo. Todo depende de las demandas de los requisitos basados en el rendimiento de que se trate.

8.3.5.14 Los reglamentos basados en el rendimiento también tienen consecuencias sobre el cumplimiento y la ejecución. La imposición del cumplimiento de reglamentos prescriptivos tiene carácter directo dado que el no cumplimiento puede determinarse fácilmente. La imposición del cumplimiento presenta más retos en el caso de los reglamentos basados en el rendimiento. Por ejemplo, un proveedor de servicios puede estar en condiciones de mostrar que ha implantado un proceso que satisface el reglamento (p. ej., cuenta con un sistema de notificación de peligros), pero no puede demostrar que el proceso puede producir el resultado previsto (p. ej., si el sistema de notificación de peligros resulta eficaz). Esto podría conducir al establecimiento de sistemas o procesos que simplemente satisfagan la “letra de la ley” pero no produzcan los resultados de seguridad operacional requeridos. Los reglamentadores pueden tener que involucrar los órganos pertinentes de imposición del cumplimiento en la elaboración de reglamentos basados en el rendimiento para asegurar que estos son ejecutables.

8.3.6 Sistema y funciones estatales

8.3.6.1 En el Doc 9734, Parte A, figura orientación sobre sistemas y funciones estatales (CE-3).

Organización responsable de coordinar el SSP

8.3.6.2 Las responsabilidades en materia de gestión de la seguridad operacional pueden ser cumplidas por múltiples autoridades aeronáuticas dentro del Estado, por ejemplo, la CAA y una AIA independiente. Los Estados deberían aclarar cuál es la autoridad responsable de coordinar el mantenimiento e implementación del SSP. Muchos Estados asignan esta función a la CAA, considerando que esta institución está normalmente encargada de la mayoría de las responsabilidades del SSP. Las funciones y responsabilidades de todas las autoridades involucradas deberían estar identificadas y documentadas.

Grupo de coordinación del SSP

8.3.6.3 El Estado debería establecer un grupo de coordinación adecuado con representación de las autoridades aeronáuticas afectadas con responsabilidades relacionadas con la implementación y mantenimiento del SSP, incluyendo las autoridades de investigación de accidentes así como las autoridades de aviación militar. La designación de un grupo de coordinación facilitará la buena comunicación, evitará la duplicación de esfuerzos y los conflictos de políticas y asegurará una implantación efectiva y eficiente del SSP. Este grupo tiene la forma de comité presidido por el jefe de la organización responsable de coordinar el SSP.

8.3.6.4 El Estado también puede considerar beneficioso asignar la planificación y la gestión cotidianas de la implantación del SSP a una persona, un departamento o un equipo. Dicha persona, departamento o equipo puede asegurar que los diversos aspectos funcionan conjuntamente para lograr los objetivos de seguridad operacional del Estado.

Funciones y actividades del SSP

8.3.6.5 Cada Estado deberá decidir la forma en que organiza su personal y estructura institucional para abordar la aceptación y observación de la implementación del SMS por parte de los proveedores de servicios en el cumplimiento del Anexo 19. El Estado puede optar por establecer una nueva oficina o añadir esta responsabilidad a las responsabilidades de oficinas existentes, por ejemplo la oficina de aeronavegabilidad, la oficina de operaciones de vuelo, las oficinas de navegación aérea y de aeródromos, etc. La decisión dependerá de la forma que el Estado escoja para abordar sus nuevos requisitos de competencia.

8.3.6.6 Es importante que las diversas autoridades aeronáuticas tengan en claro sus funciones. Esto debería incluir a todas las obligaciones, funciones y actividades de su SSP. El Estado debería asegurar que cada autoridad comprende su contribución para cumplir con cada requisito del Anexo 19, fundamentalmente su responsabilidad para gestionar la seguridad operacional en el Estado. Las obligaciones y funciones de cada autoridad aeronáutica con respecto a la implantación del SSP deberían documentarse para evitar ambigüedades.

8.3.6.7 Deberían existir estructuras de gobernanza apropiadas en los Estados en que el personal involucrado en la seguridad operacional está geográficamente disperso. Una estructura de gobernanza compleja puede no ser necesaria para sistemas aeronáuticos menos complejos, con menos personas involucradas en la gestión de la seguridad operacional. El Estado debería asegurar que todo su personal tiene la misma comprensión de la implementación del SSP a nivel nacional. Debería documentarse el enfoque de la implementación del SSP.

Política y objetivos estatales de seguridad operacional

8.3.6.8 La eficaz implementación del SSP requiere el compromiso de la administración superior del Estado y del personal de apoyo en todos los niveles. Las políticas estatales de seguridad operacional y los objetivos estatales de seguridad operacional son declaraciones de alto nivel apoyadas por las autoridades aeronáuticas del Estado. Combinados, orientan el comportamiento en materia de seguridad operacional y la asignación de recursos. La política y los objetivos estatales de seguridad operacional deberían publicarse y revisarse periódicamente para asegurar que permanecen siendo pertinentes y apropiados al Estado.

Política estatal de seguridad operacional

8.3.6.9 El compromiso de la administración superior debería estar articulado en la política estatal de seguridad operacional. Esta política es un documento formal que describe las intenciones y la dirección estatales en materia de seguridad operacional. La política estatal de seguridad operacional proyecta la actitud de la administración superior respecto de la seguridad y la promoción de una cultura de seguridad operacional positiva en el Estado. Puede considerarse como una declaración de la misión y visión del Estado en materia de seguridad operacional.

8.3.6.10 La política de seguridad operacional debería abordar las prácticas fundamentales que resultan esenciales para la gestión de la seguridad operacional y la forma en que la administración superior prevé cumplir sus responsabilidades en la materia, (p. ej., uso de un enfoque orientado a los datos). Los principios reflejados en la política de seguridad operacional deberían ser claramente visibles en las prácticas cotidianas del Estado.

8.3.6.11 La política estatal de seguridad operacional está apoyada por las autoridades aeronáuticas del Estado para demostrar su intención en materia de seguridad operacional y se aplica como procedimiento o protocolo. Una declaración de política típica es: “Alcanzaremos la seguridad operacional mediante: 1) nuestra aceptación de la obligación de rendir cuentas respecto de las condiciones y comportamientos de seguridad, 2) una cultura de liderazgo, colaboración, comunicación abierta en materia de seguridad operacional, etc.”.

Objetivos estatales de seguridad operacional

8.3.6.12 La elaboración de objetivos de seguridad operacional comienza con una clara comprensión de los riesgos de seguridad operacional más elevados en el sistema aeronáutico. El riesgo de seguridad operacional en el sistema aeronáutico está influenciado por muchos factores diferentes, como el volumen y la complejidad del sistema de aviación así como el entorno operacional. La elaboración de una buena descripción del sistema proporcionará un marco adecuado y una buena comprensión. En el párrafo 8.7 de este capítulo se aborda la implementación del SSP.

8.3.6.13 Deberían utilizarse datos cuantitativos cuando se disponga de los mismos para desarrollar una comprensión de sus principales riesgos de seguridad operacional. El Estado también puede utilizar información cualitativa y análisis de expertos. Puede crearse un grupo de expertos seleccionados para participar en debates guiados a efecto de obtener una comprensión de los más amplios riesgos de seguridad operacional en todo el sistema aeronáutico. Este grupo tendría una función similar a la del Consejo de revisión de seguridad operacional (SRB), del proveedor de servicios, como se analiza en el Capítulo 9, 9.3.6; en este caso a nivel estatal. Estos expertos pueden orientarse por la información disponible en materia de tendencias de seguridad operacional, factores contribuyentes conocidos de accidentes e incidentes graves, o deficiencias conocidas en los procesos SSO del Estado. También podrían considerar objetivos regionales u objetivos mundiales según se identifican en el GASP. Este enfoque de reuniones de reflexión podría aplicarse en forma de colaboración con los proveedores de servicios, para identificar problemas de seguridad operacional “conocidos” en cada sector de la aviación.

8.3.6.14 Los objetivos estatales de seguridad operacional son declaraciones breves y de alto nivel que proporcionan dirección a todas las autoridades aeronáuticas del Estado pertinentes. Representan los resultados deseados en materia de seguridad operacional que el Estado procura alcanzar. Cuando se definen los objetivos de

seguridad operacional también es importante tener en cuenta la capacidad del Estado para influir sobre los resultados deseados. Los objetos de seguridad operacional representan las prioridades del Estado para la gestión de la seguridad operacional y proporcionan un proyecto para asignar y dirigir los recursos del Estado.

8.3.6.15 Los objetivos de seguridad operacional apoyan la identificación de los SPI y las SPT del Estado y el posterior establecimiento del nivel aceptable de performance en materia de seguridad operacional (ALoSP), que se analiza más adelante en este capítulo. Los objetivos de seguridad operacional funcionan en conjunto como un paquete con los SPI y SPT para permitir al Estado observar y medir su rendimiento en materia de seguridad operacional. En el Capítulo 4 figura más orientación sobre los SPI y SPT.

8.3.6.16 Una vez implementado el SSP, el Estado debería reevaluar periódicamente sus riesgos de seguridad operacional identificados mediante el análisis de la información sobre seguridad operacional generada por el SSP. Este análisis también apoyará la identificación de problemas emergentes. En el Capítulo 6 figura orientación sobre los análisis de seguridad operacional. El Estado también debería revisar periódicamente sus progresos hacia el logro de sus objetivos de seguridad operacional y su continua pertinencia, teniendo en cuenta todas las reevaluaciones de los riesgos presentes.

Recursos estatales de seguridad operacional

8.3.6.17 El Estado debe asegurar que los organismos o responsabilidades de seguridad operacional reciben suficientes recursos para ejecutar sus mandatos. Esto comprende recursos financieros además de recursos humanos.

8.3.6.18 Algunas autoridades aeronáuticas reciben su financiación sobre la base de un presupuesto asignado por el Estado. Otras son financiadas mediante tasas y derechos cobrados a los participantes en el sistema aeronáutico (como tasas por licencias y aprobaciones) o a los usuarios de servicios dentro del sistema de aviación (p. ej., gravámenes sobre pasajeros o combustible). La fuente de financiación que resulta más apropiada para el Estado depende de las circunstancias del Estado en cuestión. Por ejemplo, un Estado que tenga una pequeña industria de aviación puede encontrar que no es suficiente que su CAA se base solamente en tasas y derechos para financiar sus actividades normativas. El Estado puede necesitar múltiples fuentes de financiación para sus actividades aeronáuticas.

8.3.6.19 Cuando el Estado comienza a implementar plenamente su SSP y adoptar prácticas de gestión de la seguridad operacional, puede tener que revisar su presupuesto y financiación para asegurar que continúa teniendo una corriente de ingresos suficiente. Se introducen nuevas funciones que deben llevarse a cabo correctamente para que el enfoque de gestión de la seguridad operacional tenga éxito, incluyendo por ejemplo SRM, recopilación y análisis de datos y promoción de la seguridad operacional. La gestión de la seguridad operacional también requiere que las autoridades aeronáuticas del Estado puedan observar y realizar continuamente sus propios procesos de gestión de riesgos. Quizá se tenga que readiestrar a los inspectores y otro personal. En esa situación, el Estado puede considerar necesario asignar suficientes recursos financieros a los organismos estatales cuando se realice la transición a un enfoque de gestión de la seguridad operacional.

Plan nacional de seguridad operacional de la aviación (NASP)

8.3.6.20 En la Resolución A39-12 de la Asamblea sobre Planificación mundial OACI para la seguridad operacional y la navegación aérea, se reconoce la importancia de la ejecución eficaz de los planes nacionales de seguridad operacional de la aviación. En la misma se resuelve que los Estados elaboren e implanten planes nacionales de seguridad operacional de la aviación con arreglos a los objetivos del Plan global para la seguridad operacional de la aviación (GASP, Doc 10004). A nivel internacional, el GASP establece una estrategia que apoya la priorización y mejora continua de la seguridad operacional de la aviación. Los planes regionales y nacionales de seguridad operacional de la aviación deberían elaborarse con arreglo al GASP.

8.3.6.21 A nivel regional, los grupos regionales de seguridad operacional de la aviación (RASG) coordinan el proceso de planificación. Las iniciativas regionales y nacionales de mejoramiento de la seguridad operacional (SEI) deberían adaptarse sobre la base de los problemas enfrentados por los Estados en cuestión. El plan nacional de seguridad operacional de la aviación presenta la dirección estratégica para la gestión de la seguridad operacional de la aviación a nivel nacional, por un período de tiempo establecido (p. ej., a lo largo de los próximos cinco años). En él se señalan a todos los interesados aquellos sectores en que las autoridades aeronáuticas del Estado deberían dedicar recursos en los años venideros.

8.3.6.22 Un plan nacional de seguridad operacional de la aviación permite al Estado comunicar claramente su estrategia para mejorar la seguridad operacional a nivel nacional a todas las partes interesadas, incluyendo otras instituciones gubernamentales y el público viajero. Proporciona un medio transparente para revelar la forma en que las CAA y otras entidades involucradas en la aviación civil trabajarán para identificar peligros y gestionar los riesgos de seguridad operacional y otros problemas en esa materia. También ilustra la forma en que las SEI planificadas ayudarán al Estado a lograr los objetivos establecidos. El plan nacional de seguridad operacional de la aviación subraya el compromiso del Estado respecto de dicha seguridad.

8.3.6.23 Cada Estado debería producir un plan nacional de seguridad de la aviación. Si un Estado ya cuenta con un SSP implantado, el plan nacional de seguridad operacional de la aviación podría abordarse por el Componente 1: Política, objetivos y recursos estatales de seguridad operacional. El plan nacional de seguridad operacional de la aviación puede publicarse como documento de alto nivel independiente para facilitar la comunicación con el público y otras entidades externas a la CAA.

Documentación del SSP

8.3.6.24 El Estado debería describir su SSP en un documento para asegurar que todo el personal pertinente tiene una comprensión común. El documento debería incluir su estructura y programas conexos, la forma en que sus diversos componentes funcionan en conjunto, así como las funciones de las diferentes autoridades aeronáuticas del Estado. Dicha documentación debería complementar los procesos y procedimientos existentes y describir en términos generales la forma en que los diversos subprogramas de SSP funcionan en conjunto para mejorar la seguridad operacional. También pueden incluirse en documentos de apoyo referencias a las responsabilidades y obligaciones de rendición de cuentas de las autoridades en materia de seguridad operacional. El Estado debería elegir el medio de documentación y difusión que se adapte mejor a su entorno, por ejemplo, un documento físico o un sitio web adecuadamente controlado. Independientemente del canal de comunicación elegido, el objetivo es facilitar la comprensión común del SSP por parte de todo el personal pertinente.

8.3.7 Personal técnico cualificado

8.3.7.1 En el Doc 9734, Parte A figura orientación sobre el personal técnico cualificado que desempeña funciones relacionadas con la seguridad operacional (CE-4).

Orientación general

8.3.7.2 Los Estados deberán identificar y tratar las competencias requeridas para la eficaz implementación del SSP, teniendo en cuenta las funciones y responsabilidades desempeñadas por su personal en el marco del SSP. Estas competencias se añaden a las requeridas para la vigilancia del cumplimiento y pueden tratarse mediante la instrucción del personal existente o la contratación de personal adicional. Estas competencias comprenden, entre otras, las siguientes:

a) aptitud para el liderazgo mejorada;

b) comprensión de los procesos empresariales;

c) experiencia y buen juicio para evaluar rendimiento y eficacia;

d) vigilancia de la seguridad operacional basada en riesgos;

e) recopilación y análisis de datos de seguridad operacional;

f) medición y observación del rendimiento en materia de seguridad operacional; y

g) actividades de promoción de la seguridad operacional.

8.3.7.3 En el *Manual sobre competencias de los inspectores de seguridad operacional de la aviación civil* (Doc 10070) figura orientación sobre el desarrollo y mantenimiento de un equipo de inspectores competentes.

8.3.7.4 El Estado debería determinar la instrucción más apropiada para el personal con diferentes funciones y responsabilidades en la organización. Los siguientes son ejemplos de instrucción que deberían tenerse en cuenta:

a) reuniones de información o instrucción de familiarización para el personal superior sobre SSP, SMS, política, objetivos y ALoSP relativos a la seguridad operacional;

b) instrucción para inspectores en los principios de SSP y SMS, la forma de realizar evaluaciones SMS, como evaluar los SPI de un proveedor de servicios para que resulten aceptables y cómo supervisar en general al proveedor de servicios en un entorno de gestión de la seguridad operacional;

c) instrucción en competencias interpersonales y básicas (habilidades de comunicación eficaz, habilidades de negociación, resolución de conflictos, etc.) para apoyar a los inspectores que trabajan en colaboración con proveedores de servicios a efectos de mejorar el rendimiento en materia de seguridad operacional asegurando, al mismo tiempo, el cumplimiento de los reglamentos establecidos;

d) instrucción para el personal responsable de análisis de datos, objetivos de seguridad operacional, SPI y SPT;

e) instrucción para examinadores médicos aeronáuticos y evaluadores médicos;

f) protección de datos e información sobre seguridad operacional y fuentes conexas e instrucción en políticas de cumplimiento para el personal jurídico, etc.; y

g) instrucción en SSP y SMS para los investigadores de seguridad operacional de los proveedores de servicios.

8.3.7.5 Los programas de instrucción en seguridad operacional para el personal involucrado en tareas relacionadas con el SSP deberían coordinarse entre las organizaciones del Estado, según corresponda. El ámbito de la instrucción o familiarización en SSP y SMS debería reflejar los procesos SSP verdaderos, y al propio SSP en cuanto a su evolución y maduración. La instrucción inicial en SSP y SMS puede limitarse a los elementos del SSP y del marco SMS genéricos y a la orientación en la materia.

8.3.7.6 Para asegurar que todo el personal técnico pertinente está adecuadamente calificado, el Estado debería:

a) elaborar políticas y procedimientos de instrucción internos; y

b) elaborar un programa de instrucción en SSP y SMS para el personal pertinente. Debería darse prioridad al personal involucrado en la implementación del SSP-SMS y a los inspectores de operaciones y de campo involucrados en la supervisión/vigilancia del SMS del proveedor de servicios; (incluyendo procesos SSP específicos del Estado y pertinencia de los mismos).

8.3.7.7 Hay disponibles muchos tipos diferentes de instrucción en SSP y SMS, incluyendo cursos en línea, cursos en aula, seminarios teóricos y prácticos, etc. El tipo y volumen de instrucción proporcionados debería asegurar que el personal pertinente desarrolla la competencia necesaria para ejecutar sus funciones y comprender su contribución al SSP. El objetivo es asegurar que una persona o equipo encaren cada aspecto del SSP y que están capacitados para realizar la función asignada.

8.3.7.8 Una instrucción apropiada y suficiente para los inspectores asegurará una supervisión o vigilancia coherentes y que las capacidades requeridas sean eficaces en un entorno de la gestión de la seguridad operacional. Los Estados deberían considerar lo siguiente:

a) la vigilancia y observación de los SMS de los proveedores de servicios exigirán competentes que pueden no haber sido críticas antes de que se introdujeran requisitos SMS. Los inspectores deberán complementar sus conocimientos técnicos existentes con habilidades adicionales para evaluar la adecuación y eficacia de la implementación del SMS de los proveedores de servicios. Este enfoque requiere trabajar en forma conjunta con la industria a efectos de ganar la confianza de los proveedores de servicios en cuanto a facilitar la compartición de datos e información sobre seguridad operacional. Los Estados deberán proporcionar la instrucción apropiada para asegurar que el personal responsable de la interacción con la industria tiene las competencias y flexibilidad para llevar a cabo las actividades de vigilancia en un entorno SMS. Puede utilizarse un análisis de necesidades de instrucción para identificar el tipo de formación apropiado.

b) La instrucción también debería proporcionar al personal un conocimiento de las funciones y contribuciones de otros departamentos dentro de su autoridad aeronáutica y otras instituciones aeronáuticas del Estado. Esto permitirá que los inspectores, así como el personal de diferentes autoridades aeronáuticas del Estado, apliquen un enfoque coherente. También facilitará una mejor comprensión de los riesgos de seguridad operacional en varios sectores. Los inspectores también pueden comprender mejor la forma en que contribuyen al logro de los objetivos de seguridad operacional del Estado.

8.3.8 Orientación técnica, instrumentos y suministro de información crítica en materia de seguridad operacional

8.3.8.1 En el Doc 9734, Parte A figura información sobre orientación técnica, instrumentos y suministro de información crítica en materia de seguridad operacional (CE-5).

8.3.8.2 El Estado debería considerar proporcionar orientación a sus inspectores y proveedores de servicios para ayudar en la interpretación de los reglamentos de gestión de la seguridad operacional. Esto promoverá una cultura positiva de la seguridad operacional y ayudará al proveedor de servicios a lograr sus objetivos de seguridad operacional y, en consecuencia, los objetivos estatales de seguridad operacional que a menudo se alcanzan mediante la reglamentación. La evaluación del SMS puede exigir instrumentos adicionales para determinar tanto el cumplimiento como el rendimiento del SMS de los proveedores de servicios. Todo instrumento elaborado exigirá instrucción del personal afectado antes de poderse implementar.

8.4 COMPONENTE 2: GESTIÓN ESTATAL DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

8.4.1 Los Estados deben identificar posibles riesgos de seguridad operacional en el sistema aeronáutico. El Estado debería aumentar sus métodos tradicionales de analizar las causas de un accidente o incidente mediante procesos proactivos para alcanzar dicho objetivo. Los procesos proactivos permiten al Estado identificar y abordar elementos precursores y contribuyentes de accidentes, así como gestionar estratégicamente los recursos de seguridad operacional para maximizar las mejoras en la materia. Los Estados deberían:

a) exigir que sus proveedores de servicios implementen SMS para gestionar y mejorar la seguridad de sus actividades relacionadas con la aviación;

b) establecer medios para determinar si la SRM de los proveedores de servicios es aceptable; y

c) examinar el SMS del proveedor de servicios y asegurar que permanece siendo eficaz.

8.4.2 El componente estatal de la SRM comprende la implementación de SMS por los proveedores de servicios, incluyendo procesos de identificación de peligros y gestión de riesgos de seguridad operacional conexos.

8.4.3 Los Estados deberían aplicar también los principios de la SRM a sus propias actividades. Estas comprenden la elaboración de reglamentos y la priorización de actividades de vigilancia basadas en riesgos evaluados.

8.4.4 Con frecuencia, los proveedores de servicios y reglamentadores no prestan la debida atención a los riesgos de seguridad operacional inducidos a través de interfaces con otras entidades. La interfaz entre el SSP y los SMS puede plantear un reto particular para los Estados y proveedores de servicios. El Estado debería considerar destacar la importancia de la gestión de riesgos de la interfaz SMS a través de sus reglamentos y orientación de apoyo. Entre los ejemplos de riesgos de interfaz figuran los siguientes:

a) Dependencia — la organización A depende de la organización B para proporcionar bienes o servicios. La organización B no tiene en claro las expectativas y la dependencia de la organización A y no proporciona dichos elementos.

b) Control — las organizaciones en interfaz a menudo tienen un control mínimo de la calidad o eficacia de las organizaciones involucradas.

8.4.5 En estos dos ejemplos, la gestión de los riesgos de interfaz pueden poner de relieve el riesgo, aclarar las expectativas mutuas y mitigar las consecuencias no deseadas mediante verificaciones mutuamente convenidas de los límites pertinentes. En el Capítulo 2 figura información adicional sobre las interfaces entre proveedores de servicios.

8.4.6 Obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones

8.4.6.1 En el Doc 9734, Parte A, figura orientación sobre obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones (CE-6).

8.4.6.2 Las obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones son componentes importantes de la estrategia estatal de control de riesgo de seguridad operacional. Estas brindan al Estado garantías de que los proveedores de servicios y otras organizaciones representativas de la industria pertinentes han alcanzado las normas requeridas para operar dentro del sistema aeronáutico en condiciones de seguridad. Algunos Estados han establecido reglamentos de explotación comunes para facilitar el reconocimiento o aceptación de licencias, certificados, autorizaciones y aprobaciones expedidas por otros Estados. Dichos arreglos no eximen al Estado del cumplimiento de sus obligaciones en el marco del Convenio de Chicago.

8.4.7 Obligaciones del sistema de gestión de la seguridad operacional

Requisitos normativos del SMS

8.4.7.1 Con arreglo al Anexo 19, los Estados exigirán que los proveedores de servicios y explotadores de la aviación general internacional implanten un SMS. Los requisitos se refieren al marco para un SMS que figura en el Anexo 19, Apéndice 2 y en la orientación de apoyo presentada en el Capítulo 9 de este manual. La forma en que dichos requisitos son establecidos dependerá del marco normativo del Estado.

8.4.7.2 Los Estados deberían instituir un proceso que asegure que el SMS les resulta aceptable. Un enfoque es establecer cronogramas e hitos a nivel estatal que representen el progreso requerido de la implementación del SMS. En el Capítulo 9 figura orientación adicional para los proveedores de servicios sobre cómo desarrollar y realizar un análisis de brechas del SMS y un plan de la implementación.

8.4.7.3 Los requisitos normativos del SMS y los textos de orientación sobre el SMS del Estado deberían revisarse periódicamente. Dicha revisión debería tener en cuenta: información recibida de la industria, examen periódico del perfil de riesgo de seguridad operacional del Estado, situación presente y aplicabilidad de SARPS y textos de orientación de la OACI sobre SMS.

Aviación general internacional

8.4.7.4 Las disposiciones sobre SMS para la aviación general internacional (IGA) se abordan con cierta flexibilidad en el Anexo 19 y, por consiguiente, no se incluyen en la lista correspondiente a los proveedores de servicios. Se espera que este sector de la aviación implemente el marco SMS. La diferencia entre este sector y los demás sectores es que, en este caso, los Estados pueden ejercer un grado de flexibilidad en la forma en que establecen los requisitos. De acuerdo con otras disposiciones que figuran en el Anexo 6, Parte II — *Aviación general internacional — Aviones*, el Estado de matrícula establecerá criterios para que los explotadores de IGA implementen un SMS.

8.4.7.5 El establecimiento de esos criterios debería exigir la aplicación del marco SMS según se describe en el Anexo 19, pero ello puede lograrse de varias maneras:

a) estableciendo criterios dentro de los reglamentos de explotación específicos para IGA existentes;

b) publicando requisitos dentro del marco normativo en un instrumento jurídico distinto de los reglamentos de explotación específicos que definen los criterios; o

c) haciendo referencia dentro del marco normativo a un código de práctica industrial del SMS que sea reconocido por el Estado.

8.4.7.6 Al seleccionar el mejor enfoque para establecer los criterios SMS para IGA, el Estado de matrícula debería considerar la forma en que se observará el SMS, incluyendo la posible delegación de la vigilancia a terceras partes. Al igual que con los SMS de los proveedores de servicios, al determinar la aceptabilidad del SMS el Estado de matrícula debería tener en cuenta la posibilidad de adaptación y crecimiento basada en el volumen, entorno operacional y complejidad de la operación.

8.4.7.7 En caso de aeronaves grandes o turborreactores con varios Estados de matrícula a las que se ha otorgado un certificado de explotador de servicios aéreos (AOC) con arreglo al Anexo 6, Parte I, el explotador sería considerado como proveedor de servicios y tratado como tal en el SMS para que resulte aceptable al Estado del explotador.

Aceptación del SMS

8.4.7.8 Muchos proveedores de servicios cuentan con certificados, autorizaciones o aprobaciones de más de un Estado o realizan operaciones en más de un Estado. No hay en el Anexo 19 requisitos para supervisar el SMS de un proveedor de servicios que esté fuera de la responsabilidad del Estado. No obstante, la armonización de los requisitos SMS facilita en efecto la aceptación de los SMS entre Estados. La armonización reduce la duplicación de la vigilancia y la necesidad de que los proveedores de servicios cumplan obligaciones SMS similares mediante (posibles) requisitos disimiles. Los Estados deberían tener conciencia de las políticas que aumentan la carga administrativa y financiera para los titulares de certificados sin añadir un valor demostrable en materia de seguridad operacional. Cabe destacar que para los proveedores que no se benefician de la aceptación común de su certificación, autorización o aprobación, la introducción de SMS ha exacerbado la situación. Los Estados deberían tratar de alcanzar los beneficios de la implementación sin imponer cargas adicionales indebidas a los proveedores de servicios.

8.4.7.9 Además, se alienta a los Estados a que apliquen los requisitos en forma igualitaria al otorgar certificados, autorizaciones o aprobaciones a proveedores de servicios de otros Estados, sin aplicar cargas técnicas, legales y administrativas excesivas. Muchos proveedores de servicios necesitan recursos adicionales para su aceptación inicial por varios Estados y para apoyar la observación o auditorías periódicas de Estados que han aceptado su SMS. También se requieren esfuerzos adicionales cuando los requisitos varían, se interpretan en forma diferente o resultan conflictivos.

8.4.7.10 En el Anexo 19 se proporcionan los requisitos para un marco SMS. Los Estados transponen dichos requisitos a su marco normativo. El rendimiento de un sistema o proceso institucional depende, en la práctica, de la forma en que se implementan dichos requisitos. Hay dos componentes principales involucrados en la equivalencia de SMS y en las consecuencias de la aceptación del SMS entre los Estados.

8.4.7.11 El primer componente es el aspecto formal del reconocimiento o aceptación del SMS. Algunos Estados han tratado este aspecto mediante acuerdos bilaterales o multilaterales que involucran una mezcla de arreglos diplomáticos, jurídicos y técnicos entre Estados. En algunos casos, la aceptación es mutua, aunque no en todas las circunstancias.

8.4.7.12 El segundo componente es la equivalencia técnica. Esta puede dividirse en cinco áreas:

a) *Requisitos comunes*. Aunque no es suficiente para establecer la equivalencia, el uso de un conjunto común de requisitos proporciona estructura y eficiencia a las evaluaciones técnicas. Estas se han establecido en los diversos Anexos de la OACI.

b) *Expectativas de la implantación*. Cada Estado identifica expectativas específicas para procesos, programas, métodos e instrumentos a efectos de que la otra autoridad demuestre la implementación y el rendimiento.

c) *Metodología de aceptación* Los métodos que los Estados emplean para evaluar la forma en que se aceptan procesos y capacidades de gestión varían entre los Estados. Esto es normalmente una función del sistema estatal de supervisión de la seguridad operacional (CE-6, Obligaciones del otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones).

d) *Medición del rendimiento*. La metodología aplicada por cada Estado para medir el rendimiento en materia de seguridad operacional de las organizaciones certificadas y aprobadas se dirige a mejorar la comprensión por el Estado del potencial de rendimiento y las condiciones de cada organización.

e) *Políticas y métodos de observación*. La observación debe asegurar el Estado de rendimiento de las organizaciones y sus SMS. Esto constituye un aspecto de las obligaciones de vigilancia del Estado. Cada Estado debe elaborar una comprensión y confianza en los métodos aplicados por otra autoridad para supervisar sus SMS. Esto apoya la aceptación o el reconocimiento de dichos sistemas.

8.4.7.13 El SMS del proveedor de servicios debe resultar aceptable para la autoridad estatal pertinente. Se espera que los proveedores de servicios realicen un análisis de brecha y elaboren un plan de implementación ejecutable (incluyendo la aceptación por el Estado como tarea planificada). La implementación del SMS se lleva a cabo generalmente en tres o cuatro etapas. La temprana colaboración entre el proveedor de servicios y las autoridades estatales probablemente conduzca a un proceso de elaboración y aceptación más fluido. En el Capítulo 9 figura más información sobre la implementación de SMS.

Aceptación de los SPI y las SPT

8.4.7.14 Los SPI propuestos por los proveedores de servicios son revisados y aceptados por la autoridad normativa pertinente del Estado como parte de la aceptación del SMS. Los Estados pueden considerar la planificación de la aceptación de los SPI de un proveedor de servicio más adelante en el proceso de implementación. Esto resulta especialmente práctico para los proveedores de servicios en la certificación inicial dado que a menudo no cuentan con

suficientes datos para elaborar indicaciones significativas. El reglamentador puede estar satisfecho de que los SPI propuestos son apropiados y pertinentes a las actividades aeronáuticas de cada proveedor de servicio. Algunos de los SPI y SPT del proveedor de servicio pueden relacionarse con los SPI y SPT del Estado para la medición y observación del ALoSP. Esto no es necesariamente el caso para todos los SPI y SPT. En el Capítulo 4 figura más información sobre medición del rendimiento en materia de seguridad operacional.

8.4.7.15 La aceptación de los SPT del proveedor de servicios puede abordarse después de que los SPI han sido observados durante un período de tiempo. Esto establece el rendimiento básico. Puede basarse en metas establecidas a nivel estatal, regional o mundial. El logro de las SPT de Estado exigirá la coordinación de medidas de mitigación de riesgo de seguridad operacional con el proveedor de servicios.

Un solo SMS para múltiples proveedores de servicios

8.4.7.16 Las organizaciones que cuentan con múltiples certificaciones de proveedores de servicio pueden optar por incluirlas bajo el ámbito de un solo SMS para capitalizar las ventajas de dicho sistema y abordar mejor los aspectos de i interfaz. El órgano reglamentador del Estado debería considerar lo siguiente al evaluar el SMS de estas organizaciones matrices o la implementación de requisitos SMS para proveedores de servicio que se incluyen en el ámbito de un SMS más amplio:

a) asegurar que las políticas y procesos de información del SMS se aplican en forma coherente en todo el Estado, en particular donde los inspectores de diferentes organizaciones dentro del órgano reglamentador son responsables de la vigilancia y observación de diferentes proveedores de servicio:

    1) hay pruebas del compromiso de la administración para la interpretación coherente de los reglamentos y la continua aplicación de vigilancia y observación;

    2) todo el personal dedicado a la vigilancia y la observación ha recibido instrucción normalizada; idealmente incluyendo participantes de disciplinas diferentes;

    3) deben elaborarse e implementarse políticas, procedimientos y mecanismos de auditoría comunes cuando se trata de diferentes organizaciones de vigilancia y observación;

    4) hay comunicación coherente y frecuente entre los inspectores responsables asignados a cada proveedor de servicios;

    5) hay mecanismos implantados que supervisan el grado de normalización de las actividades de vigilancia y observación. Deberían tratarse todos los problemas que se identifiquen;

    6) se reconoce que las actividades del proveedor de servicios pueden ser abordadas por el SMS a nivel corporativo (“organización matriz”). Esto puede incluir actividades que requieran SMS y actividades que no están abarcadas en la aplicación del Anexo 19.

    7) la organización matriz o principal ha documentado:

        i) sus políticas y procedimientos para compartir datos e información sobre seguridad operacional, la forma en que se transmiten las comunicaciones, se toman las decisiones, y se asignan recursos a todas las diferentes áreas de actividad y, cuando corresponde, con diferentes autoridades normativas;

        ii) las funciones y responsabilidades relacionadas con sus SMS y el marco de rendición de cuentas para el SMS; y

        iii) la estructura institucional y las interfaces entre diferentes sistemas y actividades en su descripción del sistema.

b) Asegurar la conciencia de que las organizaciones principales o matrices con múltiples certificados – algunas de las cuales incluyen certificados de reglamentadores extranjeros – pueden optar por implementar un solo SMS que abarque todos los múltiples proveedores de servicio.

1) reconocer que el ámbito de un SMS está claramente definido en la descripción del sistema y presenta en detalle cada actividad. El proveedor de servicios puede demostrar la compatibilidad entre sus procesos del SMS y el SMS corporativo.

2) tener conciencia de que este escenario puede inducir retos adicionales cuando la organización matriz posee tanto aprobaciones nacionales como internacionales, como la aceptación del SMS por diferentes autoridades normativas. Debería concertarse un acuerdo con las otras autoridades normativas sobre cómo compartir, delegar o mantener por separado (duplicado) la vigilancia y la observación, cuando todavía no se hayan establecido arreglos para la aceptación del SMS.

Sistemas de gestión integrados

8.4.7.17 El órgano reglamentador debería considerar lo siguiente al evaluar a los proveedores de servicios que han integrado sus SMS con otros sistemas de gestión:

a) elaboración de una política que aclare el ámbito de su autoridad (pueden no ser responsables de la vigilancia de los sistemas de gestión conexos); y

b) recursos necesarios para evaluar y observar un sistema de gestión integrado (esto podría incluir personal con experiencia apropiada, procesos, procedimientos e instrumentos).

8.4.7.18 Existen ventajas para el proveedor de servicios en la integración de su SMS con otros sistemas de gestión. La integración debería completarse a la entera satisfacción de la CAA, y en una forma que la CAA pueda efectivamente “ver” y observar el SMS. En el Capítulo 9 figura orientación para los proveedores de servicios que implementen SMS como parte de un sistema de gestión integrado.

8.4.8 Investigación de accidentes

8.4.8.1 La autoridad de investigación de accidentes (AIA) debe funcionar en forma independiente de cualquier otra organización. La independencia respecto de la CAA del Estado tiene particular importancia. Los intereses de la podrían estar en conflicto con las tareas confiadas a la AIA. El fundamento de la independencia de esta función con respecto a otras organizaciones es que las causas de los accidentes pueden relacionarse con factores reglamentarios o relacionados con el SSP. Además, dicha independencia aumenta la viabilidad de la AIA y evita conflictos de intereses reales o percibidos.

8.4.8.2 El proceso de investigación de accidentes tiene una función principal en el SSP. Permite al Estado identificar factores contribuyentes y cualquier posible falla dentro del sistema aeronáutico así como generar las contramedidas necesarias para prevenir repeticiones. Esta actividad contribuye a la continua mejora de la seguridad operacional de la aviación mediante el descubrimiento de fallas activas y factores contribuyentes de accidentes o incidentes proporcionando, además, informes sobre cualesquiera enseñanzas obtenidas del análisis de sucesos. Esto puede apoyar la elaboración de decisiones sobre medidas correctivas y la correspondiente asignación de recursos identificando además mejoras necesarias del sistema de aviación. Véase el Anexo 13 de la OACI y orientación conexa por más información.

8.4.8.3 Hay varios sucesos de seguridad operacional que no requieren investigación oficial con arreglo al Anexo 13. Estos sucesos y peligros identificados pueden indicar problemas sistémicos. Estos problemas pueden revelarse y solucionarse en una investigación de seguridad operacional dirigida por el proveedor de servicio. En el Capítulo 9 figura información sobre las investigaciones de seguridad operacional del proveedor de servicios.

8.4.9 Investigación de peligros y gestión de riesgos de seguridad operacional

Orientación general

8.4.9.1 Una de las funciones más importantes de las autoridades de aviación es identificar peligros y tendencias emergentes en todo el sistema aeronáutico. Esto se realiza a menudo mediante el análisis de datos de seguridad operacional consolidados de múltiples fuentes. El nivel de complejidad y perfeccionamiento del proceso de SRM del Estado variará según la envergadura, grado de madurez y complejidad del sistema aeronáutico del Estado en cuestión. En el Capítulo 2 figura orientación general sobre el proceso de SRM.

8.4.9.2 La recopilación de datos de información sobre seguridad operacional tanto internos como externos, resulta esencial para lograr un SSP eficaz. Los sistemas aeronáuticos que no son complejos pueden producir datos limitados. En este caso, la recopilación y el intercambio de datos externos deberían constituir una prioridad. A menudo se dispone de datos externos de otros Estados, como informes de investigaciones, informes anuales sobre seguridad operacional (incluyendo información y análisis sobre incidentes); alertas de seguridad operacional, boletines de seguridad operacional, estudios en la materia; iSTARS; etc. A nivel regional, los grupos de la OACI (p. ej., RASG, grupos regionales de planificación y ejecución (PIRG), etc.) también pueden proporcionar una buena fuente de información sobre seguridad operacional. El Sistema de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) del Estado, debería incluir procedimientos para presentar a la OACI informes de accidentes e incidentes, lo que facilitará la recopilación y compartición de información sobre seguridad operacional a escala mundial.

8.4.9.3 El objetivo principal de la SRM consiste en identificar y controlar las posibles consecuencias de los peligros aplicando los datos de seguridad operacional disponibles. Los principios de la SRM son los mismos para los Estados y los proveedores de servicios.

8.4.9.4 Los proveedores de servicios tienen acceso a sus propios datos de seguridad operacional. Los Estados tienen acceso a datos de seguridad operacional de múltiples proveedores de servicios. Por lo tanto, el Estado que implemente taxonomías comunes para clasificar los datos de seguridad operacional que recopila mejorará enormemente la eficacia de su proceso RSM. Esto también permite que los datos recogidos de múltiples fuentes a través de diferentes sectores de aviación sean analizados en forma más eficaz. En la siguiente Figura 8-2 se ilustran las entradas y salidas del proceso de análisis de datos.

8.4.9.5 Las entradas pueden recibirse de cualquier parte de un sistema aeronáutico, incluyendo investigaciones de accidentes, investigaciones de seguridad operacional del proveedor de servicios, informes sobre mantenimiento de la aeronavegabilidad, resultados de evaluaciones médicas, evaluaciones de riesgos de seguridad operacional, constataciones e informes de auditoría y estudios y exámenes de seguridad operacional.

8.4.9.6 Cuando sea necesario, las salidas o controles de riesgos de seguridad operacional se aplican para eliminar el peligro o reducir el nivel de riesgo a un nivel aceptable. Entre las muchas opciones de mitigación disponibles al Estado figuran: directivas de aeronavegabilidad, entradas para la vigilancia y observación refinadas de los proveedores de servicios, enmiendas de las políticas de certificación, reglamentación o seguridad operacional, programa de promoción de la misma y facilitación de seminarios. Las medidas recogidas dependerá de la gravedad y tipo del problema en cuestión.

Identificación de peligros

8.4.9.7 La identificación de peligros se basa en la recopilación de datos representativos. Puede resultar apropiado combinar o consolidar datos de múltiples sectores para asegurar una comprensión total de cada peligro. El proceso que se muestra en la Figura 8-2 es igualmente válido tanto para la identificación reactiva como proactiva. El análisis de los peligros identificados durante una investigación de incidente o accidente constituye un ejemplo de metodología reactiva. Una metodología proactiva podría incluir los peligros identificados durante auditorías o inspecciones o de las notificaciones obligatorias. Esto a su vez podría incluir el estar alerta frente a los primeros signos de deterioro del rendimiento en materia de seguridad operacional que surjan de la observación cotidiana de la fiabilidad del sistema.

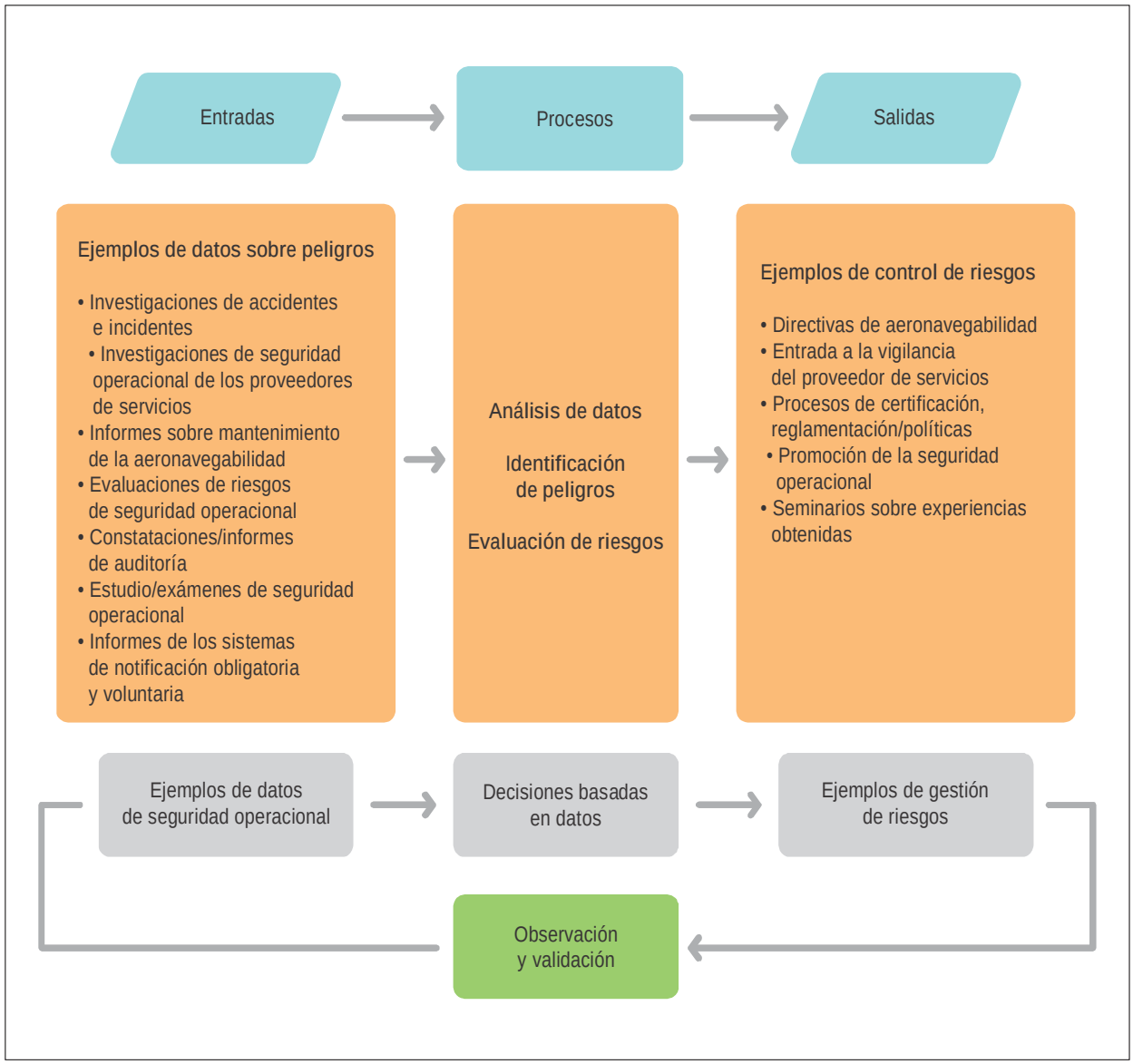


Figura 8-2. Programa de análisis basado en datos

8.4.9.8 Existen peligros en todos los niveles del sistema aeronáutico del Estado. Los accidentes o incidentes ocurren cuando los peligros interactúan con ciertos factores de activación. Como resultado, los peligros deberían identificarse antes de que conduzcan a accidentes, incidentes u otros sucesos relacionados con la seguridad operacional.

8.4.9.9 Se exhorta a los Estados a que designen un individuo o equipo para recopilar, consolidar y analizar los datos disponibles. El analista estatal de seguridad operacional debería analizar los datos para identificar y documentar posibles peligros así como sus correspondientes efectos o consecuencias. El detalle requerido en el proceso de identificación de peligros depende de la complejidad del proceso que se considere.

8.4.9.10 Debería elaborarse un proceso sistemático para asegurar la eficaz identificación de peligros. Este debería incluir los elementos siguientes:

a) acceso a las fuentes de datos necesario para apoyar la gestión de riesgos de seguridad operacional y en el Estado;

b) equipo de análisis de seguridad operacional con pericia analítica y experiencia operacional apropiadas, así como instrucción y experiencia en varias técnicas de análisis de peligros; y

c) mecanismos de análisis de peligros apropiados a los datos recopilados (o que se recopilarán) y al ámbito de las actividades aeronáuticas del Estado.

Elementos activadores de la identificación de peligros

8.4.9.11 Hay varias situaciones en que debería iniciarse una identificación de peligros. Algunas de las principales son las siguientes:

a) *Diseño del sistema:* la identificación de peligros comienza antes del inicio de las operaciones con una detallada descripción del sistema aeronáutico particular y su entorno. El equipo de análisis de seguridad operacional identifica los varios posibles peligros relacionados con el sistema así como sus consecuencias para otros sistemas interrelacionados.

b) *Cambios del sistema:* la identificación de peligros comienza antes de introducir cambios en el sistema (operacionales o institucionales) e incluso una descripción detallada del cambio particular del sistema aeronáutico. El equipo de análisis de seguridad operacional identifica luego los posibles peligros relacionados con el cambio propuesto así como sus consecuencias para otros sistemas interrelacionados.

c) *Observación a solicitud y continua:* la identificación de peligros se aplica a los sistemas existentes en funcionamiento. La observación de los datos se aplica para detectar cambios en la situación de los peligros. Por ejemplo, la manifestación del peligro puede ser más frecuente o más grave de lo previsto, o las estrategias de mitigación convenidas resultan menos eficaces de lo previsto. La observación y el análisis continuos pueden establecerse con umbrales de notificación sobre la base de un conjunto de aspectos de interés crítico.

Evaluación de riesgos de seguridad operacional

8.4.9.12 En el Capítulo 2 figura orientación general sobre la evaluación de riesgos de seguridad operacional. Cabe señalar que los riesgos de seguridad operacional pueden visualizarse y controlarse a través de todo un sector aeronáutico o una región.

8.4.9.13 Existen muchos mecanismos diferentes para analizar datos y aplicar diferentes enfoques de modelización de riesgo de seguridad operacional. Al seleccionar o elaborar una evaluación de riesgos de seguridad operacional, los Estados deberían asegurar que el proceso funciona bien para su entorno respectivo.

8.4.10 Gestión de los riesgos de seguridad operacional

8.4.10.1 En el Doc 9734, Parte A, figura orientación sobre la solución de problemas de seguridad operacional (CE-8).

8.4.10.2 El objetivo de la gestión de riesgos de seguridad operacional es asegurar que éstos se controlan y se lograr un ALoSP. La autoridad aeronáutica del Estado apropiada elabora, documenta y recomienda estrategias apropiadas de mitigación de riesgos de seguridad operacional o de control de los mismos. Entre los ejemplos figuran: la intervención directa con un proveedor de servicios, la implementación de política sobre reglamentos adicionales, la publicación de directivas de explotación o la influencia mediante actividades de promoción de la seguridad operacional.

8.4.10.3 Como etapa siguiente debería realizarse una evaluación de cada medida de control de riesgos de seguridad operacional propuesta. Los controles de riesgos ideales son rentables, de fácil ejecución, rápida implantación, eficaces y no introducen consecuencias imprevistas. Dado que la mayoría de las situaciones no satisfacen estos ideales, los posibles controles de riesgos de seguridad operacional deberían evaluarse y seleccionarse sobre la base de comparación de los atributos de eficacia, costos, oportunidad de implantación y complejidad. Una vez seleccionados e implementados los controles de riesgo de seguridad operacional, estos deberían observarse y validarse para asegurar que se han alcanzado los objetivos previstos.

8.4.10.4 Muchos de los controles de riesgos de seguridad operacional requieren que los proveedores de servicios adopten medidas. Los Estados deberían orientar a los proveedores de servicios para que logren una implementación eficaz. Los Estados pueden tener que observar la eficacia de los controles de riesgos de seguridad operacional y su impacto sobre los proveedores de servicios y en forma colectiva, el rendimiento en materia de seguridad operacional por parte del Estado. En el Capítulo 2 se presentan enfoques sobre mitigación de riesgos de seguridad operacional.

8.5 COMPONENTE 3: ASEGURAMIENTO ESTATAL DE LA SEGURIDAD OPERACIONAL

8.5.1 Las actividades de aseguramiento estatal de la seguridad operacional tienen por objeto asegurar al Estado que sus funciones están alcanzando sus objetivos y metas de seguridad operacional previstos. Los proveedores de servicios deben implementar un proceso de aseguramiento de la seguridad operacional como parte de sus SMS. La capacidad de aseguramiento del SMS garantiza a cada proveedor de servicios que sus procesos de seguridad operacional funcionan eficazmente, y que están bien dirigidos hacia el logro de sus objetivos de seguridad operacional. Análogamente, las actividades de aseguramiento estatal de la seguridad operacional, como parte de sus SSP, proporciona a los Estados seguridades de que sus procesos de seguridad operacional funcionan eficazmente y que el Estado está bien encaminado hacia el logro de sus objetivos de seguridad mediante los esfuerzos colectivo de la industria aeronáutica del Estado.

8.5.2 Las actividades de supervisión y los mecanismos de recopilación, análisis, compartición e intercambio de datos e información sobre seguridad operacional aseguran que los controles reglamentarios de los riesgos de seguridad están adecuadamente integrados en el SMS del proveedor de servicios. Esto crea confianza en que el sistema está funcionando según fue diseñado y que los controles reglamentarios tienen el efecto previsto sobre el SRM. Los Estados pueden recopilar datos e información sobre seguridad operacional de la aviación de muchas fuentes, incluyendo mediante procesos de supervisión y programas de notificación de la seguridad operacional. Los datos deberían analizarse a diversos niveles y las conclusiones obtenidas de los análisis deberían aplicarse como base para una toma de decisiones de seguridad operacional bien fundada con respecto a las actividades de supervisión y de seguridad operacional en el sistema aeronáutico del Estado.

8.5.3 Obligaciones de vigilancia

8.5.3.1 En el Doc 9734, Parte A, figura orientación sobre obligaciones de vigilancia (CE-7) relativas a la observación del cumplimiento.

Actividades de priorización de la vigilancia

8.5.3.2 La aplicación de un enfoque de vigilancia de la seguridad operacional basada en riesgos permite priorizar y asignar los recursos de gestión de la seguridad operacional del Estado en forma acorde con el perfil de riesgos de cada sector o cada proveedor de servicios. Los Estados obtienen experiencia y se familiarizan con cada proveedor de servicios mediante la observación del continuo desarrollo de madurez de sus procesos de aseguramiento de la seguridad operacional y, en particular, su gestión del rendimiento en materia de seguridad operacional. Con el tiempo, el Estado acumulará un panorama claro de las capacidades de seguridad del proveedor de servicios, en particular en su gestión de los riesgos de seguridad operacional. El Estado puede optar por enmendar el alcance o frecuencia de su vigilancia a medida que aumentan su confianza y las pruebas de la capacidad del proveedor de servicios en la materia.

8.5.3.3 La SRBS resulta más apropiada para las organizaciones con un SMS maduro. La SRBS también puede aplicarse a organizaciones en las que el SMS todavía no se ha implementado. El fundamento de una SRBS eficaz es contar con datos fiables suficientes y significativos. Sin datos fiables y significativos, resulta difícil justificar ajustes al ámbito o frecuencia de la vigilancia.

8.5.3.4 Los Estados deberían elaborar o reforzar sus capacidades de gestión de datos para asegurar que cuentan con datos fiables y completos sobre los cuales basar sus decisiones (basadas en datos). Los análisis de riesgos de seguridad operacional de cada sector también pueden permitir al Estado evaluar riesgos de seguridad operacional comunes que afecten a varios proveedores de servicios con tipos de operación similares (por ejemplo, líneas aéreas con servicios de corta distancia). Esto facilita la clasificación de los riesgos de seguridad operacional entre los proveedores de servicios dentro de un sector aeronáutico específico o a través de sectores, y apoya la asignación de recursos de vigilancia a aquellos sectores o actividades con mayores consecuencias para la seguridad operacional.

8.5.3.5 Los análisis a nivel de sector permiten que el Estado tenga un panorama del contexto del sistema aeronáutico: la forma en que las partes contribuyen al todo. Estos análisis habilitan al Estado a identificar los sectores que se beneficiarán de mayores niveles de apoyo o intervención, y aquellos sectores que son más aptos para aplicar un enfoque de mayor colaboración. Esto brinda al Estado garantías de que la reglamentación de todo el sistema aeronáutico es conmensurable y está bien dirigida en las áreas de mayor necesidad. Es más fácil identificar dónde se necesitan cambios de los reglamentos específicos para alcanzar la máxima eficacia normativa con una mínima interferencia.

8.5.3.6 La SRBS tiene un costo. Exige permanentes interacciones entre el Estado y la comunidad aeronáutica más allá de auditorías e inspecciones basadas en el cumplimiento. Un enfoque SRBS utiliza el perfil de riesgos de seguridad operacional del proveedor de servicios para adoptar sus actividades de vigilancia. Los productos de exámenes internos, análisis y toma de decisiones dentro del sistema del proveedor de servicios pasan a formar un plan de acción dirigido al tratamiento de riesgos de seguridad operacional principales y a las mitigaciones que los abordan con eficacia. Los análisis tanto del Estado como del proveedor de servicios, definen las áreas de prioridad de las preocupaciones de seguridad operacional y plantean los medios más eficaces de tratarlas.

8.5.3.7 Es importante señalar que la vigilancia de la seguridad operacional basada en riesgos puede no reducir necesariamente el volumen de la vigilancia ejercida o de los recursos. No obstante, la calidad de la vigilancia y la calidad de la interacción entre el reglamentador y el proveedor de servicios aumentarán considerablemente.

Perfiles de riesgos de seguridad operacional institucionales del proveedor de servicios

8.5.3.8 Los Estados pueden elaborar perfiles de riesgos de seguridad operacional institucionales que sean coherentes para cada sector aeronáutico a efectos de apoyar el proceso de modificar el alcance y la frecuencia de sus actividades de vigilancia. Dichos mecanismos deberían dirigirse a captar y consolidar información que ya debería estar disponible para los proveedores de servicio y pueden incluir factores como los siguientes:

a) la solidez financiera de la organización;

b) el número de años en funcionamiento;

c) índice de rotación del personal fundamental como el ejecutivo responsable y el gerente de seguridad operacional;

d) competencia y rendimiento del ejecutivo responsable;

e) competencia y rendimiento del gerente de seguridad operacional; (en el Capítulo 9 figura más información sobre las competencias del ejecutivo responsable o del gerente de seguridad operacional);

f) resultados de auditorías anteriores;

g) solución oportuna y efectiva de las constataciones anteriores;

h) medidas del nivel de actividad relativo (exposición a los riesgos de seguridad operacional);

i) indicadores del alcance y complejidad relativos de las actividades que se realizan;

j) grado de madurez del proceso de identificación de peligros y evaluación de riesgos de seguridad operacional; y

k) medición del rendimiento en materia de seguridad operacional a partir de análisis de datos de seguridad operacional del Estado y actividades de observación del rendimiento.

8.5.3.9 En la Figura 8-3 se muestra un ejemplo de proceso que puede aplicarse para modificar el alcance o la frecuencia de la vigilancia de un proveedor de servicios.

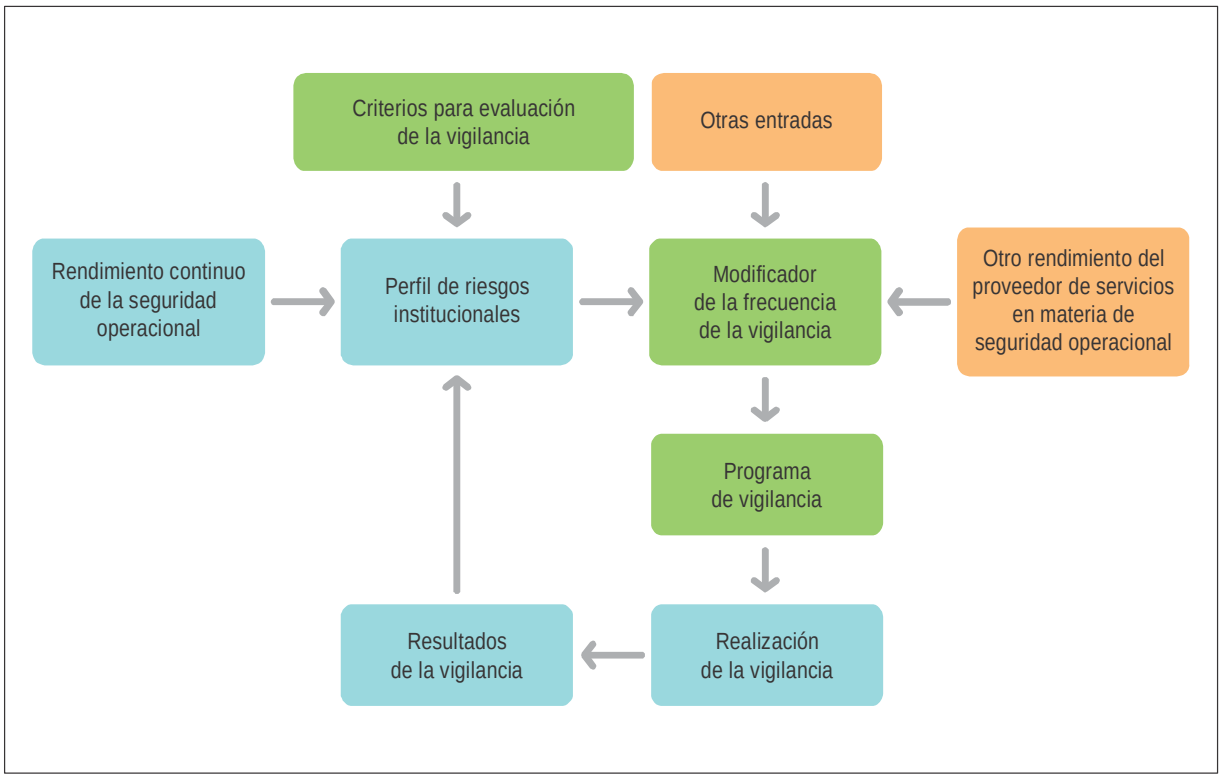


Figura 8-3. Concepto de vigilancia de la seguridad operacional basada en riesgos

8.5.4 Observación del rendimiento del proveedor de servicios en materia de seguridad operacional

El Estado debería examinar periódicamente los SPI y las SPT de cada proveedor de servicios. Dicho examen debería tener en cuenta el rendimiento y la eficacia de cada SPI y SPT. El examen puede indicar la necesidad de introducir ajustes para apoyar la continua mejora de la seguridad operacional.

8.5.5 Rendimiento estatal en materia de seguridad operacional

8.5.5.1 En el Capítulo 4 figura información general sobre gestión del rendimiento en materia de seguridad operacional.

Nivel aceptable de rendimiento en materia de seguridad operacional

8.5.5.2 Los Estados deben establecer el nivel aceptable de rendimiento en materia de seguridad operacional (ALoSP) que han de alcanzar mediante sus SSP. Esto puede lograrse por medio de:

a) implantación y mantenimiento del SSP y;

b) implantación y mantenimiento de SPI y SPT que indiquen que la seguridad operacional se está gestionando eficazmente.

8.5.5.3 El ALoSP expresa los niveles de seguridad operacional que el Estado espera lograr en su sistema aeronáutico, incluyendo las metas que cada sector debe alcanzar y mantener en relación con la seguridad operacional, así como las medidas para determinar la eficacia de sus propias actividades y funciones que afecten la seguridad operacional. Por ello, el ALoSP es un reflejo de lo que el Estado considera importante y aprueban los interesados en la aviación a nivel estatal. El ALoSP no debería elaborarse aisladamente. En vez de ello, debería definirse teniendo en cuenta una orientación estratégica de alto nivel (del GASP, planes regionales, etc.) y los objetivos de seguridad operacional establecidos en el SSP.

Establecimiento del ALoSP

8.5.5.4 La responsabilidad de establecer el ALoSP corresponde a las autoridades aeronáuticas del Estado y se expresará mediante el conjunto de SPI para el Estado, los sectores y los proveedores de servicios bajo su autoridad. El objetivo es mantener o mejorar en forma continua el rendimiento en materia de seguridad operacional del proceso de medición de todo el sistema aeronáutico que se presenta en el Capítulo 4. Esto permite al Estado comprender la forma en que está funcionando con respecto a la seguridad operacional y tomar medidas para corregir situaciones cuando sea necesario. La aceptación de los SPI y metas de los proveedores de servicios constituye parte de este proceso.

8.5.5.5 El ALoSP representa el acuerdo entre todas las autoridades aeronáuticas del Estado con respecto al nivel previsto de rendimiento en materia de seguridad operacional que su sistema aeronáutico debería alcanzar y demuestra a los interesados, tanto internos como externos, la forma en que el Estado está gestionando la seguridad operacional de la aviación. Comprende, entre otras cosas, las expectativas en cuanto a rendimiento en materia de seguridad operacional para cada sector y proveedor de servicios bajo la autoridad del Estado. El establecimiento de un ALoSP no reemplaza ni sustituye la obligación del Estado de ajustarse al Convenio sobre Aviación Civil Internacional, incluyendo la implementación de todos los SARPS aplicables.

8.5.5.6 En la Figura 8-4 se ilustra el concepto de ALoSP basado en los SPI y SPT. En el Capítulo 4 y en los párrafos que siguen figura más información sobre objetivos de seguridad operacional, SPI y SPT.

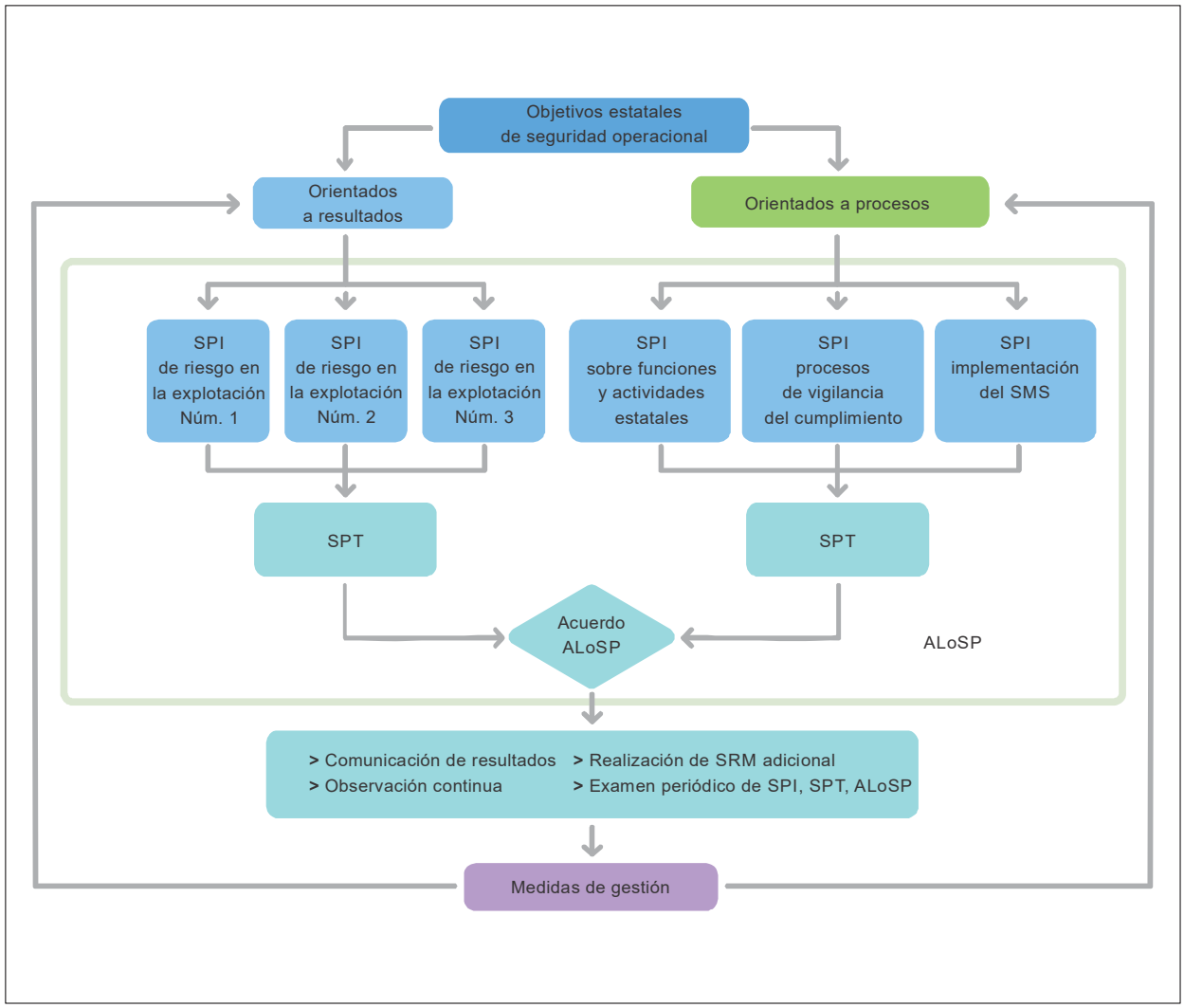


Figura 8-4. Nivel aceptable de rendimiento en materia de seguridad operacional (ALoSP)

Indicadores y metas de rendimiento en materia de seguridad operacional

8.5.5.7 Los SPI significativos deberían reflejar el entorno operacional específico y servir para subrayar las condiciones que pueden utilizarse a efectos de identificar la forma en que se controlan los riesgos de seguridad operacional. La estrategia de observación y medición del Estado debería incluir un conjunto de SPI que abarque todos los sectores del sistema aeronáutico de los cuales el Estado es responsable. Debería reflejar también tanto los resultados (p. ej., accidentes, incidentes, infracciones a reglamentos) como las funciones y actividades (operaciones en las que las mitigaciones de riesgos de seguridad operacional implantadas tuvieron los resultados previstos). Esta combinación permite evaluar el rendimiento en materia de seguridad operacional no solamente por lo que no funciona (es decir resultados), sino también con respecto a lo que sí funciona (es decir actividades en las que las mitigaciones de riesgos de seguridad operacional produjeron los resultados previstos). En términos prácticos, este enfoque abarca la consideración de SPI que reflejan dos tipos distintos de riesgos de seguridad operacional:

a) **Riesgos de seguridad operacional en la explotación** (presentados en el lado izquierdo del diagrama). Se concentran en las condiciones que podrían conducir a un resultado no deseado. Estas son las condiciones relacionadas con accidentes, incidentes, fallas y defectos. El riesgo de seguridad operacional en la explotación es esencialmente un subproducto de la prestación de servicios. Por este motivo, los SPI concentrados en el riesgo de seguridad operacional en la operación estarán en su mayoría relacionados – indirectamente – con los SMS de los proveedores de servicios. Aunque en la Figura 8-4 se muestran tres riesgos de seguridad operacional en la explotación, el número real debería basarse en la situación de cada Estado.

   Estos SPI reflejan principalmente problemas de seguridad operacional en la explotación identificados por el proceso SRM de los proveedores de servicios. El proceso SRM del Estado también puede aplicarse como entrada o insumo, reflejando los problemas de seguridad operacional en la explotación en todo el sistema aeronáutico del Estado derivados de la consolidación de los SPI del proveedor de servicios relativos a los riesgos de seguridad operacional en la explotación. Con frecuencia existirá una relación de uno a muchos entre un problema de seguridad operacional en la explotación y los SPI conexos. Es decir, un problema de ese tipo puede ser indicado por varios SPI.

b) **Riesgos de seguridad operacional en la implementación del proceso** (indicados en el lado derecho del diagrama). Se concentran en los medios y recursos necesarios para gestionar el riesgo de seguridad operacional en la explotación. La gestión del riesgo de seguridad operacional desde la perspectiva de la implementación del proceso se inicia con la evaluación de la situación de aplicación de los SARPS de la OACI (leyes y reglamentos nacionales relacionados con la seguridad operacional), la implementación de procesos SMS dentro de la industria, y la implementación del SSP a nivel del Estado (que incluye la vigilancia y observación eficaces de la industria). Si es necesario introducir mejoras en cualquiera de los anteriores, las actividades para lograrlo deberían planificarse, implementarse y observarse, y además asignarse recursos adecuados a las mismas. Los SPI se elaboran posteriormente para permitir el seguimiento de la planificación, implantación o eficacia de los cambios.

   Los SPI centrados en “riesgos de seguridad en la implementación del proceso” brindan al Estado un medio alternativo distinto del estricto cumplimiento para observar la adecuación de los arreglos institucionales del SMS y la implementación de procesos de SRM o aseguramiento de la seguridad operacional por parte de los proveedores de servicios. Estos SPI también pueden establecerse con referencia a las mejoras necesarias, como lo indiquen los análisis USOAP y las actividades de mejora continua del SSP. Los resultados de las auditorías del USOAP, la consolidación de evaluaciones SMS y la información sobre mejora continua del SSP determinarán posibles sectores que requieran mejoras. Estos deberían priorizarse con arreglo a los mayores beneficios que puedan obtenerse. Ello contribuirá también a mejorar el rendimiento en materia de seguridad operacional del sistema aeronáutico del Estado. Estos SPI deberían ser distintos de los SPI sobre riesgos de seguridad operacional en la explotación.

8.5.5.8 Los SPI para los riesgos de seguridad operacional en la explotación y en la implantación del proceso constituyen una parte fundamental del proceso de aseguramiento de la seguridad operacional del Estado. La consolidación de SPI sobre riesgos de seguridad operacional en la explotación y SPI de riesgos de seguridad operacional en la implementación del proceso amplía la fuente de información para establecer el ALoSP del Estado.

Examen periódico de los indicadores de rendimiento en materia de seguridad operacional

8.5.5.9 Es fundamental realizar exámenes periódicos una vez establecidos los SPI del Estado. Inicialmente, la identificación de los principales riesgos de seguridad operacional es una actividad apoyada por análisis basados en datos históricos. No obstante, el sistema aeronáutico es dinámico y en constante cambio. Pueden surgir nuevos problemas de seguridad operacional, pueden cambiar los procesos dentro del Estado, y así sucesivamente, el examen

periódico de los aspectos y procesos de seguridad operacional en la explotación por parte del Estado apoya la actualización y el perfeccionamiento de los objetivos del Estado en materia de seguridad operacional y en consecuencia los SPI y las SPT.

Examen periódico del ALoSP

8.5.5.10 El equipo de administración superior responsable del acuerdo ALoSP original debería determinar la adecuación continua del mismo. El examen periódico del ALoSP debería concentrarse en:

a) identificar problemas críticos para la seguridad operacional dentro de los sectores de la aviación, asegurando la inclusión de SPI que permitan la gestión de rendimiento en materia de seguridad operacional en esas áreas;

b) identificación de las SPT que definan el nivel de rendimiento en materia de seguridad operacional que debe mantenerse o la mejora deseada que ha de alcanzarse para el SPI pertinente de cada sector, con miras a mejorar la gestión del rendimiento en todo el sistema aeronáutico del Estado;

c) identificación de elementos activadores (si corresponde) cuando un SPI alcanza un punto que exija tomar medidas; y

d) examen de los SPI para determinar si es necesario introducir modificaciones o adiciones en los SPI, SPT y elementos activadores (si corresponde) existentes a efectos de alcanzar el ALoSP convenido.

8.5.5.11 Un resultado del examen periódico de los riesgos principales en el Estado es una mejor comprensión de carácter de cada problema de seguridad operacional con tanto detalle como lo permitan los datos. El Estado debería considerar sus peligros y sus posibles consecuencias en todos los niveles de su sistema aeronáutico. También debería analizar la forma en que los procesos estatales (otorgamiento de licencias, certificado, autorizaciones, aprobaciones, supervisión, etc.,) contribuyen a la SRM. Cada riesgo de seguridad operacional debe evaluarse para identificar las medidas de mitigación requeridas. Estas medidas se vigilan mediante los SPI que miden su eficacia.

8.5.5.12 El mejoramiento del rendimiento en materia de seguridad operacional respecto de esos riesgos tiende a ser reactivo, mientras que el mejoramiento de los procesos de gestión de los riesgos de seguridad operacional tiende a ser proactivo. El mejoramiento de los procesos estatales que mejor apoyan la gestión de los riesgos de seguridad operacional permite la identificación y control de peligros antes de que se manifiesten como resultados negativos.

Logro del ALoSP

8.5.5.13 El rendimiento del Estado en materia de seguridad operacional indicado por sus SPI y SPT demuestra el ALoSP alcanzado. Si algunas de las SPT no se alcanzan, puede ser necesario realizar una evaluación para comprender mejor los motivos de ello y determinar las medidas que deberían adoptarse. Lo anterior puede deberse a:

a) las metas no eran alcanzables o realistas;

b) las medidas adoptadas para alcanzar la meta no eran apropiadas o se apartaban de la intención original (desviación de la práctica);

c) cambios en otras prioridades de riesgos de seguridad operacional desviaron recursos respecto del logro de una meta determinada; o

d) surgieron riesgos emergentes que no se habían considerado cuando se establecieron las metas.

8.5.5.14 Para aquellas metas que no se alcanzaron, será necesario comprender el motivo y adoptar una decisión de gestión sobre si la mejora de la seguridad operacional es suficiente incluso si no se ha alcanzado la meta, y determinar si es necesario adoptar más medidas. Esto puede requerir análisis adicionales que podrían identificar algunos factores de riesgo que no se consideraron o quizás algunas mitigaciones implantadas que no son eficaces.

8.5.6 Gestión del cambio: perspectiva del Estado

8.5.6.1 En el Anexo 19 no se requiere explícitamente que los Estados establezcan actividades formales para la gestión de cambios en el marco de sus SSP. No obstante, los cambios son un hecho omnipresente en el sistema aeronáutico contemporáneo. Cuando se introducen cambios en un sistema, el panorama establecido de riesgos de seguridad operacional del mismo cambiará. Los cambios pueden introducir peligros con consecuencias para la eficacia de las defensas existentes. Ello podría resultar en un nuevo riesgo o en cambios en los riesgos de seguridad operacional existentes. Los Estados deberían evaluar y gestionar las consecuencias de los cambios en sus sistemas de aviación.

8.5.6.2 El SSP debería desarrollar procedimientos para evaluar las consecuencias de los cambios a nivel estatal. Los procedimientos deberían permitir que el Estado identifique en forma proactiva las consecuencias para la seguridad operacional de los cambios que se introduzcan en el sistema aeronáutico antes de implementarlos y planificar y ejecutar los cambios propuestos en forma estructurada.

8.5.6.3 Cuando se prevean cambios, el Estado debería analizar las consecuencias de los mismos respecto del sistema existente y, utilizando el proceso SRM vigente, analizar, evaluar y si es necesario mitigar cualquier riesgo de seguridad operacional tanto nuevo como alterado. Ninguna operación debería realizarse en un sistema o contexto operacional modificado hasta que se hayan evaluado todos los riesgos de seguridad operacional.

8.5.6.4 El Estado enfrentará dos tipos de cambio en el marco de su SSP: cambio institucional (por ejemplo, reasignación de responsabilidades o restructuración de las autoridades aeronáuticas del Estado) y cambio operacional (por ejemplo, un cambio en el uso del espacio aéreo). La gestión de los cambios en el marco del SSP debería concentrarse en aquellos cambios que podrían tener consecuencias significativas en la capacidad del Estado para cumplir sus obligaciones jurídicas (cambios de proceso) y en las capacidades estatales de gestión de la seguridad operacional. Esto podría comprender una combinación de procesos y cambios operacionales.

8.5.6.5 Entre los cambios que podrían tener consecuencias significativas para los riesgos de seguridad operacional del Estado figuran los siguientes:

a) reorganización de las autoridades de aeronáutica del Estado (incluyendo recortes en la plantilla);

b) cambios en los procesos SSP, incluyendo cambios de metodología como SRBS, SRM y procesos de aseguramiento de la seguridad operacional.

c) cambios en el entorno normativo, como cambios en las políticas, programas y reglamentos estatales de seguridad operacional existentes;

d) cambios en el entorno operacional, como la introducción de nuevas tecnologías, cambios en la infraestructura, equipo y servicios;

e) cambios rápidos en la industria (ampliación, reducción, fusión) y sus posibles consecuencias en las capacidades estatales de vigilancia y observación del rendimiento.

8.5.6.6 La comunicación de los cambios es fundamental para la eficacia de la gestión del cambio. Es esencial que el personal afectado dentro del Estado y de los proveedores de servicio involucrados estén bien conscientes del cambio en cuestión, su oportunidad y consecuencias.

8.6 COMPONENTE 4: PROMOCIÓN ESTATAL DE LA SEGURIDAD OPERACIONAL

8.6.1 Desde la perspectiva del Estado, la necesidad de implementar medidas de promoción de la seguridad operacional estatales tanto internas como externas está establecida en el Anexo 19 como uno de los componentes de las responsabilidades estatales en materia de gestión de la seguridad operacional. Internamente, las CAA y otras autoridades aeronáuticas involucradas en el SSP deberían establecer mecanismos para proporcionar información sobre seguridad operacional pertinente a su personal en apoyo de la creación de una cultura que fomente un SSP eficaz y eficiente. La comunicación de sus políticas y planes de seguridad operacional, así como de otra documentación SSP importante también puede mejorar la conciencia y la colaboración entre su personal, de modo que los procesos de gestión de la seguridad operacional implantados por los Estados sigan siendo eficaces.

8.6.2 La mejora del rendimiento en materia de seguridad operacional dentro de un Estado o de un sector aeronáutico específico depende en gran medida de su cultura de seguridad operacional. Las medidas relacionadas con la gestión de seguridad operacional tienden a ser más eficaces cuando la institución cuenta con una cultura positiva de seguridad operacional. Si están visiblemente apoyados por la administración superior y media, los empleados de primera línea tienden a experimentar un sentimiento de responsabilidad compartida respecto del logro de sus objetivos de seguridad operacional.

8.6.3 Entre otras medidas para mejorar la cultura de seguridad operacional dentro de un sistema aeronáutico, la necesidad de comunicación se destaca por su importancia. Mediante la constante comunicación de sus prioridades, mejores prácticas y riesgos que se destacan en una operación particular, el Estado puede fomentar una cultura de seguridad operacional positiva y maximizar la posibilidad de alcanzar sus objetivos de seguridad, ya sea entre los profesionales de las CAA o los proveedores de servicios. En el Capítulo 3 figuran más detalles sobre la cultura de seguridad operacional.

8.6.4 Una vez que los empleados aceptan y comprendan sus responsabilidades respecto del rendimiento en materia de seguridad operacional, se espera que procuren activamente obtener medios de información que puedan utilizar para el cumplimiento eficaz de sus responsabilidades para con una aviación segura. Esto constituye una oportunidad para que la promoción de la seguridad operacional desempeñe una función fundamental en la gestión de la misma. Externamente, el establecimiento de canales de comunicación con los proveedores de servicios debería permitir la compartición de las enseñanzas obtenidas, mejores prácticas, SPI y el suministro de información sobre riesgos de seguridad operacional específicos. Ello debería apoyar la implementación de prácticas de gestión de la seguridad operacional en los proveedores de servicios, así como el desarrollo de una cultura de seguridad operacional positiva entre organizaciones similares. Además, el establecimiento de actividades de comunicación rutinarias con los proveedores de servicios puede aumentar la conciencia general sobre los problemas de seguridad operacional de la aviación y fomentar una mayor colaboración en la identificación de iniciativas para mejorar la misma.

8.6.5 A medida que los Estados tomen decisiones o medidas para mejorar la seguridad operacional de la aviación (p. ej., establecimiento de reglamentos o implementación de cambios en los métodos de vigilancia) también es importante que se comuniquen en forma interna así como externa. Esto puede fortalecer la percepción del compromiso del Estado en toda la comunidad aeronáutica. Ello a su vez puede contribuir al logro de los objetivos de seguridad operacional del Estado.

8.6.6 Existen muchos recursos e instrumentos para apoyar a los Estados en el establecimiento de sus medidas de promoción de la seguridad operacional. Una forma de estructurar las muchas medidas de promoción que el Estado puede adoptar es el establecimiento de un plan de comunicaciones. Dicho plan podría incluir, como mínimo, la presentación de miembros interesados de la comunidad aeronáutica, los mensajes y la información transmitidos a cada uno de sus grupos y los medios por los cuales se transmitirá dicha información. El plan de comunicación también puede hacer las veces de una hoja de ruta en apoyo de la CAA para el desarrollo eficaz de capacidad y canales de comunicación con estos públicos internos y externos. Esto puede ser de gran importancia para los Estados en la construcción de la cultura de seguridad operacional así como para proporcionar los datos e instrumentos necesarios requeridos para la gestión exitosa de la seguridad operacional, tanto desde la perspectiva de los Estados como la de los proveedores de servicios.

8.6.7 Alguna información puede comunicarse mediante boletines y publicaciones menos formales utilizando los medios sociales, mientras que otros tipos de información se tratan de mejor manera en reuniones o seminarios especiales. Es función del Estado implementar los canales de promoción de la seguridad operacional adecuados y los medios que, en su opinión, alcanzarán los mejores resultados para desarrollar una cultura de seguridad operacional positiva dentro del Estado y, en última instancia, lograr un SSP eficaz y un sistema de aviación civil más seguro en el ámbito estatal.

8.6.8 Comunicación y divulgación internas de la información sobre seguridad operacional

Nota.— La información sobre seguridad operacional obtenida de los sistemas de notificación voluntaria de seguridad operacional estará protegida, a menos que se aplique un principio de protección. Esto puede ampliarse a la información en la materia obtenida de sistemas de notificación obligatoria. En el Capítulo 7 figuran más detalles sobre la protección de datos e información sobre seguridad operacional y fuentes conexas.

8.6.8.1 Las medidas y publicaciones de promoción de la seguridad operacional también pueden mejorar la coordinación y la colaboración entre diferentes organizaciones involucradas en la vigilancia de la seguridad operacional dentro del Estado. El documento SSP y sus políticas estatales conexas sobre seguridad operacional y cumplimiento resultan fundamentales para lograr la integración de la instrucción, la comunicación y la difusión de la información conexa. Las autoridades normativas del Estado responsables de los diferentes sectores de la aviación así como otras entidades administrativas independientes como la AIA deberían adoptar un enfoque integrado de sus respectivas funciones en la promoción estatal de la seguridad operacional. Los Estados deberían establecer canales de comunicación formales entre los miembros del grupo de coordinación del SSP (entidades estatales involucradas en la implementación y mantenimiento del SSP).

8.6.8.2 Desde el punto de vista operacional, es importante que las estrategias operacionales del SSP, incluyendo requisitos SMS armonizados y observación de los respectivos proveedores de servicios se compartan, comuniquen y coordinen entre las autoridades aeronáuticas del Estado. Un canal de comunicación abierto puede evitar la creación de requisitos SMS contradictorios o criterios de aceptación conflictivos para diferentes sectores de la aviación.

8.6.8.3 Entre los ejemplos de la información que los Estados deberían abordar en su comunicación y difusión internas figuran los siguientes:

a) documentación, políticas y procedimientos relativos al SSP;

b) SPI;

c) información sobre rendimiento en materia de seguridad operacional del sector;

d) perfiles de riesgos de seguridad operacional institucionales del sector;

e) comunicación de responsabilidades de seguridad operacional del sistema;

f) enseñanzas obtenidas de accidentes e incidentes; y

g) conceptos y mejores prácticas de gestión de la seguridad operacional.

8.6.8.4 Es particularmente necesario contar con líneas abiertas de comunicación de seguridad operacional cuando los proveedores de servicios son aprobados por más de un Estado.

8.6.8.5 Existen varios medios que las organizaciones estatales pueden adoptar para transmitir comunicaciones de seguridad operacional como circulares, boletines, folletos, publicaciones, seminarios, reuniones, instrucción, sitios web, listas de distribución, publicación en medios sociales, debates en grupos de colaboración, entre otros.

8.6.8.6 Al evaluar el tipo de medio que debería utilizarse para dar a conocer un mensaje particular, la organización debería considerar el que sea más apropiado para cada mensaje y su público destinatario. Los documentos SSP pueden publicarse en un sitio web que ya esté disponible al personal cuando sean necesarios. Otra información como las enseñanzas obtenidas y mejores prácticas puede resultar más adecuada para boletines o circulares informativas periódicos.

8.6.8.7 El establecimiento de campañas para tratar una preocupación o peligro particular utilizando múltiples medios puede resultar eficaz para aumentar la conciencia general sobre el problema y modificar actitudes del personal.

8.6.9 Comunicación y difusión externas de la información sobre seguridad operacional

8.6.9.1 Los Estados deberían establecer plataformas o medios de comunicación apropiados para facilitar la implementación del SMS y mejorar la cultura de seguridad operacional de todo el sistema.

8.6.9.2 Al comunicar y difundir externamente información sobre seguridad operacional a la industria de aviación, además de los aspectos indicados en la sección anterior, los Estados también podrían considerar la inclusión de:

a) textos de orientación para la implementación del SMS;

b) importancia de las notificaciones;

c) identificar de instrucción de seguridad operacional disponible para la comunidad aeronáutica;

d) promoción del intercambio de información de seguridad operacional:

1) con y entre los proveedores de servicios; y

2) entre los Estados.

8.6.9.3 La documentación estatal sobre el SSP y sus políticas conexas de seguridad operacional y cumplimiento también deberían ponerse a disposición de los proveedores de servicio según corresponda.

8.6.9.4 Esencialmente los mismos medios de apoyo utilizados para las comunicaciones internas pueden emplearse externamente en la medida en que su contenido resulte útil para ambos públicos. No obstante, para las comunicaciones externas, puede prestarse atención especial a las soluciones que alcanzan a públicos más amplios como los medios sociales, listas de correo, boletines, seminarios, creación de comunidades en la industria para el intercambio de información de seguridad operacional, multiplicando así el alcance de los mensajes.

8.6.9.5 Los Estados deberían promover el establecimiento de redes de compartición e intercambio de información sobre seguridad operacional entre la comunidad aeronáutica, a menos que la ley nacional disponga otra cosa.

8.7 IMPLEMENTACIÓN DEL SSP

Al igual que con cualquier implementación de un proyecto importante, la implementación del SSP involucra muchas tareas y subtareas que han de completarse dentro de un marco temporal establecido. El número de tareas, así como el alcance de cada una, depende del grado de madurez del sistema estatal de vigilancia de la seguridad operacional. En la mayoría de los casos, varias organizaciones y entidades están involucradas en la elaboración e implementación de un SSP. La elaboración de un plan de implementación puede contribuir a facilitar este proceso. En este capítulo se presentan las etapas para elaborar una descripción completa del sistema, consideraciones relativas a la modificación y adaptación, realización de análisis de brecha y desarrollo de un plan de implementación que incluya las garantías de que se ha establecido una sólida base para el SSP. En esta sección también se trata la evaluación continua del grado de madurez de un SSP.

8.7.1 Descripción y consideraciones sobre crecimiento y adaptación del sistema estatal de aviación civil

8.7.1.1 La comprensión del volumen y complejidad del sistema de aviación del Estado asi como de las interacciones entre los elementos resulta fundamental para planificar el SSP. El Estado debe implementar un SSP, pero la forma en que los requisitos pertinentes se satisfacen dependerá del volumen y complejidad del sistema aeronáutico. En el Capítulo 1 figura más información sobre la capacidad de crecimiento y adaptación.

8.7.1.2 El SSP también deberá considerar varios proveedores de servicios en cada dominio aeronáutico, así como su volumen y complejidad y entorno regional. Los Estados con pocos proveedores de servicios deberían considerar el establecimiento de asociaciones regionales. Estas asociaciones regionales con otros Estados o a través de las RSOO y la compartición de enseñanzas obtenidas e información de riesgos de seguridad operacional minimizarán las consecuencias adversas maximizando al mismo tiempo las ventajas de la implementación del SSP.

8.7.1.3 El Estado debería presentar el sistema de aviación y las diversas autoridades aeronáuticas estatales en una descripción de su sistema de aviación civil. Esto debería incluir un panorama general de las estructuras institucionales y sus interfaces. Esto es parte del proceso de planificación de la implementación del SSP. Dicho examen debería incluir una descripción de los siguientes aspectos:

a) estructura del marco normativo aeronáutico existente, incluyendo las diversas autoridades aeronáuticas del Estado;

b) funciones y obligaciones de rendición de cuentas de la gestión de la seguridad operacional para las diversas autoridades normativas;

c) plataforma o mecanismo para coordinar el SSP entre las organizaciones; y

d) un mecanismo interno de examen a nivel estatal y dentro de cada organización.

8.7.2 Análisis de brechas y plan de implementación del SSP

Análisis de brechas del SSP

8.7.2.1 Debería realizarse un análisis de brechas antes de elaborar un plan para la implementación del SSP. El análisis de brechas tiene por objeto obtener una comprensión detallada de las diferencias entre las estructuras y procesos estatales existentes, y las necesarias para una implementación eficaz del SSP en el Estado. Para muchos Estados, el análisis de brechas revela que existe ya una considerable capacidad de la gestión de la seguridad operacional. Normalmente, el reto consiste en refinar, adaptar y fomentar estas capacidades existentes. Los elementos o procesos identificados como acciones requeridas constituyen la base del plan de implementación del SSP.

Fundamentos del SSP

8.7.2.2 Es esencial que los Estados establezcan un fundamento maduro para apoyar la eficaz implementación del SSP. Los objetivos del GASP piden que los Estados implementen gradualmente sistemas eficaces de vigilancia de la seguridad operacional, SSP y capacidades avanzadas de gestión de la seguridad operacional necesarias para apoyar futuros sistemas de aviación. Estos fundamentos están integrados por los aspectos de un sistema de vigilancia de la seguridad operacional necesarios para apoyar un enfoque más basado en el rendimiento.

8.7.2.3 Los datos recopilados a través del Programa universal de auditorías de la vigilancia de la seguridad operacional (USOAP) de la OACI pueden utilizarse para identificar deficiencias en estos fundamentos. El tratamiento de cualesquiera preguntas del protocolo USOAP insatisfactorias relativas a problemas relacionados con la implementación eficaz del SSP (p. ej., sistemas de notificación obligatoria) debería constituir una primera etapa en la implantación del SSP.

Plan de implementación del SSP

8.7.2.4 La implementación del SSP tiene por objeto mejorar en forma gradual los procesos de SSO y gestión de la seguridad operacional existentes. Las tareas y subtareas apropiadas están priorizadas y documentadas en un plan de acción. El plan de implementación del SSP, conjuntamente con el documento SSP de alto nivel (exposición), proporcionan los "modelos" que orientan el avance del Estado hacia un SSP eficaz y la continua mejora del rendimiento en materia de seguridad operacional. Estos dos documentos clave deberían ser de fácil acceso para todo el personal pertinente a efectos de asegurar que todos los involucrados son conscientes del SSP y sus planes para implementación.

8.7.3 Evaluación del grado de madurez del SSP

Antecedentes y propósito

8.7.3.1 La evaluación del grado de madurez del SSP debería realizarse utilizando una herramienta que refleje los SARPS y textos de orientación de la OACI, elaborada por el Estado para satisfacer sus necesidades. Los Estados deberían utilizar dicha herramienta para realizar auditorías internas de la continua mejora del SSP. También la OACI y otras entidades externas deberían considerarla apropiada. La herramienta debería basarse en una serie de cuestiones (o expectativas) que puedan ser aplicadas por el Estado para evaluar la eficacia de su SSP. La evaluación del grado de madurez del SSP se beneficiará de interacciones, como debates y entrevistas individuales, con una muestra representativa de todas las partes interesadas. La herramienta en cuestión debería ser flexible y tener en cuenta el volumen y complejidad del sistema aeronáutico del Estado.

Evaluación

8.7.3.2 Una vez instalados los aspectos básicos del SSP, puede realizarse una evaluación de la documentación. Dicha evaluación tiene por objeto descubrir si las expectativas del cumplimiento y rendimiento del SSP están presentes y resultan adecuadas. Deberían recopilarse pruebas para apoyar la evaluación en cuestión. En una etapa posterior, se podrá evaluar el SSP para determinar cuán bien está funcionando y cuán eficaz es en cuanto al logro de sus objetivos. La eficacia se alcanza cuando se consiguen los resultados deseados cada vez. Normalmente, un equipo con competencia y experiencia técnica en ese SSP apropiadas lleva a cabo la evaluación y recopila las pruebas. Es importante estructurar la evaluación de forma que permita la interacción con varias personas en diferentes niveles de la organización para determinar la eficacia a través de la misma. Por ejemplo, la determinación del grado en que la política de seguridad operacional ha sido promulgada y comprendida por el personal exigirá interacciones con una muestra representativa del mismo.

Observación y mejora continuas

8.7.3.3 El Estado puede utilizar la misma herramienta para evaluar la eficacia de su SSP durante la observación y mejora continuas. La evaluación probablemente identificará cambios al sistema aeronáutico. Para la mayoría de los Estados, la implantación del SSP llevará tiempo, así como varios años para alcanzar el nivel de madurez en que todos los elementos funcionen eficazmente. En la Figura 8-5 se ilustran los diferentes niveles de madurez del SSP a medida que el Estado implementa y elabora su programa.

8.7.3.4 La evaluación del SSP puede realizarse en diversas etapas, examinando inicialmente la presencia y adecuación de los elementos clave. En una etapa posterior, el SSP puede evaluarse para comprender cuan bien está funcionando y cuan eficaz es en el logro de sus objetivos. Los Estados pueden continuar realizando evaluaciones periódicas en apoyo de la mejora continua para lograr la excelencia.

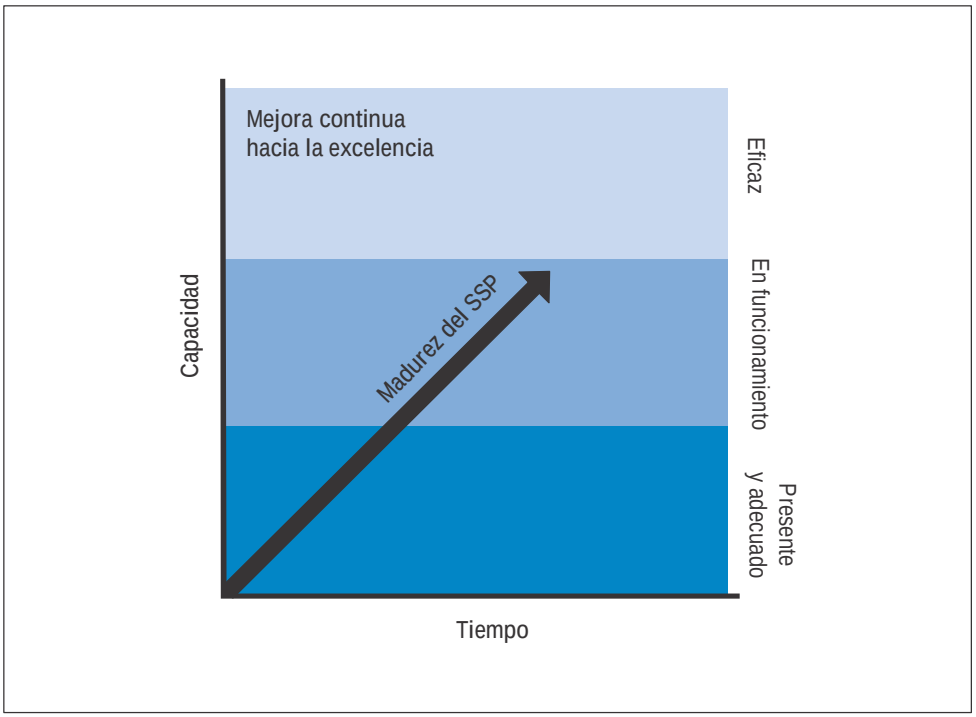


Figura 8-5. Grado de madurez del SSP

Capítulo 9

SISTEMAS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

9.1 INTRODUCCIÓN

9.1.1 En este capítulo se proporciona orientación para los proveedores de servicios sobre la implantación de un marco para el SMS con arreglo al Anexo 19, así como orientación para los Estados sobre la vigilancia del SMS.

9.1.2 La finalidad de un SMS es proporcionar a los proveedores de servicios un enfoque sistemático para gestionar la seguridad operacional. Está diseñado para mejorar continuamente la seguridad operacional mediante la identificación de peligros, la recopilación y el análisis de datos y la evaluación continua de los riesgos de la seguridad operacional. El SMS procura contener o mitigar proactivamente los riesgos de seguridad operacional antes de que produzcan accidentes e incidentes de aviación. El sistema permite que los proveedores de servicios gestionen eficazmente sus actividades, su rendimiento en materia de seguridad operacional y sus recursos, logrando, al mismo tiempo, una mayor comprensión de su contribución a la seguridad operacional de la aviación. Un SMS eficaz demuestra a los Estados la capacidad del proveedor de servicios para gestionar riesgos de seguridad operacional y contempla también la eficaz gestión de la seguridad operacional a nivel estatal.

9.1.3 Los explotadores de la aviación general internacional deberían determinar los criterios SMS para las aeronaves que operan, como lo establece el Estado de matrícula, y asegurar que sus SMS son aceptables para dicho Estado. A efectos de facilitar la aceptabilidad del SMS, los explotadores de la aviación general internacional deberían preguntar al Estado de matrícula si se permite el uso de un código de práctica de la industria.

9.1.4 Los explotadores de aviones grandes o turborreactores con múltiples Estados de matrícula a los que se ha expedido un AOC con arreglo al Anexo 6, Parte I, se consideran como proveedores de servicios y, por ello, el SMS debe ser aceptable para el Estado del explotador.

9.2 MARCO PARA EL SMS

9.2.1 En el Anexo 19 se especifica el marco para la implantación y mantenimiento de un SMS. Independientemente de la envergadura y complejidad del proveedor de servicios, se aplican todos los elementos de dicho marco para el SMS. La implementación debería adaptarse a la organización en cuestión y sus actividades.

9.2.2 El marco de la OACI para el SMS está integrado por los siguientes cuatro componentes y doce elementos:

Tabla 10. Componentes y elementos del marco de la OACI para el SMS

COMPONENTE	*ELEMENTO*
1. Políticas y objetivos de seguridad operacional	1.1 Compromiso de la administración
	1.2 Obligación de rendición de cuentas sobre la seguridad operacional y responsabilidades
	1.3 Designación del personal clave de seguridad operacional
	1.4 Coordinación de la planificación de respuestas 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. Aseguramiento de la seguridad operacional	3.1 Observación y medición del rendimiento en materia de 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

9.3 COMPONENTE 1: POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

9.3.1 El primer componente del marco SMS se concentra en la creación de un entorno en el que la gestión de seguridad operacional pueda resultar eficaz. Se basa en una política y objetivos de seguridad operacional que establecen el compromiso de la administración superior con respecto a la seguridad operacional, sus objetivos y la estructura institucional de apoyo.

9.3.2 El compromiso y el liderazgo de la administración en materia de seguridad operacional son fundamentales para la implementación de un SMS eficaz y se afirman mediante la política de seguridad operacional y el establecimiento de objetivos en la materia. El compromiso de la administración respecto de la seguridad operacional se demuestra mediante la toma de decisiones de la administración y la asignación de recursos; estas decisiones y medidas deberían ser siempre coherentes con la política y objetivos de seguridad operacional a efectos de desarrollar una cultura de seguridad operacional positiva.

9.3.3 La política de seguridad operacional debería ser desarrollada y apoyada por la administración superior y llevar la firma de un ejecutivo responsable. El personal clave de seguridad operacional y, cuando corresponda, los órganos representativos del personal (foros de empleados, sindicatos) deberían consultarse para la elaboración de una política de seguridad operacional y sus objetivos a efectos de promover un sentido de responsabilidad compartida.

9.3.4 Compromiso de la administración

Política de seguridad operacional

9.3.4.1 La política de seguridad operacional debería ser respaldada visiblemente por la administración superior y por el ejecutivo responsable. El “respaldo visible” se refiere a que el apoyo activo de la política de seguridad operacional por parte de la administración sea visible para el resto de la organización. Esto puede hacerse a través de cualesquiera medios de comunicación y la correspondencia de las actividades con la política de seguridad operacional.

9.3.4.2 Es responsabilidad de la administración comunicar la política de seguridad operacional a toda la organización para asegurar que todo el personal comprende y trabaja con arreglo a dicha política.

9.3.4.3 Para reflejar el compromiso de la organización respecto de la seguridad operacional, la política debería comprender el compromiso de:

a) mejorar continuamente el nivel del rendimiento en materia de seguridad operacional;

b) promover y mantener una cultura de seguridad operacional positiva dentro de la organización;

c) cumplir todos los requisitos normativos aplicables;

d) proporcionar los recursos necesarios para entregar un producto o servicio seguro;

e) garantizar que la seguridad operacional es una responsabilidad principal de todos los administradores; y

f) garantizar que esta se comprende, implementa y mantiene a todos los niveles.

9.3.4.4 La política de seguridad operacional también debería hacer referencia al sistema de notificación de seguridad operacional para fomentar la notificación de problemas de seguridad operacional e informar al personal respecto de la política disciplinaria aplicada en caso de sucesos o problemas de seguridad operacional que se notifiquen.

9.3.4.5 La política disciplinaria se aplica para determinar si ha ocurrido un error o una infracción de reglamentos de modo que la organización pueda establecer si debería adoptarse alguna medida disciplinaria. Para asegurar el justo tratamiento de las personas involucradas, es fundamental que los responsables de adoptar dicha determinación cuenten con la necesaria experiencia técnica de modo que pueda considerarse plenamente el contexto del suceso en cuestión.

9.3.4.6 Una política sobre la protección de datos e información sobre seguridad operacional, así como de las personas que los notifiquen, puede tener un efecto positivo en la cultura de notificación. El proveedor de servicios y el Estado deberían abordar el anonimato y la recopilación de informes para permitir la realización de análisis de seguridad operacional significativos sin tener que implicar al personal o a proveedores de servicios específicos. Debido a que los sucesos de mayor envergadura pueden involucrar procesos y procedimientos fuera del SMS del proveedor de servicios, la autoridad estatal pertinente podría no permitir la temprana no identificación de las notificaciones en todas las circunstancias. Sin embargo, una política que permita el apropiado anonimato de las notificaciones puede mejorar la calidad de los datos recopilados.

Objetivos de seguridad operacional

9.3.4.7 Teniendo en cuenta su política de seguridad operacional, el proveedor de servicios debería también establecer objetivos de seguridad operacional para definir aquello que procura obtener con respecto a resultados en la materia. Los objetivos de seguridad operacional deberían ser declaraciones breves y de alto nivel de las prioridades de seguridad operacional de la organización y deberían abordar sus riesgos de seguridad más importantes. Los objetivos de seguridad operacional pueden incluirse en la política de seguridad operacional (o documentarse por separado), y definen lo que la organización procura obtener en términos de seguridad. Los indicadores de rendimiento en materia de seguridad operacional (SPI) y las metas de rendimiento en materia de seguridad operacional (SPT) son necesarios para vigilar el logro de esos objetivos y se tratarán más adelante en este capítulo en el marco del Componente 3.

9.3.4.8 La política y los objetivos de seguridad operacional deberían revisarse periódicamente para asegurar que permanecen vigentes (por ejemplo, un cambio de ejecutivo responsable requeriría este tipo de revisión).

9.3.5 Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional

Ejecutivo responsable

9.3.5.1 El ejecutivo responsable, (normalmente el funcionario ejecutivo principal) es la persona que tiene la responsabilidad final del funcionamiento seguro de la organización. El ejecutivo responsable establece y promueve la política y los objetivos de seguridad operacional que inculcan dicha seguridad como uno de los valores principales de la institución. El ejecutivo responsable debería tener autoridad para tomar decisiones en nombre de la organización, controlar los recursos, tanto financieros como humanos, ser responsable de asegurar que se adoptan medidas apropiadas para enfrentar problemas y riesgos de seguridad operacional y también ser responsable de responder ante accidentes e incidentes.

9.3.5.2 El proveedor de servicios podría encontrar dificultades en identificar la persona más apropiada para designar como ejecutivo responsable, especialmente en grandes organizaciones complejas con múltiples entidades y varios certificados, autorizaciones o aprobaciones. Es importante que la persona seleccionada esté situada al más alto nivel de la organización, asegurando así que se adoptan las decisiones estratégicas correctas en materia de seguridad operacional.

9.3.5.3 El proveedor de servicios debe identificar al ejecutivo responsable, colocando la responsabilidad del rendimiento general en materia de seguridad operacional en un nivel de la organización con autoridad para adoptar medidas a efectos de asegurar la eficacia del SMS. Deberían definirse las líneas de responsabilidad específicas de todos los miembros de la administración y sus funciones en relación con el SMS deberían reflejar la forma en que pueden contribuir hacia una cultura de seguridad operacional positiva. La obligación de rendición de cuentas, las responsabilidades y las atribuciones de seguridad operacional deberían documentarse y comunicarse en toda la organización. La obligación de rendición de cuentas en materia de seguridad operacional de los administradores debería incluir también la asignación de los recursos humanos, técnicos, financieros o de otro tipo para el funcionamiento eficaz y eficiente del SMS.

Nota.— El concepto de "obligación de rendición de cuentas" se refiere a las obligaciones que no pueden delegarse y "responsabilidades" se refiere a las funciones y actividades que pueden delegarse.

9.3.5.4 En el caso en que un SMS se aplique a varios y diferentes certificados, autorizaciones o aprobaciones que son parte de la misma entidad jurídica, debería haber un único ejecutivo responsable. Cuando ello no es posible, deberían identificarse ejecutivos responsables individuales para cada certificado, autorización o aprobación institucional y definirse claramente las líneas de obligación de rendición de cuentas. También es importante determinar la forma en que dichas obligaciones en materia de seguridad operacional se coordinarán.

9.3.5.5 Una de las formas más efectivas en que el ejecutivo responsable puede involucrase visiblemente, es mediante la conducción de reuniones periódicas de ejecutivos sobre seguridad operacional. En su carácter de responsable final de la seguridad operacional de la organización, una participación activa en dichas reuniones permite al ejecutivo responsable:

a) revisar los objetivos de seguridad operacional;

b) observar el rendimiento en materia de seguridad operacional y el logro de las metas en la materia;

c) adoptar decisiones de seguridad operacional oportunas;

d) asignar recursos apropiados;

e) establecer la obligación de rendir cuentas de los administradores en cuanto a sus responsabilidades, rendimiento y cronogramas de implementación de la seguridad operacional; y

f) hacer que todo el personal lo perciba como un ejecutivo interesado en la seguridad operacional y a cargo de la misma.

9.3.5.6 El ejecutivo responsable no participa normalmente en las actividades cotidianas de la organización o en los problemas que se encuentren en el lugar de trabajo y debería asegurar que existe una estructura institucional apropiada para gestionar y operar el SMS. A menudo, la responsabilidad de la gestión de la seguridad operacional se delega en un equipo de administración superior y otro personal de seguridad operacional. Si bien la responsabilidad del funcionamiento cotidiano del SMS puede delegarse, el ejecutivo responsable o puede delegar la obligación de rendir cuentas respecto del sistema ni las decisiones con respecto a los riesgos de seguridad operacional. Por ejemplo, las siguientes obligaciones de rendir cuentas en materia de seguridad operacional no pueden delegarse:

a) asegurar que las políticas de seguridad operacional son apropiadas y se comunican;

b) asegurar la necesaria asignación de recursos (financieros, personal, instrucción, adquisición); y

c) establecimiento de límites aceptables de los riesgos de seguridad operacional y asignación de recursos para los controles necesarios.

9.3.5.7 Es apropiado que el ejecutivo responsable tenga las siguientes obligaciones de rendición de cuentas en materia de seguridad operacional:

a) proporcionar suficientes recursos financieros y humanos para la implementación adecuada de un SMS eficaz;

b) promover una cultura de seguridad operacional positiva;

c) establecer y promover la política de seguridad operacional;

d) establecer los objetivos de seguridad operacional de la organización;

e) asegurar que el SMS está adecuadamente implantado y funciona con arreglo a los requisitos; y

f) velar por la mejora continua del SMS.

9.3.5.8 Entre las atribuciones del ejecutivo responsable figuran la autoridad final:

a) para resolver todos los problemas de seguridad operacional; y

b) respecto de las operaciones abarcadas por el certificado, autorización o aprobación de la organización, incluyendo la autoridad para detener una operación o actividad.

9.3.5.9 Debería definirse la autoridad para tomar decisiones respecto de la tolerabilidad de los riesgos de seguridad operacional. Esto comprende las personas que pueden tomar decisiones sobre la aceptabilidad de los riesgos así como la autoridad para convenir en que pueda implementarse un cambio. La autoridad puede asignarse a un individuo, a un cargo administrativo o a un comité.

9.3.5.10 La autoridad de tomar decisiones respecto de la tolerabilidad de los riesgos de seguridad operacional debería corresponder a la autoridad general del administrador para tomar decisiones y asignar recursos. Puede autorizarse a un administrador de nivel inferior (o grupo de gestión) a tomar decisiones sobre tolerabilidad hasta un cierto nivel. Los niveles de riesgo que excedan la autoridad del administrador deben elevarse a la consideración de un estrato superior de la administración con mayor autoridad.

Obligación de rendir cuentas y responsabilidades en materia de seguridad operacional

9.3.5.11 Deberían definirse claramente las obligaciones de rendición de cuentas y las responsabilidades de todo el personal, tanto directivo como de plantilla, involucrado en tareas relacionadas con la seguridad operacional del suministro seguro de productos y operaciones. Las responsabilidades de seguridad operacional deberían concentrarse

en la contribución del personal al rendimiento en materia de seguridad operacional de la organización (resultados de seguridad operacional institucionales). La gestión de la seguridad operacional es una función principal y como tal todo administrador superior tiene un cierto grado de participación en el funcionamiento del SMS.

9.3.5.12 Todas las obligaciones de rendición de cuentas, responsabilidades y atribuciones deberían establecerse en la documentación SMS del proveedor de servicios y comunicarse a toda la organización. La obligación de rendir cuentas en materia de seguridad operacional y las responsabilidades correspondientes de cada administrador superior son componentes integrales de la descripción de sus puestos. Estas también deberían reflejar la diferencia de las funciones de gestión de la seguridad operacional entre los gerentes de línea y el gerente de seguridad operacional (véase 9.3.6 por más detalles).

9.3.5.13 Las líneas de obligación de rendición de cuentas en materia de seguridad operacional en toda la organización y la forma en que se definen dependerán del tipo y complejidad de la misma, así como de sus métodos de comunicación preferidos. Normalmente, las obligaciones de rendir cuentas y las responsabilidades se reflejarán en los organigramas, documentos que definen responsabilidades de los departamentos y descripciones de puestos o funciones del personal.

9.3.5.14 El proveedor de servicios debería tratar de evitar conflictos de intereses entre las responsabilidades de seguridad operacional del personal y sus otras responsabilidades institucionales. Se deberían asignar las obligaciones de rendir cuentas y las responsabilidades relativas al SMS en una forma que minimice superposiciones o brechas.

Obligación de rendir cuentas y responsabilidades respecto de organizaciones externas

9.3.5.15 El proveedor de servicios es responsable del rendimiento en materia de seguridad operacional de las organizaciones externas cuando hay interfaz con el SMS. El proveedor de servicios puede tener que rendir cuentas por el rendimiento en materia de seguridad operacional de los productos o servicios proporcionados por organizaciones externas en apoyo de sus actividades, incluso si no se requiere que estas organizaciones tengan un SMS. Es fundamental que el SMS del proveedor de servicios tenga una interfaz con los sistemas de seguridad operacional de las organizaciones externas que contribuyen al suministro seguro de sus productos o servicios.

9.3.6 Designación de personal clave de seguridad operacional

9.3.6.1 La designación de una o varias personas para la función de gerente de seguridad operacional es fundamental para la implementación y funcionamiento eficaces del SMS. El gerente de seguridad operacional puede identificarse con diferentes nombres en las organizaciones, pero para el propósito de este manual, se utilizará el término “gerente de seguridad operacional” con referencia a la función, y no necesariamente al individuo. La persona que realiza la función de gerente de seguridad operacional es responsable ante el ejecutivo responsable del rendimiento del SMS y de la prestación de los servicios de seguridad operacional a los demás departamentos de la organización.

9.3.6.2 El gerente de seguridad operacional asesora al ejecutivo responsable y a los gerentes de línea respecto de asuntos de gestión de la seguridad operacional, y es responsable de coordinar y comunicar los problemas de seguridad operacional dentro de la organización así como con los miembros externos de la comunidad aeronáutica. Entre las funciones de gerente de seguridad operacional figuran las siguientes:

a) gestionar el plan de implementación del SMS en nombre del ejecutivo responsable (después de la implantación inicial);

b) realizar o facilitar la identificación de peligros y el análisis de riesgos de seguridad operacional;

c) controlar las medidas correctivas y evaluar sus resultados;

d) proporcionar informes periódicos sobre el rendimiento en materia de seguridad operacional de la organización;

e) mantener registros y documentación de seguridad operacional;

f) planificar y facilitar la capacitación en seguridad operacional del personal;

g) proporcionar asesoramiento independiente sobre asuntos de seguridad operacional;

h) controlar las preocupaciones de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones de la organización orientadas a la entrega de servicios; y

i) coordinar y comunicarse (en nombre del ejecutivo responsable) con la CAA del Estado y otras entidades estatales, según sea necesario, sobre temas relacionados con la seguridad operacional.

9.3.6.3 En la mayoría de las organizaciones, se designa a un individuo como gerente de seguridad operacional. Dependiendo de la envergadura, características y complejidad de la organización, la función de gerente de seguridad operacional puede ser de carácter exclusivo o puede combinarse con otras tareas. Además, algunas organizaciones pueden tener que adjudicar la función a un grupo de personas. La institución debe asegurarse de que la opción escogida no resulte en conflictos de intereses. Siempre que sea posible, el gerente de seguridad operacional no debería involucrarse directamente en la entrega de productos o servicios pero debería tener conocimientos prácticos de los mismos. La designación también debería considerar posibles conflictos de intereses con otras tareas y funciones. Dichos conflictos podrían incluir:

a) competencia para el logro de financiación (p. ej., si el gerente financiero es el gerente de seguridad operacional);

b) prioridades conflictivas para la obtención de recursos; y

c) los casos en que el gerente tiene una función operacional y puede evaluar la eficacia respecto del SMS de las actividades operacionales en que está involucrado.

9.3.6.4 En los casos en que la función se asigne a un grupo de personas (p. ej., cuando los proveedores de servicios amplían su SMS para abarcar múltiples actividades) debería designarse una persona como gerente de seguridad operacional “principal”, a efectos de mantener una línea de notificación directa e inequívoca hacia el ejecutivo responsable.

9.3.6.5 Entre las competencias del gerente de seguridad operacional figuran las siguientes:

a) experiencia en gestión de la seguridad operacional/calidad;

b) experiencia operacional relacionada con el producto o servicio proporcionado por la organización;

c) antecedentes técnicos para comprender los sistemas que respaldan las operaciones o los productos a servicios proporcionados;

d) habilidades para relacionarse con las personas;

e) habilidades analíticas y de solución de problemas;

f) habilidades de gestión de proyectos;

g) habilidades de comunicación oral y escrita; y

h) comprensión de los factores humanos.

9.3.6.6 Dependiendo de la envergadura, características y complejidad de la organización, puede ser necesario contar con personal adicional para respaldar al gerente de seguridad operacional. El gerente de seguridad operacional y el personal de apoyo son responsables de asegurar la rápida recopilación y análisis de datos de seguridad operacional y la apropiada distribución dentro de la organización de la información sobre seguridad operacional conexa de modo que puedan adoptarse decisiones sobre riesgos de seguridad operacional y medidas de control, según sea necesario.

9.3.6.7 Los proveedores de servicios deberían establecer comités de seguridad operacional apropiados que respalden las funciones SMS en toda la organización. Esto debería comprender la determinación de quienes deberían integrar el comité de seguridad operacional y la frecuencia de las reuniones de éste.

9.3.6.8 El comité de seguridad operacional de mayor nivel, denominado a veces consejo de revisión de seguridad operacional (SRB), está integrado por el ejecutivo responsable y los administradores superiores participando como asesor el gerente de seguridad operacional. El SRB tiene carácter estratégico y trata de asuntos de alto nivel relacionados con las políticas de seguridad operacional, asignación de recursos y rendimiento de la organización. El SRB controla:

a) la eficacia del SMS;

b) la adopción oportuna de cualquier medida de control de riesgos de seguridad operacional que sean necesarias;

c) el rendimiento en materia de seguridad operacional en comparación con la política y los objetivos de seguridad operacional de la organización;

d) la eficacia general de las estrategias de mitigación de riesgos de seguridad operacional;

e) la eficacia de los procesos de gestión de la seguridad operacional de la organización que respaldan:

1) la prioridad institucional declarada de la gestión de la seguridad operacional; y

2) la promoción de la seguridad operacional en toda la organización.

9.3.6.9 Una vez que el comité de seguridad operacional de mayor nivel ha elaborado una dirección estratégica, la implementación de las estrategias de seguridad operacional deberían coordinarse en toda la organización. Esto puede lograrse mediante la creación de grupos de acción de seguridad operacional (SAG) que están más concentrados en las operaciones. Los SAG se componen normalmente de gerentes y personal de primera línea y están presididos por un gerente de línea designado. Los SAG son entidades tácticas que abordan problemas de implementación específicos según la dirección del SRM. Los SAG:

a) supervisan el rendimiento en materia de seguridad operacional dentro de las áreas funcionales de la organización y garantizan que se lleven a cabo las actividades de SRM apropiadas;

b) revisan los datos de seguridad operacional disponibles e identifican la implementación de estrategias apropiadas de control de riesgo de seguridad operacional y garantizan que se proporcionan comentarios de los empleados;

c) evalúan el impacto de seguridad operacional relacionado con la introducción de cambios operacionales o nuevas tecnologías;

d) coordinan la implementación de medidas correctivas relacionadas con los controles de seguridad operacional y garantizan que dichas medidas se tomen rapidamente; y

e) revisan la eficacia de los controles de riesgo de seguridad operacional específicos.

9.3.7 Coordinación de la planificación de respuestas ante emergencias

9.3.7.1 Por definición, una emergencia es una situación o un suceso repentino e imprevisto que requiere medidas inmediatas. La coordinación de la planificación de respuestas ante emergencias se refiere a la planificación de actividades que tiene lugar dentro de un período de tiempo limitado durante una situación de emergencia operacional aeronáutica imprevista. Un plan de respuestas ante emergencias (ERP) es un componente integral del proceso SRM de proveedor de servicio para enfrentar emergencias, crisis o sucesos relacionados con la aviación. Cuando existe la posibilidad de que las operaciones o actividades aeronáuticas de un proveedor de servicios se vean comprometidas por emergencias como casos de salud pública o pandemias, estos escenarios también deberían abordarse en su ERP según corresponda. El ERP debería abordar también emergencias previsibles que se identifiquen en el SMS y comprender medidas, procesos y controles de mitigación para gestionar eficazmente las emergencias relacionadas con la aviación.

9.3.7.2 El objetivo general del ERP es la continuación de las operaciones en condiciones de seguridad y el retorno a las operaciones normales tan pronto como sea posible. Esto debería garantizar que exista una transición ordenada y eficiente de operaciones normales a operaciones de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de la autoridad. Se incluye también el período de tiempo necesario para restablecer las operaciones “normales” después de una emergencia. El ERP determina las medidas que debe adoptar el personal responsable durante una emergencia. La mayoría de estos casos exigirá acciones coordinadas entre diferentes organizaciones, posiblemente con otros proveedores de servicios y con otras organizaciones externas como las de servicios de emergencia no relacionados con la aviación. El ERP debería ser de fácil acceso para el personal clave apropiado así como para las organizaciones externas de coordinación.

9.3.7.3 La coordinación de la planificación de respuesta ante emergencias se aplica solamente a aquellos proveedores de servicios que deben establecer y mantener un ERP. En el Anexo 19 no se exige la creación o elaboración de un ERP; la planificación de respuestas ante emergencias se aplica solamente a proveedores de servicios específicos según se establece en los Anexos pertinentes de la OACI (en los diversos Anexos pueden utilizarse términos diferentes para las disposiciones relativas al tratamiento de situaciones de emergencia). Esta coordinación debería ejercerse como parte del ensayo periódico del ERP.

9.3.8 Documentación del SMS

9.3.8.1 La documentación del SMS debería incluir un “manual SMS”, de alto nivel, en el que se describa las políticas, procesos y procedimientos SMS del proveedor de servicios a efectos de facilitar la administración, comunicación y mantenimientos internos del SMS por parte de la organización. Ello debería contribuir a que el personal comprendiera la forma en que funciona el SMS de la organización y cómo se satisfarán las políticas y objetivos de seguridad operacional. La documentación debería incluir una descripción del sistema que proporcione los límites del SMS. También debería ayudar a aclarar la relación entre las diversas políticas, procedimientos, procesos y prácticas y definir como estos se relacionan con la política y objetivos de seguridad operacional del proveedor de servicios. La documentación debería adaptarse y redactarse para abordar las actividades cotidianas de gestión de la seguridad operacional de forma que puedan ser fácilmente comprensibles por todo el personal de la organización.

9.3.8.2 El manual SMS también sirve de mecanismo principal de comunicación de seguridad operacional entre el proveedor de servicios y los interesados principales en la seguridad operacional (p. ej., la CAA para fines de aceptación normativa, evaluación y subsiguiente observación del SMS). El manual SMS puede ser un documento independiente, o puede estar integrado en otros documentos institucionales mantenidos por el proveedor de servicios. Cuando los detalles de los procesos SMS de la organización ya están abarcados en los documentos existentes, alcanza con hacer referencia apropiada a tales documentos. Este documento SMS debe mantenerse actualizado. Puede ser necesario contar con la aprobación de la CAA antes de introducir enmiendas importantes en el manual SMS, dado que es un documento controlado.

9.3.8.3 El manual SMS debería incluir una descripción detallada de las políticas, procesos y procedimientos del proveedor de servicios incluyendo:

a) la política y los objetivos de seguridad operacional;

b) referencias a cualesquiera requisitos SMS normativos aplicables;

c) una descripción del sistema;

d) obligaciones de rendición de cuentas en materia de seguridad operacional y personal clave de seguridad operacional;

e) procesos y procedimientos de sistemas de notificación voluntaria y obligatoria de seguridad operacional;

f) procesos y procedimientos de identificación de peligros y evaluación de riesgos de seguridad operacional;

g) procedimientos de investigación de seguridad operacional;

h) procedimientos para establecer y observar los indicadores de rendimiento en materia de seguridad operacional;

i) procesos y procedimientos de instrucción en SMS y comunicaciones;

j) procesos y procedimientos de comunicación de seguridad operacional;

k) procedimientos de auditoría interna;

l) gestión de procedimientos de cambio;

m) procedimientos de gestión de la documentación SMS; y

n) cuando corresponda, coordinación de la planificación de respuestas ante emergencias.

9.3.8.4 La documentación del SMS también comprende la recopilación y mantenimiento de registros operacionales que apoyen la existencia y el funcionamiento continuo del sistema. Los registros operacionales son las salidas de los procesos y procedimientos SMS tales como la SRM y las actividades de aseguramiento de la seguridad operacional. Los registros operacionales del SMS deberían almacenarse y mantenerse con arreglo a períodos de retención vigentes. Entre los registros operacionales SMS típicos deberían figurar los siguientes:

a) registros de informes de peligros e informes sobre peligros/seguridad operacional;

b) SPI y gráficos relacionados;

c) registro de evaluaciones de seguridad operacional completadas;

d) registros de revisión o auditoría internas del SMS;

e) registros de auditoría interna;

f) registros de instrucción en SMS/seguridad operacional;

g) actas de reuniones del comité del SMS/ seguridad operacional;

h) plan de implementación del SMS (durante el período de implementación inicial); y

i) análisis de brechas para respaldar el plan de implementación.

9.4 COMPONENTE 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

9.4.1 Los proveedores de servicios deberían asegurar que están gestionando sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional (SRM), y comprende la identificación de peligros, la evaluación de riesgos de seguridad operacional y la mitigación de dichos riesgos.

9.4.2 El proceso de SRM identifica sistemáticamente los peligros que existen en el contexto de la entrega de sus productos o servicios. Puede que los peligros sean resultado de los sistemas que son deficientes en su diseño, función técnica, interfaz humana o interacciones con otros procesos y sistemas. También pueden resultar de una falla de los procesos o sistemas existentes para adaptar los cambios en el entorno de operación del proveedor de servicios. A menudo, un análisis cuidadoso de estos factores puede identificar posibles peligros en cualquier punto de la operación o del ciclo de vida de la actividad.

9.4.3 Es fundamental comprender el sistema y su entorno operacional para lograr un alto rendimiento en materia de seguridad operacional. Contribuirá a ello contar con una descripción detallada del sistema y sus interfaces. Se pueden descubrir peligros durante el ciclo de vida operacional a partir de fuentes internas y externas. Deberán revisarse continuamente las evaluaciones y mitigaciones de riesgos de seguridad operacional para asegurar que permanecen vigentes. En la Figura 9-1 se presenta un panorama del proceso de identificación de peligros y gestión de riesgo de seguridad operacional del proveedor de servicios.

Nota.— En el Capítulo 2 figura orientación detallada sobre procedimientos de identificación de peligros y evaluación de riesgos de seguridad operacional.

9.4.4 Identificación de peligros

La identificación de peligros es la primera etapa del proceso SRM. El proveedor de servicios debería desarrollar y mantener un proceso formal para identificar peligros que puedan tener consecuencias en la seguridad operacional de la aviación en todos los sectores de operación y actividades. Esto comprende equipo, instalaciones y sistemas. La identificación y el control de los peligros relacionados con la seguridad operacional de la aviación son beneficiosos para la seguridad de la operación de que se trate. También es importante considerar los peligros que puedan existir como resultado de las interfaces del SMS con organizaciones externas.

Fuentes para la identificación de peligros

9.4.4.1 Existen varias fuentes para la identificación de peligros, tanto internas como externas a la organización. Entre algunas fuentes internas figuran:

a) *Observación normal de las operaciones*; se aplican técnicas de observación para el seguimiento de las operaciones y actividades cotidianas como las auditorías de la seguridad de las operaciones en línea (LOSA).

b) *Sistemas automáticos de observación*; se utilizan sistemas automáticos de registro para observar parámetros que puedan analizarse, como el análisis de datos de vuelo (FDM).

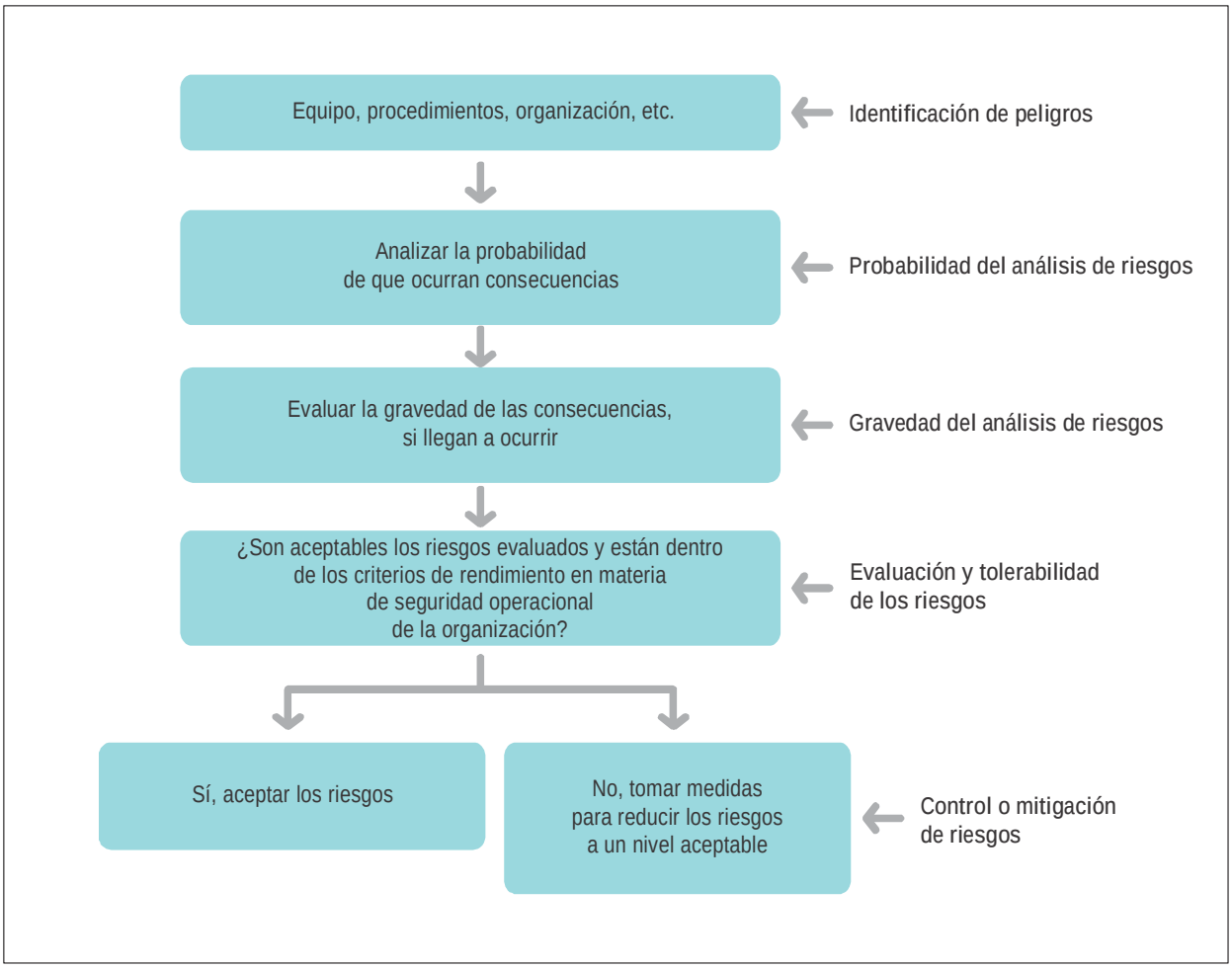


Figura 9-1. Proceso de identificación de peligros y gestión de riesgos

c) *Sistemas de notificación voluntaria y obligatoria de seguridad operacional*; esto brinda a todos, incluyendo el personal de organizaciones externas, oportunidades para notificar a la organización peligros y otros problemas de seguridad operacional.

d) *Auditorías*; pueden utilizarse para identificar peligros en la tarea o proceso que se está auditando. Estos también deberían coordinarse con los cambios que hubiere en la organización para identificar peligros relacionados con la implementación de dichos cambios.

e) *Comentarios procedentes de la instrucción*; una instrucción interactiva (en ambos sentidos) puede facilitar la identificación de nuevos peligros por parte de los participantes.

f) *Investigaciones de la seguridad operacional del proveedor de servicios*; peligros identificados en investigaciones internas de la seguridad operacional y notificaciones de seguimiento sobre accidentes/incidentes.

9.4.4.2 Entre los ejemplos de fuentes externas para la identificación de peligros figuran los siguientes:

a) *Informes de accidentes de aviación*; informes de accidentes que pueden estar relacionados con accidentes en el mismo Estado o con un tipo similar de aeronave, región o entorno operacional.

b) *Sistemas estatales de notificación obligatoria y voluntaria de seguridad operacional*; algunos Estados proporcionan resúmenes de las notificaciones de seguridad operacional recibidas de los proveedores de servicios.

c) *Auditorías estatales de vigilancia y auditorías de terceras partes*; las auditorías externas pueden a veces estar en condiciones de identificar peligros que pueden haberse documentado como no identificados o captados en forma menos evidente dentro de una constatación de auditoría.

d) *Asociaciones comerciales y sistemas de intercambio de información*; muchas asociaciones comerciales y grupos industriales pueden compartir datos que pueden incluir peligros identificados.

Sistema de notificación de seguridad operacional

9.4.4.3 Una de las fuentes principales para la identificación de peligros es el sistema de notificación de seguridad operacional, especialmente el sistema de notificación voluntaria de seguridad operacional. Aunque normalmente se utiliza el sistema obligatorio para incidentes que han ocurrido, el sistema voluntario proporciona un canal adicional de notificación de posibles problemas de seguridad operacional como peligros, cuasicolisiones o errores. También pueden proporcionar información valiosa al Estado y al proveedor de servicios sobre sucesos con consecuencias menos graves.

9.4.4.4 Es importante que los proveedores de servicios brinden adecuadas protecciones para alentar a las personas a que notifiquen lo que han visto o experimentado. Por ejemplo, puede no exigirse medidas de cumplimiento en casos de informes de errores o, en algunas circunstancias infracción de reglamentos. Debería declararse claramente que la información notificada se utilizará solamente para apoyar la mejora de la seguridad operacional. La intención de esto es promover una cultura de notificación eficaz y la identificación proactiva de posibles deficiencias de seguridad operacional.

9.4.4.5 Los sistemas de notificación voluntaria de seguridad operacional deberían tener carácter confidencial, exigiéndose que toda información sobre la identificación de la persona que notifica sea conocida solamente por el custodio a efectos de permitir medidas de seguimiento. La función de custodio debería limitarse a algunos pocos individuos, normalmente el gerente de seguridad operacional y el personal involucrado en la investigación de que se trate. El mantenimiento de la confidencialidad ayudará a facilitar la revelación de peligros relacionados con errores humanos, sin temer castigos o experimentar vergüenza. Las notificaciones voluntarias de seguridad operacional pueden ser anónimas y archivarse una vez adoptadas las necesarias medidas de seguimiento. Los informes anónimos pueden apoyar futuros análisis de tendencias para el seguimiento de la eficacia de la mitigación de riesgos e identificar peligros emergentes.

9.4.4.6 Se alienta al personal a todos los niveles y en todas las disciplinas a que identifiquen y notifiquen peligros y otros problemas de seguridad operacional a través de sus sistemas de notificación de seguridad operacional. Para ser eficaces, los sistemas de notificación de seguridad operacional deberían ser fácilmente accesibles a todo el personal. Dependiendo de la situación, puede utilizarse un formulario en papel, en un sitio web o en computadora de mesa. Disponer de múltiples métodos de entrada maximiza la probabilidad de participación del personal. Todos deberían ser conscientes de los beneficios de las notificaciones de seguridad operacional y de cuál debería ser el contenido de las mismas.

9.4.4.7 Las personas que presenten notificaciones de seguridad operacional deberían recibir información sobre las decisiones o medidas que se han adoptado al respecto. La armonización de los requisitos de los sistemas de notificación, herramientas y métodos de análisis, puede facilitar el intercambio de información de seguridad operacional

así como las comparaciones de ciertos indicadores de rendimiento en materia de seguridad operacional. Los comentarios e información proporcionados a las personas que presentaron notificaciones en los programas voluntarios también sirven para demostrar que dichas notificaciones se consideran seriamente. Esto contribuye a promover una cultura de seguridad operacional positiva y a fomentar futuras notificaciones.

9.4.4.8 Puede ser necesario filtrar las notificaciones de seguridad operacional al ingreso de las mismas cuando hay un número elevado. Esto puede involucrar una evaluación inicial de riesgos de seguridad operacional para determinar si es necesaria una investigación ulterior y qué nivel de la misma se requiere.

9.4.4.9 Los informes de seguridad operacional se filtran normalmente mediante el uso de una taxonomía o sistema de clasificación. El filtrado de la información aplicando una taxonomía también puede hacer más fácil la identificación de problemas y tendencias comunes. El proveedor de servicios debería desarrollar taxonomías que abarquen sus tipos de operación. La desventaja de utilizar una taxonomía es que a veces el peligro identificado no se ajusta claramente a ninguna de las categorías definidas. El reto, entonces, es aplicar taxonomías con un grado apropiado de detalle y que sean suficientemente específicas para que los peligros sean de fácil ubicación, pero suficientemente genéricas como para que los peligros resulten de valor para los análisis. Algunos Estados y asociaciones comerciales internacionales han desarrollado taxonomías que podrían utilizarse. En el Capítulo 5 figura información adicional sobre taxonomías.

9.4.4.10 Otros métodos de identificación de peligros incluyen seminarios o reuniones en los cuales expertos temáticos presentan escenarios de análisis detallados. Estas reuniones se benefician de las contribuciones de una amplia gama de personal operacional y técnico experimentado. Para dichas actividades podrían utilizarse las reuniones de comités de seguridad operacional existentes (SRB, SAG, etc.) pudiéndose utilizar el mismo grupo para evaluar riesgos de seguridad operacional conexos.

9.4.4.11 Deberían documentarse los peligros identificados y sus posibles consecuencias. Esta información se utilizará en los procesos de evaluación de riesgos de seguridad operacional.

9.4.4.12 El proceso de identificación de peligros considera todos los posibles peligros que puedan existir en el ámbito de las actividades aeronáuticas del proveedor de servicios, incluyendo las interfaces con otros sistemas, tanto dentro como fuera de la organización. Una vez identificado los peligros, deberían determinarse sus consecuencias (es decir todo suceso o resultado específico).

Investigación de peligros

9.4.4.13 La identificación de peligros debería ser continua y formar parte de las actividades permanentes del proveedor de servicios. Entre algunas de las condiciones que merecerían una investigación más detallada figuran las siguientes:

a) casos en que la organización experimenta un crecimiento inexplicado de sucesos relacionados con la seguridad operacional de la aviación o de incumplimiento normativo; o

b) cambios significativos en la organización o sus actividades.

9.4.5 Investigación de seguridad operacional del proveedor de servicios

9.4.5.1 La gestión eficaz de la seguridad operacional depende de las investigaciones de calidad para analizar sucesos y peligros de seguridad operacional y notificar conclusiones y recomendaciones a efectos de mejorar la seguridad del entorno operacional.

9.4.5.2 Existe una clara distinción entre las investigaciones de accidentes e incidentes en el marco del Anexo 13 y las investigaciones de seguridad operacional del proveedor de servicios. La investigación de accidentes e incidentes graves abarcadas en el Anexo 13 son responsabilidad del Estado, según allí se define. Este tipo de información es fundamental para difundir experiencias obtenidas en accidentes e incidentes. Las investigaciones de seguridad operacional del proveedor de servicios son realizadas por este como parte de su SMS a efectos de apoyar los procesos de identificación de peligros y evaluación de riesgos. Existen varios sucesos de seguridad operacional que caen fuera del ámbito del Anexo 13 y que podrían proporcionar una fuente valiosa de identificación de peligros o de carencias en los controles de riesgos. Estos problemas pueden revelarse y remediarse mediante una investigación de seguridad operacional llevada a cabo por el proveedor de servicios.

9.4.5.3 El objetivo principal de la investigación de seguridad operacional del proveedor de servicios es comprender lo que sucedió y cómo prevenir que ocurran en el futuro situaciones similares mediante la eliminación o mitigación de las deficiencias de seguridad operacional que se hubieren encontrado. Esto se logra mediante un examen cuidadoso y metódico del suceso y la aplicación de las enseñanzas obtenidas para reducir la probabilidad o consecuencia de futuras repeticiones. Las investigaciones de seguridad operacional del proveedor de servicios son parte integral del SMS de éste.

9.4.5.4 Las investigaciones de sucesos y peligros de seguridad operacional por parte del proveedor de servicios constituyen una actividad fundamental del proceso general de gestión de riesgos en la aviación. Entre las ventajas de realizar una investigación de seguridad operacional figuran:

a) obtener una mejor comprensión de los hechos que condujeron al suceso;

b) identificación de factores humanos, técnicos e institucionales contribuyentes;

c) identificación de peligros y realización de evaluaciones de riesgo;

d) formulación de recomendaciones para reducir o eliminar riesgos inaceptables; y

e) identificación de enseñanzas obtenidas que deberían compartirse con los miembros apropiados de la comunidad aeronáutica.

Activadores de la investigación

9.4.5.5 La investigación de seguridad operacional de proveedor de servicios es activada normalmente mediante una notificación (informe) presentado por conducto del sistema de notificación de seguridad operacional. En la Figura 9-2 se presenta el proceso de decisión de una investigación de seguridad operacional y la distinción entre el momento en que debería tener lugar la investigación de seguridad operacional del proveedor de servicios y el momento en que debería iniciarse una investigación en el marco de las disposiciones del Anexo 13.

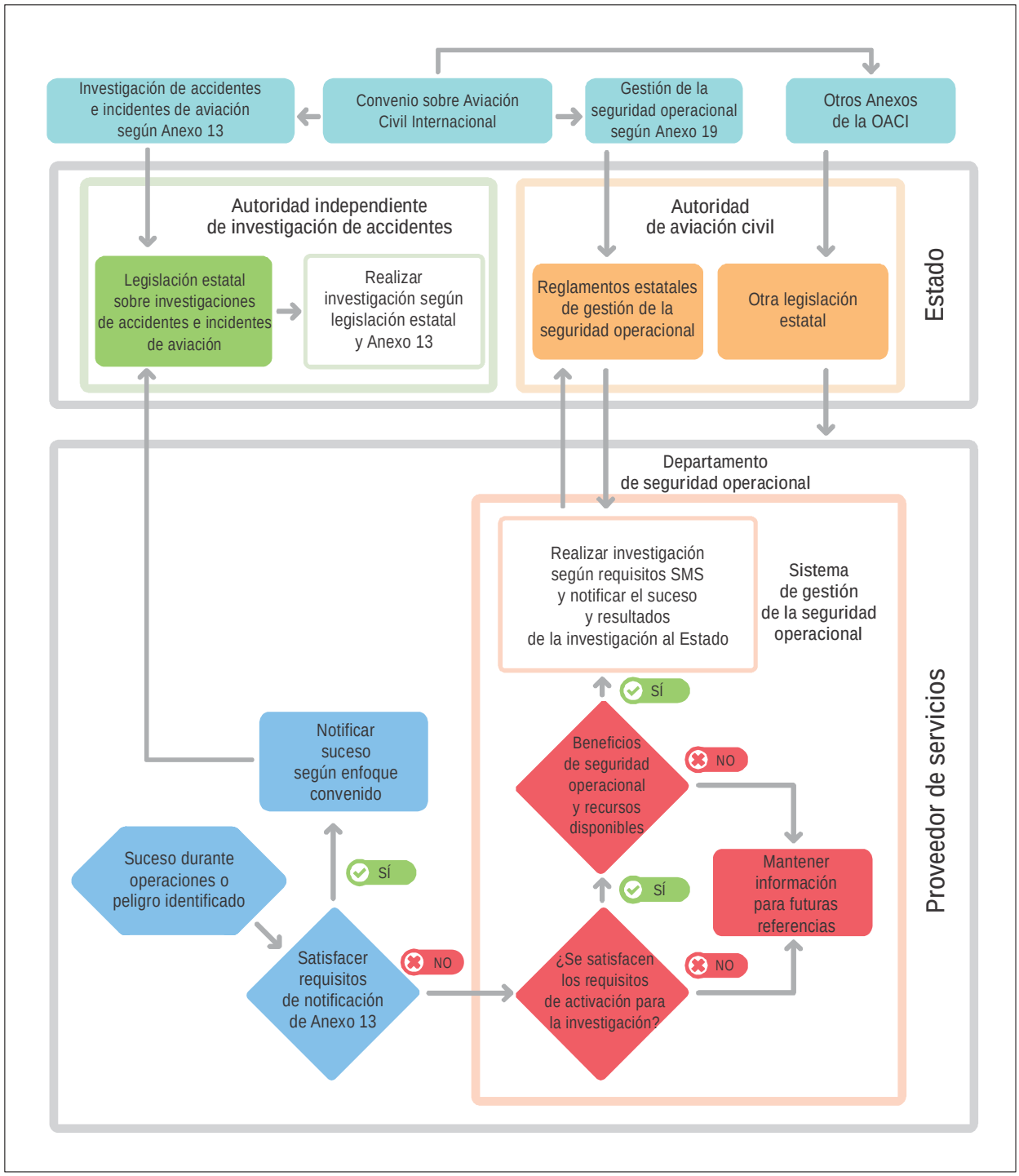


Figura 9-2. Proceso de decisión de una investigación de seguridad operacional

9.4.5.6 No todos los sucesos o peligros pueden o deberían ser investigados; la decisión de realizar una investigación y la profundidad de la misma debería depender de las consecuencias reales o posibles del suceso o peligro en cuestión. Es más probable que se investiguen los sucesos y peligros considerados como de posible alto riesgo y dicha investigación debería hacerse con mayor profundidad que las de menor riesgo potencial. Los proveedores de servicios deberían aplicar un enfoque estructurado de toma de decisiones con puntos definidos de activación. Estos deberían orientar las decisiones de las investigaciones de seguridad operacional, es decir el objeto y el alcance de la investigación, lo que podría comprender:

a) la gravedad o posible gravedad del resultado;

b) requisitos normativos o institucionales para realizar una investigación;

c) valor de seguridad operacional que ha de obtenerse;

d) oportunidad para tomar medidas de seguridad operacional;

e) riesgos relacionados con la no investigación;

f) contribución a programas de seguridad operacional especificados;

g) tendencias identificadas;

h) beneficios para la instrucción; y

i) disponibilidad de recursos.

Designación de un investigador

9.4.5.7 Si debe iniciarse una investigación, la primera medida será designar un investigador o, cuando se dispone de recursos, un equipo de investigación con las habilidades y experiencia necesarias. El tamaño del equipo y el perfil de experiencias y conocimientos de sus miembros dependen del carácter y la gravedad del suceso que se investiga. El equipo de investigación puede requerir la asistencia de otros especialistas. A menudo, se asigna a una sola persona la realización de una investigación interna, con apoyo de expertos de operaciones y de la oficina de seguridad operacional.

9.4.5.8 Idealmente, las investigaciones de seguridad operacional del proveedor de servicios son independientes del sector relacionado el suceso o el peligro identificado. Los mejores resultados se obtendrán si los investigadores tienen conocimiento (están capacitados) y pericia (tienen experiencia) en las investigaciones de seguridad operacional del proveedor de servicios. Idealmente también, los investigadores deberían ser escogidos para la función en base de sus conocimientos, pericia y características de personalidad, que deberían incluir: integridad, objetividad, pensamiento lógico, pragmatismo y pensamiento lateral.

El proceso de investigación

9.4.5.9 La investigación debería identificar lo que sucedió y por qué sucedió y esto puede requerir que se aplique un análisis de causas básicas como parte de la investigación. Idealmente, las personas involucradas en el suceso deberían entrevistarse tan pronto como sea posible después de este. La investigación debería comprender:

a) el establecimiento de cronogramas de sucesos clave, incluyendo las acciones de las personas involucradas;

b) el examen de las políticas y procedimientos relacionados con las actividades;

c) el examen de las decisiones adoptadas con respecto al suceso;

d) la identificación de los controles de riesgos que estaban implantados y que deberían haber evitado que ocurriera el suceso; y

e) el examen de los datos de seguridad operacional de sucesos previos o similares.

9.4.5.10 La investigación de seguridad operacional debería concentrarse en los peligros y riesgos de seguridad operacional identificados y en las oportunidades para introducir mejoras y no en asignar culpas o imponer castigos. La forma en que se realiza la investigación y, lo que es más importante, la forma en que se redacta el informe, influirán en el probable impacto en la seguridad operacional, la futura cultura de seguridad operacional de la organización y la eficacia de futuras iniciativas en la materia.

9.4.5.11 La investigación debería concluir con constataciones y recomendaciones claramente definidas que eliminen o mitiguen las deficiencias de seguridad operacional.

9.4.6 Evaluación y mitigación de riesgos de seguridad operacional

9.4.6.1 El proveedor de servicios debe desarrollar un modelo y procedimientos de evaluación de riesgos de seguridad operacional que permitan aplicar un enfoque coherente y sistemático para la evaluación de dichos riesgos. Esto debería incluir un método que contribuya a determinar qué tipo de riesgo es aceptable o inaceptable y priorizar las medidas pertinentes.

9.4.6.2 Los mecanismos de SRM utilizados pueden tener que revisarse y ajustarse periódicamente para asegurar que siguen siendo adecuados al entorno de explotación del proveedor de servicios. El proveedor de servicios puede encontrar enfoques más perfeccionados que reflejen mejor las necesidades de su operación a medida que su SMS logra madurez. El proveedor de servicios y la CAA deberían convenir en una metodología al respecto.

9.4.6.3 Existen enfoques más perfeccionados para la clasificación de riesgos de seguridad operacional. Estos pueden resultar más adecuados si el proveedor de servicios tiene más experiencia en gestión de la seguridad operacional o en manejarse en un entorno de alto riesgo.

9.4.6.4 El proceso de evaluación de riesgos de seguridad operacional debería utilizar cualesquiera datos e información sobre seguridad operacional que estén disponibles. Una vez evaluados los riesgos de seguridad operacional, el proveedor de servicios emprenderá un proceso de toma de decisiones basada en datos para determinar los tipos de controles de riesgos de seguridad operacional que se necesitan.

9.4.6.5 A veces las evaluaciones de riesgos de seguridad operacional tienen que utilizar información cualitativa (juicios de expertos) en vez de datos cuantitativos debido a que no se dispone de estos. El uso de una matriz de riesgos de seguridad operacional permite al usuario expresar los riesgos de seguridad operacional relacionados con el peligro identificado en un formato cuantitativo. Esto permite realizar comparaciones directas de magnitud entre los riesgos de seguridad operacional identificados. Puede asignarse un criterio de evaluación cualitativa de riesgos de seguridad operacional como “probable que ocurra” o “improbable” a cada riesgo de seguridad operacional identificado cuando no se dispone de datos cuantitativos.

9.4.6.6 Para los proveedores de servicios que funcionan en varios lugares con entornos de operación específicos, puede resultar más eficaz establecer comités locales de seguridad operacional a efectos de realizar evaluaciones de riesgos de seguridad operacional e identificación de controles para los mismos. A menudo se procura obtener asesoramiento de especialistas en la esfera operacional (internos o externos al proveedor de servicios). Puede ser necesario obtener decisiones finales o aceptaciones de controles de parte de autoridades superiores para que se puedan proporcionar los recursos apropiados.

9.4.6.7 La decisión sobre la forma en que los proveedores de servicios priorizan sus evaluaciones de riesgos de seguridad operacional y adoptan controles de dichos riesgos corresponde a dichos proveedores. Como orientación, el proveedor de servicios debería determinar que el proceso de priorización:

a) evalúa y controla los mayores riesgos de seguridad operacional;

b) asigna recursos a los mayores riesgos de seguridad operacional;

c) mantiene o mejora eficazmente la seguridad operacional;

d) alcanza los objetivos y SPT declarados y convenidos en materia de seguridad operacional; y

e) satisface los requisitos de los reglamentos estatales con respecto al control de los riesgos de seguridad operacional.

9.4.6.8 Una vez evaluado los riesgos de seguridad operacional, pueden implementarse los controles apropiados. Es importante involucrar a los “usuarios finales” y expertos temáticos en la determinación de los controles de riesgo de seguridad operacional apropiados. Si se asegura la participación de las personas adecuadas se podrá maximizar la viabilidad de las mitigaciones de riesgo de seguridad operacional escogidas. Antes de implementar controles de riesgos de seguridad operacional debería realizarse una determinación de cualesquiera consecuencias no deseadas, en particular la introducción de nuevos peligros.

9.4.6.9 Una vez acordado e implantado el control de riesgos de seguridad operacional, debería observarse el rendimiento en materia de seguridad operacional para asegurar la eficacia de dicho control. Es necesario verificar la integridad, eficiencia y eficacia de los nuevos controles de riesgo de seguridad operacional en condiciones de operación reales.

9.4.6.10 Deberían documentarse los resultados de la SRM. Esto debería incluir los peligros y cualesquiera consecuencias, la evaluación de los riesgos de seguridad operacional y todas las medidas adoptadas para controlar dichos riesgos. Estos elementos se integran a menudo en un registro para que pueda llevarse a cabo su seguimiento y observación. Esta documentación de la SRM pasa a ser una fuente básica de conocimientos institucionales en materia de seguridad operacional que puede utilizarse como referencia al tomar decisiones en esa materia e intercambiar información al respecto. Este conocimiento en materia de seguridad operacional proporciona material para análisis de tendencias e instrucción y comunicación en ese ámbito. Resulta también útil para llevar a cabo auditorías internas a efectos de evaluar si se han implementado y resultan eficaces los controles y medidas sobre riesgos de seguridad operacional.

9.5 COMPONENTE 3: ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

9.5.1 En el Anexo 19, Apéndice 2, 3.1.1 se exige que el proveedor de servicios desarrolle y mantenga los medios para verificar el rendimiento en materia de seguridad operacional de la organización y para confirmar la eficacia de los controles de riesgo de seguridad operacional. El componente de aseguramiento de la seguridad operacional del SMS del proveedor de servicios proporciona estas capacidades.

9.5.2 El aseguramiento de la seguridad operacional consta de procesos y actividades realizadas por el proveedor de servicios para determinar si el SMS funciona de acuerdo con las expectativas y los requisitos. Esto involucra la observación continua de sus procesos internos así como su entorno de operación para detectar cambios o desviaciones que puedan introducir riesgos de seguridad operacional emergentes o el deterioro de los controles de riesgos existentes. Dichos cambios o desviaciones pueden entonces abordarse mediante el proceso SRM.

9.5.3 Las actividades de aseguramiento de la seguridad operacional deberían incluir el desarrollo e implementación de las medidas adoptadas en respuesta a los problemas identificados con posibles consecuencias para la seguridad operacional. Estas acciones mejoran continuamente el rendimiento del SMS del proveedor de servicios.

9.5.4 Observación y medición del rendimiento en materia de seguridad operacional

Para verificar el rendimiento en materia de seguridad operacional y validar la eficacia de los controles de riesgos de seguridad operacional se requiere utilizar una combinación de auditorías internas y establecimiento y observación de indicadores del rendimiento en esa materia. La evaluación de la eficacia de los controles de riesgos de seguridad operacional es importante dado que su aplicación no siempre alcanza los resultados previstos. Esto ayudará a determinar si se ha elegido el control correcto para dichos riesgos y puede resultar en la aplicación de una estrategia de control de riesgos de seguridad operacional diferente.

Auditorías internas

9.5.4.1 Las auditorías internas se llevan a cabo para evaluar la eficacia del SMS e identificar áreas de posible mejora. La mayoría de los reglamentos de seguridad operacional de la aviación son controles genéricos de riesgos de seguridad operacional que han sido establecidos por el Estado. Garantizar el cumplimiento de los reglamentos mediante la realización de auditorías internas es un aspecto principal del aseguramiento de la seguridad operacional.

9.5.4.2 También es necesario asegurar que los controles de riesgo se implementan y observan eficazmente. Las causas y los factores contribuyentes deberían investigarse y analizarse cuando se han identificado casos de no cumplimiento y otros problemas. La auditoría interna se concentra principalmente en las políticas, procesos y procedimientos que proporcionen controles de los riesgos de seguridad operacional.

9.5.4.3 Las auditorías internas resultan más eficaces cuando las realizan personas o departamentos independientes de las funciones que se están auditando. Dichas auditorías deberían proporcionar al ejecutivo responsable y a la administración superior información y comentarios sobre la situación de:

a) el cumplimiento de los reglamentos;

b) el cumplimiento de las políticas, procesos y procedimientos;

c) la eficacia de los controles de riesgos de seguridad operacional;

d) la eficacia de las medidas correctivas; y

e) la eficacia del SMS.

9.5.4.4 Algunas organizaciones no pueden asegurar la independencia apropiada de una auditoría interna, en cuyo caso el proveedor de servicios debería considerar la contratación de auditores externos (p. ej., auditores independientes o auditores de otra organización).

9.5.4.5 La planificación de las auditorías internas debería tener en cuenta la criticidad para la seguridad operacional de los procesos, los resultados de auditorías y evaluaciones anteriores (de todas las fuentes) y los controles de riesgo de seguridad operacional implementados. Las auditorías internas deberían identificar los casos de no cumplimiento de reglamentos y políticas, procesos y procedimientos. También deberían identificar deficiencias del sistema, falta de eficacia de los controles de riesgos de seguridad operacional y oportunidades para introducir mejoras.

9.5.4.6 La evaluación del cumplimiento y la eficacia son esenciales para el logro de un buen rendimiento en materia de seguridad operacional. El proceso de auditoría interna puede aplicarse para determinar tanto el cumplimiento como la eficacia. Las preguntas siguientes pueden plantearse para evaluar el cumplimiento y la eficacia de cada proceso o procedimiento:

a) Determinación del cumplimiento

1) ¿Existe el proceso o procedimiento requerido?

2) ¿Está documentado el proceso o procedimiento (se definen entradas, actividades, interfaces y salidas)?

3) ¿Satisface el proceso o procedimiento los requisitos (criterios)?

4) ¿Se está aplicando el proceso o procedimiento?

5) ¿Aplica sistemáticamente el proceso o procedimiento todo el personal afectado?

6) ¿Se obtienen los resultados definidos?

7) ¿Se ha documentado e implementado algún cambio en el proceso o procedimiento?

b) Evaluación de la eficacia

1) ¿Comprenden los usuarios el proceso o procedimiento?

2) ¿Se logra sistemáticamente el propósito del proceso o procedimiento?

3) ¿Son los resultados del proceso o procedimiento los que el “cliente” pidió?

4) ¿Se examina regularmente el proceso o procedimiento?

5) ¿Se realiza una evaluación de riesgos de seguridad operacional cuando se han introducido cambios en el proceso o procedimiento?

6) ¿Han producido las mejoras del proceso o procedimiento los beneficios esperados?

9.5.4.7 Además, las auditorías internas deberían observar los progresos hacia la solución de los casos de no cumplimiento identificados previamente. Estos deberían haberse abordado mediante análisis de causas básicas y elaboración e implementación de planes de medidas correctivas y preventivas. Los resultados de los análisis de causas y factores contribuyentes de todo caso de no cumplimiento deberían introducirse en los procesos SRM de los proveedores de servicios.

9.5.4.8 Los resultados del proceso de auditoría interna constituyen una de las diversas entradas de las funciones de la SRM y el aseguramiento de la seguridad operacional. Las auditorías internas informan a la administración del proveedor de servicios sobre el nivel de cumplimiento dentro de la organización, el grado en que resultan eficaces los controles de riesgos de seguridad operacional y los casos en que se requieren medidas correctivas o preventivas.

9.5.4.9 Las CAA pueden proporcionar información y comentarios adicionales sobre la situación del cumplimiento de los reglamentos y la eficacia del SMS a asociaciones industriales u otras terceras partes seleccionadas por el proveedor de servicios para auditar su organización y procesos. Los resultados de dichas auditorías por segundas y terceras partes constituyen entradas de la función de aseguramiento de la seguridad operacional, proporcionando al proveedor de servicios indicaciones sobre la eficacia de sus procesos de auditoría interna y oportunidades para mejorar su SMS.

Observación del rendimiento en materia de seguridad operacional

9.5.4.10 La observación del rendimiento en materia de seguridad operacional se lleva a cabo mediante la recopilación de datos e información sobre seguridad operacional de varias fuentes normalmente disponibles a una

organización. La disponibilidad de datos para apoyar, sus decisiones bien fundamentadas es uno de los aspectos más importantes del SMS. Estos datos son utilizados para la observación y medición del rendimiento en materia de seguridad operacional que constituyen actividades fundamentales que generan la información necesaria para la toma de decisiones en materia de riesgos de seguridad operacional.

9.5.4.11 La observación y la medición del rendimiento en materia de seguridad operacional deberían realizarse aplicando algunos principios básicos. El rendimiento en materia de seguridad operacional alcanzado es una indicación del desempeño de la organización y también una medida de la eficacia de su SMS. Para ello la organización debe definir:

a) objetivos de seguridad operacional, que deberían establecerse en primer lugar para reflejar los logros estratégicos o resultados deseados relativos a las preocupaciones de seguridad operacional específicas del contexto de funcionamiento de la organización;

b) los SPI, que son parámetros tácticos relativos a los objetivos de seguridad operacional y, por consiguiente, constituyen la referencia para la recopilación de datos; y

c) las SPT, que también son parámetros tácticos utilizados para vigilar el progreso hacia el logro de los objetivos de seguridad operacional.

9.5.4.12 Se alcanzará un panorama más completo y realista del rendimiento en materia de seguridad operacional del proveedor de servicios si los SPI abarcan un amplio espectro de indicadores. Estos deberían comprender:

a) sucesos de baja probabilidad/alta gravedad (p. ej., accidentes e incidentes graves);

b) sucesos de alta probabilidad/baja gravedad (p. ej., sucesos operacionales de poca consecuencia, informes de no cumplimiento, desviaciones, etc.): y

c) rendimiento del proceso (p. ej., instrucción, mejoras del sistema y procesamiento de informes).

9.5.4.13 Los SPI se utilizan para medir el rendimiento en materia de seguridad operacional del proveedor de servicios y el funcionamiento de su SMS. Los SPI se basan en la observación de datos e información procedente de diversas fuentes incluyendo el sistema de notificación de seguridad operacional. Dichos indicadores deben ser específicos de cada proveedor de servicios y estar relacionados con los objetivos de seguridad operacional ya establecidos.

9.5.4.14 Al establecer SPI los proveedores de servicios deberían considerar:

a) *La medición de los elementos correctos*: determinación de los mejores SPI que indiquen que la organización está encaminada a lograr sus objetivos de seguridad operacional. También se debe considerar cuáles son los principales problemas y riesgos de seguridad operacional que enfrenta la organización e identificar los SPI que indiquen un control eficaz de los mismos.

b) *La disponibilidad de datos*: determinación de si se dispone de datos que correspondan a lo que la organización quiere medir. De no ser así, puede ser necesario establecer fuentes adicionales de recopilación de datos. Para pequeñas organizaciones con cantidades limitadas de datos, la consolidación de conjuntos de datos también puede contribuir a identificar tendencias, respaldada por asociaciones industriales que recopilen datos de seguridad operacional de múltiples organizaciones.

c) *La fiabilidad de los datos*: los datos pueden ser no fiables debido a su carácter subjetivo o porque no están completos.

d) *SPI comunes de la industria*: puede resultar útil convenir respecto de SPI comunes con organizaciones similares de modo que se puedan efectuar comparaciones entre organizaciones. El reglamentador o las asociaciones industriales pueden facilitar este aspecto.

9.5.4.15 Una vez establecidos los SPI el proveedor de servicios debería considerar si resulta apropiado identificar SPT y niveles de alerta. Las SPT son útiles para contribuir a mejoras de la seguridad operacional pero, si no se implementan bien, pueden conducir a comportamientos no deseados – es decir, individuos y departamentos demasiado concentrados en alcanzar la meta y que quizás pierdan de vista lo que ésta debía lograr – en vez de a una mejora del rendimiento en materia de seguridad operacional de la organización. En tales casos, podría ser más apropiado vigilar los SPI para determinar tendencias.

9.5.4.16 Las actividades siguientes pueden ser fuentes para respaldar la observación y la medición del rendimiento en materia de seguridad operacional:

a) *Los estudios de seguridad operacional* son análisis para obtener una comprensión más profunda de los temas de seguridad operacional o comprender mejor tendencias en materia de rendimiento.

b) *Los análisis de datos de seguridad operacional* utilizan los datos de las notificaciones de seguridad operacional para revelar problemas o tendencias comunes que puedan requerir investigación ulterior.

c) *Los estudios de seguridad operacional* examinan los procedimientos o procesos relacionados con una operación específica. Dichos estudios pueden involucrar el uso de listas de verificación, cuestionarios y entrevistas confidenciales e informales. Los estudios de seguridad operacional proporcionan generalmente información cualitativa que puede requerir validación mediante la recopilación de datos para determinar si se necesitan medidas correctivas. No obstante, los estudios pueden proporcionar una fuente económica de información de seguridad operacional importante.

d) *Las auditorías de seguridad operacional* se centran en la integridad del SMS del proveedor de servicios y en sus sistemas de respaldo. Las auditorías de seguridad operacional también pueden utilizarse para evaluar la eficacia de los controles de riesgos de seguridad operacional instalados o vigilar el cumplimiento de los reglamentos de seguridad operacional. Garantizar la independencia y objetividad constituye un reto para las auditorías de seguridad operacional. La independencia y la objetividad pueden alcanzarse mediante la participación de entidades externas o realización de auditorías internas con elementos de protección implantados – políticas, procedimientos, funciones, protocolos de comunicación.

e) *Las constataciones y recomendaciones de investigaciones de seguridad operacional* pueden proporcionar información útil en la materia que puede analizarse comparando con otros datos de seguridad operacional recopilados.

f) *Los sistemas de recopilación de datos operacionales* como el FDA o la información radar pueden proporcionar datos útiles de sucesos y rendimiento operacional.

9.5.4.17 La elaboración de los SPI debería estar relacionada con los objetivos de seguridad operacional y basarse en el análisis de datos disponibles o que puedan obtenerse. El proceso de observación y medición involucra el uso de indicadores seleccionados de rendimiento en materia de seguridad operacional, SPT correspondientes y activadores de seguridad operacional.

9.5.4.18 La organización debería observar el rendimiento de los SPI y las SPT establecidos para identificar cambios anormales en el rendimiento en materia de seguridad operacional. Las SPT deberían ser realistas, específicas del contexto y alcanzables cuando se consideren los recursos disponibles a la organización y al sector aeronáutico conexo.

9.5.4.19 En primer lugar, la observación y medición del rendimiento en materia de seguridad operacional proporciona un medio para verificar la eficacia de los controles de riesgos de seguridad operacional. Además, proporcionan una medida de la integridad y eficacia de los procesos y actividades del SMS.

9.5.4.20 El Estado pueden tener procesos específicos para la aceptación de SPI y SPT que deberán seguirse. Por consiguiente, durante la elaboración de SPI y SPT, el proveedor de servicios debería consultar a la autoridad normativa de la organización así como toda información conexa que el Estado haya publicado.

9.5.4.21 En el Capítulo 4 figura más información sobre gestión del rendimiento en materia de seguridad operacional.

9.5.5 La gestión del cambio

9.5.5.1 La experiencia de los proveedores de servicios cambia debido a varios factores, los que incluyen entre otros:

a) expansión o contracción institucional;

b) mejoras empresariales que puede tener consecuencias para la seguridad operacional; estas pueden resultar en cambios a los sistemas, procesos o procedimientos internos que respaldan la entrega de productos y servicios;

c) cambios al entorno de operación de la organización;

d) cambios a las interfaces del SMS con organizaciones externas; y

e) cambios normativos externos, cambios económicos y riesgos emergentes.

9.5.5.2 Los cambios pueden afectar la eficacia de los controles de riesgos de seguridad operacional existentes. Además, nuevos peligros y riesgos de seguridad operacional conexos pueden introducirse involuntariamente en una operación cuando ocurren cambios. Los peligros deberían identificarse y los riesgos de seguridad operacional conexos evaluarse y controlarse, según se defina en los procedimientos de identificación de riesgos o de SRM existentes en la organización.

9.5.5.3 La gestión de los procesos de cambios por parte de la organización debería tener en cuenta las consideraciones siguientes:

a) Criticidad. Determinación de cuán crítico es el cambio. El proveedor de servicios debería considerar las consecuencias para las actividades de su organización así como para otras organizaciones y el sistema aeronáutico.

b) Disponibilidad de expertos temáticos. Es importante que miembros clave de la comunidad aeronáutica estén involucrados en las actividades de gestión de cambios, pudiéndose incluir individuos de organizaciones externas.

c) Disponibilidad de datos e información sobre rendimiento en materia de seguridad operacional. Determinación de los datos e información de que se disponen y que pueden utilizarse para proporcionar información sobre la situación y facilitar el análisis del cambio.

9.5.5.4 A menudo, los pequeños cambios incrementales pueden pasar desapercibidos, pero su efecto acumulativo puede ser considerable. Los cambios, tanto grandes como pequeños pueden afectar la descripción del sistema de la organización y conducir a la necesidad de su revisión. Por consiguiente, la descripción del sistema debería revisarse periódicamente para determinar su validez continua, dado que la mayoría de los proveedores de servicio experimentan cambios periódicos o incluso continuos.

9.5.5.5 El proveedor de servicios debería definir el elemento activador del proceso de cambios formal. Los cambios que probablemente activen una gestión de cambios oficial comprenden:

a) introducción de nueva tecnología o equipo;

b) cambios en el entorno operacional;

c) cambios en el personal clave;

d) cambios significativos en los niveles de plantilla;

e) cambios en los requisitos normativos de seguridad operacional;

f) reestructuración significativa de la organización; y

g) cambios físicos (nueva instalación o base, cambios en la disposición general del aeródromo, etc.).

9.5.5.6 El proveedor de servicios debería considerar también las consecuencias del cambio sobre el personal. Esto podría afectar la forma en que los individuos afectados aceptan el cambio. La comunicación y participación tempranas normalmente mejorarán la forma en que se perciben e implementan los cambios.

9.5.5.7 El proceso de gestión del cambio debería incluir las actividades siguientes:

a) *comprensión y definición del cambio;* esto debería incluir una descripción del cambio y las razones de su implementación;

b) *comprensión y definición de quiénes y qué aspectos se verán afectados;* estos pueden ser individuos dentro de la organización, otros departamentos o personas u organizaciones externas. También puede haber consecuencias para los equipos, sistemas y procesos. Puede ser necesario realizar un examen de la descripción del sistema y de las interfaces de las organizaciones. Este aspecto constituye una oportunidad para determinar quienes deberían estar involucrados en el cambio. Los cambios podrían afectar los controles de riesgos ya implantados para mitigar otros riesgos, y por lo tanto los cambios podrían aumentar los riesgos en sectores que no son inmediatamente obvios;

c) *identificación de peligros relacionados con el cambio y realización de evaluaciones de riesgos de seguridad operacional;* deberían identificarse los peligros directamente relacionados con el cambio. También deberían examinarse las consecuencias sobre peligros y controles de riesgos de seguridad operacional existentes que puedan verse afectados por el cambio. Esta etapa debería aplicar los procesos SRM de la organización existentes;

d) *elaboración de un plan de acción;* este debería definir lo que ha de hacerse, por quiénes y para cuándo. También debería haber un plan claro que describa la forma en que se implementará el cambio y quiénes serán responsables de las medidas que se apliquen, así como la secuencia y programación de las tareas;

e) *aprobación del cambio;* esto es necesario para confirmar que el cambio puede implementarse en condiciones de seguridad. El individuo con responsabilidad y autoridad generales para la implantación del cambio debería firmar el plan correspondiente; y

f) *plan de seguridades;* esto es para determinar las medidas de seguimiento que sean necesarias. Se habrá de considerar la forma en que se comunicará el cambio y si se requieren actividades adicionales (como auditorías) durante o después del mismo. Deberán comprobarse todas las hipótesis o suposiciones que hubiere.

9.5.6 Mejora continua del SMS

9.5.6.1 El Anexo 19, Apéndice 2, 3.3 establece que… “el proveedor de servicios observará y evaluará la eficacia de sus procesos SMS para permitir el mejoramiento continuo del rendimiento general del SMS.” El mantenimiento y la mejora continua de la eficacia del SMS del proveedor de servicios es apoyada por las actividades de aseguramiento de la seguridad operacional que comprende la verificación y seguimiento de las medidas y los procesos de auditoría interna. Debería reconocerse que el mantenimiento y la mejora continua del SMS son actividades permanentes puesto que la propia organización y su entorno operacional estarán cambiando constantemente.

9.5.6.2 Las auditorías internas involucran la evaluación de las actividades aeronáuticas del proveedor de servicios que puede proporcionar información útil a los procesos de toma de decisiones de la organización. La función de auditoría interna comprende la evaluación de todas las funciones de gestión de la seguridad operacional en toda la organización.

9.5.6.3 La eficacia del SMS no debería basarse solamente en los SPI; los proveedores de servicios deberían proponerse la implantación de varios métodos para determinar su eficacia, medir los productos así como los resultados de los procesos y evaluar la información recopilada con estas actividades. Tales métodos pueden incluir lo siguiente:

a) *Auditorías*; comprende las auditorías internas y las auditorías realizadas por otras organizaciones.

b) *Evaluaciones*; comprende las evaluaciones de la cultura de seguridad operacional y la eficacia del SMS.

c) *Observación de sucesos*: vigila la repetición de sucesos de seguridad operacional incluyendo accidentes e incidentes así como errores y situaciones de infracción de reglamentos.

d) *Estudios de seguridad operacional*; incluye estudios de carácter cultural para proporcionar información útil respecto de la participación del personal en el SMS. También puede servir de indicador de la cultura de seguridad operacional de la organización.

e) *Exámenes de la gestión*; examinan si la organización está alcanzando sus objetivos de seguridad operacional y constituyen una oportunidad para realizar toda la información disponible sobre rendimiento en materia de seguridad operacional a efectos de identificar tendencias generales. Es importante que la administración superior examine la eficacia del SMS. Esto puede realizarse como una de las funciones del comité de seguridad operacional de más alto nivel.

f) *Evaluación de los SPI y las SPT*; posiblemente como parte del examen de la gestión. Considera tendencias y, cuando se dispone de datos apropiados, pueden compararse con los datos de otros proveedores de servicios o estatales o mundiales.

g) *Aprovechamiento de las enseñanzas obtenidas*; a partir de sistemas de notificación de seguridad operacional e investigaciones de seguridad operacional del proveedor de servicios. Estas deberían conducir a la implantación de mejoras de la seguridad operacional.

9.5.6.4 En resumen, los procesos de observación del rendimiento en materia de seguridad operacional y de auditoría interna contribuyen a la capacidad del proveedor de servicios de lograr una mejora continua del rendimiento en materia de seguridad operacional. La observación continua del SMS, sus controles de riesgos de seguridad operacional conexos y sistemas de apoyo garantizan al proveedor de servicios y al Estado que los procesos de gestión de la seguridad operacional están logrando sus objetivos deseados de rendimiento en materia de seguridad operacional.

9.6 COMPONENTE 4: PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

9.6.1 La promoción de la seguridad operacional alienta una cultura de seguridad operacional positiva y contribuye a alcanzar los objetivos de seguridad operacional del proveedor de servicios mediante la combinación de competencias técnicas que mejoran continuamente con la instrucción y la educación, la comunicación eficaz y la compartición de información. La administración superior proporciona el liderazgo para promover la cultura de seguridad operacional en toda la organización.

9.6.2 La gestión eficaz de la seguridad operacional no puede lograrse solamente siguiendo una orden o una adherencia estricta a las políticas y procedimientos. La promoción de la seguridad operacional afecta el comportamiento tanto individual como institucional y complementa las políticas, procedimientos y procesos de la organización, proporcionando un sistema de valores que respalda las actividades de seguridad operacional.

9.6.3 El proveedor de servicios debería establecer e implementar procesos y procedimientos que faciliten la comunicación eficaz en ambos sentidos a través de todos los niveles de la organización. Esto debería comprender una clara dirección estratégica desde los estratos más altos de la organización y la habilitación de la comunicación "jerárquica ascendente" que fomenta los comentarios abiertos y constructivos de todo el personal.

9.6.4 Instrucción y educación

9.6.4.1 En el Anexo 19 se establece que "el proveedor de servicios creará y mantendrá un programa de instrucción en seguridad operacional que garantice que el personal cuente con la instrucción y las competencias necesarias para cumplir sus funciones en el marco del SMS". También establece que "el alcance del programa de instrucción en seguridad operacional será apropiado para el tipo de participación que cada persona tenga en el SMS". El gerente de seguridad operacional es responsable de garantizar que se ha implantado un adecuado programa de instrucción en seguridad operacional. Esto comprende el suministro de información de seguridad operacional apropiada y pertinente a los problemas de seguridad específicos que enfrente la organización. Contar con personal capacitado y competente para cumplir sus funciones en el marco del SMS, sin importar su nivel en la organización, es un indicio del compromiso de la administración con un SMS eficaz. El programa de instrucción debería incluir instrucción inicial y periódica para mantener las competencias. La instrucción inicial en seguridad operacional debería considerar, como mínimo, los siguientes aspectos:

a) políticas y objetivos de seguridad operacional de la organización;

b) funciones de seguridad operacional institucional y responsabilidades relacionadas con la seguridad operacional;

c) principios básicos de la SRM;

d) sistemas de notificación de seguridad operacional;

e) procesos y procedimientos SMS de la organización; y

f) factores humanos.

9.6.4.2 La instrucción periódica de seguridad operacional debería concentrarse en los cambios que se introduzcan en las políticas, procesos y procedimientos SMS y deberían destacar problemas específicos de seguridad operacional pertinentes a la organización o enseñanzas obtenidas.

9.6.4.3 El programa de instrucción debería adaptarse a las necesidades de la función de cada individuo dentro del SMS. Por ejemplo, el nivel y profundidad de la instrucción para los gerentes superiores involucrados en los comités de seguridad operacional de la organización serán más extensos que para el personal involucrado directamente con la

entrega de productos o servicios de la organización. El personal que no participa directamente en las operaciones puede requerir solamente un panorama general de alto nivel del SMS de la organización.

Análisis de las necesidades de instrucción

9.6.4.4 Para la mayoría de las organizaciones, es necesario realizar evaluaciones de las necesidades de instrucción (TNA) formales para asegurar que existe una clara comprensión de la operación, las funciones de seguridad operacional del personal y la instrucción disponible. Una TNA típica se iniciará normalmente con la realización de un análisis de audiencias, que por lo general comprende las etapas siguientes:

a) Todos y cada uno de los miembros del personal del proveedor de servicios se verán afectados por la implementación del SMS, pero no de la misma manera o en el mismo grado. Se deberá identificar cada grupo de personal y las formas en que interactuarán con los procesos de gestión de la seguridad operacional, sus entradas y salidas, en particular con respecto a las funciones de seguridad operacional. Esta información debería estar disponible en las descripciones de puestos o funciones. Normalmente, comenzarán a surgir grupos de individuos con necesidades de aprendizaje similares. El proveedor de servicios debería considerar si vale la pena extender el análisis al personal de organizaciones externas interconectadas.

b) Identificar los conocimientos y las competencias necesarias para realizar cada función de seguridad operacional que requiere cada agrupamiento de personal.

c) Realizar un análisis para identificar las brechas entre las habilidades y conocimientos actuales en seguridad operacional de todo el personal y los necesarios para la realización eficaz de las funciones de seguridad operacional asignadas.

d) Identificar el enfoque más apropiado para desarrollar habilidades y conocimientos respecto de cada grupo con miras a elaborar un programa de instrucción adecuado a la participación de cada individuo o grupo en la gestión de la seguridad operacional. El programa de instrucción también debería considerar las necesidades continuas del personal en materia de conocimientos y competencias de seguridad operacional; estas necesidades se abordarán normalmente mediante un programa de instrucción periódica.

9.6.4.5 También es importante notificar el método apropiado para impartir la instrucción. El objetivo principal es que, al terminar la instrucción, el personal tenga competencia para ejecutar sus funciones en el marco del SMS. La consideración más importante es normalmente contar con instructores competentes, cuyo compromiso, capacidad didáctica y experiencia en gestión de la seguridad operacional tendrán consecuencias importantes en la eficacia de la instrucción impartida. El programa de instrucción en seguridad operacional también debería especificar las responsabilidades para la elaboración de contenidos y programas de instrucción así como la gestión de registros de instrucción y competencias.

9.6.4.6 La organización debería determinar quiénes deberían recibir capacitación y con qué grado de profundidad, dependiendo de su participación en el SMS. La mayoría de las personas que trabajan en la organización tendrán cierta relación directa o indirecta con la seguridad operacional de la aviación y, por consiguiente, tendrán algunas funciones en el marco del SMS. Esto se aplica a todo el personal directamente involucrado en la entrega de productos y servicios y al personal que participa en los comités de seguridad operacional de la organización. Algunos miembros del personal administrativo y de apoyo tendrán funciones SMS limitadas y requerirán cierta instrucción en la materia, dado que su trabajo todavía puede tener consecuencias indirectas sobre la seguridad operacional de la aviación.

9.6.4.7 El proveedor de servicios debería identificar las funciones SMS del personal y utilizar la información para examinar el programa de instrucción en la materia y asegurar que cada individuo recibe instrucción correspondiente a su participación en el SMS. El programa de instrucción en seguridad operacional debería especificar el contenido de la misma para el personal de apoyo, el personal de operaciones, los administradores y supervisores, los gerentes superiores y el ejecutivo responsable.

9.6.4.8 Debería impartirse instrucción específica en seguridad operacional para el ejecutivo responsable y los gerentes superiores que comprenda los temas siguientes:

a) concientización específica para nuevos ejecutivos y titulares de puestos responsables con respecto a sus obligaciones de rendición de cuentas y responsabilidades;

b) importancia de cumplir los requisitos de seguridad operacional nacionales e institucionales;

c) compromiso de la administración;

d) asignación de recursos;

e) promoción de la política de seguridad operacional y del SMS;

f) promoción de la cultura de seguridad operacional positiva;

g) comunicación eficaz de seguridad operacional entre los departamentos;

h) objetivos de seguridad operacional, SPT y niveles de alerta; y

i) política disciplinaria.

9.6.4.9 El propósito principal del programa de instrucción en seguridad operacional es garantizar que el personal, a todos los niveles de la organización, mantiene su competencia para la realización de sus funciones de seguridad operacional; por consiguiente, las competencias del personal deberían realizarse con carácter periódico.

9.6.5 Comunicación de la seguridad operacional

9.6.5.1 El proveedor de servicios debería comunicar los objetivos y procedimientos del SMS de la organización a todo el personal apropiado. Debería existir una estrategia de comunicación que permita que la comunicación de seguridad operacional sea transmitida por el método más apropiado sobre la base de la función de cada individuo y su necesidad de recibir dicha información. Esto puede realizarse mediante circulares informativas, avisos, boletines, sesiones informativas o cursos de instrucción. El gerente de seguridad operacional también debería garantizar que las enseñanzas extraídas de investigaciones y casos prácticos o experiencias, tanto internos como de otras organizaciones, se distribuyen ampliamente. Por consiguiente, la comunicación de seguridad operacional se dirige a:

a) *garantizar que el personal es plenamente consciente del SMS;* esta es una buena forma de promover la política y los objetivos de seguridad operacional de la organización.

b) *transmitir información crítica para la seguridad operacional;* la información crítica para la seguridad operacional es información específica relacionada con problemas y riesgos de seguridad operacional que podrían exponer a la organización a ese tipo de riesgo. Podría tratarse de información recopilada de fuentes internas o externas como enseñanzas obtenidas o relacionadas con controles de riesgos de seguridad operacional. El proveedor de servicios determina el tipo de información que se considera crítica para la seguridad operacional así como la oportunidad de comunicarla.

c) *crear conciencia sobre nuevos controles de riesgos de seguridad operacional y medidas correctivas;* los riesgos de seguridad operacional que enfrenta el proveedor de servicios cambiarán con el tiempo, y si se trata de un nuevo riesgo de seguridad operacional que ha sido identificado o de cambios en los controles de riesgos de seguridad operacional dichos cambios deberán comunicarse al personal apropiado.

d) *proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados;* cuando se actualizan los procedimientos de seguridad operacional es importante que las personas apropiadas tengan conocimientos de dichos cambios.

e) *promover una cultura de seguridad operacional positiva y alentar al personal a identificar y notificar peligros;* la comunicación de seguridad operacional es en ambos sentidos. Es importante que todo el personal comunique los problemas de seguridad operacional a la organización a través del sistema de notificaciones de seguridad operacional.

f) *proporcionar comentarios e información;* proporcionar comentarios al personal que presenta notificaciones de seguridad operacional respecto de las medidas que se han adoptado para abordar las preocupaciones identificadas.

9.6.5.2 Los proveedores de servicios deberían considerar si algunos de los tipos de información de seguridad operacional indicados anteriormente deben comunicarse a organizaciones externas.

9.6.5.3 Los proveedores de servicios deberían evaluar la eficacia de su comunicación de seguridad operacional mediante la verificación de que el personal ha recibido y comprendido la información crítica sobre seguridad operacional que se ha distribuido. Esto puede hacerse como parte de las actividades de auditoría interna o al evaluar la eficacia del SMS.

9.6.5.4 Las actividades de promoción de la seguridad operacional deberían llevarse a cabo durante todo el ciclo de vida del SMS, y no solo al comienzo de este.

9.7 PLANIFICACIÓN DE LA IMPLEMENTACIÓN

9.7.1 Descripción del sistema

9.7.1.1 Una descripción del sistema contribuye a identificar los procesos institucionales, incluyendo sus interfaces, para definir el alcance del SMS. Esto proporciona una oportunidad para identificar cualquier brecha relacionada con los componentes y elementos del SMS del proveedor de servicios y puede servir de punto de partida para identificar peligros institucionales y operacionales. Una descripción del sistema sirve para identificar las características del producto, el servicio o la actividad de modo que la SRM y el aseguramiento de la seguridad operacional resulten eficaces.

9.7.1.2 La mayoría de las organizaciones constan de una compleja red de interfaces e interacciones que involucran diferentes departamentos internos así como diferentes organizaciones externas que contribuyen al funcionamiento seguro de la organización. El uso de una descripción del sistema permite que la organización tenga un panorama más claro de sus muchas interacciones e interfaces. Ello facilitará la mejor gestión de los riesgos de seguridad operacional y los controles de estos si están bien descritos, y contribuirá a comprender las consecuencias de los cambios para los procesos y procedimientos del SMS.

9.7.1.3 Al considerar la descripción del sistema, es importante comprender que un “sistema” es un conjunto de elementos que funcionan conjuntamente como partes de una red interconectada. En un SMS, se trata de cualesquiera productos, personas, procesos, procedimientos, instalaciones, servicios y otros aspectos (incluyendo factores externos) de la organización que se relacionan con las actividades de seguridad operacional de la aviación de esta y pueden afectarlas. A menudo un “sistema” es un conjunto de sistemas que también pueden considerarse como un sistema con subsistemas. Estos sistemas y sus interacciones mutuas constituyen las fuentes de peligros y contribuyen al control de los riesgos de seguridad operacional. Los sistemas importantes comprenden aquellos que podrían tener consecuencias directas para la seguridad operacional de la aviación y aquellos que afectan la capacidad de una organización de llevar a cabo una gestión eficaz de la seguridad operacional.

9.7.1.4 En la documentación del SMS debería incluirse una reseña general de la descripción del sistema y las interfaces del SMS. La descripción del sistema puede comprender una lista no ordenada con viñetas haciendo referencia a políticas y procedimientos. Una representación gráfica, como un diagrama de flujo de procesos o un organigrama anotado de la institución, puede resultar suficiente para algunas organizaciones. La organización debería utilizar el método y formato que mejor convenga a su funcionamiento.

9.7.1.5 Debido a que cada organización es única, no existe un método genérico o universal para la implantación del SMS. Se espera que cada organización implemente un SMS que funcione en forma adecuada para su situación singular. Cada organización debería definir por sí misma la forma en que cumplirá los requisitos fundamentales. Para lograr esto, es importante que cada organización prepare una descripción del sistema que identifique sus estructuras, procesos y arreglos empresariales institucionales que considere importantes para las funciones de gestión de la seguridad operacional. Sobre la base de esta descripción del sistema, la organización debería identificar o elaborar políticas, procesos y procedimientos que establezcan sus propios requisitos en materia de gestión de la seguridad operacional.

9.7.1.6 Cuando una organización opta por introducir cambios importantes o sustantivos en los procesos identificados en la descripción del sistema, debería considerarse que dichos cambios podrían afectar su evaluación básica de los riesgos de seguridad operacional. Así pues, debería examinarse la descripción del sistema como parte de la gestión de los procesos de cambio.

9.7.2 Gestión de las interfaces

Los riesgos de seguridad operacional de los proveedores de servicios se ven afectados por las interfaces que pueden ser internas (entre departamentos) o externas (otros proveedores de servicios o servicios contratados). Mediante la identificación y gestión de estas interfaces el proveedor de servicios tendrá más control sobre cualesquiera riesgos de seguridad operacional relacionados con las mismas. Estas interfaces deberían definirse en la descripción del sistema.

9.7.3 Identificación de interfaces del SMS

9.7.3.1 Inicialmente, los proveedores de servicios deberían concentrarse en las interfaces relacionadas con sus actividades empresariales. La identificación de esas interfaces, internas y externas, debería detallarse en la descripción del sistema que establece el alcance del SMS.

9.7.3.2 En la Figura 9-3 se muestra un ejemplo de interfaces del SMS. El objetivo es producir una lista completa de todas las interfaces, pues puede haber interfaces SMS de las cuales la organización no tiene necesariamente pleno conocimiento o sin acuerdos formales establecidos, como las que se dan con las compañías de electricidad o de mantenimiento de edificios.

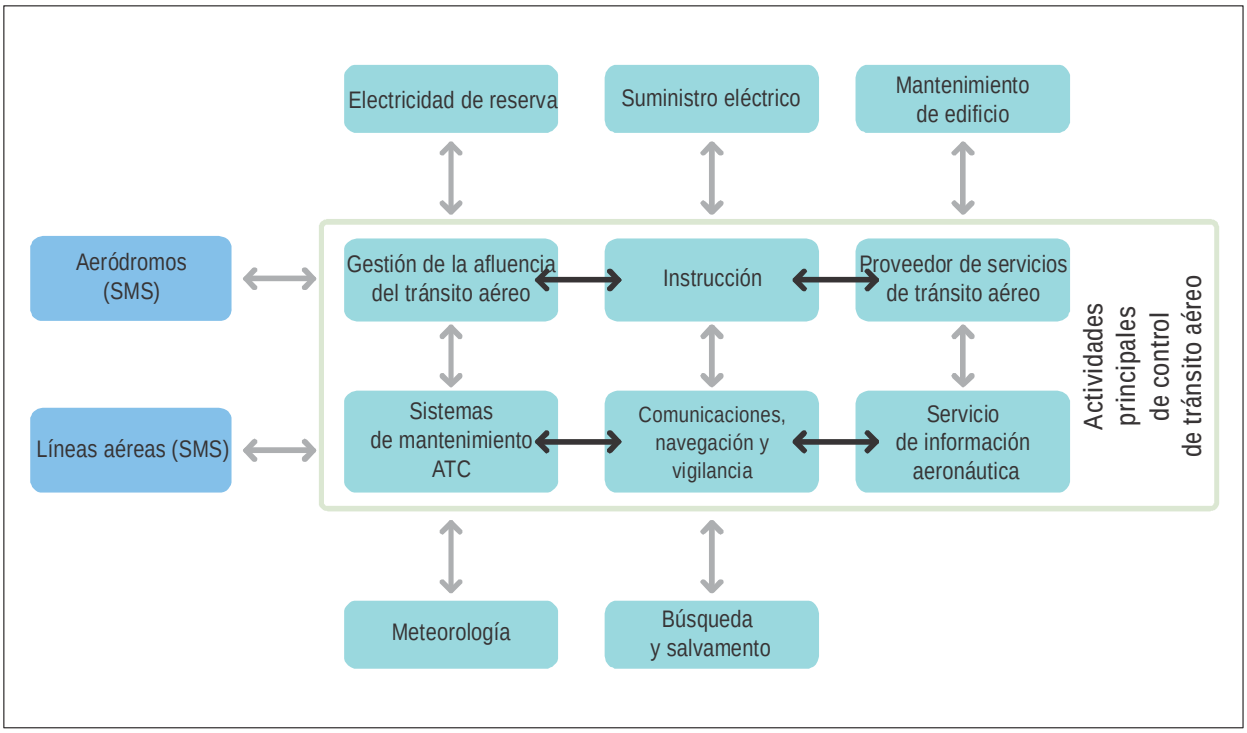


Figura 9-3. Ejemplo de interfaces del SMS de un proveedor de servicios de tránsito aéreo

9.7.3.3 Algunas de las interfaces internas pueden relacionarse con sectores empresariales que no están directamente relacionados con la seguridad operacional, como comercialización, finanzas, aspectos jurídicos y recursos humanos. Estos sectores pueden tener consecuencias para la seguridad operacional a través de sus decisiones que afectan los recursos internos y las inversiones, así como mediante acuerdos y contratos con organizaciones externas pero sin abordar necesariamente la seguridad operacional.

9.7.3.4 Una vez identificadas las interfaces del SMS, el proveedor de servicios debería considerar su criticidad relativa. Esto le permite priorizar la gestión de las interfaces más críticas y sus posibles riesgos de seguridad operacional. Se debería considerar lo siguiente:

a) lo que se proporciona;

b) por qué es necesaria;

c) si las organizaciones involucradas tienen implantado un SMS u otro sistema de gestión; y

d) si la interfaz entraña compartir datos o información sobre seguridad operacional.

Evaluación de las consecuencias de las interfaces para la seguridad operacional

9.7.3.5 Después de lo anterior el proveedor de servicios debería identificar cualesquiera peligros relacionados con las interfaces y llevar a cabo una evaluación de riesgos de seguridad operacional utilizando sus procesos de identificación de peligros y evaluación de riesgos de seguridad operacional.

9.7.3.6 Sobre la base de los riesgos de seguridad operacional identificados, el proveedor de servicios puede considerar trabajar conjuntamente con la otra organización para determinar y definir una estrategia apropiada de control de riesgos de seguridad operacional. Mediante la participación de la otra organización, pueden estar en condiciones de contribuir a identificar peligros, evaluar riesgos de seguridad operacional y determinar el control apropiado para dichos riesgos. Es necesario una actividad en colaboración debido a que la percepción de los riesgos de seguridad operacional no puede ser la misma para cada organización. El control de riesgos debería ser ejecutado por el proveedor de servicios o la organización externa.

9.7.3.7 También es importante reconocer que cada organización involucrada es responsable y de identificar y gestionar los peligros que afectan a su propia organización. Esto puede significar que el carácter crítico de la interfaz es diferente para cada organización dado que estas pueden aplicar diferentes clasificaciones de riesgos y tener diferentes prioridades para los mismos (en términos de rendimiento en materia de seguridad operacional, recursos, tiempo, etc.).

Gestión y vigilancia de las interfaces

9.7.3.8 El proveedor de servicios es responsable de gestionar y observar las interfaces para garantizar el seguro suministro de sus productos y servicios. Esto garantizará, a su vez, que las interfaces se gestionan eficazmente y permanecen actualizadas y pertinentes. Los acuerdos formales son una forma eficaz de lograr lo anterior dado que las interfaces y responsabilidades conexas pueden definirse claramente en los mismos. Todo cambio en las interfaces y las consecuencias conexas deberían comunicarse a las organizaciones pertinentes.

9.7.3.9 Entre los retos relacionados con la capacidad del proveedor de servicios para gestionar los riesgos de seguridad operacional de las interfaces figuran los siguientes:

a) los controles de riesgos de seguridad operacional de una organización no son compatibles con los de otras organizaciones;

b) la disposición de ambas organizaciones para aceptar cambios a sus propios procesos y procedimientos;

c) insuficiencia de recursos o conocimientos técnicos disponibles para gestionar y observar la interfaz; y

d) el número y la ubicación de las interfaces.

9.7.3.10 Es importante reconocer la necesidad de coordinación entre las organizaciones involucradas en la interfaz. La coordinación eficaz debería comprender:

a) aclaración de las funciones y responsabilidades de cada organización;

b) acuerdo de decisiones sobre las medidas que han de adoptarse (p. ej., medidas de control) de riesgos de seguridad operacional y cronogramas;

c) identificación de las necesidades de información de seguridad operacional que deben compartirse y comunicarse;

d) cómo y cuándo debería tener lugar la coordinación (equipo especial, reuniones regulares, reuniones ad hoc o especiales); y

e) acuerdos sobre soluciones que beneficien a ambas organizaciones pero que no afectan negativamente la eficacia del SMS.

9.7.3.11 Todos los problemas de seguridad operacional o los riesgos en la materia relacionados con las interfaces deberían documentarse y ponerse a disposición de cada organización para compartirlos y examinarlos. Esto permitirá intercambiar las experiencias obtenidas y reunir los datos de seguridad operacional que resultarán valiosos para ambas organizaciones. Pueden lograrse beneficios de seguridad operacional mediante la mejora de la seguridad alcanzada por cada organización como resultado de los conocimientos compartidos de los riesgos de seguridad operacional y las responsabilidades.

9.7.4 Adaptabilidad y escalonamiento del SMS

9.7.4.1 El SMS de una organización, incluyendo políticas, procesos y procedimientos, debería reflejar la magnitud y complejidad de la organización y sus actividades y tener en cuenta lo siguiente:

a) la estructura de organización y disponibilidad de recursos;

b) magnitud y complejidad de la organización (incluyendo múltiples sitios y bases); y

c) la complejidad de las actividades y las interfaces con organizaciones externas.

9.7.4.2 El proveedor de servicios debería realizar un análisis de sus actividades a efectos de determinar el adecuado nivel de recursos para gestionar el SMS. Esto debería comprender la determinación de la estructura de organización necesaria para gestionar el SMS, incluyendo consideraciones sobre quién será responsable de gestionar y mantener el SMS, los comités de seguridad operacional que sean necesarios, en caso de haberlos, y la necesidad de contar con especialistas específicos en seguridad operacional.

Consideraciones de riesgos de seguridad operacional

9.7.4.3 Independientemente de la magnitud del proveedor de servicios, la adaptabilidad y el escalonamiento deberían ser también función del riesgo de seguridad operacional inherente a las actividades del proveedor de servicios. Incluso las organizaciones pequeñas pueden estar involucradas en actividades que pueden entrañar considerables riesgos de seguridad operacional. Por consiguiente, la capacidad de gestión de la seguridad operacional debería ser conmensurable con el riesgo de seguridad operacional que se ha de gestionar.

Datos e información sobre seguridad operacional y su análisis

9.7.4.4 Para las organizaciones pequeñas, el bajo volumen de datos puede significar que es más difícil identificar tendencias o cambios en el rendimiento en materia de seguridad operacional. Ello podría exigir reuniones para plantear y analizar problemas de seguridad operacional con expertos apropiados, lo que podría tener un carácter más cualitativo que cuantitativo pero que contribuirá a identificar peligros y riesgos para el proveedor de servicios. La colaboración con otros proveedores de servicios o asociaciones industriales puede resultar útil, puesto que pueden tener datos que el proveedor de servicios no posea. Por ejemplo, los proveedores de servicios más pequeños pueden intercambiar información con organizaciones u operaciones similares a efectos de compartir información sobre riesgos de seguridad operacional e identificar tendencias de rendimiento en la materia. Los proveedores de servicios deberían analizar y procesar en forma adecuada sus datos internos, aunque estos puedan ser limitados.

9.7.4.5 Los proveedores de servicios con muchas interacciones e interfaces deberán considerar la forma en que recopilan datos e información sobre seguridad operacional de múltiples organizaciones. Esto podría resultar en la recolección de grandes volúmenes de datos que han de consolidarse y analizarse posteriormente. Estos proveedores de servicios deberían utilizar un método apropiado para gestionar tales datos. También debería considerarse la calidad de los datos recopilados y el uso de taxonomías para ayudar en el análisis de los mismos.

9.7.5 Integración de los sistemas de gestión

9.7.5.1 La gestión de la seguridad operacional debería considerarse como parte de un sistema de gestión (y no aisladamente). Por consiguiente, un proveedor de servicios puede implementar un sistema de gestión integrado que incluya al SMS. El sistema de gestión integrado puede utilizarse para captar múltiples certificados, autorizaciones o aprobaciones o para abarcar otros sistemas de gestión empresarial tales como los sistemas de gestión de la calidad, la seguridad y protección, salud laboral y medio ambiente. Esto se lleva a cabo para evitar la duplicación y aprovechar sinergias mediante la gestión de los riesgos de seguridad operacional en múltiples actividades. Por ejemplo, cuando un proveedor de servicios es titular de varios certificados puede optar por implementar un único sistema de gestión que abarque todas sus actividades. El proveedor de servicios debería decidir el medio de integración o segregación de su SMS que se adapte mejor a sus necesidades empresariales o institucionales.

9.7.5.2 Un sistema típico de gestión integrada puede comprender lo siguiente:

a) un sistema de gestión de la calidad (QMS);

b) un sistema de gestión de la seguridad operacional (SMS);

c) un sistema de gestión de la seguridad de la aviación (SeMS). En el *Manual de seguridad de la aviación* (Doc 8973 — distribución limitada) figura más orientación al respecto;

d) un sistema de gestión ambiental (EMS);

e) un sistema de gestión sobre cuestiones de salud y seguridad en el trabajo (OHSMS);

f) un sistema de gestión financiera (FMS);

g) un sistema de gestión de documentación (DMS); y

h) un sistema de gestión de riesgos asociados a la fatiga (FRMS).

9.7.5.3 El proveedor de servicios puede optar por integrar estos sistemas de gestión sobre la base de sus necesidades singulares. Los procesos de gestión de riesgos y los procesos de auditoría interna son características fundamentales de la mayoría de estos sistemas de gestión. Cabe reconocer que los riesgos y los controles de riesgos incluidos en cualquiera de estos sistemas podrían tener consecuencias sobre otros sistemas. Además, puede haber otros sistemas operacionales relacionados con las actividades empresariales que puedan también integrarse, como la gestión de proveedores, gestión de instalaciones, etc.

9.7.5.4 El proveedor de servicios también puede considerar la aplicación del SMS a otros sectores que no tienen requisitos normativos actuales para SMS. Los proveedores de servicios deberían determinar los medios para integrar o segregar su sistema de gestión que resulten más adecuados a su modelo empresarial, entorno operacional, requisitos normativos y estatutarios así como las expectativas de la comunidad aeronáutica. Cualquiera fuera la opción que se adopte, se debería garantizar que satisface los requisitos SMS.

Beneficios y retos de la integración de sistemas de gestión

9.7.5.5 La integración de diferentes sectores en un único sistema de gestión mejorará la eficiencia mediante:

a) la reducción de la duplicación y la superposición de procesos y recursos;

b) la reducción de posibles responsabilidades y relaciones conflictivas;

c) la consideración de impactos más amplios de los riesgos y las oportunidades en todas las actividades; y

d) la habilitación de observación y gestión eficaces del rendimiento en todas las actividades.

9.7.5.6 Entre los posibles retos de la integración de sistemas de gestión figuran los siguientes:

a) los sistemas existentes pueden tener diferentes gerentes funcionales que se resistan a la integración, lo que provocaría conflictos;

b) puede haber resistencias al cambio por parte del personal afectado por la integración puesto que ello exigirá mayor cooperación y coordinación;

c) las consecuencias para la cultura de seguridad operacional general dentro de la organización, puesto que pueden haber diferentes culturas con respecto a cada sistema, lo que crearía conflictos;

d) reglamentos que impidan dicha integración o diferentes reglamentadores y órganos normativos que tengan expectativas divergentes sobre cómo satisfacer sus requisitos; y

e) la integración de sistemas de gestión diferentes (como los QMS y SMS) pueden crear tareas adicionales a efectos de demostrar que se satisfacen los requisitos individuales.

9.7.5.7 Para maximizar los beneficios de la integración y abordar los retos conexos, el compromiso y el liderazgo de la administración superior resultan esenciales para la gestión eficaz de los cambios. Es importante identificar las personas que tengan responsabilidad general por el sistema de gestión integrado.

9.7.6 Integración de SMS y QMS

9.7.6.1 Algunos proveedores de servicios tienen SMS y QMS. Estos sistemas están a veces integrados en un único sistema de gestión. El QMS se define generalmente como la estructura institucional y las responsabilidades, los recursos, los procesos y los procedimientos conexos que son necesarios para establecer y promover un sistema de aseguramiento y mejora de la calidad continuos mientras se suministra un producto o servicio.

9.7.6.2 Ambos sistemas son complementarios; el SMS se concentra en la gestión de los riesgos de seguridad operacional y en el rendimiento en la materia, mientras que el QMS se concentra en el cumplimiento de los reglamentos y requisitos prescriptivos para satisfacer las expectativas y obligaciones contractuales del cliente. Los objetivos del SMS son identificar peligros relacionados con la seguridad operacional, evaluar el riesgo conexo e implementar controles de riesgos eficaces. En contraste, el QMS se centra en el suministro constante de productos y servicios que cumplan las especificaciones pertinentes. No obstante, tanto el SMS como el QMS:

a) deberían planificarse y gestionarse;

b) implican todas las funciones institucionales relacionadas con el suministro de productos y servicios de aviación;

c) identifican procesos y procedimientos ineficaces;

d) buscan una mejora continua; y

e) tienen los mismos objetivos de proporcionar a los clientes productos y servicios seguros y fiables.

9.7.6.3 El SMS se concentra en:

a) la identificación de peligros relacionados con la seguridad operacional enfrentados por la organización;

b) la evaluación del riesgo de seguridad operacional conexo;

c) la implementación de controles de riesgos de seguridad operacional eficaces para mitigar dichos riesgos;

d) la medición del rendimiento en materia de seguridad operacional; y

e) el mantenimiento de una asignación adecuada de recursos para satisfacer requisitos de rendimiento en materia de seguridad operacional.

9.7.6.4 El QMS se concentra en:

a) el cumplimiento de reglamentos y requisitos;

b) la coherencia en la entrega de productos y servicios;

c) la satisfacción de normas de rendimiento especificadas; y

d) la entrega de productos de servicios adecuados a sus propósitos y libres de defectos o errores.

9.7.6.5 La observación del cumplimiento de los reglamentos es necesaria para asegurar que los controles de riesgo de seguridad operacional, aplicados en forma de reglamentos, se implementan y observan eficazmente por el proveedor de servicios. También deberían analizarse y abordarse las causas y los factores contribuyentes de cualquier caso de incumplimiento.

9.7.6.6 Dado los aspectos complementarios del SMS y el QMS, es posible integrar ambos sistemas sin poner en peligro la función de cada cual. Esto puede resumirse como sigue:

a) un SMS recibe el respaldo de los procesos del QMS como auditorías, inspecciones, investigaciones, análisis de causas básicas, diseño de procesos y medidas preventivas;

b) un QMS puede identificar problemas de seguridad operacional o puntos débiles en los controles de riesgos de seguridad operacional;

c) un QMS puede anticipar problemas de seguridad operacional que existan a pesar del cumplimiento de normas y especificaciones de la organización;

d) los principios, políticas y prácticas de calidad están vinculados a los objetivos de la gestión de seguridad operacional; y

e) las actividades del QMS deberían considerar los peligros identificados y los controles de riesgos de seguridad operacional para planificar y llevar a cabo auditorías internas.

9.7.6.7 En conclusión, en un sistema de gestión integrado con objetivos unificados y toma de decisiones que considere las consecuencias más amplias en todas las actividades, los procesos de gestión de la calidad y la seguridad operacional tendrán carácter ampliamente complementario y apoyarán el logro de los objetivos generales de seguridad operacional.

9.7.7 Análisis de brechas e implementación del SMS

9.7.7.1 Antes de implementar un SMS, el proveedor de servicios debería realizar un análisis de brechas. Este análisis para los procesos y procedimientos existentes de la gestión de la seguridad operacional del proveedor de servicios con los requisitos del SMS determinados por el Estado. Es probable que el proveedor de servicios ya haya implantado algunas de las funciones SMS. El desarrollo del SMS debería basarse en las políticas y procesos institucionales existentes. El análisis de brechas identifica las brechas que deberían abordarse en un plan de implementación SMS que defina las acciones necesarias para implementar un SMS plenamente funcional y eficaz.

9.7.7.2 El plan de implementación del SMS debería proporcionar un panorama claro de los recursos, tareas y procesos necesarios para implementar el sistema. La cronología y la secuencia del plan de implementación pueden depender de varios factores que serán específicos a cada organización, como los siguientes:

a) requisitos normativos, de cliente y estatutarios;

b) posesión de múltiples certificados (con fechas de implementación normativa posiblemente diferentes);

c) la medida en que el SMS puede basarse en estructuras y procesos existentes;

d) la disponibilidad de recursos y presupuestos;

e) las interdependencias entre diferentes etapas (debería implementarse un sistema de notificación antes de establecer un sistema de análisis de datos); y

f) la cultura de seguridad operacional existente.

9.7.7.3 El plan de implementación del SMS debería elaborarse en consulta con el ejecutivo responsable y otros administradores superiores y debería incluir la designación del responsable de las actividades conjuntamente con cronogramas. El plan debería abordar la coordinación con organizaciones o contratistas externos, cuando corresponda.

9.7.7.4 El plan de implementación del SMS puede documentarse en formas diferentes, que varían de una simple hoja de cálculo hasta un soporte lógico especializado de gestión de proyectos. El plan debería ser vigilado regularmente y actualizado según sea necesario y también aclarar cuándo puede considerarse que un determinado elemento ha sido implementado satisfactoriamente.

9.7.7.5 Tanto el Estado como el proveedor de servicios deberían reconocer que el logro de un SMS eficaz puede insumir varios años. Los proveedores de servicios deberían consultar con su Estado puesto que puede ser necesario aplicar un enfoque por etapas para la implantación del SMS.

— FIN —

ISBN 978-92-9258-655-3

