Doc 9859
AN/474

Manual de gestión de la seguridad operacional (SMM)

Aprobado por el Secretario General
y publicado bajo su responsabilidad

Tercera edición — 2013

Organización de Aviación Civil Internacional

Doc 9859
AN/474

Manual de gestión de la seguridad operacional (SMM)

Aprobado por el Secretario General
y publicado bajo su responsabilidad

Tercera edición — 2013

Organización de Aviación Civil Internacional

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

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

Primera edición, 2006
Segunda edición, 2009
Tercera edición, 2013

Doc 9859, *Manual de gestión de la seguridad operacional (SMM)*
Número de pedido: 9859
ISBN 978-92-9249-315-8

ENMIENDAS

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

REGISTRO DE ENMIENDAS Y CORRIGENDOS

ENMIENDAS		
Núm.	Fecha	Anotada por

CORRIGENDOS		
Núm.	Fecha	Anotado por

ÍNDICE

Página

Página

Página

GLOSARIO

ABREVIATURAS Y ACRÓNIMOS

AD	Directriz de aeronavegabilidad
ADREP	Notificación de datos sobre accidentes/incidentes (OACI)
AIB	Comité de investigación de accidentes
AIR	Aeronavegabilidad
ALoSP	Nivel aceptable del rendimiento en materia de seguridad operacional
AMAN	Maniobra abrupta
AME	Mecánico de mantenimiento de aeronaves
AMO	Organismo de mantenimiento reconocido
AMS	Programa de mantenimiento de aeronaves
ANS	Servicios de navegación aérea
AOC	Certificado de explotador de servicios aéreos
AOG	Aeronave en tierra
ASB	Boletín de servicio de alerta
ATC	Control de tránsito aéreo
ATM	Gestión del tránsito aéreo
ATS	Servicios de tránsito aéreo
CAA	Autoridad de aviación civil
CAN	Aviso de medida correctiva
CBA	Análisis de costo/beneficios
CEO	Funcionario ejecutivo principal
CFIT	Impacto contra el suelo sin pérdida de control
Cir	Circular
CM	Control de la condición
CMA	Enfoque de observación continua
CMC	Centro de gestión de crisis
CNS	Comunicaciones, navegación y vigilancia
CP	Puesto de mando
CRM	Gestión de recursos de tripulación
CVR	Registrador de la voz en el puesto de pilotaje
D&M	Diseño y fabricación
DGR	Reglamentos sobre mercancías peligrosas
DMS	Sistema de gestión de documentación
DOA	Aprobación como organización de diseño
Doc	Documento
EAD	Directiva de aeronavegabilidad de emergencia
DEC	Control de escalada
ECCAIRS	Centro europeo de coordinación de sistemas de informes de incidentes y accidentes de aviación
EDTO	Operación con tiempo de desviación extendido
EF	Factor de escalada

EMC	Centro de gestión de emergencia
EMS	Sistema de gestión ambiental
ERP	Plan de respuesta ante emergencias
FDR	Registrador de datos de vuelo
FH	Horas de vuelo
FIR	Región de información de vuelo
FL	Nivel de vuelo
FMS	Sistema de gestión financiera
FRMS	Sistema de gestión de riesgos asociados a la fatiga
FTL	Limitación del tiempo de vuelo
FTM	Gestión técnica de la flota
GAQ	Cuestionario del análisis de brechas
H	Peligro
HF	Factores humanos
HIRA	Identificación de peligros y evaluación de riesgos
HIRM	Identificación de peligros y mitigación de riesgos
IATA	Asociación del Transporte Aéreo Internacional
IFSD	Parada de motor en vuelo
ILS	Sistema de aterrizaje por instrumentos
IMC	Condiciones meteorológicas de vuelo por instrumentos
ISO	Organización Internacional de Normalización
iSTARS	Sistema integrado de análisis y notificación de tendencias de seguridad operacional
ITM	Gestión técnica del inventario
kg	Kilogramos
LEI	Falta de aplicación eficaz
LOC-I	Pérdida de control en vuelo
LOFT	Instrucción de vuelo orientada a las líneas aéreas
LOS	Pérdida de separación
LOSA	Auditoría de la seguridad de las operaciones de línea
LRU	Unidad reemplazable en el sitio
LSI	Inspección de la estación de línea
MCM	Manual de control de mantenimiento
MDR	Informe obligatorio de defectos
MEDA	Ayuda en caso de decisiones erróneas en el mantenimiento
MEL	Lista de equipo mínimo
MFF	Vuelo de flota mixta
MOR	Informe obligatorio de sucesos
MPD	Documento de planificación de mantenimiento
MRM	Gestión de los recursos de mantenimiento
MRO	Organización de reparación de mantenimiento
MSL	Nivel medio del mar
N/A	No corresponde

OACI	Organización de Aviación Civil Internacional
OEM	Fabricante de equipo original
OHSMS	Sistema de gestión sobre cuestiones de salud y seguridad en el trabajo
OPS	Operaciones
ORP	Perfil de riesgo de la organización
OSC	Cultura de seguridad operacional de la organización
OSHE	Seguridad, salud y ambiente en el trabajo
PC	Control preventivo
PMI	Inspector principal de mantenimiento
POA	Aprobación como organización de producción
POI	Inspector principal de operaciones
QA	Aseguramiento de la calidad
QC	Control de la calidad
QM	Gestión de la calidad
QMS	Sistema de gestión de la calidad
RAIO	Organización regional de investigación de accidentes e incidentes
RM	Medida de recuperación
RSOO	Organización regional de vigilancia de la seguridad operacional
SA	Garantía de seguridad operacional
SAG	Grupo de acción de seguridad operacional
SARPS	Normas y métodos recomendados (OACI)
SB	Boletín de servicio
SCF-NP	Falla en los componentes del sistema — No de la planta eléctrica
SD	Desviación estándar
SDCPS	Sistema de recopilación y procesamiento de datos sobre seguridad operacional
SeMS	Sistema de gestión de la seguridad de la aviación
SHEL	Software/hardware/entorno/liveware
SM	Gestión de la seguridad operacional
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
SOP	Procedimientos operacionales normalizados
SPI	Indicador de rendimiento en materia de seguridad operacional
SRB	Consejo de revisión de seguridad operacional
SRC	Comité de revisión de seguridad operacional
SRM	Gestión de riesgos de seguridad operacional
SSO	Oficina de servicios de seguridad operacional
SSP	Programa estatal de seguridad operacional
STDEVP	Desviación estándar de la población
TBD	Se determinará
TOR	Atribuciones
UC	Consecuencia final
UE	Evento inseguro
USOAP	Programa universal de auditoría de la vigilancia de la seguridad operacional (OACI)
WIP	Obras en progreso

DEFINICIONES

Nota.— Las siguientes definiciones se desarrollaron mientras se redactaba el Anexo 19 — Gestión de la seguridad operacional*. Cuando el Anexo 19 sea aplicable en noviembre de 2013, si existen diferencias en las definiciones, prevalecerán aquellas contenidas en dicho Anexo.*

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 SSP del Estado o del SMS del proveedor de servicio.

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.

Indicadores de alto impacto. Indicadores de rendimiento en materia de seguridad operacional relacionados con el control y la medición de sucesos de alto impacto, como accidentes o incidentes graves. A menudo, los indicadores de alto impacto se conocen como indicadores reactivos.

Indicadores de bajo impacto. Indicadores de rendimiento en materia de seguridad operacional relacionados con el control y la medición de sucesos, eventos o actividades de bajo impacto, como incidentes, hallazgos que no cumplen las normas o irregularidades. Los indicadores de bajo impacto se conocen a menudo como indicadores proactivos/predictivos.

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

Nivel aceptable del rendimiento en materia de seguridad operacional (ALoSP). Nivel mínimo de rendimiento en materia de seguridad operacional de la aviación civil en un Estado, como se define en el programa estatal de seguridad operacional, o de un proveedor de servicios, como se define en el sistema de gestión de la seguridad operacional, expresado en términos de objetivos e indicadores de rendimiento en materia de seguridad operacional.

Programa estatal de seguridad operacional. Conjunto integrado de reglamentación y actividades encaminados 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 gravedad predichas de las consecuencias o los resultados de un peligro.

Sistema de gestión de la seguridad operacional. Enfoque sistemático para la gestión de la seguridad operacional, que incluye las estructuras organizativas, líneas de responsabilidad, políticas y procedimientos necesarios.

Capítulo 1

DESCRIPCIÓN GENERAL DEL MANUAL

1.1 GENERALIDADES

1.1.1 Esta tercera edición del *Manual de gestión de la seguridad operacional (SMM)* (Doc 9859) de la OACI reemplaza a la segunda edición, publicada en 2009, en su totalidad. También reemplaza al *Manual de prevención de accidentes* (Doc 9422) de la OACI, el que está obsoleto.

1.1.2 Este manual tiene como fin proporcionar a los Estados una guía sobre el desarrollo y la implementación de un programa estatal de seguridad operacional (SSP), de acuerdo con las normas y los métodos recomendados (SARPS) internacionales incluidos en el Anexo 1 — *Licencias al personal*, Anexo 6 — *Operación de aeronaves*, Anexo 8 — *Aeronavegabilidad*, Anexo 11 — *Servicios de tránsito aéreo*, Anexo 13 — *Investigación de accidentes e incidentes de aviación* y el Anexo 14 — *Aeródromos, V*olumen I — *Diseño y operaciones de aeródromos*. Se debe tener presente que las disposiciones del SSP se incorporarán en el Anexo 19 — *Gestión de la seguridad operacional*, el que aún estaba en desarrollo a la fecha de publicación de esta tercera edición. Este manual también ofrece material guía sobre el establecimiento de requisitos del sistema de gestión de la seguridad operacional (SMS) por parte de los Estados, así como también, sobre el desarrollo y la implementación del SMS por parte de los proveedores de productos y servicios afectados.

1.1.3 Se debe tener en cuenta que este manual tiene como fin usarse junto con otros materiales guía correspondientes, los que pueden usarse para complementar o mejorar los conceptos o las guías del presente documento.

Nota.— En el contexto de la gestión de la seguridad operacional, el término "proveedor de servicios" o "proveedor de productos y servicios" hace referencia a cualquier organización que proporcione productos o servicios de aviación. Por tanto, los términos abarcan organizaciones de capacitación reconocidas que están expuestas a riesgos de seguridad operacional durante la entrega de sus servicios, explotadores de aeronaves, organismos de mantenimiento reconocidos, organizaciones responsables del diseño o fabricación de aeronaves, proveedores de servicios de tránsito aéreo y aeródromos certificados.

1.2 OBJETIVO

El objetivo de este manual es proporcionar a los Estados y proveedores de servicios:

a) una descripción general de los aspectos básicos de la gestión de la seguridad operacional;

b) un resumen de los SARPS de la gestión de seguridad operacional de la OACI, incluidos en los Anexos 1, 6, 8, 11, 13 y 14;

c) una guía sobre cómo desarrollar e implementar un SSP que cumpla con los SARPS pertinentes de la OACI, como un marco de trabajo reglamentario armonizado para la vigilancia del SMS de los proveedores de productos y servicios; y

d) una guía sobre el desarrollo, la implementación y el mantenimiento del SMS.

1.3 ESTRUCTURA

El Capítulo 1 presenta una descripción general del manual mientras que el Capítulo 2 analiza los conceptos y los procesos fundamentales de la gestión de la seguridad operacional. El Capítulo 3 proporciona una recopilación de los SARPS de gestión de la seguridad operacional de la OACI, incluidos en los Anexos 1, 6, 8, 11, 13 y 14. Finalmente, los Capítulos 4 y 5 detallan un enfoque progresivo del desarrollo, la implementación y el mantenimiento de un SSP y SMS. Los últimos dos capítulos también incluyen apéndices que ofrecen guías prácticas e ilustraciones. El documento adjunto al manual ofrece una lista de materiales guía relacionados de la OACI.

Nota.— En este manual, el uso del género masculino debe entenderse como si incluyera tanto a hombres como a mujeres.

Capítulo 2

FUNDAMENTOS DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

Nota.— Este capítulo proporciona una descripción general de los conceptos y las prácticas fundamentales de la gestión de la seguridad operacional que corresponden a la implementación de programas estatales de seguridad operacional, así como también, la implementación y la vigilancia de sistemas de gestión de la seguridad operacional por parte de proveedores de productos y servicios. El contenido de este capítulo se ofrece solo con fines introductorios, sin mayores detalles sobre los temas abordados en los capítulos posteriores de este manual.

2.1 EL CONCEPTO DE SEGURIDAD OPERACIONAL

2.1.1 Dentro del contexto de la aviación, la seguridad operacional es “el estado donde la posibilidad de dañar a las personas o las propiedades se reduce y mantiene al mismo nivel o debajo de un nivel aceptable mediante el proceso continuo de identificación de peligros y gestión de riesgos de la seguridad operacional”.

2.1.2 Si bien la eliminación de los accidentes o incidentes graves en aeronaves sigue siendo la meta final, se reconoce que el sistema de aviación no puede estar completamente libre de peligros y riesgos asociados. Las actividades humanas o los sistemas construidos por humanos no pueden garantizar estar completamente libres de errores de operaciones y de sus consecuencias. Por lo tanto, la seguridad es una característica dinámica del sistema de aviación, por el cual los riesgos de seguridad operacional deben mitigarse continuamente. Es importante tener presente que la aceptabilidad del rendimiento en materia de seguridad operacional se ve influenciado comúnmente por las normas y la cultura tanto nacionales como internacionales. 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 gestionándose para mantener el equilibrio correcto de producción y protección.

2.2 LA EVOLUCIÓN DE LA SEGURIDAD OPERACIONAL

La historia del progreso en la seguridad operacional de la aviación puede dividirse en tres épocas.

a) *La época técnica, desde principios de la década de 1900 hasta fines de la década de 1960.* La aviación surgió como una forma de transporte en masa, en el 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 factores técnicos. En la década de 1950, las mejoras tecnológicas generaron una reducción gradual en la frecuencia de accidentes y los procesos de seguridad operacional se ampliaron para abarcar el cumplimiento reglamentario y la vigilancia.

b) *La época de los factores humanos, desde principios de la década de 1970 hasta mediados de la década de 1990.* 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 factor humano, como la interfaz hombre-máquina. Esto produjo una búsqueda de información de seguridad operacional más allá de la que se había generado con los primeros procesos de investigación de accidentes. A pesar de la inversión de recursos en la mitigación de errores, el desempeño humano seguía citándose como un factor recurrente en los accidentes (Figura 2-1). La aplicación de la ciencia de factores humanos tendía a centrarse en la persona, sin considerar por completo 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, el que incluye múltiples factores que tienen el potencial de afectar la conducta.

c) *La época institucional, desde mediados de 1990 hasta la actualidad.* Durante la época institucional, la seguridad operacional comenzó a verse desde una perspectiva sistémica, la cual era abordar los factores institucionales además de los factores humanos y técnicos. Como resultado, se presentó la noción de “accidente institucional”, lo que consideró el impacto de la cultura y las políticas institucionales en la eficacia de los controles de riesgos de la seguridad operacional. Además, los esfuerzos de recopilación y el análisis de datos tradicionales, que estaban limitados al uso de datos recopilados mediante la investigación de accidentes e incidentes graves, se complementaron con un nuevo enfoque proactivo para la seguridad operacional. Este nuevo enfoque se basó en la recopilación y el análisis rutinario de datos mediante metodologías proactivas y reactivas, con el fin de controlar los riesgos de seguridad operacional conocidos y detectar problemas de seguridad emergentes. Estas mejoras formularon la lógica de avanzar hacia un enfoque de gestión de la seguridad operacional.

2.3.1 El modelo del “Queso suizo”, desarrollado por el profesor James Reason, ilustra que los accidentes implican violaciones sucesivas de múltiples defensas del sistema. Estas violaciones pueden generarse por muchos factores, como fallas de los equipos o errores operacionales. Dado que el modelo del Queso suizo sostiene que los sistemas complejos, como los de la aviación, están muy bien protegidos con capas de defensas, las fallas en un solo punto rara vez traen consecuencias en dichos sistemas. Las violaciones en las defensas de seguridad pueden ser una consecuencia atrasada de las decisiones tomadas en los niveles más altos del sistema, las que pueden permanecer latentes hasta que sus efectos o potencial de daños se activen bajo circunstancias operacionales específicas. Bajo dichas circunstancias, las fallas humanas o activas a nivel operacional actúan para violar las defensas naturales de seguridad operacional del sistema. El modelo de Reason propone que todos los accidentes incluyen una combinación de condiciones activas y 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 al personal de primera línea (pilotos, controladores de tránsito aéreo, ingenieros mecánicos de aeronaves, etc.) y pueden producir resultados dañinos.

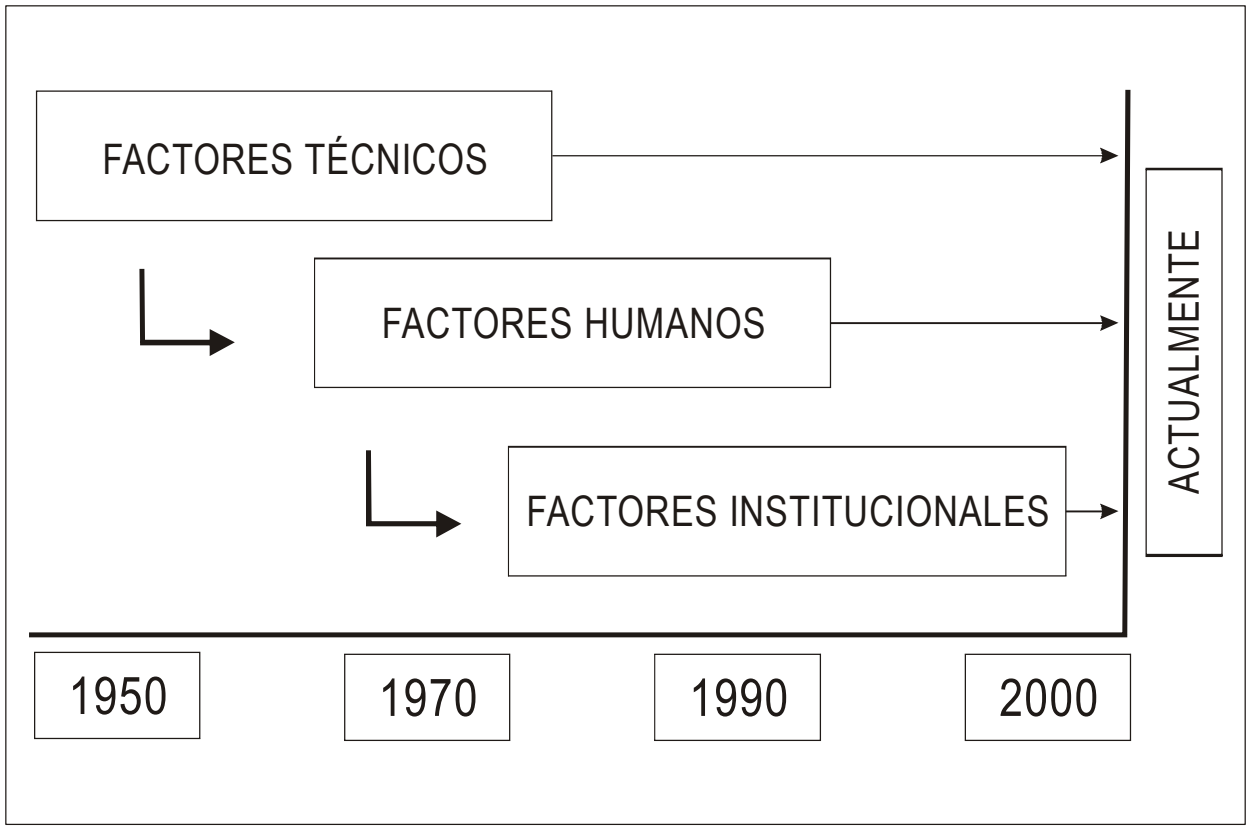


Figura 2-1. La evolución de la seguridad operacional

2.3 CAUSALIDAD DE ACCIDENTES

2.3.3 Las condiciones latentes son aquellas que existen en el sistema de aviación mucho antes de experimentar un resultado dañino. Las consecuencias de las condiciones latentes pueden permanecer ocultas por mucho tiempo. En un principio, dichas condiciones no se perciben como perjudiciales, pero serán evidentes luego de la violación de las defensas del sistema. Generalmente, estas condiciones las generan personas muy lejanas en tiempo y espacio del suceso. Las condiciones latentes en el sistema pueden incluir aquellas generadas por la falta de cultura de seguridad operacional; mal diseño del equipo o los procedimientos; metas institucionales en conflicto; sistemas institucionales o decisiones de gestión incompletos. La perspectiva de fondo de los accidentes institucionales apunta a identificar y mitigar dichas condiciones latentes a nivel del sistema y no mediante esfuerzos localizados para minimizar las fallas activas de las personas.

2.3.4 La Figura 2-2 muestra cómo el modelo del Queso suizo ayuda a comprender la interacción de los factores institucionales y de gestión en la causalidad de accidentes. 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. Mientras estas defensas actúan para proteger contra los riesgos de seguridad operacional, las violaciones que penetren todas la barreras defensivas posiblemente generen una situación catastrófica. Además, el modelo de Reason representa cómo las condiciones latentes siempre están presentes dentro del sistema antes de un accidente y que pueden manifestarse mediante factores activadores locales.

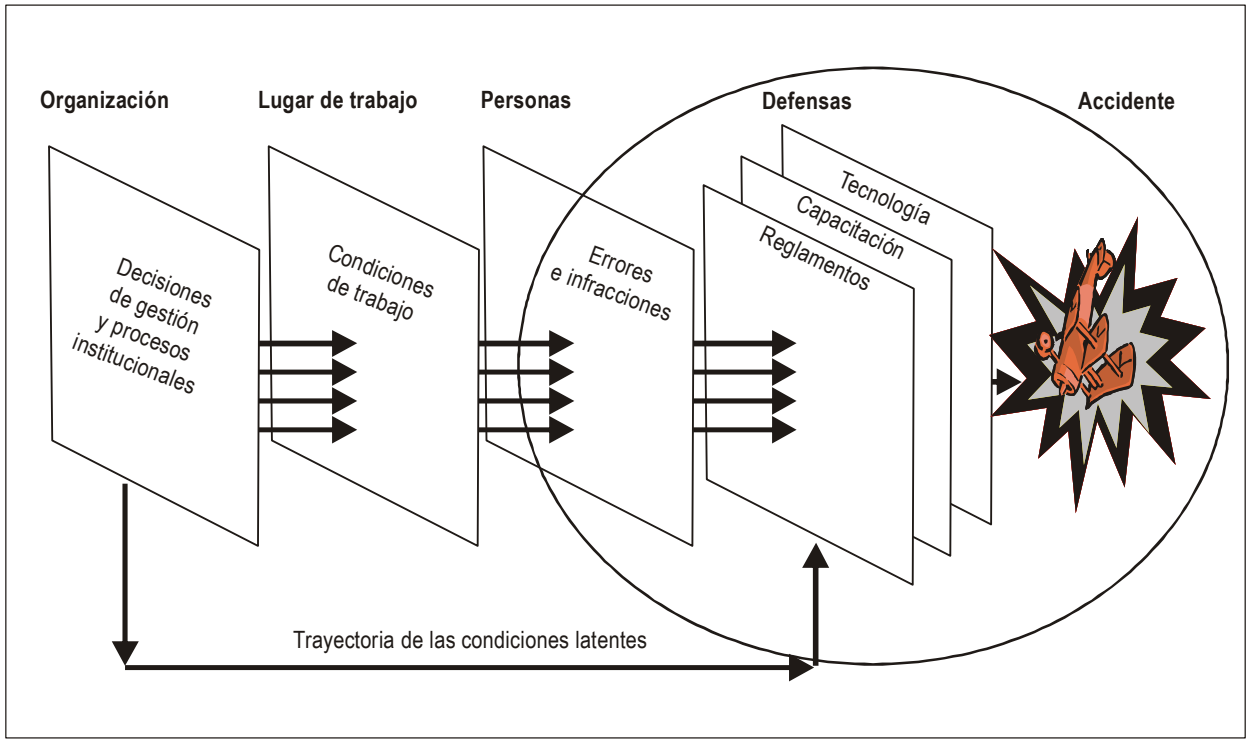


Figura 2-2. El concepto de la causalidad de accidentes

El accidente institucional

2.3.5 La noción de un accidente institucional subyacente al modelo de Reason puede entenderse mejor mediante un enfoque de bloques base, que consta de cinco bloques (Figura 2-3). El bloque superior representa los procesos institucionales. Estos representan actividades en las cuales cualquier organización tiene un grado razonable de control directo. Entre los ejemplos típicos se incluyen la elaboración de políticas, planificación, comunicación, asignación de recursos y supervisión. Sin duda, los dos procesos institucionales fundamentales relacionados con la seguridad operacional son la asignación de recursos y la comunicación. Las desventajas o deficiencias en estos procesos institucionales representan un ambiente propicio para crear un camino doble hacia el fracaso.

2.3.6 Un camino es el camino de las condiciones latentes. Entre los ejemplos de condiciones latentes se pueden incluir deficiencias en el diseño de los equipos, procedimientos de operación estándar incompletos o incorrectos, y deficiencias de capacitación. En términos genéricos, las condiciones latentes pueden agruparse en dos grandes grupos. Un grupo es la identificación de peligros y gestión de riesgos de la seguridad operacional insuficientes, a través de los cuales los riesgos de seguridad operacional de las consecuencias de los peligros no se mantienen bajo control, sino que quedan libres en el sistema para activarse finalmente mediante activadores operacionales.

2.3.7 El segundo grupo se conoce como normalización de irregularidades, una noción que, en términos simples, señala contextos operacionales donde la excepción se convierte en la norma. En este caso, la asignación de recursos es extremadamente errónea. Como consecuencia de la carencia de recursos, la única forma en que el personal de operaciones, que es directamente responsable del rendimiento real de las actividades de producción, pueda lograr exitosamente estas actividades, es al adoptar atajos que impliquen la infracción constante de las normas y los procedimientos.

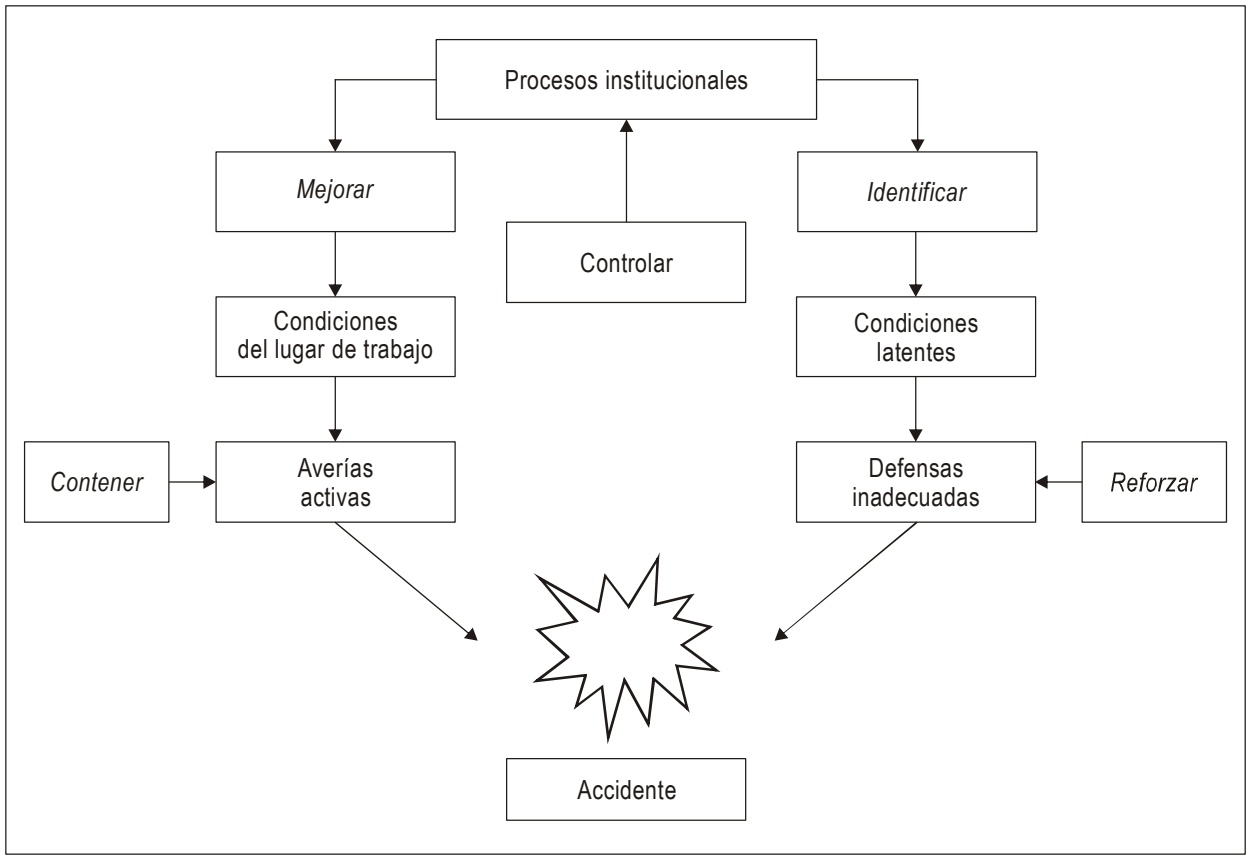


Figura 2-3 El accidente institucional

2.3.8 Las condiciones latentes tienen el potencial de violar las defensas del sistema de aviación. Normalmente, las defensas en la aviación pueden agruparse en tres grandes áreas: tecnología, capacitación y reglamentos. Las defensas son comúnmente la última red de seguridad operacional para contener las condiciones latentes, así como también, las consecuencias de los lapsos en el desempeño humano. La mayoría de las estrategias de mitigación, sino todas, que van en contra de los riesgos de seguridad operacional de las consecuencias de los peligros se basan en el fortalecimiento de las defensas existentes o en el desarrollo de nuevas defensas.

2.3.9 El otro camino que se origina de los procesos institucionales es el camino de las condiciones del lugar de trabajo. Las condiciones del lugar de trabajo son factores que influyen directamente en la eficiencia de las personas en los lugares de trabajo de la aviación. Las condiciones del lugar de trabajo son principalmente intuitivas, ya que todas las personas con experiencia operacional las han experimentado en diversos grados, además, estas incluyen la estabilidad de la fuerza de trabajo, las calificaciones y la experiencia, la moral, la credibilidad administrativa y los factores de ergonomía tradicionales, como iluminación, calefacción y enfriamiento.

2.3.10 Las condiciones del lugar de trabajo con un nivel inferior al óptimo representan fallas activas del personal de operaciones. Las fallas activas pueden considerarse errores o infracciones. La diferencia entre un error y una infracción es el componente motivacional. Una persona que trata de hacer lo mejor posible para cumplir una tarea, siguiendo las normas y los procedimientos según la capacitación que ha recibido, pero que no logra cumplir el objetivo de la tarea actual, comete un error. Una persona que, mientras cumple una tarea, no sigue las normas, los procedimientos o la capacitación recibida a propósito, comete una infracción. Por tanto, la diferencia básica entre un error y una infracción es la intención.

2.3.11 A partir de la perspectiva del accidente institucional, las actividades de seguridad operacional deben controlar los procesos institucionales para identificar las condiciones latentes y, así, reforzar las defensas. Las actividades de seguridad operacional también deben mejorar las condiciones del lugar de trabajo, ya que es la combinación de todos estos factores lo que produce rupturas en la seguridad.

La desviación de la práctica

2.3.12 La teoría de Scott A. Snook sobre la desviación de la práctica se usa como la base para comprender cómo, en la aviación, el performance base de cualquier sistema se "desvía" desde su diseño original cuando los procesos y los procedimientos de la organización no pueden anticipar todas las situaciones que pueden ocurrir en las operaciones diarias.

2.3.13 Durante las primeras etapas del diseño del sistema (por ejemplo, espacio aéreo del ATC, introducción de equipo específico, expansión de un esquema de operación de vuelo), las interacciones operacionales entre las personas y la tecnología, así como también, el contexto operacional, se toman en cuenta para identificar las limitaciones del rendimiento esperado al igual que de los peligros potenciales. El diseño del sistema inicial se basa en tres suposiciones fundamentales: está disponible la tecnología necesaria para lograr las metas de producción del sistema; las personas están capacitadas para operar correctamente la tecnología; y los reglamentos y los procedimientos indicarán el comportamiento humano y del sistema. Estas suposiciones son el trasfondo del rendimiento del sistema base (o ideal), las que pueden representarse gráficamente como una línea recta desde la fecha de implementación operacional hasta que el sistema se pone fuera de servicio (Figura 2-4).

2.3.14 Luego de implementarse operacionalmente, el sistema actúa según el diseño, siguiendo el rendimiento base la mayor parte del tiempo. No obstante, en la realidad, el rendimiento operacional es diferente del rendimiento base, como consecuencia de las operaciones y los cambios de la vida real en el entorno operacional y reglamentario. Dado que la desviación es una consecuencia de la práctica diaria, se le conoce como “desviación de la práctica". El término "desviación" se usa en este contexto como el alejamiento gradual desde un curso definido a causa de influencias externas.

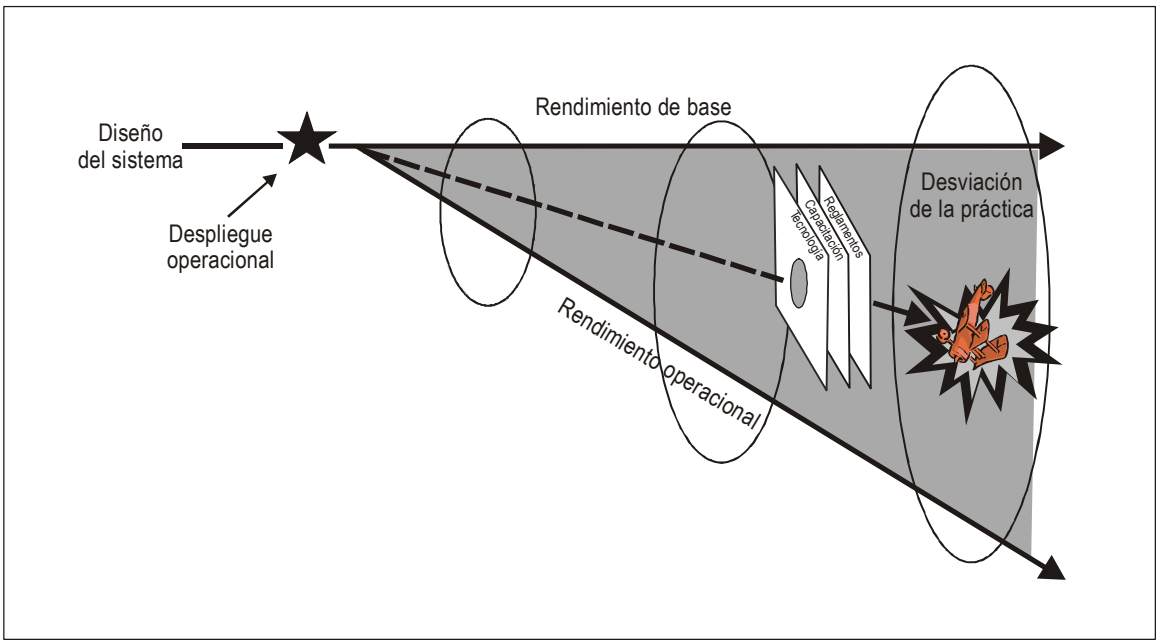


Figura 2-4. La desviación de la práctica

2.3.15 Una desviación de la práctica desde un rendimiento base hasta un rendimiento operacional es predecible en cualquier sistema, sin importar cuán cuidadosa y bien pensada haya sido la planificación del diseño. Algunos motivos de la desviación de la práctica pueden incluir: tecnología que no siempre funciona como se predice; procedimientos que no pueden ejecutarse según lo planificado bajo ciertas condiciones operacionales; reglamentos que no corresponden dentro de ciertas limitaciones contextuales; introducción de cambios al sistema, como la adición de nuevos componentes; la interacción con otros sistemas, etc. No obstante, la realidad es que, a pesar de todas las fallas del sistema que producen la desviación, las personas que operan dentro de la desviación de la práctica hacen que el sistema funcione diariamente, aplicando adaptaciones (o soluciones) locales, además de estrategias personales "más allá de lo que dice el manual".

2.3.16 Como se explicó en la Figura 2-4, la captura y el análisis de la información sobre lo que sucede dentro de la desviación de la práctica representan un potencial de aprendizaje significativo sobre las adaptaciones de seguridad operacional exitosas y, por lo tanto, para el control y la mitigación de los riesgos de seguridad operacional. Mientras más cerca del inicio de la desviación de la práctica se esté al momento de recopilar información sistemáticamente, mayor será la cantidad de peligros y riesgos de seguridad operacional que podrán predecirse y abordarse, lo que genera intervenciones formales para rediseñar o mejorar el sistema. No obstante, la proliferación sin revisar de las adaptaciones locales y las estrategias personales pueden generar que la desviación de la práctica se aleje demasiado del rendimiento base esperado, hasta el punto donde un incidente o accidente se vuelve una mayor posibilidad.

2.4 PERSONAS, CONTEXTO Y SEGURIDAD OPERACIONAL

2.4.1 El sistema de aviación incluye a proveedores de productos y servicios, y organizaciones del Estado. Es un sistema complejo que requiere una evaluación de la contribución humana para la seguridad operacional y una comprensión de cómo el desempeño humano puede verse afectado por sus múltiples e interrelacionados componentes.

2.4.2 El modelo SHEL es una herramienta conceptual usada para analizar la interacción de múltiples componentes del sistema. La Figura 2-5 ofrece una descripción básica de la relación entre las personas y otros componentes del lugar de trabajo. El modelo SHEL contiene los siguientes cuatro componentes:

a) *Software (S):* procedimientos, capacitación, asistencia técnica, etc.;

b) *Hardware (H):* máquinas y equipos;

c) *Entorno (E):* el entorno de trabajo donde debe funcionar el resto del sistema L-H-S; y

d) *Liveware (L):* las personas en el lugar de trabajo.

2.4.3 *Liveware.* En el centro del modelo SHEL se encuentran las personas en la primera línea de operaciones. Aunque las personas son increíblemente adaptables, están sujetas a importantes variaciones en el rendimiento. Las personas no están estandarizadas al mismo grado que el hardware, así que los bordes de este bloque no son simples ni rectos. Las personas no se interconectan perfectamente con los diversos componentes del mundo donde trabajan. Para evitar las tensiones que pueden conformar el desempeño humano, se deben entender los efectos de las irregularidades en las interfaces entre los diversos bloques de SHEL y el bloque central Liveware. Los otros componentes del sistema se deben hacer coincidir con cuidado con las personas si se desea evitar el estrés en el sistema. El modelo SHEL es útil para observar las siguientes interfaces entre los diversos componentes del sistema de aviación:

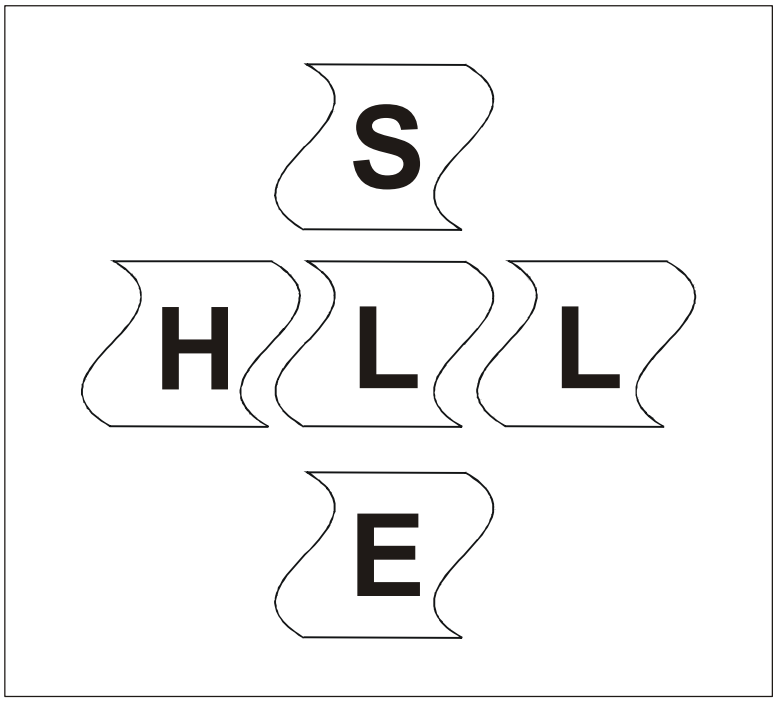


Figura 2-5. El modelo SHEL — Componentes e interfaces

a) *Liveware-Hardware (L-H).* La interfaz L-H hace referencia a la relación entre la persona y los atributos físicos del equipo, máquina e instalaciones. La interfaz entre una persona y la tecnología se considera comúnmente con relación al rendimiento humano, en el contexto de las operaciones de aviación; existe además una tendencia humana natural a adaptar las diferencias de L-H. Sin embargo, esta tendencia tiene el potencial de enmascarar deficiencias graves, las que llegan a ser evidentes solo después de que suceden.

b) *Liveware-Software (L-S).* La interfaz L-S es la relación entre una persona y los sistemas de asistencia que se encuentran en el lugar de trabajo, por ejemplo, reglamentos, manuales, listas de verificación, publicaciones, procedimientos de operación estándar (SOP) y software de computadora. Incluye temas tales como experiencia, precisión, formato y presentación, vocabulario, claridad y simbología recientes.

c) *Liveware-Liveware (L-L).* La interfaz L-L es la relación entre personas en el mismo entorno de trabajo. Dado que la tripulación de vuelo, los controladores de tránsito aéreo, los mecánicos de mantenimiento de aeronaves y otro personal de operaciones funcionan en grupos, es importante reconocer que la comunicación y las habilidades interpersonales, así como también, la dinámica de grupo, juegan un papel para determinar el desempeño humano. La llegada de la gestión de recursos de tripulación (CRM) y su extensión a los servicios de tránsito aéreo (ATS), además de las operaciones de mantenimiento, han creado un enfoque en la gestión de errores operacionales en varios dominios de la aviación. Las relaciones del personal/administración, al igual que la cultura institucional general, también están dentro del alcance de esta interfaz.

d) *Liveware-Entorno (L-E).* Esta interfaz implica la relación entre las personas y los entornos internos y externos. El entorno del lugar de trabajo interno incluye consideraciones físicas como temperatura, luz ambiental, ruido, vibración y calidad del aire. El entorno externo incluye aspectos operacionales como factores meteorológicos, infraestructura de aviación y terreno. Esta interfaz también implica la relación entre el entorno interno humano y su entorno externo. Las fuerzas sicológicas y fisiológicas, como enfermedades, fatiga, inquietudes financieras y preocupaciones sobre relaciones y carreras, pueden inducirse con la interacción L-E o pueden originarse de fuentes externas secundarias. El entorno de trabajo de aviación incluye perturbaciones para los ritmos biológicos normales y los patrones de sueño. Puede que haya aspectos ambientales adicionales que se relacionen con atributos institucionales que puedan afectar los procesos de toma de decisiones y ejercer presión para desarrollar “soluciones” o desviaciones leves de los procedimientos operacionales estándar.

2.4.4 De acuerdo con el modelo SHEL, una diferencia entre Liveware y los otros cuatro componentes contribuye con el error humano. Por lo tanto, estas interacciones deben evaluarse y considerarse en todos los sectores del sistema de aviación.

2.5 ERRORES E INFRACCIONES

2.5.1 La implementación eficaz del SMS por parte del proveedor de productos y servicios, así como también, la vigilancia eficaz del SMS por parte del Estado, depende de una clara y mutua comprensión de los errores y las infracciones, además de la diferenciación entre ambos conceptos. La diferencia entre error e infracción yace en la intencionalidad. Mientras que un error es accidental, una infracción es un acto o una omisión deliberado que se lleva a cabo para desviarse de los procedimientos, los protocolos, las normas o las prácticas establecidos.

2.5.2 Los errores o las infracciones pueden generar una falta de cumplimiento de los reglamentos o los procedimientos operacionales reconocidos. Las medidas punitivas tomadas en respuesta a las acciones de no cumplimiento pueden generar una reducción en la notificación de errores en ausencia de otros procesos. En consecuencia, el Estado y el proveedor de productos y servicios deben considerar si las acciones de no cumplimiento son el resultado de una infracción o error accidental al determinar si corresponde implementar una medida punitiva, siendo los criterios normalmente si el no cumplimiento es resultado de una conducta impropia deliberada o una negligencia grave.

Errores

2.5.3 Como se indicó previamente, un error se define como una "medida tomada o no tomada por un miembro del personal de operaciones que genera un desvío de las intenciones o expectativas del miembro del personal de operaciones o institucional”. En el contexto de un SMS, tanto el Estado como el proveedor de productos y servicios deben comprender y esperar que los seres humanos cometan errores sin importar el nivel de tecnología usado, el nivel de capacitación o la existencia de reglamentos, procesos y procedimientos. Una meta importante entonces es establecer y mantener defensas para reducir la probabilidad de errores e, igualmente importante, reducir las consecuencias de los errores cuando ocurren. Para lograr eficazmente esta tarea, se debe identificar, informar y analizar los errores para tomar una medida correctiva adecuada. Los errores pueden dividirse en las siguientes dos categorías:

a) Las c*onfusiones y omisiones* son fallas en la ejecución de una medida determinada. Las confusiones son acciones que no se llevaron a cabo según lo planificado, mientras que las omisiones son fallas de memoria. Por ejemplo, accionar la palanca de flap en lugar de la palanca de engranajes (prevista) es una confusión. Olvidar una lista de verificación es una omisión.

b) Las e*quivocaciones* son fallas en el plan de acción. Incluso si la ejecución del plan fuera correcta, no podría haber sido posible lograr el resultado esperado.

2.5.4 Se deben implementar estrategias de seguridad operacional para controlar o eliminar los errores. Las estrategias para controlar errores aprovechan las defensas básicas dentro del sistema de aviación. Estas incluyen lo siguiente:

a) *Las estrategias de reducción* proporcionan intervención directa para reducir o eliminar los factores que contribuyen con el error. Entre los ejemplos de estrategias de reducción se incluye la mejora de factores ergonómicos y la reducción de distracciones ambientales.

b) *Las estrategias de captura* suponen que el error sucederá. La intención es "capturar" el error antes de detectar alguna consecuencia adversa del error. Las estrategias de captura son diferentes de las estrategias de reducción, ya que utilizan listas de verificación y otras intervenciones de procesamientos en lugar de eliminar directamente el error.

c) *Las estrategias de tolerancia* hacen referencia a la capacidad de un sistema de aceptar que un error se cometerá sin experimentar consecuencias graves. La incorporación de sistemas redundantes o múltiples procesos de inspección son ejemplos de medidas que aumentan la tolerancia a errores del sistema.

2.5.5 Ya que el rendimiento del personal se ve influenciado generalmente por factores institucionales, reglamentarios y ambientales, la gestión de riesgos de seguridad operacional debe incluir la consideración de políticas, procesos y procedimientos institucionales relacionados con la comunicación, la programación de personal, la asignación de recursos y las limitaciones presupuestarias que pueden contribuir con la incidencia de errores.

Infracciones

2.5.6 Una infracción se define como **"**un acto deliberado de conducta impropia deliberada u omisión que genere una desviación de los reglamentos, los procedimientos, las normas o las prácticas establecidas". Sin embargo, el incumplimiento no es necesariamente el resultado de una infracción, ya que las desviaciones de los requisitos reglamentarios o procedimientos operacionales pueden ser el resultado de un error. Para complicar aún más el problema, aunque las infracciones son actos intencionales, no siempre actúan con intenciones maliciosas. Las personas pueden desviarse conscientemente de las normas, creyendo que la infracción facilita el cumplimiento de la misión sin crear consecuencias adversas. Las infracciones de esta naturaleza son errores de criterio y puede que no generen automáticamente medidas disciplinarias, según las políticas implementadas. Las infracciones de este tipo pueden categorizarse de la siguiente forma:

a) *Las infracciones situacionales* se cometen en respuesta a los factores experimentados en un contexto específico, como presión de tiempo o alta carga de trabajo.

b) *Las infracciones rutinarias* se vuelven la forma normal de hacer negocios dentro de un grupo de trabajo. Tales infracciones se cometen en respuesta a las situaciones en las cuales el cumplimiento de los procedimientos establecidos dificulta la finalización de la tarea. Esto se puede deber a problemas de funcionalidad/viabilidad de trabajo, deficiencias en el diseño de la interfaz humana-tecnológica y otros problemas que causan que las personas adopten "soluciones", las que finalmente se vuelven rutinarias. Estas modificaciones, conocidas como "desviaciones", pueden continuar sin consecuencias, pero con el paso del tiempo pueden volverse frecuentes y generar consecuencias potencialmente graves. En algunos casos, las infracciones rutinarias tienen buenos fundamentos y pueden incorporarse como procedimientos aceptados luego de realizar una evaluación de seguridad operacional adecuada y que se demuestre que no se compromete la seguridad operacional.

c) *Las infracciones inducidas por la organización* pueden considerarse una extensión de las infracciones rutinarias. Este tipo de infracción tiende a ocurrir cuando una organización intenta satisfacer demandas de mucha producción ignorando o extendiendo las defensas de seguridad operacional.

2.6 CULTURA DE SEGURIDAD OPERACIONAL

2.6.1 La cultura se caracteriza por tener creencias, valores, tendencias y sus conductas resultantes que se comparten entre miembros de una sociedad, grupo u organización. Una comprensión de estos componentes culturales, además de la interacción entre sí, es importante para la gestión de la seguridad operacional. Los tres componentes culturales más influyentes son la cultura institucional, profesional y nacional. Una cultura de notificación es un componente clave de estas diferentes culturas. La mezcla de los componentes culturales puede variar enormemente entre las organizaciones y puede influenciar negativamente la notificación eficaz de peligros, el análisis colaborativo de la causa de origen y la mitigación de riesgos aceptable. La mejora continua del rendimiento en materia de seguridad operacional es posible cuando la seguridad operacional se convierte en un valor dentro de la organización, así como también, una prioridad a nivel nacional o profesional.

2.6.2 Una cultura de seguridad operacional abarca las percepciones y creencias más comunes de los miembros de una organización en relación con la seguridad operacional del público y puede llegar a ser un comportamiento determinante de los miembros. Una cultura de seguridad operacional saludable depende en un alto grado de confianza y respeto entre el personal y la administración, y debe, por tanto, crearse y respaldarse a nivel de la administración superior.

2.6.3 Una cultura de seguridad operacional saludable busca activamente mejoras, permanece vigilante y consciente de los peligros y usa los sistemas y las herramientas para obtener control, análisis e investigación continuos. Debe existir en las organizaciones de aviación del Estado, así como también, en las organizaciones proveedoras de productos y servicios. Otra característica de una cultura de seguridad operacional saludable incluye un compromiso compartido del personal y la administración con las responsabilidades de seguridad personal, la confianza en el sistema de seguridad operacional y un conjunto de normas y políticas documentado. La administración de la organización es responsable del establecimiento y respeto de las sólidas prácticas de seguridad operacional. Una cultura de seguridad operacional no puede ser eficaz a menos que esté incorporada dentro de la propia cultura de la organización.

2.6.4 *La cultura institucional* hace referencia a las características y percepciones de seguridad operacional entre miembros que interactúan dentro de una entidad particular. Los sistemas de valores institucionales incluyen políticas de priorización o equilibrio que abarcan áreas como, por ejemplo, productividad versus calidad, seguridad operacional versus eficiencia, área financiera versus área técnica, profesional versus académico, y cumplimiento versus medida correctiva.

2.6.5 El mayor potencial de creación y mantenimiento de una cultura eficaz y autosustentable para la gestión de seguridad operacional se encuentra a nivel de la organización. La organización es un importante factor determinante del comportamiento que desempeñarán las personas mientras realizan actividades de gestión y operacionales durante la entrega o vigilancia de las actividades de aviación. La cultura institucional ajusta los límites aceptados del rendimiento ejecutivo y operacional al establecer las normas y los límites. Por lo tanto, la cultura institucional proporciona la piedra angular para la toma de decisiones administrativas y de los empleados.

2.6.6 La cultura institucional tiene el potencial de afectar lo siguiente:

a) las interacciones entre los miembros superiores e iniciales de un grupo;

b) las interacciones entre el personal de autoridad industrial y reglamentario;

c) el grado hasta donde se comparte la información de forma interna y con las autoridades reglamentarias;

d) la prevalencia del trabajo en equipo en la autoridad reglamentaria o la organización industrial;

e) las reacciones del personal bajo condiciones operacionales exigentes;

f) la aceptación y el uso de tecnologías determinadas; y

g) la tendencia de tomar medidas punitivas en respuesta a errores operacionales dentro de un proveedor de productos o servicios, o mediante autoridades reglamentarias.

2.6.7 La cultura institucional también puede verse afectada por factores como:

a) políticas y procedimientos comerciales;

b) comportamiento y prácticas de vigilancia;

c) metas de mejora de seguridad operacional, así como también, niveles de tolerancia mínimos;

d) la actitud de la administración hacia problemas de calidad o seguridad operacional;

e) capacitación y motivación de los empleados;

f) la relación entre las autoridades reglamentarias y los proveedores de productos y servicios; y

g) las políticas sobre el equilibrio entre el trabajo y la vida personal.

2.6.8 La forma en que la administración aborda los problemas de seguridad operacional diarios es también fundamental para mejorar la cultura institucional. La interacción colaborativa entre el personal de primera línea y sus contrapartes de seguridad operacional y calidad, así como también, los representantes de la autoridad reglamentaria, da indicios de una cultura institucional positiva. Esta relación debe caracterizarse por cortesía profesional, mientras se mantienen los papeles respectivos, según sea necesario, para garantizar objetividad y responsabilidad.

2.6.9 Una forma eficaz de promover las operaciones seguras es garantizar que una organización haya desarrollado un entorno donde todo el personal se sienta responsable de la seguridad operacional. Esto se vuelve evidente cuando el personal considera el impacto de todo lo que hacen, informan todos los peligros, los errores y las amenazas, y dan respaldo a la identificación y gestión de todos sus riesgos asociados. Además, la administración debe crear un entorno donde el personal esté consciente de los riesgos de seguridad operacional, tengan sistemas suficientes para protegerse y se les garantice protección cuando divulgan información de seguridad operacional mediante el sistema de notificación de seguridad operacional. Una cultura de seguridad operacional eficaz sirve como método para sincronizar diversas culturas nacionales y profesionales dentro del contexto de la organización.

2.6.10 *La cultura profesional* diferencia las características de los grupos profesionales particulares (es decir, el comportamiento característico de los pilotos en relación con aquél de los controladores de tránsito aéreo, el personal de la autoridad de aviación civil o los mecánicos de mantenimiento). Mediante la selección de personal, educación, capacitación, experiencia en el trabajo, presión de pares, etc., los profesionales tienden a adoptar el sistema de valores y desarrollar patrones de conducta coherentes con sus pares o predecesores. Una cultura profesional eficaz refleja la capacidad de los grupos profesionales de diferenciar entre los problemas de rendimiento en materia de seguridad operacional y los problemas contractuales o industriales. Una cultura profesional saludable puede describirse como la capacidad que disponen todos los grupos profesionales dentro de la organización para abordar de forma colaborativa los problemas del rendimiento en materia de seguridad operacional.

2.6.11 *La cultura nacional* diferencia las características de naciones determinadas, como el papel de cada persona dentro de la sociedad, la forma en que se distribuye la autoridad, las prioridades nacionales en relación con los recursos, las responsabilidades, la moralidad, los objetivos y los diferentes sistemas legales. Desde una perspectiva de gestión de la seguridad operacional, la cultura nacional juega un gran papel en la determinación de la naturaleza y el alcance de políticas de cumplimiento reglamentario, como la relación entre el personal de la autoridad reglamentaria y el personal industrial, y el punto hasta donde se protege la información relacionada con la seguridad operacional.

2.6.12 La cultura nacional forma un componente intrínseco de creencias personales que da forma inherentemente a las perspectivas de seguridad operacional de las personas antes de que formen parte de una organización. Por lo tanto, la cultura institucional puede verse significativamente afectada por las culturas nacionales presentes entre los miembros de su fuerza de trabajo.

2.6.13 Cuando se implementa un programa de gestión de la seguridad operacional, los gerentes deben evaluar y considerar en detalle las diferencias en la culturas nacionales de su personal. Por ejemplo, las percepciones de riesgos de seguridad operacional pueden ser muy diferentes entre distintas culturas nacionales. Es posible que los aspectos relacionados con la seguridad operacional, como las comunicaciones y los estilos de liderazgo, además de la interacción entre supervisores y subalternos, deban adaptarse a una fuerza de trabajo multicultural.

2.6.14 *La cultura de notificación* se origina a partir de las creencias y actitudes del personal acerca de los beneficios y los posibles perjuicios asociados con los sistemas de notificación y el efecto final que tiene en la aceptación o uso de tales sistemas. Las culturas institucional, profesional y nacional son las que más influyen en ella y, además, es un criterio para juzgar la eficacia de un sistema de seguridad operacional. Una cultura de notificación saludable apunta a diferenciar entre las desviaciones intencionales y accidentales, y a determinar el mejor curso de acción para la organización como un todo y para las personas que participan directamente.

2.6.15 El éxito de un sistema de notificación depende del flujo continuo de información del personal de primera línea. Las políticas que distinguen los actos deliberados de conducta impropia de los errores accidentales, y ofrecen una respuesta punitiva o no punitiva correspondiente, son esenciales para garantizar una notificación eficaz de deficiencias sistemáticas de seguridad operacional. Una cultura “sin culpa en lo absoluto” no solo es poco razonable, sino que no es viable. Mientras la administración obtiene información de seguridad operacional, el sistema será ineficaz si interfiere con las medidas punitivas correspondientes. Por el contrario, una cultura que no puede distinguir errores accidentales/equivocaciones de actos deliberados de conducta impropia inhibirá el proceso de notificación. Si el personal evita notificar por miedo a castigos, la administración no obtiene información de seguridad operacional importante.

2.6.16 En general, el personal debe creer que recibirán apoyo con cualquier decisión que tomen por el interés de la seguridad operacional, pero también deben comprender que cualquier violación intencional de la política de seguridad operacional no será tolerada. Por lo tanto, un sistema de notificación voluntaria debe ser confidencial y debe operarse de acuerdo con las políticas no punitivas correspondientes. El sistema también debe proporcionar comentarios al personal sobre las mejoras de seguridad operacional que se han alcanzado como resultado de los informes recibidos. Este objetivo requiere un acceso seguro y fácil a los sistemas de notificación de seguridad operacional, la recopilación de datos de seguridad operacional y el tratamiento proactivo de los datos por parte de la administración.

2.6.17 La información de la seguridad operacional debe recopilarse solamente para la mejora de la seguridad operacional de la aviación; además, la protección de la información es fundamental para garantizar que esté constantemente disponible. Esto puede llevarse a cabo mediante un sistema de notificación de la seguridad operacional que sea confidencial, voluntario y no punitivo. Los beneficios se duplican. A menudo, los miembros del personal son quienes se encuentran más cerca de los peligros de seguridad operacional, de modo que el sistema de notificación les permite identificar activamente estos peligros. Al mismo tiempo, la administración puede recopilar información de peligros de seguridad operacional pertinentes y generar confianza con el personal.

2.6.18 Luego de recopilar y guardar los datos, dicha información se debe procesar para confirmar la implementación de las medidas adecuadas que se deben comunicar al personal de primera línea de forma oportuna.

Promoción y evaluación de una cultura de seguridad operacional

2.6.19 La eficacia de una cultura de seguridad operacional puede medirse y controlarse en realidad mediante métricas tangibles. En un entorno de cultura de seguridad operacional maduro, se puede anticipar que las organizaciones pueden estar en una posición para introducir un mecanismo a fin de realizar una evaluación interna de la cultura de seguridad operacional de la organización (OSC). Tal evaluación puede mejorarse más al usar la evaluación de perfil de riesgo de la organización (ORP) con mayor participación técnica y específica de la industria. Al mismo tiempo, las organizaciones o reguladores industriales pueden considerar desarrollar esquemas promocionales (por ejemplo, un galardón a la cultura de la seguridad operacional) para alentar a los proveedores de productos y servicios para que participen en la evaluación voluntaria OSC/ORP de sus organizaciones. Los parámetros que se tienen que evaluar en una evaluación OSC/ORP deben incluir los factores y resultados institucionales que vayan más allá de los requisitos reglamentarios convencionales, pero que sigan siendo pertinentes para la cultura de seguridad operacional de una organización y, por lo tanto, tengan un impacto en su rendimiento en materia de seguridad operacional. Este es el principal fin de una evaluación OSC/ORP. Funciona para complementar la vigilancia reglamentaria tradicional al abordar los factores institucionales (condiciones latentes) que, de lo contrario, están más allá del ámbito reglamentario. Una lista de verificación de la evaluación OSC sería más genérica en cuanto a su contenido, mientras que una lista de verificación ORP estaría más personalizada según la naturaleza de las operaciones de la organización. En el Apéndice 1 se brinda la ilustración de una posible lista de verificación de la evaluación OSC/ORP específica de la industria.

2.7 EL DILEMA DE LA GESTIÓN

2.7.1 Los procesos de gestión de la seguridad operacional identifican peligros con el potencial de afectar negativamente la seguridad operacional. Estos procesos también ofrecen mecanismos objetivos para evaluar el riesgo que representan los peligros e implementar formas de eliminar estos últimos o mitigar los riesgos asociados con ellos. El resultado de estos procesos es facilitar el logro de un nivel aceptable de seguridad operacional mientras se equilibra la asignación de recursos entre la producción y la protección. A partir de una perspectiva de asignación de recursos, el concepto de espacio de seguridad operacional es particularmente útil para describir cómo se logra este equilibrio.

Espacio de seguridad operacional

2.7.2 En una organización comprometida con el suministro de servicios, los riesgos de producción y seguridad operacional están vinculados. A medida que aumenta la producción, también pueden hacerlo los riesgos de seguridad operacional, si no están disponibles las mejoras necesarias de recursos o procesos. Una organización debe definir sus objetivos de producción y seguridad operacional al equilibrar la producción con riesgos de seguridad operacional aceptables. Además, cuando define sus objetivos de producción, la organización necesita definir defensas para mantener bajo control los riesgos de seguridad operacional. Para un proveedor de productos o servicios, las defensas de seguridad operacional básicas son la tecnología, la capacitación y los procesos y los procedimientos internos. Para el Estado, las defensas básicas son parecidas, es decir, la capacitación del personal, el uso adecuado de la tecnología, la vigilancia eficaz y los procesos y los procedimientos internos que respalden la vigilancia. El espacio de seguridad operacional es la zona donde una organización equilibra la producción deseada mientras mantiene la protección de la seguridad operacional necesaria mediante controles de riesgos de seguridad operacional. Por ejemplo, un fabricante o proveedor de servicios de navegación aérea puede querer fomentar un crecimiento anticipado mediante la inversión en nuevas tecnologías. Dichas tecnologías pueden proporcionar, al mismo tiempo, las mejoras de eficiencia necesarias además de una mejor confiabilidad y rendimiento en materia de seguridad operacional. Tal toma de decisiones debe implicar la evaluación del valor agregado a los objetivos de productos y servicios de la organización, así como también, los riesgos de seguridad operacional involucrados. La asignación de recursos excesivos para la protección o los controles de riesgo puede causar que el producto o servicio sea poco rentable, lo que pone en peligro la viabilidad de la organización.

2.7.3 Por otro lado, la asignación excesiva de recursos para la producción a expensas de la protección puede tener un impacto en el rendimiento en materia de seguridad operacional del producto o servicio, y puede producir finalmente 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. A raíz de esto, los límites del espacio de seguridad operacional deben definirse en la administración de la organización y deben revisarse continuamente para garantizar que reflejan con exactitud la situación actual. Véase en la Figura 2-6 una ilustración de los límites del espacio de seguridad operacional de una organización.

2.7.4 La necesidad de equilibrar la producción y la protección se ha convertido en un requisito fácilmente comprendido y aceptado a partir de la perspectiva de un proveedor de productos y servicios. Este equilibrio es igualmente aplicable para la gestión de SSP del Estado, dado el requisito para equilibrar los recursos necesarios para las funciones de protección del Estado que incluyen certificación y vigilancia.

2.8 GESTIÓN DE CAMBIO

2.8.1 Las organizaciones de aviación, incluidas las autoridades reglamentarias, experimentan cambios debido a la expansión y reducción, y a los cambios en sistemas, equipos, políticas, programas, servicios y reglamentos existentes. Puede que se introduzcan peligros de forma accidental en el sistema de aviación cuando sucede un cambio. Los procesos base de la mitigación de riesgos de la seguridad operacional existentes también pueden verse afectados. Las prácticas de gestión de la seguridad operacional requieren que se identifiquen sistemáticamente los peligros a causa de los cambios y que se desarrollen, implementen y posteriormente evalúen las estrategias para gestionar los riesgos de seguridad operacional resultantes. Una gestión sólida de los riesgos de seguridad operacional asociados con el cambio es un requisito fundamental del SSP y el SMS.

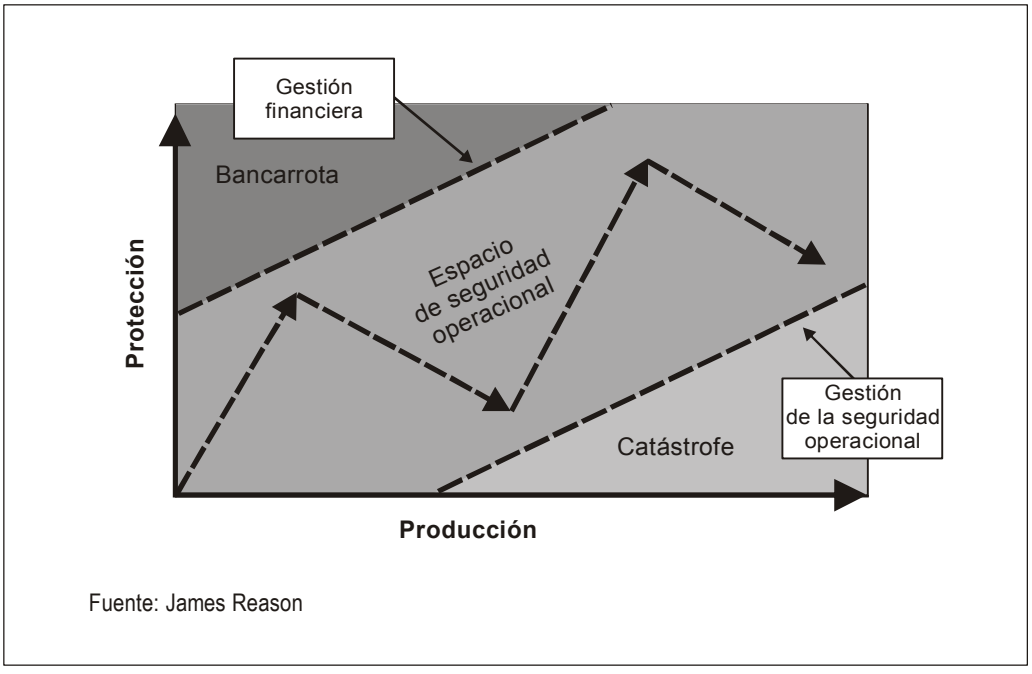


Figura 2-6. El espacio de la seguridad operacional

2.8.2 La gestión de los riesgos de seguridad operacional resultantes de los cambios pueden considerar los siguientes tres puntos:

a) *Criticidad de los sistemas y las actividades.* La criticidad se asocia a las posibles consecuencias de los riesgos de seguridad operacional, ya sea una consideración durante el proceso de diseño del sistema o durante una situación relacionada con el cambio sistémico. Se deben revisar los cambios al equipo y las actividades asociadas con riesgos de seguridad operacional relativamente altos para asegurarse de que se están tomando las medidas correctivas necesarias para controlar los riesgos de seguridad operacional potencialmente emergentes.

b) *Estabilidad de los sistemas y entornos operacionales.* Los cambios pueden ser planificados y estar bajo el control directo de la organización. Los cambios planificados pueden asociarse al crecimiento o reducción de la organización, así como también, a la introducción de nuevo equipos, productos o servicios. Los cambios no planificados, como aquellos que son de naturaleza operacional, política o económica, también pueden crear riesgos que requieren una respuesta de mitigación de la organización. Las instancias donde ocurren cambios sistémicos o del entorno frecuentes indican que los gerentes deben actualizar las evaluaciones de riesgo clave y la información asociada con más frecuencia que en situaciones más estables.

c) *Performance pasado.* El performance pasado de los sistemas fundamentales puede ser un indicador fiable de un performance futuro. Los análisis de tendencias en el proceso de aseguramiento de la seguridad operacional deben usarse para rastrear las medidas de rendimiento en materia de seguridad operacional y para incluir tal información en la planificación de actividades futuras bajo situaciones de cambio. Es más, en aquellos lugares donde se han encontrado deficiencias y se han corregido, como resultado de auditorías, evaluaciones, análisis de datos, investigaciones o informes pasados, es esencial que dicha información se considere para garantizar la eficacia de las medidas correctivas.

2.9 INTEGRACIÓN DE LOS SISTEMAS DE GESTIÓN

2.9.1 Las organizaciones de aviación varían en gran medida en términos de envergadura y complejidad generales. Cada organización tiene un sistema de gestión en capas que se compone de múltiples subsistemas, que reciben sus instrucciones mediante algún tipo de sistema de control. La organización debe integrar los sistemas de gestión institucional diseñados para lograr metas institucionales específicas, es decir, proporcionar productos y servicios a los clientes. A menudo, un sistema de gestión institucional holístico se conoce como un sistema de gestión integrado o, simplemente, el "sistema de gestión" de la organización.

2.9.2 Entre los sistemas de gestión típicos dentro de una organización de aviación pueden incluirse:

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 seguridad de la aviación (SeMS);

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); y

g) un sistema de gestión de documentación (DMS).

2.9.3 Cada sistema de gestión se controla a través de un "líder responsable". Las organizaciones de proveedores de productos y servicios complejas pueden tener más de treinta sistemas de gestión que deben integrarse en la empresa. Entre los ejemplos de tales sistemas se incluyen:

a) un sistema de gestión del proveedor;

b) un sistema de gestión de marketing;

c) un sistema de gestión del personal;

d) un sistema de gestión de las instalaciones;

e) un sistema de gestión del equipo en tierra;

f) un sistema de gestión de la producción;

g) un sistema de gestión de la capacitación;

h) un sistema de gestión de las operaciones de vuelo;

i) un sistema de gestión de las operaciones de carga;

j) un sistema de gestión del mantenimiento de aeronaves;

k) un sistema de gestión de despacho; y

l) un sistema de gestión de riesgos asociados a la fatiga (FRMS).

2.9.4 Existe una tendencia en desarrollo en la aviación civil, la que trata de integrar todos estos sistemas de gestión como componentes funcionales del sistema de gestión empresarial dominante. Existen varios beneficios claros para dicha integración:

a) reducción de la duplicación y, por tanto, de los costos;

b) reducción de los riesgos institucionales generales y un aumento en la rentabilidad;

c) equilibrio de objetivos potencialmente conflictivos; y

d) eliminación de responsabilidades y relaciones potencialmente conflictivas.

2.9.5 Cada organización integrará estos sistemas según sus requisitos de producción únicos. Los procesos de gestión de riesgos son características esenciales de SMS, QMS, EMS, FMS, OSHSMS y SeMS. Si el SMS fuese a funcionar aislado de estos otros sistemas de gestión, puede existir la tendencia de enfocarse solamente en los riesgos de seguridad operacional sin comprender la naturaleza de la calidad, la seguridad de la aviación o las amenazas del entorno para la organización.

2.9.6 Aunque es cierto que actualmente la integración del sistema va más allá del alcance de los SARPS de gestión de la seguridad operacional de la OACI armonizados y de este manual, muchas autoridades de aviación civil y proveedores de productos y servicios han notado los beneficios de integrar y alinear múltiples sistemas de gestión. Para obtener detalles sobre la integración de SMS y QMS, consulte el Capítulo 5.

2.10 NOTIFICACIÓN E INVESTIGACIÓN DE LA SEGURIDAD OPERACIONAL

Notificación de seguridad operacional eficaz

2.10.1 La notificación precisa y oportuna de información relevante relacionada con peligros, incidentes o accidentes es una actividad fundamental de la gestión de la seguridad operacional. Los datos usados para respaldar los análisis de seguridad operacional se informan usando múltiples fuentes. Una de las mejores fuentes de datos es la notificación directa del personal de primera línea, ya que estos observan los peligros como parte de sus actividades diarias. Un lugar de trabajo donde se haya capacitado y se aliente constantemente al personal a informar sus errores y experiencias es un requisito previo para lograr una notificación de seguridad operacional eficaz.

2.10.2 Existen cinco características básicas que están universalmente asociadas con los sistemas de notificación de seguridad operacional eficaces (véase la Figura 2-7). La notificación de peligros eficaz es un componente clave de la gestión de la seguridad operacional. Una vez informados, los datos sobre peligros pueden analizarse con otras fuentes de datos para respaldar los procesos de SRM y SA.

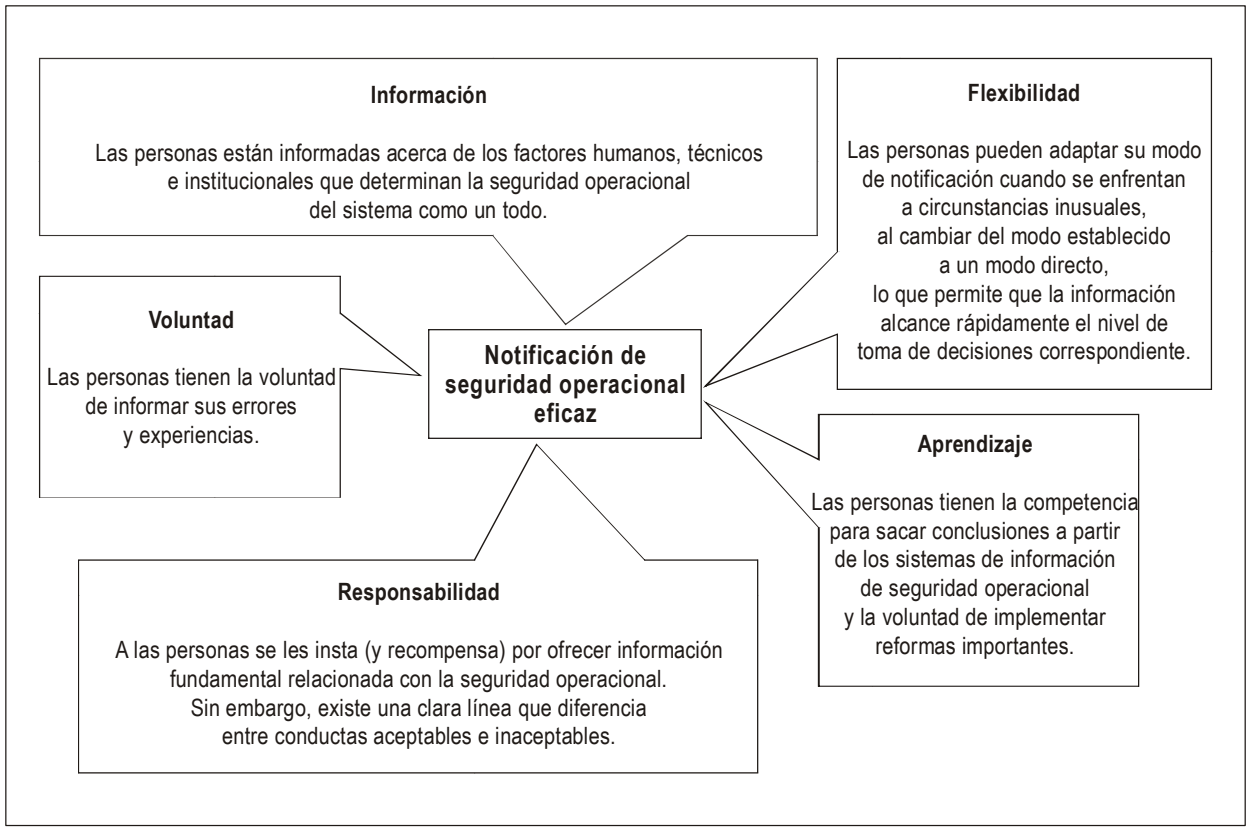


Figura 2-7. Notificación de seguridad operacional eficaz — cinco características básicas

2.10.3 Otra fuente de datos usada para respaldar los procesos de SRM y SA es la notificación de sucesos. Esto puede variar desde sucesos de alto impacto (accidentes, incidentes graves) hasta eventos de bajo impacto, como incidentes operacionales, averías del sistema/equipo o defectos. Aunque los requisitos reglamentarios para la notificación obligatoria de sucesos de alto impacto (accidentes, incidentes graves) son comunes, un entorno de gestión de seguridad operacional maduro también proporcionará la notificación de eventos de bajo impacto. Esto permite que los mecanismos de control necesarios aborden todos los posibles resultados de alto impacto. La tendencia (tasa de suceso) de los eventos de bajo impacto es inevitablemente un precursor de los resultados de alto impacto que seguirían.

2.10.4 En los Apéndices 2 y 3, respectivamente, del Capítulo 4 se ofrece una guía detallada sobre los sistemas de notificación de incidentes voluntaria y obligatoria del Estado. En el Apéndice 5 del Capítulo 5 se proporciona una guía sobre los sistemas de notificación voluntaria del SMS.

Investigación de accidentes e incidentes

2.10.5 Cuando ocurre un accidente o incidente grave, se inicia el proceso de investigación de accidentes para encontrar cualquier posible avería dentro del sistema de aviación, los motivos de esto y para generar las contramedidas necesarias a fin de evitar la recurrencia. Por tanto, en un entorno de gestión de la seguridad operacional, el proceso de investigación de accidentes tiene un papel distintivo, ya que es un proceso fundamental que se aplica cuando han fallado las defensas de seguridad operacional, las barreras, las revisiones y las compensaciones en el sistema.

2.10.6 Al ser un componente reactivo importante de los elementos incluidos en los marcos de trabajo del SMS y SSP, las investigaciones de accidentes contribuyen con la mejora continua del sistema de aviación al proporcionar las causas de origen de los accidentes/incidentes y las lecciones aprendidas a partir de los eventos. Esto puede respaldar las decisiones sobre el desarrollo de medidas correctivas y la asignación de recursos correspondiente; además, puede identificar las mejoras necesarias para el sistema de aviación, como SMS, SSP, así como también, el proceso de investigación de accidentes del Estado. Aunque es común que las investigaciones obligatorias a nivel de Estado se limiten a accidentes e incidentes graves, un entorno de gestión de la seguridad operacional maduro también puede proporcionar la investigación de eventos de bajo impacto.

2.10.7 Aparte de establecer los hallazgos y las causas de origen de los accidentes/incidentes, la mayoría de los ejercicios de investigación también descubren peligros/amenazas. Un proceso de investigación eficaz e integral incluye la identificación y diferenciación entre una consecuencia final, un evento inseguro y peligros/amenazas que contribuyen con los accidentes/incidentes. Esto puede incluir cualquier factor sistémico, latente o institucional dentro de todo el marco de trabajo del sistema de aviación. En el entorno de gestión de la seguridad operacional proactivo actual, existe una importante y necesaria integración entre un proceso de investigación de accidentes/incidentes y el proceso de identificación/notificación de peligros de una organización. El formato de la notificación de la investigación debe disponer claramente que se documenten los peligros/las amenazas descubiertos durante el proceso de investigación, el que puede requerir una medida de seguimiento por separado mediante el proceso de identificación de peligros y mitigación de riesgos de la organización. Es común que algunos informes de investigación limiten su "conclusión" y "medida tomada/recomendada" solo para las causas directas o inmediatas. Por lo tanto, cualquier peligro/amenaza secundaria o indirecta tiende a omitirse, a menos que esta brecha pueda completarse al vincular la investigación de accidentes/incidentes y los procesos de identificación de peligros.

2.11 RECOPILACIÓN Y ANÁLISIS DE DATOS DE LA SEGURIDAD OPERACIONAL

Recopilación y calidad de los datos de seguridad operacional

2.11.1 La toma de decisiones basada en datos es una de las facetas más importantes de cualquier sistema de gestión. El tipo de datos de seguridad operacional que se recopila puede incluir accidentes e incidentes, eventos, no

cumplimientos o desvíos e informes de peligros. Se debe considerar la calidad de los datos que se usan para permitir una toma de decisiones eficaz en todo el desarrollo e implementación del SSP y SMS. Desafortunadamente, muchas bases de datos carecen de la calidad de datos necesaria para ofrecer una base confiable a fin de evaluar las prioridades y la eficacia de las medidas de mitigación de riesgos. Si no se consideran las limitaciones de los datos usados para respaldar las funciones de la gestión de riesgos de seguridad operacional y el aseguramiento de la seguridad operacional, se generarán resultados erróneos del análisis, los que, a su vez, pueden producir decisiones incompletas y desacreditación del proceso de gestión de la seguridad.

2.11.2 Dada la importancia de la calidad de los datos, las organizaciones deben evaluar los datos usados para respaldar la gestión de riesgos de seguridad operacional y los procesos de aseguramiento de la seguridad operacional mediante los siguientes criterios:

a) *Validez.* Los datos recopilados son aceptables según los criterios establecidos para su uso previsto.

b) *Integridad.* No falta ningún dato relevante.

c) *Congruencia.* Se puede reproducir el grado hasta donde la medición de un parámetro determinado es congruente y evita errores.

d) *Accesibilidad.* Los datos están fácilmente disponibles para su análisis.

e) *Puntualidad.* Los datos son relevantes para el período de interés y están disponibles de forma oportuna.

f) *Seguridad.* Los datos están protegidos contra modificación accidental o maliciosa.

g) *Precisión.* Los datos no contienen errores.

Al considerar estos siete criterios para la calidad de datos, los análisis de datos de seguridad operacional generarán la información más precisa posible que se usará para respaldar la toma de decisiones estratégica.

Base de datos de la seguridad operacional

2.11.3 En el contexto de la recopilación y análisis de datos de seguridad operacional, el término “base de datos de seguridad” puede incluir el siguiente tipo de datos o información que puede usarse para respaldar los análisis de datos de la seguridad operacional:

a) datos de la investigación de accidentes;

b) datos de la investigación de incidentes obligatoria;

c) datos de la notificación voluntaria;

d) datos de la notificación de la aeronavegabilidad continua;

e) datos del control de rendimiento operacional;

f) datos de la evaluación de riesgos de seguridad operacional;

g) datos de los informes/hallazgos de la auditoría;

h) datos de los estudios/revisiones de seguridad operacional; E

i) datos de seguridad de otros Estados, organizaciones regionales de vigilancia de la seguridad operacional (RSOO) u organizaciones regionales de investigación de accidentes e incidentes (RAIO), etc.

2.11.4 Una base de datos de seguridad operacional puede hacer referencia a las bases de datos relacionadas con SSP del Estado o con la base de datos relacionada con SMS de un proveedor de servicios, según el contexto. Los informes voluntarios pueden provenir del personal de operaciones (proveedores de servicio, pilotos, etc.) al igual que desde pasajeros o el público general.

2.11.5 Gran parte de los datos en las bases de datos de seguridad operacional están en el formato de informes relacionados con eventos complejos, como accidentes e incidentes. Los informes en estos tipos de bases de datos responden, normalmente, a una serie de preguntas. ¿Quién estuvo involucrado en el evento? ¿Qué pasó que produjo la redacción de un informe? ¿Cuándo sucedió el evento? ¿Dónde sucedió el evento? ¿Por qué sucedió? Otros tipos de bases de datos se relacionan con temas relativamente estrechos, como información de vuelo, clima y volúmenes de tránsito. Estos informes contienen hechos simples.

2.11.6 Las bases de datos de seguridad operacional se alojan comúnmente en varias partes de una organización. Muchas organizaciones proporcionan acceso a las bases de datos mediante una interfaz que permite que los analistas de seguridad operacional especifiquen y extraigan eficientemente informes de interés. Los informes pueden verse de forma individual o colectiva mediante la agregación. Las herramientas analíticas permiten que los analistas de seguridad operacional vean los datos extraídos en múltiples formatos. Entre los ejemplos se incluyen hojas de cálculo, mapas y diversos tipos de gráficos.

2.11.7 Para garantizar que se comprenda y use correctamente una base de datos, la información relacionada con la base de datos (metadatos) debe documentarse debidamente y estar disponible para los usuarios. Entre los tipos de metadatos se incluyen las definiciones de campo, los cambios hechos a la base de datos con el tiempo, las reglas de uso, el formulario de recopilación de datos y las referencias a valores válidos.

2.11.8 Muchas organizaciones distintas han desarrollado varias bases de datos de seguridad operacional de forma independiente con áreas muy específicas de responsabilidad y necesidades de análisis. Para ofrecer a los analistas de seguridad operacional de aviación vistas ampliadas de problemas de seguridad operacional, es necesario desarrollar instalaciones de integración de información de seguridad operacional que puedan extraer la información desde múltiples fuentes, aplicar normas de datos comunes, consolidar metadatos y cargar la información en una plataforma común alojada en una arquitectura de almacenamiento de datos centralizada.

2.11.9 Luego de procesar los datos de seguridad operacional, los analistas de seguridad operacional pueden acceder a ellos mediante una interfaz común y un conjunto común de herramientas analíticas. Si un analista requiere datos desde múltiples bases de datos, la aplicación de normas de datos comunes hace posible que los técnicos de la base de datos extraigan tales datos desde las bases de datos necesarias y construyan una base de datos totalmente nueva. En la Figura 2-8 se muestra una vista esquemática del sistema de datos de seguridad operacional de un Estado, indicando las entradas, los procesos y los resultados relacionados con la recopilación, el análisis y el intercambio de datos de seguridad operacional.

Entradas (recopilación)	• informes de accidentes e incidentes; • sistemas de notificación de incidentes voluntarios; • sistemas de notificación de incidentes obligatorios; • sistemas de recopilación de datos operacionales (provistos directamente desde los proveedores de servicio); • sistemas de recopilación de datos de vigilancia de la seguridad operacional.
Procesos (Análisis)	• herramientas de recopilación de datos y sistemas de gestión de datos para capturar y almacenar datos desde: — sistemas de notificación de accidentes e incidentes; — sistemas de recopilación de datos operacionales; — sistemas de recopilación de datos de vigilancia de la seguridad operacional; — recomendaciones de las investigaciones de accidentes e incidentes graves; • métodos de análisis para evaluar riesgos conocidos y emergentes desde todas las fuentes de datos disponibles; • indicadores de seguridad operacional, niveles de objetivos y alertas (nivel individual o colectivo) para medir el rendimiento en materia de seguridad operacional y detectar las tendencias no deseadas; • desarrollo de procesos de vigilancia de seguridad operacional basada en riesgos, lo que incluye la priorización de las inspecciones y auditorías.
Resultados (intercambio)	• recomendaciones de seguridad operacional emitidas por autoridades pertinentes del Estado, según el análisis de todas las entradas del sistema de datos de seguridad operacional; • informes sobre los indicadores, los objetivos y las alertas de seguridad operacional (proveedor de servicios y nivel de Estado) generados mediante el análisis de las entradas de datos, como: — análisis de “punto de referencia” comparativo; — análisis de tendencia histórica; — correlaciones entre los indicadores proactivos y los resultados de seguridad operacional (accidentes e incidentes graves); • revisiones de los reglamentos del Estado y los procesos de vigilancia, como la priorización de las actividades de vigilancia de acuerdo con áreas de mayor riesgo; • medidas administrativas necesarias para propósitos de seguridad operacional; • el intercambio de información sobre temas de seguridad operacional entre autoridades reglamentarias del Estado y autoridades de investigación de accidentes; • el intercambio de información sobre temas de seguridad operacional entre proveedores de servicios, autoridades reglamentarias, así como también, organizaciones de investigación de accidentes e incidentes, a niveles nacional, regional e internacional.

Figura 2-8. Vista esquemática del sistema de datos de la seguridad operacional de un Estado

Análisis de datos de la seguridad operacional

2.11.10 Luego de recopilar datos de seguridad operacional mediante diversas fuentes, las organizaciones deben realizar el análisis necesario para identificar peligros y controlar sus consecuencias potenciales. Entre otros propósitos, el análisis se puede usar para:

a) ayudar a decidir qué hechos son necesarios;

b) determinar factores latentes subyacentes a las deficiencias de seguridad operacional;

c) ayudar a alcanzar conclusiones válidas; y

d) controlar y medir las tendencias o el rendimiento en materia de seguridad operacional.

2.11.11 A menudo, el análisis de seguridad operacional es reiterativo y requiere múltiples ciclos. Puede ser cuantitativo o cualitativo. La ausencia de datos de la línea base cuantitativa puede forzar a depender de métodos de análisis más cualitativos.

2.11.12 Los criterios humanos pueden estar sometidos a algún grado de parcialidad según experiencias pasadas, lo que podría influenciar la interpretación de los resultados del análisis o la prueba de hipótesis. Una de las formas más frecuentes de error de criterio se conoce como "sesgo de confirmación". Esta es una tendencia a buscar y conservar información que confirme lo que una persona ya cree que es cierto.

Métodos y herramientas analíticos

2.11.13 Se pueden usar los siguientes métodos de análisis de seguridad operacional:

a) *Análisis estadístico.* Este método puede usarse para evaluar la importancia de las tendencias de seguridad operacional percibidas, que se describen con frecuencia en presentaciones gráficas de resultados de análisis. Aunque los análisis estadísticos pueden producir información significativa sobre la importancia de ciertas tendencias, se debe considerar con cuidado la calidad de los datos y los métodos analíticos para evitar llegar a conclusiones erróneas.

b) *Análisis de tendencia.* Al controlar las tendencias en datos de seguridad operacional, se pueden hacer predicciones sobre eventos futuros. Las tendencias pueden indicar peligros emergentes.

c) *Comparaciones normativas.* Puede que no haya datos suficientes disponibles para proporcionar una base fáctica con la cual se puedan comparar las circunstancias de posibles eventos. En tales casos, puede que sea necesario tomar una muestra de experiencias del mundo real en condiciones operacionales similares.

d) *Simulación y prueba.* En algunos casos, los peligros pueden quedar en evidencia mediante la simulación y también con pruebas de laboratorio para validar las implicaciones de seguridad operacional de tipos de operaciones, equipos o procedimientos nuevos o existentes.

e) *Grupo de expertos.* Las visiones de pares y especialistas pueden resultar útiles para evaluar la naturaleza diversa de peligros relacionados con una condición insegura en particular. Un equipo multidisciplinario formado para evaluar la evidencia de una condición insegura puede ayudar a identificar el mejor curso de la medida correctiva.

f) *Análisis de costo-beneficios.* La aceptación de medidas recomendadas de control de riesgos de seguridad operacional puede depender del análisis de costo-beneficios creíble. El costo de implementar las medidas propuestas se compara con los beneficios esperados con el tiempo. El análisis de costo-beneficios puede sugerir que la aceptación de las consecuencias del riesgo de seguridad operacional es tolerable al considerar el tiempo, el esfuerzo y el costo necesarios para implementar la medida correctiva.

Gestión de información de la seguridad operacional

2.11.14 La gestión de la seguridad operacional eficaz se “basa en datos”. Una gestión sólida de las bases de datos de la organización es fundamental para garantizar un análisis eficaz y confiable de las fuentes de datos consolidadas.

2.11.15 El establecimiento y mantenimiento de una base de datos de seguridad operacional proporciona una herramienta fundamental para los problemas de seguridad operacional del sistema de control del personal. Se dispone de forma comercial de una amplia gama de bases de datos electrónicas económicas, compatibles con los requisitos de gestión de datos de la organización.

2.11.16 Según la envergadura y complejidad de la organización, los requisitos del sistema pueden incluir una gama de capacidades para gestionar eficazmente los datos de la seguridad operacional. En general, el sistema debe:

a) incluir una interfaz sencilla para el usuario para la entrada y consulta de datos;

b) tener la capacidad de transformar grandes cantidades de datos de seguridad operacional en información útil que respalde la toma de decisiones;

c) reducir la carga de trabajo para los gerentes y el personal de seguridad operacional; y

d) operar a un costo relativamente bajo.

2.11.17 Para sacarle provecho a los beneficios potenciales de las bases de datos de seguridad operacional, se requiere una comprensión básica de su operación. Si bien cualquier tipo de información agrupada de forma organizada puede considerarse como una base de datos, el análisis de registros en papel en un sistema de archivo simple será suficiente solo para operaciones pequeñas. El almacenamiento, el registro, el retiro y la recuperación mediante sistemas en papel son tareas difíciles de manejar. Es preferible que los datos se almacenen en una base de datos electrónica que facilite la consulta de los registros y la generación de resultados del análisis en varios formatos.

2.11.18 Las propiedades y los atributos funcionales de diferentes sistemas de gestión de bases de datos varían y cada uno de ellos deben considerarse antes de decidir el sistema más adecuado. Las funciones básicas deben permitir que el usuario realice tareas como:

a) registrar eventos de seguridad operacional en varias categorías;

b) vincular eventos con documentos asociados (por ejemplo, informes y fotografías);

c) controlar tendencias;

d) compilar análisis, gráficos e informes;

e) revisar registros históricos;

f) compartir datos de seguridad operacional con otras organizaciones;

g) controlar investigaciones de eventos; y

h) controlar la implementación de medidas correctivas.

Protección de los datos de seguridad operacional

2.11.19 Dado el potencial de mal uso de los datos de seguridad operacional que se compilaron estrictamente para el propósito de potenciar la seguridad operacional de la aviación, la gestión de la base de datos debe incluir la protección de tales datos. Los gerentes de base de datos deben equilibrar la necesidad de la protección de datos con aquella que hará accesible los datos a aquellos que pueden potenciar la seguridad operacional de la aviación. Entre las consideraciones de protección se incluye:

a) suficiencia de los reglamentos de "acceso a la información" en comparación con los requisitos de gestión de la seguridad operacional;

b) políticas y procedimientos institucionales sobre la protección de los datos de seguridad operacional que limitan el acceso a aquellos con la "necesidad de saber";

c) eliminación de la identificación, al borrar todos los detalles que puedan causar que un tercero infiera la identidad de las personas (por ejemplo, números de vuelo, fechas/horas, ubicaciones y tipos de aeronave);

d) seguridad de los sistemas de información, almacenamiento de datos y redes de comunicación;

e) prohibiciones en el uso no autorizado de los datos.

Puede encontrar más información sobre la protección de datos de la seguridad operacional en el Apéndice 5 del Capítulo 4.

2.12 INDICADORES DE SEGURIDAD OPERACIONAL Y CONTROL DE RENDIMIENTO

2.12.1 El resultado del sistema de recopilación y análisis de datos de una organización se describe normalmente en el formato de diagramas o gráficos. Tales diagramas o gráficos, usados comúnmente en sistemas de gestión de calidad/confiabilidad convencionales, muestran típicamente una "instantánea" del análisis de datos resultantes de una consulta única.

2.12.2 La Figura 2-9 es un diagrama de análisis de datos básico (captura de pantalla) y muestra la cantidad absoluta de incidentes del informe obligatorio de sucesos (MOR) de un explotador por el tipo de flota para el año 2009. Este diagrama básico no refleja la cantidad de aeronaves de cada flota ni explica la cantidad de vuelos de cada flota. Por lo tanto, existe una utilidad limitada que deriva de este tipo de diagrama. No sería adecuado para el propósito de un indicador de rendimiento en materia de seguridad operacional.

2.12.3 El análisis usado para controlar continuamente la seguridad operacional debe estar en la forma de una extracción de datos periódica para generar un diagrama o gráfico de tendencia, actualizado de forma mensual o trimestral, como se muestra en la Figura 2-10. Este diagrama de datos proporciona información sobre la tasa de incidentes de notificación mensual, considerando la cantidad de horas de vuelo (FH) acumuladas por la flota del explotador. Una carga

periódica (mensual) de los datos de la tasa de incidentes permitirá que el gráfico sirva como un indicador de control de tendencia continua. Luego de aplicar el diagrama del indicador de control de tendencia continuo, el siguiente paso será transformarlo en un indicador de medición del rendimiento en materia de seguridad operacional al configurar los niveles de objetivos y alertas dentro del diagrama. Este paso se debe hacer de preferencia donde los puntos de datos históricos ya se hayan generado en el diagrama. Estos puntos de datos históricos (rendimiento histórico) será la base para configurar o definir niveles de tendencia inaceptables, así como también, cualquier nivel de mejora deseado que se deba lograr dentro de un período especificado. En el Capítulo 4 (SSP) y Capítulo 5 (SMS) podrá encontrar más detalles sobre el desarrollo de los indicadores de rendimiento en materia de seguridad operacional y la configuración de objetivos y alertas asociada.

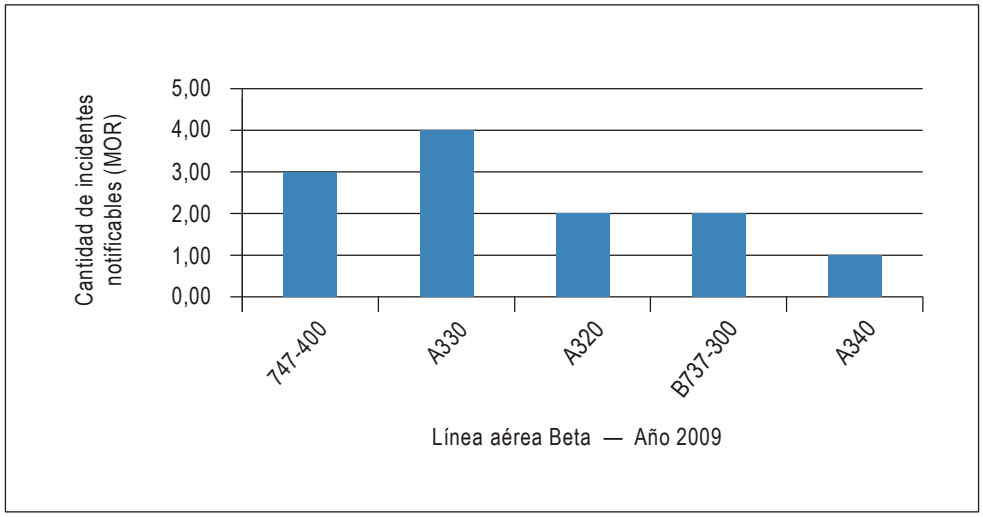


Figura 2-9. Un diagrama de análisis de datos básico (captura de pantalla)

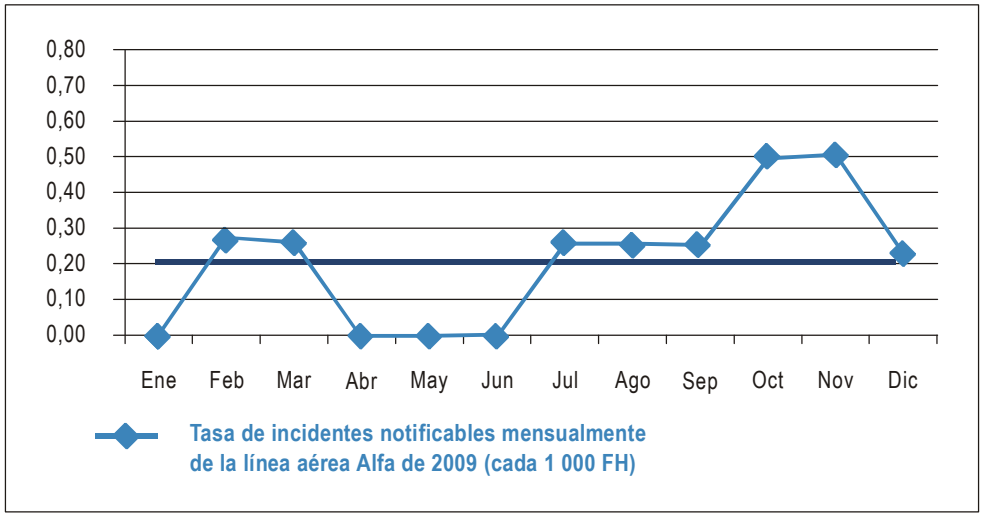


Figura 2-10. Un diagrama del indicador de seguridad operacional de control continuo

2.13 PELIGROS

2.13.1 La identificación de peligros es un requisito previo para el proceso de gestión de riesgos de seguridad operacional. Cualquier diferenciación incorrecta entre peligros y riesgos de seguridad operacional puede causar confusión. Una comprensión clara de los peligros y sus consecuencias relacionadas es fundamental para la implementación de una sólida gestión de riesgos de seguridad operacional.

Comprensión de peligros y las consecuencias

2.13.2 Generalmente, los profesionales de la seguridad operacional definen un peligro como una condición u objeto con el potencial de matar, causar lesiones al personal, dañar el equipo o las estructuras, perder material o reducir la capacidad de realizar funciones prescritas. Para propósitos de la gestión de riesgos de seguridad operacional de la aviación, el término peligro debe enfocarse en aquellas condiciones que pueden causar o contribuir con una operación insegura de la aeronave o del equipo, los productos y servicios relacionados con la seguridad operacional de la aviación. (La guía sobre la distinción de peligros directamente pertinentes a la seguridad operacional de la aviación a partir de otros peligros generales/industriales se aborda en 2.13.12 y 2.13.13).

2.13.3 Por ejemplo, considere un viento de 15 kt, lo que no es necesariamente una condición peligrosa. De hecho, un viento de 15 kt que sopla directamente por la pista mejora el despegue de la aeronave y el performance de aterrizaje. Sin embargo, un viento de 15 kt que sopla en una dirección a 90º por una pista de despegue o aterrizaje previstas, genera una condición de viento de costado que puede ser peligrosa a causa de su potencial de contribución con un suceso operacional de la aeronave, como una salida por el lado de la pista.

2.13.4 Los peligros son parte inevitable de las actividades de aviación. No obstante, su manifestación y posibles consecuencias pueden abordarse mediante diversas estrategias de mitigación para contener el potencial de un peligro que puede generar operaciones inseguras de la aeronave o del equipo de aviación.

2.13.5 Existe una tendencia común para confundir los peligros con sus consecuencias o resultados. Una consecuencia es un resultado que puede activarse por un peligro. Por ejemplo, la salida de la pista (aterrizaje largo) es una consecuencia proyectada en relación con el peligro de una pista contaminada. Al definir claramente el peligro primero, uno puede proyectar la consecuencia o el resultado adecuados. Se debe tener presente que las consecuencias pueden tener múltiples capas, incluidos eventos intermedios inseguros antes de la consecuencia final (accidente). Véase el Apéndice 2, Tabla 2-A2-3, para obtener información adicional.

2.13.6 En el ejemplo de viento de costado anterior, un resultado inmediato del peligro sería la pérdida de control lateral, seguido de una posterior salida de la pista. La consecuencia final sería un accidente. El potencial de daño de un peligro se materializa mediante una o muchas consecuencias. Por lo tanto, es importante incluir un recuento integral, para las evaluaciones de seguridad operacional, de todas las consecuencias probables, descritas con precisión y en términos prácticos. La consecuencia más extrema, la muerte de personas, debe diferenciarse de aquellas que implican el potencial de consecuencias leves, como un aumento en la carga de trabajo de la tripulación de vuelo, incomodidad de los pasajeros o reducción en los márgenes de seguridad operacional. La descripción de las consecuencias, de acuerdo con sus resultados factibles, facilita el desarrollo e implementación de estrategias de mitigación eficaces mediante la priorización adecuada y la asignación de recursos limitados. Una identificación de peligros adecuada genera una evaluación adecuada de los posibles resultados.

2.13.7 Los peligros deben diferenciarse de los errores, un componente normal e inevitable del desempeño humano, el que se debe controlar.

Identificación y priorización de peligros

2.13.8 Los peligros existen en todos los niveles en la organización y son detectables mediante el uso de sistemas de notificación, inspecciones o auditorías. Los contratiempos ocurren cuando los peligros interactúan con ciertos factores activadores. Como resultado, los peligros deben identificarse 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 peligros/incidentes. En el Capítulo 4, Apéndice 2, y Capítulo 5, Apéndice 5, podrá encontrar guías adicionales sobre los sistemas de notificación voluntaria. La información recopilada mediante tales sistemas puede complementarse con las observaciones o los hallazgos registrados durante las inspecciones de rutina en el sitio o las auditorías de la organización.

2.13.9 Los peligros también pueden identificarse a partir de la revisión o el estudio de los informes de investigación, particularmente aquellos peligros que se consideran factores contribuyentes indirectos y que posiblemente no se abordaron correctamente con las medidas correctivas resultantes del proceso de investigación. Por lo tanto, un procedimiento sistemático para revisar los informes de investigación de accidentes/incidentes en busca de peligros pendientes es un buen mecanismo para mejorar el sistema de identificación de peligros de la organización. Esto resulta particularmente pertinente cuando la cultura de seguridad operacional de una organización no está lo suficientemente madura como para respaldar un sistema de notificación de peligros voluntaria eficaz.

2.13.10 Los peligros pueden categorizarse de acuerdo con su fuente o ubicación. La priorización de peligros objetiva puede necesitar de categorías, de acuerdo con la gravedad/probabilidad de sus consecuencias proyectadas. Esto facilita la priorización de las estrategias de mitigación de riesgos, tanto como para usar recursos limitados de la forma más eficaz. Véase el Apéndice 3 de este capítulo para ver un ejemplo de un procedimiento de priorización de peligros.

Metodologías de identificación de peligros

2.13.11 Las tres metodologías para identificar peligros son:

a) *Reactiva.* Esta metodología implica el análisis de resultados o eventos pasados. Los peligros se identifican mediante la investigación de sucesos de seguridad operacional. Los incidentes y accidentes son claros indicadores de deficiencias del sistema y, por lo tanto, pueden usarse para determinar peligros que contribuyeron con el evento o que estén latentes.

b) *Proactiva.* Esta metodología implica el análisis de situaciones existentes o en tiempo real, lo cual es el principal trabajo de la función de aseguramiento de la seguridad operacional con sus auditorías, evaluaciones, notificación de empleados y los procesos de análisis y evaluación asociados. Esto implica la búsqueda activa de peligros en los procesos existentes.

c) *Predictiva.* Esta metodología implica la recopilación de datos para identificar resultados o eventos futuros posiblemente negativos, el análisis de los procesos del sistema y del entorno para identificar posibles peligros futuros y el inicio de medidas de mitigación**.**

Distinción entre peligros de aviación y peligros de seguridad, salud y ambiente en el trabajo (OSHE)

2.13.12 La comprensión de si un peligro es pertinente para la seguridad operacional de la aviación u OSHE depende de su consecuencia o riesgo potencial o predecible. Cualquier peligro que pueda tener un impacto (ya sea directo o indirecto) en la seguridad operacional de aeronaves o en equipos, productos y servicios relacionados con la seguridad operacional de la aviación debe considerarse pertinente para un SMS de aviación. Un peligro que tenga solo

consecuencias OSHE (es decir, sin ningún impacto en la seguridad operacional de la aviación), debe abordarse por separado del sistema/procedimientos OSHE de la organización, de acuerdo con sus requisitos OSHE pertinentes a nivel nacional o institucional, según corresponda. Los peligros y las consecuencias OSHE sin impacto en la seguridad operacional de la aviación no son relevantes para un SMS de aviación.

2.13.13 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 de 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 la 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 del lugar de trabajo" (seguridad operacional del personal de tierra/lugar de trabajo). Para un inspector de la seguridad operacional de aviación, es también un peligro de aviación con el riesgo de dañar la aeronave y la seguridad operacional de los pasajeros. Dado que las consecuencias de seguridad operacional de OSHE y de la aviación de tales peligros combinados no son las mismas, se deben considerar cuidadosamente para gestionarlas por separado. El propósito y enfoque de los controles preventivos para las consecuencias de seguridad operacional de OSHE y aviación deben ser diferentes.

2.14 RIESGOS DE LA SEGURIDAD OPERACIONAL

2.14.1 La gestión de riesgos de seguridad operacional es otro componente clave de un sistema de gestión de la seguridad operacional. El término gestión de riesgos de seguridad operacional fue creado para diferenciar esta función de la gestión de riesgos financieros, legales, económicos, etc. Esta sección presenta los fundamentos del riesgo de seguridad operacional e incluye los siguientes temas:

a) definición de un riesgo de seguridad operacional;

b) probabilidad del riesgo de seguridad operacional;

c) gravedad del riesgo de seguridad operacional;

d) tolerabilidad del riesgo de seguridad operacional; y

e) gestión del riesgo de seguridad operacional.

Definición de riesgo de seguridad operacional

2.14.2 El riesgo de seguridad operacional es la probabilidad y gravedad proyectada de la consecuencia o el resultado de una situación o peligro existente. Aunque el resultado puede ser un accidente, una "consecuencia/evento intermedio inseguro" puede identificarse como "el resultado más creíble". La disposición de la identificación de tales consecuencias en capas se asocia normalmente con un software de mitigación de riesgos más sofisticado. La hoja de cálculo de mitigación de riesgos de seguridad operacional ilustrada en el Apéndice 2 de este capítulo también tiene esta disposición.

Probabilidad del riesgo de seguridad operacional

2.14.3 El proceso de controlar los riesgos de seguridad operacional comienza al evaluar la probabilidad de que las consecuencias de los peligros se materialicen durante las actividades de aviación realizadas por la organización.

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

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

b) ¿Qué otros equipos o componentes del mismo tipo tienen defectos similares?

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

d) ¿Qué porcentaje del tiempo se usa el equipo sospechoso o el procedimiento cuestionable?

e) ¿Hasta qué grado existen implicaciones institucionales, administrativas o reglamentarias que pueden reflejar mayores amenazas para la seguridad pública?

2.14.4 Cualquier factor subyacente a estas preguntas ayudará a evaluar la probabilidad de que exista un peligro, considerando todos los casos potencialmente válidos. La determinación de la probabilidad puede usarse para ayudar a determinar la probabilidad del riesgo de seguridad operacional.

2.14.5 La Figura 2-11 presenta una tabla de probabilidad de riesgo de seguridad operacional típica, en este caso, una tabla de cinco puntos. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un evento o una condición inseguros, la descripción de cada categoría y una asignación de valor a cada categoría.

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 si ha ocurrido)	2
Sumamente improbable	Es casi inconcebible que ocurra el evento	1

Figura 2-11. Tabla de probabilidad del riesgo de seguridad operacional

2.14.6 Se debe enfatizar que este es solo un ejemplo y que el nivel de detalle y complejidad de las tablas y matrices debe adaptarse para ser proporcional con las necesidades y complejidades particulares de las diferentes organizaciones. Además, se debe tener presente que las organizaciones pueden incluir criterios tanto cualitativos como cuantitativos, que pueden incluir hasta 15 valores.

Gravedad del riesgo de seguridad operacional

2.14.7 Luego de completar la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional, considerando 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 evaluación de la gravedad puede basarse en:

a) *Fatalidades/lesión.* ¿Cuántas vidas podrían perderse? (empleados, pasajeros, peatones y público general)

b) *Daño.* ¿Cuál es el grado probable de daño para la aeronave, la propiedad y los equipos?

2.14.8 La evaluación de gravedad debe considerar todas las posibles consecuencias relacionadas con una condición o un objeto inseguros, considerando la peor situación predecible. La Figura 2-12 presenta una tabla de gravedad de riesgo de seguridad operacional típico. Incluye cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada categoría. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla solo es un ejemplo.

Tolerabilidad del riesgo de seguridad operacional

2.14.9 El proceso de evaluación de la probabilidad y gravedad del riesgo de seguridad operacional puede usarse para derivar un índice de riesgo de seguridad operacional. El índice que se crea mediante la metodología descrita anteriormente consta de un identificador alfanumérico, que indica los resultados combinados de las evaluaciones de probabilidad y gravedad. Las combinaciones de gravedad/probabilidad respectivas se presentan en la matriz de evaluación del riesgo de seguridad operacional en la Figura 2-13.

Gravedad	*Significado*	*Valor*
Catastrófico	— Equipo destruido — Varias muertes	A
Peligroso	— Una gran reducción de los márgenes de seguridad operacional, estrés físico o una carga de trabajo tal que ya no se pueda confiar en los explotadores para que realicen sus tareas con precisión o por completo — Lesiones graves — Daño importante al equipo	B
Grave	— Una reducción importante de los márgenes de seguridad operacional, una reducción en la capacidad de los explotadores 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 — Incidente grave — Lesiones para las personas	C
Leve	— Molestias — Limitaciones operacionales — Uso de procedimientos de emergencia — Incidente leve	Dr.
Insignificante	— Pocas consecuencias	E

Figura 2-12. Tabla de gravedad del riesgo de seguridad operacional

Probabilidad del riesgo		Gravedad del riesgo				
		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

Figura 2-13. Matriz de evaluación del riesgo de seguridad operacional

2.14.10 El tercer paso en el proceso es determinar la tolerabilidad del riesgo de seguridad operacional. Primero, es necesario obtener los índices en la matriz de evaluación del riesgo de seguridad operacional. Por ejemplo, considere una situación donde una probabilidad de riesgo de seguridad operacional se haya evaluado como ocasional (4) y una probabilidad de riesgo de seguridad operacional que se haya evaluado como peligrosa (B). La combinación de probabilidad y gravedad (4B) es el índice de riesgo de seguridad operacional de la consecuencia.

2.14.11 El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a una matriz de tolerabilidad del riesgo de seguridad operacional (véase la Figura 2-14) que describe los criterios de tolerabilidad para una organización en particular. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B cae en la categoría “inaceptable bajo las circunstancias existentes”. En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por tanto, la organización debe:

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

b) tomar medidas para reducir la gravedad de las consecuencias relacionadas con el peligro, es decir, reducir el componente de gravedad del índice de riesgo; o

c) cancelar la operación si la mitigación no es posible.

Nota.— La pirámide invertida en la Figura 2-14 refleja un esfuerzo constante para impulsar el índice de riesgo hacia la APEX de la parte inferior de la pirámide. La Figura 2-15 proporciona un ejemplo de una matriz de tolerabilidad de riesgo de seguridad operacional alternativa.

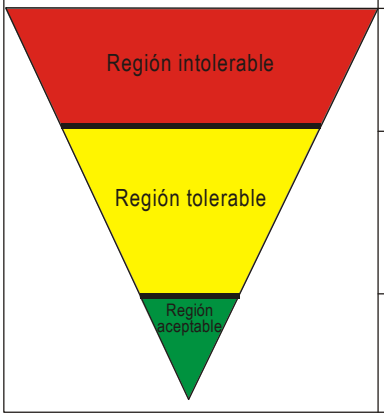
Descripción de la tolerabilidad	Índice de riesgo evaluado	Criterios sugeridos
	**5A, 5B, 5C, 4A, 4B, 3A**	Inaceptable según las circunstancias existentes
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Aceptable según la mitigación de riesgos. Puede necesitar una decisión de gestión.
	3E, 2D, 2E, 1B, 1C, 1D, 1E	Aceptable

Figura 2-14. Matriz de tolerabilidad del riesgo de seguridad operacional

Rango del índice de riesgo	Descripción	Medida recomendada
5A, 5B, 5C, 4A, 4B, 3A	Riesgo alto	Cese o disminuya la operación oportunamente si fuera necesario. Realice la mitigación de riesgos de prioridad para garantizar que haya controles preventivos adicionales o mejorados implementados para reducir el índice de riesgos al rango moderado o bajo
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Riesgo moderado	Programe el performance de una evaluación de seguridad operacional para reducir el índice de riesgos hasta el rango bajo, si fuera factible.
3E, 2D, 2E, 1B, 1C, 1D, 1E	Riesgo bajo	Aceptable tal cual. No se necesita una mitigación de riesgos posterior.

Figura 2-15 Matriz de tolerabilidad del riesgo de seguridad operacional alternativa

2.15 GESTIÓN DE RIESGOS DE LA SEGURIDAD OPERACIONAL

2.15.1 La gestión de riesgo de seguridad operacional abarca la evaluación y mitigación de los riesgos de seguridad operacional. El objetivo de la gestión de riesgo de seguridad operacional es evaluar los riesgos asociados con los peligros identificados y desarrollar e implementar mitigaciones eficaces y adecuadas. Por lo tanto, la gestión de riesgos de seguridad operacional es un componente clave del proceso de gestión de la seguridad operacional a nivel de Estado y del proveedor de productos/servicios.

2.15.2 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 son 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.

2.15.3 Los riesgos de seguridad operacional evaluados en la región tolerable son aceptables, siempre y cuando la organización implemente las estrategias de mitigación correspondientes. Un riesgo de seguridad operacional evaluado inicialmente como intolerable puede mitigarse y, posteriormente, trasladarse a una región tolerable, siempre y cuando dicho riesgo siga bajo el control de estrategias de mitigación adecuadas. En ambos casos, se debe realizar un análisis de costo-beneficios complementario, si se considera adecuado. Véase 2.15.7 para obtener más detalles.

2.15.4 Los riesgos de seguridad operacional evaluados que desde un principio estaban identificados en la región aceptable son aceptables tal y como están, y no requieren medidas para llevar o mantener la probabilidad o gravedad de las consecuencias de los peligros bajo control institucional.

Documentación/hoja de cálculo de la gestión de riesgo

2.15.5 Cada ejercicio de mitigación de riesgos deberá estar documentado, según sea necesario. Esto se puede hacer en una hoja de cálculo o una tabla básica para la mitigación de riesgos que implica operaciones, procesos o sistemas no complejos. Para la identificación de peligros y mitigación de riesgos que implican procesos, sistemas u operaciones complejas, puede que sea necesario usar un software de mitigación de riesgos para facilitar el proceso de documentación. Los documentos de mitigación de riesgos completos deben recibir la aprobación del nivel correspondiente de la administración. Para ver un ejemplo de una hoja de cálculo de mitigación de riesgos básica, véase el Apéndice 2.

Factores humanos y gestión de riesgos

2.15.6 Dado que los SSP y SMS maduros tienen por objetivo los factores humanos e institucionales, un proceso de análisis específico es un componente de cualquier sistema de gestión de riesgos maduro y eficaz. En el curso de cualquier ejercicio de identificación de peligros y mitigación de riesgos que impliquen elementos humanos, es necesario garantizar que las defensas existentes o recomendadas han considerado los factores humanos (HF). Cuando sea necesario, se puede realizar un análisis de HF complementario para respaldar el ejercicio/equipo de mitigación de riesgos en particular. Un análisis de HF proporciona una comprensión del impacto del error humano en la situación y, finalmente, contribuye con el desarrollo de medidas correctivas/mitigación más integrales y eficaces. Un modelo de error humano es la base del proceso de análisis y define la relación entre el rendimiento y los errores, además de categorizar los errores para permitir que se identifiquen más fácilmente y se entiendan mejor los peligros de origen. Esta comprensión garantiza la finalización adecuada de un análisis de causa de origen. Las medidas y decisiones individuales vistas fuera de contexto pueden parecer eventos prácticamente aleatorios, que escapan de su debida atención. El comportamiento humano no es necesariamente aleatorio. Por lo general sigue un tipo de patrón y puede analizarse y comprenderse correctamente. Finalmente, esta importante perspectiva de HF genera un proceso de mitigación más integral y en profundidad. Un análisis de HF garantiza que durante el proceso de mitigación de riesgos de la organización, al identificar el origen, los factores contribuyentes o de incremento, los factores humanos y sus impactos circunstanciales, de supervisión e institucionales asociados son debidamente considerados.

Análisis de costo-beneficios (CBA)

2.15.7 El análisis de costo beneficio o rentabilidad es normalmente un proceso independiente de la mitigación o evaluación de riesgo de seguridad operacional. Se asocia comúnmente con un protocolo de gestión de mayor nivel,

como una evaluación de impacto reglamentario o un proyecto de expansión comercial. Sin embargo, puede que haya situaciones donde una evaluación de riesgos esté en un nivel lo suficientemente alto o tenga un impacto financiero importante. En tales situaciones, se puede garantizar un proceso de CBA o rentabilidad complementario para dar respaldo a la evaluación de riesgos. Esto es para garantizar que el análisis de rentabilidad o la justificación de medidas de mitigación recomendadas o los controles preventivos han considerado las implicaciones financieras asociadas.

2.16 REQUISITOS PRESCRIPTIVOS Y BASADOS EN RENDIMIENTO

Comprensión de requisitos basados en rendimiento

2.16.1 Hay una creciente creencia dentro de la comunidad de aviación que señala que la implementación eficaz de un programa estatal de seguridad operacional (SSP) y un sistema de gestión de la seguridad operacional (SMS) requiere que un enfoque prescriptivo existente para la seguridad operacional sea complementado con un enfoque basado en rendimiento. Un enfoque basado en rendimiento, con el respaldo de la recopilación y el análisis de datos pertinentes, tiene un buen sentido comercial, mientras proporciona simultáneamente un nivel equivalente de seguridad operacional.

2.16.2 Una meta de un SMS es introducir elementos basados en rendimiento complementarios para conseguir un control más eficaz de los riesgos de seguridad operacional. En un entorno reglamentario convencional basado en cumplimiento, el enfoque de la gestión de seguridad operacional es relativamente rígido y prescriptivo, mediante el cual los reglamentos de seguridad operacional se usan como controles administrativos. Un marco de trabajo reglamentario recibe el respaldo de inspecciones y auditorías para garantizar un cumplimiento reglamentario.

2.16.3 En un entorno de seguridad operacional mejorado, basado en rendimiento, ciertos elementos basados en rendimiento se introducen dentro de un marco de trabajo prescriptivo. Esto permitirá que el aspecto de “cumplimiento” de un reglamento tenga espacio para un rendimiento más flexible basado en riesgos (y, por lo tanto, más dinámico). Como resultado, algunos elementos dentro de los marcos de trabajo de SMS y SSP pueden administrarse en un enfoque cada vez más basado en rendimiento que tan solo prescriptivo. Estos elementos basados en rendimiento están bajo los componentes del aseguramiento de la seguridad operacional y la gestión de riesgo de seguridad operacional de los marcos de trabajo respectivos.

2.16.4 Los elementos basados en rendimiento dentro de un marco de trabajo de SMS/SSP incluyen el proceso de control y la medición del rendimiento en materia de seguridad operacional a nivel de proveedor de productos y servicios individual y también a nivel del Estado. Este elemento permite que la organización seleccione sus propios indicadores de control de la seguridad operacional y la configuración de alertas y objetivos pertinentes para su propio contexto, el historial de rendimiento y las expectativas. No existen indicadores de seguridad operacional prescritos fijos (obligatorios) o niveles de alerta o valores prescritos según la expectativa de SMS/SSP.

Requisitos previos para los requisitos basados en rendimiento

2.16.5 El Estado y sus proveedores de productos y servicios, respectivamente, deben tener implementado un SSP y un SMS. Debe existir una interfaz implementada para que las organizaciones reglamentarias concuerden con los proveedores de productos y servicios sobre los indicadores de rendimiento en materia de seguridad operacional relacionados con SMS y la configuración de objetivos y alerta asociada. El regulador también necesitará un proceso para el control continuo del rendimiento en materia de seguridad operacional del proveedor de productos y servicios individual. Los nuevos procesos adicionales basados en rendimiento y debidamente aceptados/aprobados por el regulador deben tener indicadores de rendimiento adecuados para controlar tales procesos basados en rendimiento.

Tales indicadores específicos del proceso pueden verse como indicadores complementarios de los indicadores de rendimiento en materia de seguridad operacional del SMS de mayor nivel.

Línea base y nivel equivalente de seguridad operacional

2.16.6 El resultado del rendimiento en materia de seguridad operacional de la introducción de los elementos basados en rendimiento, dentro o complementarios a un marco de trabajo de SMS, no debe ser peor que el de un marco de trabajo reglamentario existente solo prescriptivo. Para evaluar o controlar que tal “equivalencia” sea de hecho el caso, deben existir indicadores de seguridad operacional para controlar el resultado general de los eventos (sucesos de no cumplimiento) del sistema/proceso pertinente para el cual se introducirá el elemento basado en rendimiento. Como ejemplo, la tasa de incidentes promedio de la planificación de vuelo y gestión de combustible (FPFM) general luego de la introducción de las disposiciones basadas en rendimiento no debe ser peor que la tasa de incidentes antes de la introducción de las disposiciones de FPFM basadas en rendimiento. Mediante un proceso de comparación, el rendimiento de "línea base" previo a la implementación puede verificarse si se compara con el rendimiento posterior a la implementación, para ver si se ha mantenido un nivel de rendimiento “equivalente”. Si el rendimiento posterior a la implementación resulta ser mejor, entonces se ha manifestado realmente un "mejor" nivel de rendimiento. Donde exista una degradación del rendimiento del sistema, el proveedor de servicios debe trabajar junto con el regulador para verificar los factores causativos y tomar medidas según corresponda, las que pueden incluir la modificación del requisito basado en rendimiento o, donde corresponda, la restauración de los requisitos preceptivos básicos. En la sección 2.16.7 y en los Capítulos 4 y 5 de este manual se señalan detalles de cómo se puede medir el rendimiento del sistema mediante indicadores de rendimiento en materia de seguridad operacional.

Control y medición basado en rendimiento

2.16.7 El control y la medición de un proceso basado en rendimiento se deben llevar a cabo mediante indicadores de rendimiento, calidad o seguridad operacional adecuados que rastreen continuamente el rendimiento de dicho proceso. Los parámetros de dicho seguimiento de rendimiento pueden ser resultados de sucesos, desviaciones o cualquier tipo de evento que refleje el nivel de seguridad operacional, calidad o riesgo del proceso. Se debe usar un diagrama de tendencia de datos para rastrear tales resultados. Los sucesos del resultado deben rastrearse normalmente como tasas de sucesos en lugar de números absolutos. Junto con tales indicadores, se deben ajustar los niveles de alertas al igual que los niveles perseguidos de mejora que desee para cada indicador, donde corresponda. Estos sirven como marcadores para definir qué es una tasa de sucesos anormal/inaceptable, así como también, la tasa (mejora) de objetivos deseada del indicador. La configuración del nivel de alerta servirá eficazmente como la línea demarcada entre la región de tendencia aceptable y la región inaceptable para un indicador de seguridad operacional. Así que, mientras la tasa de sucesos de un proceso no presente una tendencia que vaya más allá o viole los criterios del nivel de alerta establecidos, la cantidad de tales sucesos se considerará aceptable (no anormal) para ese período de control. Por otra parte, el propósito de un nivel de mejora objetivo es lograr el nivel de mejora deseado dentro de un hito futuro definido o período de control. Con tal configuración de alertas y objetivos, se vuelve aparente que el resultado del rendimiento cualitativo/cuantitativo puede derivarse al final de un período de control dado. Esto se puede hacer al contar la cantidad de violaciones de alertas o la cantidad de objetivos logrados para un indicador individual o un paquete de indicadores de seguridad operacional. Los ejemplos de los indicadores de rendimiento en materia de seguridad operacional y las metodologías de configuración de objetivos/alertas se abordan más a fondo en los Capítulos 4 y 5, respectivamente.

Vigilancia de los requisitos basados en rendimiento

2.16.8 A diferencia de la auditoría de requisitos prescriptivos independientes, la evaluación de un proceso basado en rendimiento requeriría que el asesor tomara en cuenta el contexto de dicho proceso/elemento dentro de su

marco de trabajo reglamentario general, así como también, dentro de la complejidad de la organización auditada. Puede que no existan criterios simples de "procede/no procede" o de aprobación/reprobación que puedan aplicarse. Un ejemplo sería la aceptabilidad de un sistema de notificación de peligros o la aceptabilidad de los niveles de objetivos/alertas propuestos para un proceso basado en rendimiento, el que puede implicar más interacción, control, negociación y criterio objetivo para el auditor. El nivel o grado de cumplimiento o rendimiento de tales elementos también puede variar según la complejidad del proceso u operación auditada. Un ejemplo del rendimiento o cumplimiento del elemento, que está sujeto a la complejidad institucional o del proceso, es el proceso de mitigación de riesgos. Un proceso de mitigación de riesgos puede implicar el uso de una sola hoja de cálculo para una tarea de taller de una operación simple de un solo hombre. Por otra parte, la mitigación de riesgos de un proceso complejo y multidisciplinario (por ejemplo, las operaciones en espacio aéreo afectadas por erupciones volcánicas) puede necesitar el uso de software de mitigación de riesgos para realizar una evaluación de seguridad operacional satisfactoriamente integral.

Apéndice 1 del Capítulo 2

LISTA DE VERIFICACIÓN DE LA EVALUACIÓN DE CULTURA DE SEGURIDAD OPERACIONAL DE LA ORGANIZACIÓN (OSC)/ PERFIL DE RIESGO DE LA ORGANIZACIÓN (ORP) — EXPLOTADORES AÉREOS

Nota.— Esta lista de verificación de evaluación de OSC/ORP es solo una ilustración conceptual. Los 37 parámetros ilustrados no son todos los que existen y se aplican para una organización explotadora aérea. Sería necesario personalizar estos parámetros para la evaluación de otros tipos de proveedores de servicios. Las puntuaciones del resultado anotado son solo ilustrativas. Esta evaluación de OSC/ORP debe realizarse de forma voluntaria en vista de los parámetros del perfil/cultura de la organización, que van más allá del ámbito reglamentario normal. Véanse los Capítulos 2, 2.6.19, para conocer una aplicación sugerida de tal diagrama de evaluación de OSC/ORP.

Columna de resultado: en el menú desplegable, seleccione “1” (L1), “2” (L2), “3” (L3) o “N/A” según la evaluación de POI/PMI /AOC ORP Marzo 12

Nombre de la organización:	Evaluado por/fecha:

	Parámetro de riesgo de la organización	*Nivel/perfil de riesgo*			*Resultado (nivel #)*
		Nivel 3 (menos deseado)	*Nivel 2 (promedio)*	*Nivel 1 (más deseado)*	
1	Gerente responsable — propiedad de las funciones de seguridad operacional/calidad	No existen funciones de seguridad operacional/calidad en las TOR del gerente responsable	Las TOR del gerente responsable tienen una mención insignificante o vaga de las funciones de seguridad operacional/calidad	Responsabilidad final de los asuntos de seguridad operacional y calidad abordados claramente en las TOR del gerente responsable.	3
2	Estado financiero de la organización	TBD	TBD	TBD	2
3	Edad promedio de la flota	Más de 12 años	De 8 a menos de 12 años	Menos de 8 años	2
4	Puntuación de performance del SMS	Año 2011: 65% al 75%	76% al 90%	Más de 90%	3
5	Programa activo de identificación de peligros y evaluación de riesgos (HIRA)	No hay ningún programa HIRA activo implementado	Programa HIRA implementado. Finalización o revisión de 1 a 3 proyectos de evaluación de riesgos (cada 100 empleados de operaciones) dentro de los últimos 12 meses.	Implemente el programa HIRA para todas las áreas de operaciones principales. Finalización o revisión de más de 3 proyectos de evaluación de riesgos (cada 100 empleados de operaciones) para todas las áreas de operaciones dentro de los últimos 12 meses.	2

	Parámetro de riesgo de la organización	*Nivel/perfil de riesgo*			*Resultado (nivel #)*
		Nivel 3 (menos deseado)	*Nivel 2 (promedio)*	*Nivel 1 (más deseado)*	
6	Organización o cronograma exigente de la tripulación de vuelo (¿cantidad de incidentes de la limitación del tiempo de vuelo?)	TBD	TBD	TBD	2
7	Relación entre la seguridad operacional interna más el personal de control de calidad y todo el personal de operaciones	1: más que 20	1:15 a 20	1: menos que 15	3
8	Vuelo con flota mixta (MFF) (porcentaje de pilotos implicados en MFF — un mayor porcentaje es menos recomendable)	TBD	TBD	TBD	1
9	Rutas de EDTO (porcentaje de sectores de EDTO operados) (un porcentaje mayor es menos recomendable)	TBD	TBD	TBD	2
10	Duración de EDTO (una mayor duración es menos recomendable)	TBD	TBD	TBD	2
11	Experiencia de la empresa (años de operación)	Menos de 5 años	De 5 a 10 años	Más de 10 años	3
12	Rotación combinada del ejecutivo responsable, el gerente de seguridad operacional y el gerente de calidad en los últimos 36 meses	De 3 o más	2	1 o ninguno	2
13	Experiencia y calificaciones del ejecutivo responsable (a partir de la fecha de evaluación)	Tiene menos de 3 años de experiencia en aviación y ninguna calificación técnica	Tiene más de 3 años de experiencia en aviación o calificaciones técnicas	Tiene más de 3 años de experiencia en aviación y calificaciones técnicas en aviación	3
14	Experiencia y calificación del gerente de seguridad operacional (SM)	Tiene menos de 5 años de experiencia de seguridad operacional/calidad en aviación civil o ninguna calificación técnica en aviación	Tiene más de 5 años de experiencia de seguridad operacional/calidad en aviación civil y calificaciones técnicas en aviación	Tiene más de 15 años de experiencia de seguridad operacional/calidad en aviación civil y calificaciones técnicas en aviación	2
15	Experiencia y calificaciones del gerente de calidad	Tiene menos de 5 años de experiencia de QC/QA en aviación civil o ninguna calificación técnica en aviación civil	Tiene más de 5 años de experiencia de QC/QA en aviación civil y calificaciones técnicas en aviación civil	Tiene más de 15 años de experiencia de QC/QA en aviación civil y calificaciones técnicas en aviación civil	1

	Parámetro de riesgo de la organización	*Nivel/perfil de riesgo*			*Resultado (nivel #)*
		Nivel 3 (menos deseado)	*Nivel 2 (promedio)*	*Nivel 1 (más deseado)*	
16	Personal de gestión de seguridad operacional/calidad de cartera múltiple (QM/SM)	La SM o QM incluye otras posiciones ejecutivas simultáneas dentro o fuera de la organización	Las TOR de SM o QM incluyen otras funciones de seguridad operacional/ calidad no directas, por ejemplo, TI, administración, capacitación	La SM o QM no incluye ningún otro cargo ejecutivo simultáneo dentro o fuera de la organización y sus TOR no incluyen otras funciones de calidad/seguridad operacional no directas	2
17	Multiplicidad de los tipos de aeronaves	Más de 4 tipos de aeronaves	De 3 a 4 tipos de aeronaves	Menos de 3 tipos de aeronaves	1
18	La tasa de incidentes de notificación obligatoria de la flota combinada (cada 1 000 FH) por los últimos 24 meses	TBD	TBD	TBD	2
19	Reservado				
20	Tasa de IFSD de la flota combinada cada 1 000 FH	TBD	TBD	TBD	2
21	Tasa de aplicación promedio de MEL de la flota (cada 1 000 FH)	Más de 30 aplicaciones de MEL por cada 1 000 FH	De 10 a 30 aplicaciones de MEL por cada 1 000 FH	Menos de 10 aplicaciones de MEL por cada 1 000 FH	2
22	Tasa de aplicación de concesión técnica interna	3 concesiones por aeronave por año	Más de 1 concesión por aeronave por año	Menos de 1 concesión por aeronave por año	2
23	Tasa de aplicación de concesión técnica de CAA.	Más de 1 concesión por aeronave por año	Más de 0,5 concesiones por aeronave por año	Menos de 0,5 concesiones por aeronave por año	2
24	Estructura de responsabilidad de seguridad operacional	La función/oficina/gerente de gestión de seguridad operacional es responsable o subordinada de algunas funciones operacionales	La función/oficina/gerente de gestión de seguridad operacional es responsable de la administración superior y es independiente de todas las funciones operacionales	La función/oficina/gerente de gestión de seguridad operacional tiene responsabilidad y notificación directa al CEO	3
25	Estructura de responsabilidad de la calidad	La función/oficina/gerente de gestión de calidad es responsable o subordinada a funciones relacionadas que no sean de calidad ni seguridad operacional	La función/oficina/gerente de gestión de calidad es responsable de la administración superior y es independiente de todas las funciones operacionales	La función/oficina/gerente de gestión de calidad tiene responsabilidad y notificación directa al CEO	3
26	Tasa de hallazgos de la auditoría de la organización de CAA de AOC (solo hallazgos de niveles 1 y 2, observaciones excluidas) por los últimos 24 meses	Cualquier hallazgo de Nivel 1 o más de 5 hallazgos por auditoría por aeronave	Más de 1 hallazgo por auditoría por aeronave	Menos de 1 hallazgo por auditoría por aeronave	2
27	Tasa de hallazgos de LSI de CAA (solo hallazgos de niveles 1 y 2, observaciones excluidas) por los últimos 24 meses	Cualquier hallazgo de Nivel 1 o más de 3 hallazgos por auditoría por estación de línea	Más de 0,5 hallazgos por auditoría por estación de línea	Menos de 0,5 hallazgos por auditoría por estación de línea	2

	Parámetro de riesgo de la organización	*Nivel/perfil de riesgo*			*Resultado (nivel #)*
		Nivel 3 (menos deseado)	*Nivel 2 (promedio)*	*Nivel 1 (más deseado)*	
28	Política de vida útil máxima/CM/mínima de los componentes (rotables/LRU) más allá de lo obligatorio o de los requisitos de MPD	Sin política de control de la vida útil de los componentes (máxima/ mínima) más allá de lo obligatorio o de los requisitos de MPD	Política y procedimientos de control de la vida útil máxima de los componentes activos. Al menos del 5% al 10% de todos los rotables de control del motor y de vuelo (indicados en MPD/ AMS) (más allá de lo obligatorio y de los requisitos de MPD) han recibido una vida útil máxima o mínima.	Política y procedimientos de control de la vida útil máxima de los componentes activos. Más del 10% de todos los rotables de control del motor y de vuelo (indicados en MPD/AMS) (más allá de lo obligatorio y de los requisitos de MPD) han recibido una vida útil máxima o mínima.	3
29	Alcance de la investigación de QA y el proceso de MEDA	Proceso de investigación interna de QA aplicado solo a los incidentes obligatorios	Proceso de investigación interna de QA para todos los incidentes notificados	Proceso de investigación interna de QA para todos los incidentes notificados + proceso de MEDA (o equivalente)	
30	Disponibilidad del programa de protección ambiental	No existe	Participación aislada en un programa de protección ambiental de aviación	Programa rutinario y compromiso y participación regular en un programa de protección ambiental de aviación	3
31	Disponibilidad del programa de inspección especial basado en publicaciones de servicios de OEM no obligatorios	Programa de inspección especial solo para SB relacionados con AD	Programa de inspección especial solo para AD y SB de alerta	Programa de inspección especial para AD, SB de alerta y publicaciones de servicios de OEM de rutina	2
32	Control de la gestión técnica de la flota	Contrata totalmente una organización externa (FTM + ITM)	Contrata parcialmente una organización externa	Gestión interna mediante una organización de AOC	2
33	Uso de personal técnico contratado	Más del 15% de personal contratado (de otra organización) para funciones de ingeniería/técnicas internas	De 5% a 15% de personal contratado (de otra organización) para funciones de ingeniería/técnicas internas	Menos del 5% de personal contratado (de otra organización) para funciones de ingeniería/técnicas internas	2
34	Certificación de inspección de tránsito de piloto, técnico o AME	Practica la certificación de la inspección de tránsito de piloto en reemplazo de un técnico de ingeniería/AME calificado	Practica la certificación de inspección de tránsito (clasificación limitada) de técnico en reemplazo de AME	Practica solo certificación de inspección de tránsito (clasificación completa) de AME	3
35	Sistema de notificación de peligros	Ninguno implementado	Sistema de notificación de peligros voluntario implementado	Sistema de notificación de peligros voluntario implementado. Además de un procedimiento de identificación de peligros junto con el proceso de investigación de incidentes.	2
36	Notificación e investigación de incidentes y procedimientos de medidas correctivas	Sin investigación ni notificación de incidentes o procedimientos de medidas correctivas documentados	Notificación e investigación de incidentes o procedimientos de medidas correctivas documentados	Notificación e investigación de incidentes o procedimientos de medidas correctivas documentados, y aceptados por la CAA	2

	Parámetro de riesgo de la organización	*Nivel/perfil de riesgo*			*Resultado (nivel #)*
		Nivel 3 (menos deseado)	*Nivel 2 (promedio)*	*Nivel 1 (más deseado)*	
37	Gestión de registros técnicos, almacenes técnicos y planificación de flota	Contrata completamente la gestión de registros técnicos, almacenes técnicos y planificación de flota a una organización externa	Contrata la gestión de registros técnicos, almacenes técnicos o planificación de flota a una organización externa	Gestión interna de registros técnicos, almacenes técnicos y planificación de flota	3

	Subtotal
Nivel 3	11
Nivel 2	21
Nivel 1	3
N/A	0
Cantidad total de preguntas	37

Resultado de la evaluación	
Puntos totales	Categoría de ORP
78	D

Categorización de ORP	
Puntuación total	**Categoría de ORP**
35–49	A (deseado)
50–63	B
64–77	C
78–91	D
92–105	E (menos deseado)

Notas.—

1. Las descripciones/cifras de los criterios de nivel de riesgo son solo ilustrativas y están sujetas a la personalización y validación de las cifras reales que se usarán.

2. La lista de verificación debe actualizarse para proveedores de servicio de AMO, aeródromo y ATS.

3. Puntos que deben asignarse para cada parámetro evaluado; es decir, 1, 2 o 3 para los Niveles 1, 2 y 3, respectivamente.

4. Esta evaluación de lista de verificación de OSC/ORP puede completarla de forma programada el inspector/encuestador asignado (como durante una auditoría de la organización). Puede que deba colaborar con el proveedor de servicios para obtener parte de los datos necesarios.

5. Este proceso de evaluación de OSC/ORP puede no ser obligatorio en vista de aquellos parámetros que están fuera del ámbito reglamentario normal, por ejemplo, la tasa de rotación del personal. Puede administrarse de acuerdo con una participación complementaria/voluntaria.

6. Los puntos totales alcanzados y la categoría de ORP correspondiente (Cat A a E) deberán anotarse. Los resultados deben proporcionarse a la organización evaluada.

7. Los resultados de esta evaluación de OSC/ORP pueden correlacionarse con otros hallazgos del programa de inspección/auditoría reglamentario a fin de identificar las áreas (organizaciones) con una mayor preocupación o necesidad según los requisitos del Elemento 3.3 del SSP. De lo contrario, la notificación de los resultados de ORP a cada organización por sí sola podría ser suficiente como mecanismo para alentar el comportamiento institucional (cultura de seguridad operacional) hacia la categoría que se desee, donde corresponda.

Apéndice 2 del Capítulo 2

Ejemplo de una hoja de cálculo de mitigación de riesgos de la seguridad operacional

Nota.— Para obtener una gestión de hoja de cálculo más fácil, es preferible usar una hoja de cálculo para cada combinación diferente de Peligro>Evento inseguro>Consecuencia final.

Tabla 2-A2-1. Peligro y consecuencia

Operación/proceso:	Describir el proceso/operación/equipo/sistema sujeto a este ejercicio de HIRM.
Peligro (H):	Si hay más de un peligro en la operación/proceso, use una hoja de cálculo por separado para abordar cada peligro.
Evento inseguro (UE):	Si hay más de un UE en el peligro, use una hoja de cálculo por separado para abordar cada combinación de UE-UC.
Consecuencia final (UC):	Si hay más de un UC en el peligro, use una hoja de cálculo por separado para abordar cada UC.

Tabla 2-A2-2. Índice de riesgo y tolerabilidad de la consecuencia/UE (véase el Adjunto 1)

	Tolerabilidad de riesgos actual (considerando cualquier PC/RM/EC existente)				*Índice de riesgo y tolerabilidad resultante (considerando cualquier PC/RM/EC nueva)*		
	Gravedad	Probabilidad	Tolerabilidad		Gravedad	Probabilidad	Tolerabilidad
Evento inseguro							
Consecuencia final							

Tabla 2-A2-3. Mitigación de riesgos

Peligro (H)	*PC*	*EF*	*EC*		*RM*	*EF*	*EC*	
H	PC1 (Existente)	EF (Existente)	EC1 (Existente)	UE	RM1	EF (a RM1)	EC (a EF)	UC
			EC2 (nuevo)					
	PC2 (Existente)	EF1 (nuevo)	EC (nuevo)		RM2	EF (a RM2)	EC (a EF)	
		EF2 (nuevo)	EC (nuevo)					
	PC3 (nuevo)	EF (nuevo)	EC (nuevo)		RM3	EF (a RM3)	EC (a EF)	

Notas explicativas.—

1. *Operación/proceso (Tabla 2-A2-1).* Descripción de la operación o el proceso que está sujeto a este ejercicio de mitigación de peligros/riesgos.

2. *Peligro (H).* Condición o situación indeseable que puede resultar en eventos u ocurrencias inseguros. Algunas veces, el término “amenaza” (por ejemplo, TEM) se usa en lugar de “peligro”.

3. *Evento inseguro (UE).* Posible evento inseguro intermedio antes de cualquier consecuencia final, accidente o resultado más creíble. La identificación de un evento inseguro corresponde solo cuando existe la necesidad de distinguir y establecer medidas mitigadoras corriente arriba y corriente abajo de dicho evento intermedio (antes de la consecuencia final/accidente) (por ejemplo, “evento de sobretemperatura” antes de una “falla de motor”). Si este estado de UE intermedio no corresponde para una operación en particular, entonces puede excluirse según corresponda.

4. *Consecuencia final (UC).* Resultado más creíble, evento final o accidente.

5. *Control preventivo (PC).* Medida/mecanismo/defensa mitigadora para bloquear o evitar que un peligro/amenaza aumente en intensidad hacia un evento inseguro o consecuencia final.

6. *Factor de escalada (EF).* Una posible condición latente/factor que puede debilitar la eficacia de un control preventivo (o medida de recuperación). Use solo donde corresponda. Es posible que un factor de escalada pueda nombrarse algunas veces como "amenaza".

7. *Control de escalada (EC).* Medida/mecanismo de mitigación para bloquear o evitar que un factor de escalada comprometa o debilite un control preventivo (o medida de recuperación). Use solo donde corresponda.

8. *Índice de riesgo actual y tolerabilidad.* La medida de mitigación de riesgo (Tabla 2-A2-3) se aplica cada vez que el nivel de tolerabilidad actual inaceptable de un evento inseguro o consecuencia final se identifica en la Tabla 2-A2-2. El índice de riesgo actual y la tolerabilidad deben considerar los controles preventivos existentes, donde corresponda.

9. *Índice de riesgo y tolerabilidad resultantes.* El índice de riesgo y tolerabilidad resultantes se basan en los controles preventivos actuales combinados (si los hubiera) junto con los nuevos controles preventivos/controles de escalada/medidas de recuperación implementados como resultado de un ejercicio de mitigación de riesgos completado.

Adjunto al Apéndice 2. Tablas de ejemplo de gravedad, probabilidad, índice de riesgo y tolerabilidad

Tabla Adj-1. Tabla de gravedad (básica)

Nivel	*Descripción*	*Descripción de gravedad (personalización de acuerdo con la naturaleza de las operaciones del proveedor de productos o servicios)*
1	Insignificante	No tiene importancia para la seguridad operacional relacionada con la aeronave
2	Leve	Degrada o afecta los procedimientos o performance operacional de la aeronave
3	Moderado	Pérdida parcial de los sistemas de aeronave significativos/importantes o resultados en la aplicación anormal de procedimientos de operaciones de vuelo
4	Grave	Falla completa de los sistemas de aeronave significativos/importantes o resultados en la aplicación de emergencia de procedimientos de operaciones de vuelo
5	Catastrófico	Pérdida de la aeronave o vidas

Tabla Adj-2. Tabla de gravedad (alternativa)

Nivel	*Descripción*	*Descripción de gravedad (personalización de acuerdo con la naturaleza de las operaciones del proveedor de productos o servicios)*					
		Seguridad operacional de la aeronave	*Lesión física*	*Daños a activos*	*Potencial pérdida de ganancias*	*Daños al ambiente*	*Daño a la reputación empresarial*
1	Insignificante	No tiene importancia para la seguridad operacional relacionada con la aeronave	Sin lesiones	Sin daños	Sin pérdida de ganancias	Sin efectos	Sin implicancias
2	Leve	Degrada o afecta los procedimientos o performance operacional de la aeronave	Lesión leve	Daño leve Menor que $__	Pérdida leve Menor que $__	Efecto leve	Implicancia localizada y limitada
3	Moderado	Pérdida parcial de los sistemas de aeronave significativos/importantes o resultados de la aplicación del procedimiento de las operaciones de vuelo	Lesión grave	Daño sustancial Menor que $__	Pérdida sustancial Menor que $__	Efecto contenido	Implicancia regional
4	Grave	Falla completa de los sistemas de aeronave significativos/importantes o resultados en la aplicación de emergencia de procedimientos de operaciones de vuelo	Un caso mortal	Daño importante Menor que $__	Pérdida importante Menor que $__	Efecto importante	Implicancia nacional
5	Catastrófico	Pérdida de aeronave/casco	Varios casos mortales	Daño catastrófico Más que $__	Pérdida masiva Más que $__	Efecto masivo	Implicancia internacional

Nota.— Use el nivel de gravedad más alto que haya obtenido para derivar el índice de riesgo en la tabla de matriz de índice de riesgo.

Tabla Adj-3. Tabla de probabilidad

Nivel	*Descripción*	*Descripción de probabilidad*
A	Seguro/frecuente	Se espera que ocurra en la mayoría de las circunstancias
B	Probable/ocasional	Probablemente suceda en algún momento
C	Posible/remoto	Podría ocurrir en algún momento
Dr.	Poco probable/ improbable	Puede ocurrir en algún momento
E	Excepcional	Puede ocurrir solo en circunstancias excepcionales

Tabla Adj-4. Matriz de índice de riesgo (gravedad × probabilidad)

Probabilidad	*Gravedad*				
	1. Insignificante	*2. Leve*	*3. Moderado*	*4. Grave*	*5. Catastrófico*
A. Seguro/frecuente	**Moderado (1A)**	**Moderado (2A)**	**Alto (3A)**	**Extremo (4A)**	**Extremo (5A)**
B. Probable/ocasional	**Bajo (1B)**	**Moderado (2B)**	**Moderado (3B)**	**Alto (4B)**	**Extremo (5B)**
C. Posible/remoto	**Bajo (1C)**	**Bajo (2C)**	**Moderado (3C)**	**Moderado (4C)**	**Alto (5C)**
D. Poco probable/ improbable	**Insignificante (1D)**	**Bajo (2D)**	**Bajo (3D)**	**Moderado (4D)**	**Moderado (5D)**
E. Excepcional	**Insignificante (1E)**	**Insignificante (2E)**	**Bajo (3E)**	**Bajo (4E)**	**Moderado (5E)**

Tabla Adj-5. Tabla de aceptabilidad (tolerabilidad) de riesgos

Índice de riesgo	*Tolerabilidad*	*Medida necesaria (personalización según sea necesario)*
5A, 5B, 4A	Riesgo extremo	Detenga la operación o el proceso de inmediato. Inaceptable según las circunstancias existentes. No permita ninguna operación hasta que se hayan implementado medidas de control adecuadas para reducir el riesgo a un nivel aceptable. Se requiere la aprobación del máximo nivel de la administración.
5C, 4B, 3A	Alto riesgo	Precaución. Asegúrese de que la evaluación de riesgos se ha completado satisfactoriamente y que los controles preventivos declarados están implementados. Aprobación de la evaluación de riesgos por parte de la administración superior antes del inicio de la operación o proceso.
1A, 2A, 2B, 3B, 3C, 4C, 4D, 5D, 5E	Riesgo moderado	Realice o revise la mitigación de riesgos, según sea necesario. Aprobación por departamentos de la evaluación de riesgos.
1B, 1C, 2C, 2D, 3D, 3E, 4E	Bajo riesgo	La mitigación o revisión de riesgos es opcional.
1D, 1E, 2E	Riesgo insignificante	Aceptable tal cual. No se necesita una mitigación de riesgos.

Apéndice 3 del Capítulo 2

ILUSTRACIÓN DE UN PROCEDIMIENTO DE PRIORIZACIÓN DE PELIGROS

<table>
<tr><th></th><th>Opción 1 (básico)</th><th>Opción 2 (avanzado)</th></tr>
<tr><td>Criterios</td><td>Priorización en relación con la categoría de peor consecuencia posible del peligro (gravedad del incidente).</td><td>Priorización en relación con la categoría del índice de riesgo (gravedad y probabilidad) de la peor consecuencia posible del peligro.</td></tr>
<tr><td>Metodología</td><td>a) proyectar la peor consecuencia posible del peligro;

b) proyectar la clasificación de suceso probable de esta consecuencia (es decir, ¿se considerará un accidente, incidente grave o incidente?);

c) concluir que la priorización del peligro es:

<table><tr><th>Consecuencia proyectada</th><th>Nivel de peligro</th></tr><tr><td>Accidente
Incidente grave
Incidente</td><td>Nivel 1
Nivel 2
Nivel 3</td></tr></table></td><td>a) proyectar el número de índice de riesgo (según la matriz de gravedad y probabilidad pertinente) de la peor consecuencia posible del peligro (véase la Figura 2-13 de este capítulo);

b) en relación con la matriz de tolerabilidad relacionada, determine la categoría de tolerabilidad del índice de riesgo (es decir, intolerable, tolerable o aceptable) o terminología/categorización equivalente;

c) concluir que la priorización del peligro es:

<table><tr><th>Índice de riesgo proyectado</th><th>Nivel de peligro</th></tr><tr><td>Intolerable/alto riesgo
Tolerable/riesgo moderado
Aceptable/bajo riesgo</td><td>Nivel 1
Nivel 2

Nivel 3</td></tr></table></td></tr>
<tr><td>Observaciones</td><td>La Opción 1 considera solo la gravedad de la consecuencia proyectada del peligro.</td><td>La Opción 2 considera la gravedad y probabilidad de la consecuencia proyectada del peligro; este es un criterio más completo que la Opción 1.</td></tr>
</table>

Nota.— A partir de un punto de vista práctico, la Opción 1 es más viable que la Opción 2 para fines de un sistema de priorización más simple. El propósito de tal sistema es facilitar la organización y priorización de los peligros para la medida de mitigación de riesgos.

Luego de que cada peligro se haya priorizado, será aparente que se organicen como peligros de Nivel 1, 2 y 3. Entonces, se puede asignar la prioridad o atención de la mitigación de riesgos según su nivel (1, 2 o 3), según corresponda.

Capítulo 3

SARPS DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL DE LA OACI

3.1 INTRODUCCIÓN

3.1.1 Este capítulo proporciona una descripción general de las normas y métodos recomendados (SARPS) en relación con la gestión de la seguridad operacional, inicialmente adoptados en el Anexo 1 — *Licencias al personal*, Anexo 6 — *Operación de aeronaves*, Anexo 8 — *Aeronavegabilidad*, Anexo 11 — *Servicios de tránsito aéreo,* Anexo 13 — *Investigación de accidentes e incidentes de aviación* y Anexo 14 — *Aeródromos*. Este capítulo también incluye información sobre el nuevo Anexo 19 — *Gestión de la seguridad operacional* que trata con las responsabilidades y los procesos de la gestión de la seguridad operacional, y consolida las disposiciones de gestión de la seguridad operacional dominantes.

3.1.2 Los SARPS de gestión de la seguridad operacional de la OACI proporcionan los requisitos de alto nivel que los Estados deben implementar para cumplir con sus responsabilidades de gestión de la seguridad operacional en relación con la operación segura de la aeronave, o en respaldo directo de esta. Estas disposiciones van dirigidas a dos grupos de público: Estados y proveedores de servicios. En el contexto de la gestión de la seguridad operacional, el término "proveedor de servicios" hace referencia a cualquier organización que requiera implementar un sistema de gestión de la seguridad operacional (SMS) de acuerdo con el marco de trabajo de SMS de la OACI. Por lo tanto, los proveedores de servicios en este contexto incluyen:

a) organizaciones de capacitación aprobadas que estén expuestas a riesgos de seguridad operacional durante la entrega de sus servicios;

b) explotadores de aeronaves y helicópteros autorizados para realizar transporte aéreo comercial internacional;

c) organizaciones de mantenimiento aprobadas que ofrezcan servicios para los explotadores de aeroplanos o helicópteros que participan en el transporte aéreo comercial internacional;

d) organizaciones responsables del diseño o fabricación de aeronaves;

e) proveedores de servicios de tránsito aéreo; y

f) explotadores de aeródromos certificados.

3.1.3 Los SARPS de gestión de la seguridad operacional de la OACI también requieren que los Estados establezcan un nivel aceptable de seguridad operacional, como lo definen sus metas de rendimiento en materia de seguridad operacional e indicadores de rendimiento en materia de seguridad operacional. Puede encontrar más detalles sobre estos dos temas en los Capítulos 4 y 5, respectivamente.

3.2 REQUISITOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL ESTATAL

3.2.1 Los requisitos de gestión estatales de la seguridad operacional proporcionan especificaciones de rendimiento, personal y procesos, bajo responsabilidad directa de los Estados, necesarios para la seguridad

operacional del transporte aéreo. Estos requisitos incluyen el establecimiento y mantenimiento de un programa estatal de seguridad operacional (SSP), la recopilación, el análisis y el intercambio de datos de seguridad operacional y la protección de información de seguridad operacional.

3.2.2 Un SSP requiere funciones específicas que efectúan los Estados, como la promulgación de legislaciones, reglamentos, políticas y directrices para respaldar la entrega segura y eficiente de productos y servicios de aviación bajo su autoridad. Para el establecimiento y mantenimiento de SSP, la OACI desarrolló un marco de trabajo que se compone, como mínimo, de los siguientes cuatro componentes que incluyen 11 elementos subyacentes:

a) política y objetivos de seguridad operacional estatal;

b) gestión de riesgos de seguridad operacional estatal;

c) aseguramiento de la seguridad operacional estatal; y

d) promoción de la seguridad operacional estatal.

La Tabla 3-1 proporciona un resumen de las referencias a los requisitos de la gestión de la seguridad operacional estatal y el marco de trabajo de SSP como se adoptó inicialmente en los Anexos del Convenio sobre Aviación Civil Internacional. En el Capítulo 4 podrá encontrar una guía más detallada sobre los requisitos de SSP, el marco de trabajo de SSP y el nivel aceptable de seguridad operacional.

3.3 REQUISITOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL DEL PROVEEDOR DE SERVICIOS

3.3.1 Los SARPS de la OACI también incluyen requisitos para la implementación de un SMS por parte de proveedores de servicios y explotadores de aviación general como un elemento de cada SSP del Estado. El SMS proporciona los medios para identificar los peligros de seguridad operacional, implementar medidas para reducir los riesgos de seguridad operacional, controlar el rendimiento en materia de seguridad operacional y lograr una mejora continua en el rendimiento en materia de seguridad operacional.

3.3.2 Un marco de trabajo del SMS requiere actividades y procesos específicos que deben llevar a cabo los proveedores de servicios de aviación. El marco de trabajo del SMS de la OACI se compone de los siguientes cuatro componentes y de doce elementos subyacentes:

a) política y objetivos de seguridad operacional;

b) gestión de riesgos de seguridad operacional;

c) aseguramiento de la seguridad operacional; y

d) promoción de la seguridad operacional.

3.3.3 Los explotadores de aviación general internacional de aeroplanos grandes o de turborreactor, como se describe en el Anexo 6, Parte II, Sección III, deberán establecer y mantener un SMS que sea adecuado para la envergadura y complejidad de la operación y, como mínimo, debe incluir:

a) un proceso para identificar peligros de seguridad operacional reales y potenciales, y evaluar los riesgos asociados;

Tabla 3-1. Resumen de las referencias a los requisitos de gestión de la seguridad operacional estatal y el marco de trabajo de SSP, como se adoptó inicialmente en el Anexo del Convenio

Fuente		*Tema*
Anexo	*Disposición*	
1 6, Partes I, II y III 8 11 13 14, Volumen I	Definiciones	Programa estatal de seguridad operacional
6, Parte I	3.3.1 y 8.7.3.1	Establecimiento del SSP
6, Parte III	1.3.1	
8	5.1	
11	2.27.1	
13	3.2	
14, Volumen I	1.5.1	
6, Parte I	3.3.2 y 8.7.3.2	Nivel de concepto de rendimiento en materia de seguridad operacional aceptable
6, Parte III	1.3.2	
8	5.2	
11	2.27.2	
14, Volumen I	1.5.2	
13	5.12	Protección de registros de accidentes e incidentes
13	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.9	Recopilación, análisis e intercambio de datos de seguridad operacional
1	Adjunto C	Marco de trabajo del SSP — componentes y elementos
6, Parte I	Adjunto I	
6, Parte III	Adjunto I	
8	Adjunto de la Parte II	
11	Adjunto D	
13	Adjunto F	
14	Adjunto C	
13	Adjunto E	Guía legal para la protección de información reunida a partir de los sistemas de recopilación y procesamiento de datos de seguridad operacional

b) un proceso para desarrollar e implementar la medida correctiva necesaria para mantener un nivel de seguridad operacional aceptable; y

c) disposiciones para el control continuo y evaluación regular de la relevancia y eficacia de las actividades de gestión de la seguridad operacional.

3.3.4 La Tabla 3-2 proporciona un resumen de las referencias a los requisitos de gestión de la seguridad operacional para los proveedores de servicios y los explotadores de aviación general, como el marco de trabajo del SMS, como se adoptó inicialmente en los Anexos del Convenio sobre Aviación Civil Internacional. En el Capítulo 5 podrá encontrar una guía en detalle sobre los requisitos de los proveedores de servicios y el marco de trabajo del SMS.

Tabla 3-2. Resumen de las referencias a los requisitos de gestión de la seguridad operacional para los proveedores de servicios y explotadores de aviación general, incluyendo el marco de trabajo del SMS, como se adoptó inicialmente en los Anexos del Convenio

Fuente		*Tema*
Anexo	*Disposición*	
1 6, Partes I, II y III 8 11 13 14, Volumen I	Definiciones	Sistema de gestión de la seguridad operacional
1	Apéndice 2, 4.1 y 4.2	Requisitos del SMS para organizaciones de capacitación aprobadas
6, Parte I	3.3.3, 3.3.4, 8.7.3.3 y 8.7.3.4	Requisitos del SMS para los explotadores de aeronaves y las organizaciones de mantenimiento
6, Parte II	Sección 3, 3.3.2.1 y 3.3.2.2	Requisitos del SMS para los aeroplanos que participan en la aviación internacional general
6, Parte III	1.3.3 y 1.3.4	Requisitos del SMS para los explotadores de helicópteros
8	5.3 y 5.4	Requisitos del SMS para las organizaciones responsables del tipo de diseño y fabricación de la aeronave (aplicable a partir del 14 de noviembre de 2013)
11	2.27.3 y 2.27.4	Requisitos del SMS para los proveedores de servicios de tránsito aéreo
14, Volumen I	1.5.3 y 1.5.4	Requisitos del SMS para los explotadores de aeródromos certificados
1	Apéndice 4	Marco de trabajo del SMS
6, Parte I	Apéndice 7	
6, Parte III	Apéndice 4	
11	Apéndice 6	
14, Volumen I	Apéndice 7	

3.4 NUEVO ANEXO 19 — *GESTIÓN DE LA SEGURIDAD OPERACIONAL*

3.4.1 Se recomendó la necesidad de desarrollar un solo Anexo dedicado a las responsabilidades y los procesos de la gestión de la seguridad operacional durante la Conferencia de Directores Generales de Aviación Civil sobre una Estrategia global para la seguridad operacional de las aeronaves, realizada entre el 20 y el 22 de marzo de 2006 (DGCA/06) en Montreal y la Conferencia de alto nivel sobre seguridad operacional también realizada en Montreal entre el 29 de marzo y el 1 de abril de 2010 (HLSC/2010).

3.4.2 Como lo dictaminan las Conferencias, la Comisión de Aeronavegación acordó establecer el Grupo de expertos sobre gestión de la seguridad operacional (SMP) para proporcionar recomendaciones para el desarrollo de un nuevo Anexo dedicado a las responsabilidades y los procesos de la gestión de la seguridad operacional.

3.4.3 En febrero de 2012, el SMP recomendó la transferencia de disposiciones de la gestión de la seguridad operacional en los Anexos 1; 6, Partes I, II y III; 8; 11; 13 y 14, Volumen I (véanse las Tablas 3-1 y 3-2) al nuevo Anexo 19. La mayoría de estos requisitos se modificaron para obtener congruencia y claridad, y al mismo tiempo mantener los requisitos originales para los que se adoptaron.

3.4.4 Las disposiciones del Anexo 19, como las propone el SMP, tienen como fin armonizar la implementación de las prácticas de gestión de la seguridad operacional para los Estados y las organizaciones implicadas en las actividades de aviación. Por consiguiente, el Anexo 19 incluye requisitos de gestión de la seguridad operacional para los Estados, los proveedores de productos y servicios, así como también, los explotadores de aeroplanos involucrados en las operaciones de aviación general internacional. Los requisitos de gestión de la seguridad operacional específicos de la industria seleccionados permanecen en el Anexo correspondiente al campo o actividad de cada proveedor de servicios específico (por ejemplo, los requisitos de los programas de análisis de datos de vuelo para los explotadores aéreos se conservan en el Anexo 6, Parte I).

3.4.5 Luego de adoptarse, el Anexo 19 tendrá un impacto en varios Anexos del Convenio sobre Aviación Civil Internacional de la OACI. Por tanto, las enmiendas posteriores a los Anexos 1, 6, 8, 11, 13 y 14 que se desprendan de la adopción del Anexo 19 se introducirán de forma simultánea para evitar requisitos duplicados.

3.4.6 La fecha de aplicabilidad del Anexo 19 es independiente de las fechas de aplicabilidad de las disposiciones de gestión de la seguridad operacional existentes. Por lo tanto, la fecha de aplicabilidad del Anexo 19 no afecta la aplicabilidad existente de los SARPS de la gestión de la seguridad operacional en los otros Anexos.

Capítulo 4

PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

4.1 INTRODUCCIÓN

4.1.1 Este capítulo presenta los objetivos, el marco de trabajo y el enfoque de implementación de un programa estatal de seguridad operacional (SSP). También analiza la importancia de establecer los procesos para mantener y evaluar la eficacia del SSP en sí.

4.1.2 Un SSP es un sistema de gestión para la regulación y administración de seguridad operacional por parte de un Estado. La implementación de un SSP es proporcional a la envergadura y complejidad del sistema de aviación civil del Estado y requiere coordinación entre múltiples autoridades responsables de las funciones de aviación del Estado. Los objetivos del SSP son:

a) garantizar que un Estado tenga implementado el marco de trabajo reglamentario mínimo necesario;

b) garantizar la armonización entre las organizaciones reglamentarias y administrativas del Estado en cuanto a sus papeles en la gestión de riesgos de seguridad operacional respectivos;

c) facilitar el control y la medición del rendimiento colectivo en materia de seguridad operacional colectivo de la industria de aviación del Estado;

d) coordinar y mejorar continuamente las funciones de gestión de la seguridad operacional del Estado; y

e) respaldar la implementación e interacción eficaces con el SMS del proveedor de servicios.

4.1.3 Los principios de la gestión de seguridad operacional proporcionan una plataforma para el desarrollo paralelo del SSP por parte del Estado y del SMS por parte de los proveedores de servicios. Al desarrollar el marco de trabajo legislativo de la seguridad operacional estatal, el Estado promulga los requisitos de SMS que requieren de proveedores de servicios para implementar sus capacidades de gestión de seguridad operacional, lo que permite una identificación eficaz de las deficiencias de seguridad operacional sistemáticas y la resolución de preocupaciones de seguridad operacional.

4.1.4 El SMS del proveedor de servicios requiere una vigilancia reglamentaria eficaz. Además, el SMS es un sistema principalmente basado en rendimiento que requiere el intercambio adecuado de información de seguridad operacional con accionistas internos y externos. El Estado, mediante sus funciones de SSP, proporciona las funciones de vigilancia y facilita la implementación de la adición de datos adecuados e iniciativas de distribución de información.

4.2 MARCO DE TRABAJO DEL SSP

4.2.1 Existen cuatro componentes que conforman los fundamentos de un SSP. Cada componente se subdivide en elementos que conforman los procesos o las actividades que realiza el Estado para gestionar la seguridad operacional. Estos 11 elementos combinan enfoques prescriptivos y basados en rendimiento, y respaldan la

implementación del SMS por parte de proveedores de servicios. Los cuatro componentes y los once elementos de un marco de trabajo de SSP son:

1. Política y objetivos estatales de la seguridad operacional

   1.1 Marco de trabajo legislativo de seguridad operacional estatal
   1.2 Responsabilidades de seguridad operacional estatal
   1.3 Investigación de accidentes e incidentes
   1.4 Política de cumplimiento

2. Gestión de riesgos de seguridad operacional estatal

   2.1 Requisitos de seguridad operacional para el SMS del proveedor de servicios
   2.2 Acuerdo sobre el rendimiento en materia de seguridad operacional del proveedor de servicios

3. Aseguramiento de la seguridad operacional estatal

   3.1 Vigilancia de la seguridad operacional
   3.2 Recopilación, análisis e intercambio de datos de seguridad operacional
   3.3 Enfoque basado en datos de seguridad operacional de la vigilancia de áreas de mayor preocupación o necesidad

4. Promoción de la seguridad operacional estatal

   4.1 Capacitación interna, comunicación y distribución de información de seguridad operacional
   4.2 Capacitación externa, comunicación y distribución de información de seguridad operacional.

4.2.2 Sigue una breve explicación de los componentes y elementos de un marco de trabajo de SSP.

Componente 1 del SSP. Política y objetivos estatales de la seguridad operacional

4.2.3 El componente de la política y los objetivos de seguridad operacional estatal define cómo el Estado gestionará la seguridad operacional en todo su sistema de aviación. Esto incluye la determinación de responsabilidades de las diferentes organizaciones del Estado, en relación con el SSP, así como también, los amplios objetivos de seguridad operacional que debe lograr el SSP.

4.2.4 La política y los objetivos de seguridad operacional estatal proporcionan a la administración y al personal las políticas, las instrucciones, los procedimientos, los controles de gestión, la documentación y los procesos de medidas correctivas explícitos que mantienen los esfuerzos de gestión de la seguridad operacional de la autoridad de aviación civil del Estado y otras organizaciones del Estado en el camino. Esto permite que el Estado ofrezca liderazgo de seguridad operacional en un sistema de transporte aéreo cada vez más complejo y siempre variable. En el Apéndice 1 de este capítulo se incluye una guía sobre el desarrollo de una declaración de política de seguridad operacional estatal.

Elemento 1.1 del SSP Marco de trabajo legislativo de la seguridad operacional estatal

El Estado ha promulgado un marco de trabajo legislativo de seguridad operacional nacional y reglamentos específicos, en cumplimiento de normas nacionales e internacionales, que definen cómo el Estado debe realizar la gestión de la seguridad operacional en el Estado. Esto incluye la participación de las organizaciones de aviación del Estado en actividades específicas relacionadas con la gestión de la seguridad operacional en el Estado y el establecimiento de los papeles, las responsabilidades y las relaciones de tales organizaciones. El marco de trabajo legislativo de seguridad operacional y los reglamentos específicos se revisan periódicamente para garantizar que sigan siendo relevantes y adecuados para el Estado.

4.2.5 Se debe establecer o enmendar un marco de trabajo legislativo de seguridad operacional nacional, según sea necesario. Tal marco de trabajo abarca todos los sectores de aviación y las funciones administrativas correspondientes al Estado y está de acuerdo con normas internacionales. Tal legislación define claramente los roles y las responsabilidades de cada organización del Estado que tenga una función reglamentaria o administrativa de aviación. Es posible que algunos marcos de trabajo legislativos consten de legislaciones separadas para distintos ministerios que pueden haberse desarrollado de forma independiente del resto. Por ejemplo, el marco de trabajo legislativo relacionado con la responsabilidad del Estado para la administración y operación directas de los aeródromos y servicios ATS puede haberse desarrollado de forma separada con el paso del tiempo. Tal legislación puede concentrarse en estos dos sectores con un posterior énfasis en los aspectos operacionales y técnicos del suministro de estos servicios. Un marco de trabajo operacionalmente parcial podría no abordar correctamente la coordinación de las actividades de gestión de la seguridad operacional en todas las organizaciones pertinentes del Estado.

4.2.6 Un mecanismo para la revisión periódica del marco de trabajo legislativo de aviación integral del Estado garantizará la mejora continua y correlación entre su legislación y los requisitos reglamentarios operacionales. Aunque la revisión de los requisitos operativos específicos esté dentro del ámbito de las organizaciones reglamentarias respectivas, puede que sea necesario abordar la integración y cohesión necesaria de la legislación de mayor nivel mediante una plataforma de coordinación a nivel nacional, particularmente donde múltiples organizaciones y ministerios estén involucrados.

Elemento 1.2 del SSP Responsabilidades de la seguridad operacional estatal

El Estado ha identificado, definido y documentado los requisitos y las responsabilidades acerca del establecimiento y mantenimiento del SSP. Esto incluye las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar continuamente el SSP, de forma que se cumplan los objetivos de seguridad operacional estatal. También incluye una clara declaración acerca de la disposición de los recursos necesarios para la implementación del SSP.

4.2.7 La responsabilidad de implementación inicial del SSP del Estado es identificar al ejecutivo responsable del SSP y a la organización del Estado que administrará y coordinará la implementación y operación del SSP. En este documento, esta entidad también se conoce como una organización apoderada del SSP.

4.2.8 Para los Estados donde múltiples organizaciones reglamentarias y administrativas estén involucradas, puede que también sea necesario identificar un comité nacional adecuado, con representación de estas organizaciones, para actuar como la plataforma de coordinación del SSP continua del Estado.

4.2.9 El ejecutivo responsable del SSP asignado y la organización apoderada iniciarán el proceso de implementación del SSP al asignar un equipo de implementación del SSP. Este equipo de implementación será responsable de trabajar con el ejecutivo responsable y las diversas organizaciones para iniciar la planificación del SSP y los procesos de implementación.

4.2.10 La implementación y la operación continua subsiguiente del SSP deberá definirse y documentarse. Este sistema de documentación del SSP debe incluir un documento del SSP de alto nivel que defina/describa al SSP, junto con otros registros, formatos y SOP asociados con la implementación y operación del SSP.

4.2.11 Junto a la definición de las responsabilidades de la gestión de seguridad operacional se encuentra el desarrollo coordinado de una política (declaración) de seguridad operacional estatal que corresponda a todo el marco de trabajo reglamentario y administrativo del Estado. De igual forma, los amplios objetivos de la seguridad operacional estatal son parte de las declaraciones generales de la misión de todas las organizaciones pertinentes del Estado. Los objetivos de seguridad operacional de alto nivel pueden respaldarse con indicadores de seguridad operacional relevantes para facilitar la evaluación o medición, según corresponda.

Elemento 1.3 del SSP Investigación de accidentes e incidentes

El Estado ha establecido un proceso de investigación de accidentes e incidentes independiente, cuyo único objetivo es prevenir accidentes e incidentes y no buscar culpables ni responsables. Tales investigaciones respaldan la gestión de la seguridad operacional en el Estado. En la operación del SSP, el Estado mantiene la independencia de la organización de investigación de accidentes e incidentes de otras organizaciones de aviación del Estado.

4.2.12 A partir de una perspectiva de SSP, la función de investigación de accidentes e incidentes se centra en su administración a un nivel de Estado. Una organización o entidad de investigación debe ser funcionalmente independiente de cualquier otra organización, en particular de la autoridad de aviación civil del Estado, cuyos intereses pueden entrar en conflicto con las tareas encomendadas a la autoridad de investigación. El motivo fundamental de la independencia de esta función de aquellas de otras organizaciones, es que la causalidad de los accidentes puede vincularse a factores reglamentarios o relacionados con el SSP. Además, tal independencia mejora la viabilidad de la organización de investigación de accidentes e incidentes, y evita conflictos de intereses reales o percibidos.

4.2.13 Puede que algunos Estados no tengan los recursos necesarios para descargar las responsabilidades de su investigación. Para tales Estados, unirse a una Organización regional de investigación de accidentes e incidentes (RAIO) podría ser una solución viable para alcanzar el intento de un proceso de investigación independiente. Para este fin, se debe prestar atención al *Manual sobre organizaciones regionales de investigación de accidentes e incidentes* (Doc 9946) de la OACI.

Elemento 1.4 del SSP Política de cumplimiento

El Estado ha promulgado una política de cumplimiento que establece las condiciones y circunstancias en las cuales los proveedores de servicios tienen permitido abordar y resolver eventos que impliquen ciertas desviaciones de seguridad operacional, de forma interna, dentro del contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios y a la satisfacción de la autoridad estatal correspondiente. La política de cumplimiento también establece las condiciones y las circunstancias en las cuales se pueden abordar las desviaciones de seguridad operacional mediante procedimientos de cumplimiento establecidos.

4.2.14 Al igual que con otras legislaciones nacionales, se puede esperar que el marco de trabajo legislativo de la aviación incluya una disposición básica para la medida de cumplimiento. Una disposición de cumplimiento legislativo básica probablemente estaría limitada a abordar solo el alcance de las penalidades de infracciones. En un entorno de SSP-SMS, se prevé que las políticas y los procedimientos de cumplimiento, ya sea a nivel del proveedor de servicios individual o de Estado (CAA), deben mejorarse para incorporar disposiciones que moderen la naturaleza y el alcance de las medidas de cumplimiento y disciplinarias, de acuerdo con las condiciones y las circunstancias reales que rodean una infracción o un acto de incumplimiento. La intención de tal mejora es garantizar que se haga una distinción necesaria entre una infracción deliberada/flagrante y un error/equivocación accidental.

4.2.15 Para que dicha mejora se implemente, el Estado necesitará manifestar dicha intención mediante su política y procedimientos de cumplimiento. Al mismo tiempo, el Estado puede necesitar formalizar la necesidad de que sus proveedores de servicios tengan procedimientos disciplinarios internos que incorporen una mejora equivalente. Esto implicaría que se espera que los proveedores de servicios tengan un proceso aceptable implementado para gestionar sus propias desviaciones de seguridad operacional/calidad de rutina mediante políticas y procedimientos disciplinarios internos. El Estado podría indicar que se espera una intervención reglamentaria en ciertas condiciones y circunstancias, mediante las cuales el Estado (CAA) se hará cargo del proceso de investigación con relación a una infracción o un incumplimiento en particular.

Componente 2 del SSP. Gestión de riesgos de la seguridad operacional estatal

4.2.16 El componente de gestión de riesgos de seguridad operacional estatal incluye el establecimiento de requisitos del SMS para garantizar que cada proveedor de servicios del Estado implemente los procesos de identificación de peligros y los controles de gestión de riesgos necesarios. Parte de este requisito incluye un mecanismo para acordar niveles de rendimiento en materia de seguridad operacional aceptables con proveedores de servicios individuales, que deberán alcanzarse mediante su SMS.

4.2.17 Aparte de garantizar que los proveedores de servicios participen en la identificación de peligros y gestión de riesgos eficaz mediante los requisitos de SMS, el Estado también podrá aplicar los principios de gestión de riesgos de seguridad operacional en sus propias actividades reglamentarias y del SSP. La reglamentación, la selección de los indicadores de seguridad operacional del SSP y su configuración de objetivos y alertas asociada, y la priorización del programa de vigilancia, entre otros, son procesos que pueden mejorar mediante un enfoque basado en datos y riesgos.

4.2.18 Los riesgos sustanciales, que se manifiestan mediante el análisis de datos de seguridad operacional generados internamente e indicadores de rendimiento en materia de seguridad operacional relacionados de un proveedor de servicios individual, pueden requerir la coordinación o el acuerdo con la autoridad reglamentaria de aviación del Estado sobre la medida de mitigación adecuada, en particular donde tales riesgos probablemente tengan un impacto en otros proveedores de servicios o accionistas.

Elemento 2.1 del SSP Requisitos de seguridad operacional para el SMS del proveedor de servicios

El Estado ha establecido los controles que rigen cómo los proveedores de servicio identificarán los peligros y gestionarán los riesgos de seguridad operacional. Estos incluyen los requisitos, los reglamentos de operación específicos y las políticas de implementación para el SMS del proveedor de servicios. Los requisitos, los reglamentos de operación específicos y las políticas de implementación se revisan periódicamente para garantizar que sigan siendo relevantes y adecuadas para los proveedores de servicios.

4.2.19 El Estado establece los requisitos de seguridad operacional para el SMS de un proveedor de servicios mediante la promulgación de los reglamentos que definen los componentes y elementos necesarios del marco de trabajo del SMS. Dentro del marco de trabajo del SMS, la implementación eficaz del componente de gestión de riesgos de seguridad operacional (SRM) garantizará que los proveedores de servicios identifiquen peligros y gestionen los riesgos relacionados. Los detalles de los procedimientos del proveedor de servicios individual para la identificación de peligros y la gestión de riesgos serán proporcionales a la complejidad de cada organización y se reflejarán de acuerdo con la documentación de su SMS. Para las organizaciones no reguladas, como subcontratistas, puede que sea necesario que una organización aprobada por el SMS requiera (mediante contrato), de dichos subcontratistas, procesos de identificación de peligros y gestión de riesgos, donde corresponda. Donde el subcontratista tenga un SMS aceptado, se debe abordar el tema de la integración necesaria.

4.2.20 Los requisitos reglamentarios del SMS del Estado y el material guía del SMS se deberán revisar periódicamente, considerando la retroalimentación de la industria y el estado y aplicabilidad actuales de los SARPS de SMS de la OACI y el materia guía.

Elemento 2.2 del SSP Acuerdo sobre el rendimiento en materia de seguridad operacional del proveedor de servicios

El Estado ha acordado con proveedores de servicio individuales sobre el rendimiento en materia de seguridad operacional de su SMS. El rendimiento en materia de seguridad operacional acordado del SMS de un proveedor de servicios individual se revisa periódicamente para garantizar que siga siendo pertinente y adecuado para los proveedores de servicios.

4.2.21 Como parte del proceso de aceptación del SMS, la organización reglamentaria del Estado revisa y acuerda los indicadores de rendimiento en materia de seguridad operacional (SPI) del proveedor de servicios y sus objetivos y alertas asociados. También es posible que un Estado acepte el plan de implementación de un SMS, lo que permite aceptar los SPI de un proveedor de servicios en una etapa posterior al proceso de implementación del SMS. En cualquier caso, la aceptación completa de un SMS requiere que el regulador esté satisfecho con que los SPI propuestos sean adecuados y pertinentes para las actividades de aviación del proveedor de servicios individual.

4.2.22 Es posible que este proceso de acuerdo del rendimiento en materia de seguridad operacional incluya posteriormente que el proveedor de servicios realice evaluaciones de seguridad operacional específicas o que implemente medidas de mitigación de riesgos. También puede ser el resultado de riesgos específicos que se manifiestan mediante fuentes como el proveedor de servicios, la industria, el Estado o los datos de seguridad operacional global.

4.2.23 Debe haber una revisión periódica de cada SPI del proveedor de servicios y la configuración de objetivos y alertas asociada. Dicha revisión debe considerar el rendimiento y la eficacia de cada SPI y su configuración de objetivos y alertas asociada. Cualquier ajuste necesario a los SPI y la configuración de objetivos y alertas acordados con anterioridad debe confirmarse mediante datos de seguridad operacional y debe documentarse según corresponda.

Componente 3 del SSP. Aseguramiento de la seguridad operacional estatal

4.2.24 El aseguramiento de la seguridad operacional estatal se logra mediante actividades de vigilancia de los proveedores de servicios, así como también, la revisión interna de los procesos reglamentarios y administrativos del Estado. También se aborda el importante papel de los datos de seguridad operacional y la recopilación, el análisis y la distribución de tales datos. Los programas de vigilancia del Estado deben basarse en datos, para que sus recursos puedan centrarse y priorizarse de acuerdo a las áreas de más alto riesgo o con preocupaciones de seguridad operacional.

Elemento 3.1 del SSP Vigilancia de la seguridad operacional

El Estado ha establecido mecanismos para garantizar el control eficaz de ocho elementos críticos de la función de vigilancia de la seguridad operacional. El Estado también ha establecido los mecanismos para garantizar que la identificación de peligros y la gestión de riesgos de seguridad operacional, realizada por proveedores de servicios, sigan controles reglamentarios establecidos (requisitos, reglamentos de operación específicos y políticas de implementación). Estos mecanismos incluyen inspecciones, auditorías y encuestas para garantizar que los controles de riesgos de seguridad operacional reglamentarios se integran correctamente en los SMS del proveedor de servicios, se practican como fueron diseñados y que los controles reglamentarios tienen el efecto previsto en los riesgos de seguridad operacional.

4.2.25 La implementación de los SARPS de la OACI forman la base de la estrategia de seguridad operacional de la aviación del Estado. El Elemento 3.1 del SSP hace referencia a los métodos que usa el Estado para controlar el establecimiento y la implementación de su sistema de vigilancia de la seguridad operacional. Los detalles de los elementos esenciales de un sistema de vigilancia de la seguridad operacional estatal se abordan en Doc 9734, Parte A.

4.2.26 El sistema de vigilancia de la seguridad operacional estatal incluye obligaciones relacionadas con la aprobación inicial y la vigilancia continuada de sus proveedores de servicios de aviación, a fin de garantizar el cumplimiento de reglamentos nacionales establecidos según los SARPS de la OACI.

Nota.— El proceso de aprobación inicial incluye la autorización, certificación o designación de proveedores de servicio por parte del Estado, según corresponda.

4.2.27 La aprobación, autorización, certificación o designación inicial de un proveedor de servicios por parte del Estado incluye la aceptación del plan de implementación del SMS de la organización. Ciertos elementos del plan de implementación del SMS del proveedor de servicios se implementarán al momento de la aprobación inicial de la organización, mientras que otros elementos se implementarán después del enfoque en etapas descrito en el Capítulo 5.

4.2.28 Las obligaciones de vigilancia del Estado se aplican mediante auditorías e inspecciones para garantizar que los proveedores de servicios mantienen un nivel suficiente de cumplimiento reglamentario y que las actividades relacionadas con la aviación respectivas se llevan a cabo de forma segura. Las obligaciones de vigilancia del Estado también incluyen la aceptación de un SMS implementado por cada uno de sus proveedores de servicios existentes, así como también, la evaluación periódica del rendimiento del SMS.

4.2.29 Las actividades de control y revisión del Estado, además de cualquier medida recomendada relacionada, se coordinan para la evaluación o resolución en la plataforma de coordinación del SSP nacional, donde sea necesario.

Elemento 3.2 del SSP Recopilación, análisis e intercambio de datos de seguridad operacional

El Estado ha establecido mecanismos para garantizar la recopilación y el almacenamiento de datos sobre peligros y riesgos de seguridad operacional a nivel individual y colectivo del Estado. El Estado también ha establecido mecanismos para desarrollar información a partir de datos almacenados y para intercambiar activamente la información de seguridad operacional con proveedores de servicios u otros Estados, según corresponda.

4.2.30 El Estado ha establecido un sistema de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) para garantizar la recopilación, el almacenamiento y la adición de datos sobre accidentes, incidentes y peligros obtenidos mediante los informes obligatorios y voluntarios del Estado. Este sistema debe respaldarse con los requisitos del Estado para que los proveedores de servicios notifiquen accidentes, incidentes graves y cualquier otro incidente que el Estado considere que puede notificarse. Se debe hacer una distinción adecuada entre informes de accidente e incidentes e informes de peligros. De igual forma, existe una distinción entre los sistemas de notificación obligatoria (reglamentaria) y los sistema de notificación voluntaria, como los requisitos de confidencialidad adecuados para los sistemas voluntarios. Véase el Apéndice 2 para ver una guía sobre el sistema de notificación voluntaria de un Estado y el Apéndice 3 para ver un ejemplo del procedimiento de notificación obligatoria de un Estado.

4.2.31 La recopilación de datos sobre accidentes e incidentes que pueden notificarse debe incluir informes de investigación pertinentes. Los informes voluntarios recibidos pueden requerir cierta forma de investigación o evaluación de seguimiento para verificar su validez. Los informes de peligros validados pueden necesitar un proceso de evaluación y mitigación de riesgos de seguimiento a nivel de proveedor de servicios o CAA, según corresponda. Los diversos tipos de datos de seguridad operacional pueden consolidarse dentro de un SDCPS centralizado o recopilarse y archivarse dentro de módulos integrados de una red de SDCPS distribuida, según corresponda.

4.2.32 El Estado también ha establecido procedimientos para desarrollar y procesar información de datos almacenados colectivos y para compartir activamente la información de seguridad operacional con los proveedores de servicios y otros Estados, según corresponda. La disponibilidad de estas fuentes de datos de seguridad operacional para el Estado permite el desarrollo de los indicadores de seguridad operacional del SSP, como tasas de accidentes e incidentes. Los indicadores de seguridad operacional establecidos, junto con su configuración respectiva de objetivos y alertas respectiva, servirán como el mecanismo de medición y control de la seguridad operacional del Estado (ALoSP). En 4.3.5.1 a 4.3.5.12 y Apéndice 4 de este capítulo se encuentran más detalles sobre el desarrollo de los indicadores de seguridad operacional.

4.2.33 Para garantizar la disponibilidad continuada de datos de seguridad operacional, particularmente desde sistemas de notificación voluntaria, el SDCPS debe proporcionar la protección correspondiente a la información de seguridad operacional. Véase el Apéndice 5 para encontrar una guía sobre la protección de la información de seguridad operacional.

4.2.34 Para los Estados con varias autoridades responsables de la regulación de la seguridad operacional, se debe establecer una coordinación, integración y accesibilidad adecuadas de sus bases de datos de seguridad operacional relacionadas con el SSP. Esto también es relevante para los Estados donde una organización independiente de CAA lleva a cabo el proceso de investigación de accidentes. Puede que también se deba tener una consideración parecida para aquellos Estados donde un RSOO o un RAIO descarga ciertas funciones de gestión de la seguridad operacional (como procesamiento de datos relacionados con SSP) en nombre del Estado.

4.2.35 El SDCPS del Estado debe incluir procedimientos para el envío de informes de accidentes e incidentes a la OACI, lo que facilitará la recopilación y distribución de información de seguridad operacional global. En el Apéndice 6 de este capítulo se incluye una guía sobre la notificación e información de accidentes e incidentes, según los requisitos del Anexo 13 de la OACI.

Elemento 3.3 del SSP Enfoque basado en datos de seguridad operacional de la vigilancia de áreas de mayor preocupación o necesidad

El Estado ha establecido los procedimientos para priorizar las inspecciones, las auditorías y las encuestas hacia aquellas áreas de mayor preocupación o necesidad, como se identifica con el análisis de datos de peligros, sus consecuencias en las operaciones y los riesgos de seguridad operacional evaluados.

4.2.36 Los programas de vigilancia o inspección convencionales tienden a aplicarse constante e invariablemente en cada proveedor de servicios, sin mecanismos de personalización de frecuencia o alcance de las actividades de vigilancia. Un entorno de gestión de la seguridad operacional proporciona una evaluación más dinámica del rendimiento en materia de seguridad operacional. Según el SSP, los programas de vigilancia reglamentarios deben, por tanto, incluir un mecanismo para calibrar el alcance o la frecuencia de la vigilancia, de acuerdo con el rendimiento en materia de seguridad operacional real. Tal enfoque basado en riesgos para la priorización de vigilancia facilitará la asignación de recursos de acuerdo con las áreas de mayor riesgo, preocupación o necesidad. Los datos que se usarán para tal calibración de vigilancia pueden incluir los indicadores de rendimiento en materia de seguridad operacional relacionados con sectores específicos de la actividad de la aviación, al igual que informes o auditorías de vigilancia anteriores de proveedores de servicios individuales. Para tal fin, pueden necesitarse criterios para cuantificar el resultado (por ejemplo, el porcentaje del cumplimiento eficaz) de cada auditoría completa.

4.2.37 Un concepto de vigilancia basado en riesgos más integral puede implicar la entrada de datos de riesgos de seguridad operacional externos al programa de vigilancia. Tal entrada modificadora adicional de la frecuencia/ alcance de la vigilancia puede provenir de (por ejemplo) un programa de evaluación de ORP. (Véase el Capítulo 2, Apéndice 1, para obtener información sobre el concepto de evaluación del ORP). Las entradas/preocupaciones adicionales también pueden provenir de los indicadores de seguridad operacional o del SDCPS del Estado. Se debe realizar una interacción adecuada con los proveedores de servicios antes de implementar cualquier modificación de la vigilancia. En la Figura 4-1 se muestra la ilustración de un concepto de datos de seguridad operacional mejorada y de vigilancia basada en riesgos.

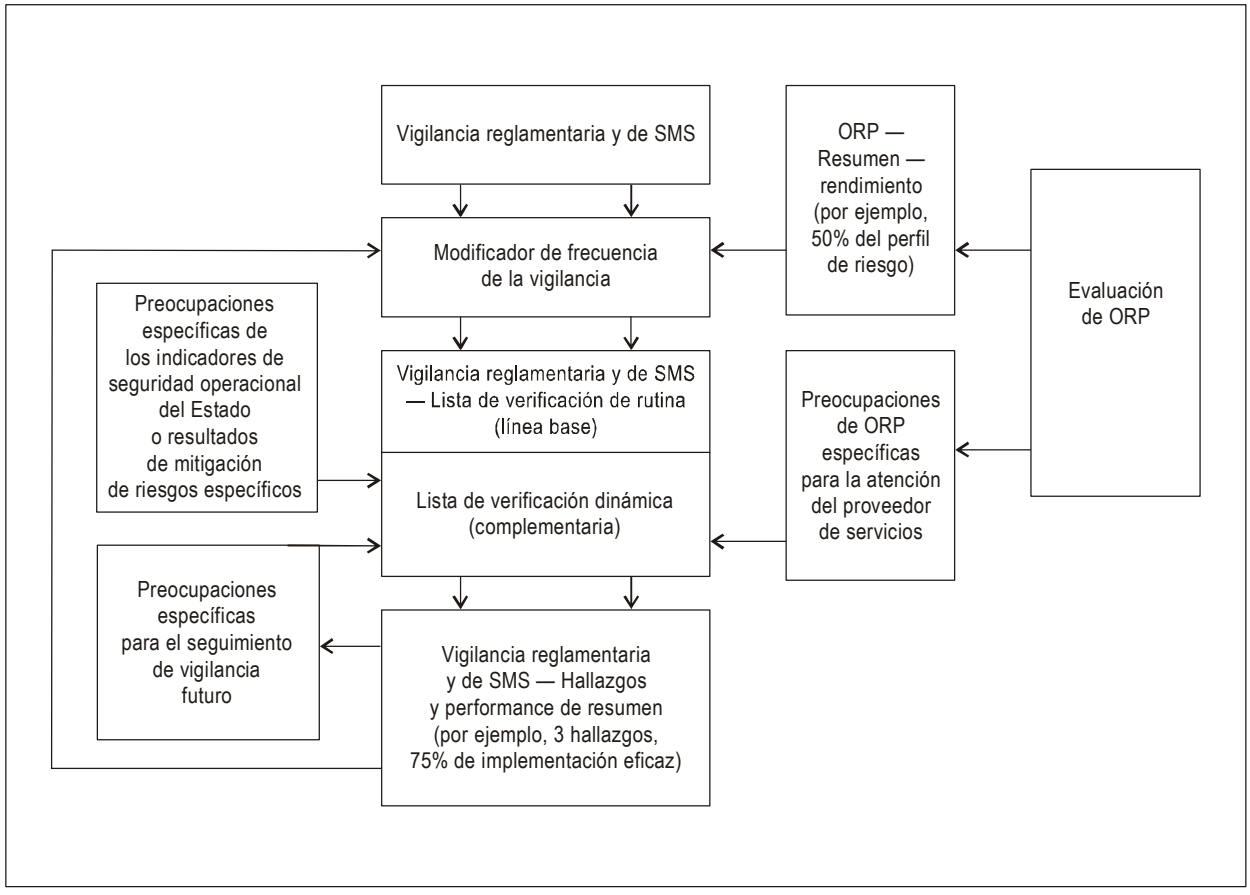


Figura 4-1. Concepto de datos de seguridad operacional y vigilancia basada en riesgos

Componente 4 del SSP. Promoción de la seguridad operacional estatal

4.2.38 La promoción de la seguridad operacional estatal implica el establecimiento de procesos internos y externos por parte del Estado para proporcionar o facilitar la capacitación en seguridad operacional, la comunicación y la distribución de información de la seguridad operacional.

Elemento 4.1 del SSP Capacitación interna, comunicación y distribución de información de la seguridad operacional

El Estado proporciona la capacitación e impulsa la toma de conciencia, además de la comunicación bidireccional de la información pertinente de la seguridad operacional para respaldar, dentro de las organizaciones de aviación del Estado, el desarrollo de una cultura institucional que impulse un SSP eficaz y eficiente.

4.2.39 Las organizaciones reglamentarias estatales responsables de los diferentes sectores de aviación, así como también, otras entidades administrativas independientes, como la organización de investigación de accidentes, deben tener un enfoque integrado con sus papeles respectivos. Por lo tanto, es importante garantizar que exista un canal de comunicación de seguridad operacional dedicado entre ellos y, en particular, con la organización apoderada del SSP. El documento del SSP y sus políticas de cumplimiento y seguridad operacional del Estado son fundamentales para lograr la integración de la capacitación, comunicación y distribución de la información asociada. El resto de las estrategias operacionales del SSP, incluidos los requisitos armonizados del SMS y la vigilancia de los proveedores de servicios respectivos, deben compartirse, comunicarse y coordinarse entre las organizaciones. Esto evitará la creación de requisitos de SMS en conflicto o criterios de vigilancia/aceptación para diferentes sectores de la aviación.

4.2.40 El programa de capacitación de la seguridad operacional interna para el personal que participa en las tareas relacionadas con el SSP debe coordinarse entre las diversas organizaciones del Estado, según corresponda. Se debe dar prioridad al personal que forma parte de la implementación o vigilancia de estos programas para recibir la capacitación de SSP y SMS, en particular, a los inspectores operacionales o de campo quienes participarán en la determinación de los criterios de aceptación del SMS y en otros asuntos de rendimiento en materia de seguridad operacional. El alcance del material de capacitación/familiarización del SSP y SMS evolucionará para reflejar los procesos reales del SSP del Estado a medida que se implementan por completo. La capacitación inicial de SSP y SMS puede limitarse a los elementos del marco de trabajo genéricos de SSP/SMS y al material guía, como el que se incluye en los cursos de capacitación de SSP/SMS de la OACI.

Elemento 4.2 del SSP Capacitación externa, comunicación y distribución de información de la seguridad operacional

El Estado proporciona educación y promueve la toma de conciencia de los riesgos de seguridad operacional y la comunicación bidireccional de la información relevante de seguridad operacional para respaldar, entre los proveedores de servicios, el desarrollo de una cultura institucional que fomente un SMS eficaz y eficiente.

4.2.41 El Estado debe tener una plataforma o medio de comunicación adecuados para facilitar la implementación del SMS. Este puede ser un medio integrado para los proveedores de servicios de todos los sectores de aviación o un canal dedicado de la organización reglamentaria pertinente para los proveedores de servicios específicamente bajo su jurisdicción. El contenido básico para dicho SMS externo y la comunicación relacionada con la seguridad operacional le concierne a los requisitos del SMS y el material guía. El documento del SSP del Estado y su política de seguridad operacional estatal y la política de cumplimiento deben estar disponibles para los proveedores de servicios, según

corresponda. Dichos canales de comunicación externa también pueden mejorarse para incluir otros asuntos relacionados con la seguridad operacional, según corresponda. De preferencia, debe haber una comunicación bidireccional para permitir la retroalimentación de la industria.

4.2.42 El Estado también debe facilitar la educación o capacitación de SMS de sus proveedores de servicios donde sea posible y adecuado.

4.3 PLANIFICACIÓN DE LA IMPLEMENTACIÓN DEL SSP

4.3.1 Generalidades

El SSP de un Estado debe ser proporcional a la envergadura y complejidad de su sistema de aviación, el que puede necesitar la coordinación entre múltiples organizaciones reglamentarias de aviación responsables de los sectores respectivos. La implementación de un SSP no altera los papeles respectivos de las organizaciones de aviación del Estado o su interacción normal con otros. Por el contrario, mejora las funciones y capacidades reglamentarias/administrativas colectivas en nombre del Estado. La mayoría de los Estados ya tiene procesos existentes que cumplen las expectativas de algunos elementos del SSP. La tarea es consolidar y mejorar estos procesos existentes con elementos de rendimiento y basados en riesgos adicionales para formar un marco de trabajo de gestión de la seguridad operacional integrada. Este marco de trabajo del SSP también facilitará la implementación y vigilancia eficaz del SMS por parte de la industria. Esta sección destaca algunas consideraciones importantes para la implementación del SSP.

4.3.2 Descripción del sistema reglamentario

Una revisión del sistema reglamentario es parte del proceso de planificación de la implementación del SSP. Dicha revisión debe incluir una descripción de lo siguiente:

a) la estructura del marco de trabajo reglamentario de aviación existente, a partir del nivel ministerial hasta diversas organizaciones reglamentarias o administrativas;

b) los papeles y responsabilidades de la gestión de seguridad operacional de las diversas organizaciones reglamentarias;

c) la plataforma o mecanismo para la coordinación del SSP entre las organizaciones; y

d) un mecanismo de revisión interno de seguridad operacional/calidad a nivel del Estado y dentro de cada organización.

Se debe incluir la estructura/diagrama de la organización reglamentaria y administrativa del Estado en el documento del SSP.

4.3.3 Análisis de brechas

Antes de desarrollar un plan de implementación del SSP, se necesita un análisis de brechas de las estructuras y los procesos del Estado existentes en comparación con el marco de trabajo del SSP de la OACI para evaluar la existencia y madurez de los elementos del SSP respectivos. Los elementos o procesos identificados como que requieren de

medidas, como resultado del análisis de brechas, formarán la base del plan de implementación del SSP. En el Apéndice 7 de este capítulo podrá encontrar una guía detallada sobre el proceso de análisis de brechas del SSP.

4.3.4 Plan de implementación del SSP

Al igual que con cualquier ejercicio de implementación de un proyecto importante, la implementación del SSP implica muchas tareas y subtareas que deben completarse dentro de un período determinado. La cantidad de tareas, así como también, el alcance de cada una de ellas, depende de la madurez actual del sistema de vigilancia de la seguridad operacional del Estado. El objetivo del proceso de implementación es lograr la mejora progresiva de los procesos de gestión, administración y vigilancia de la seguridad operacional existente de un Estado. Las tareas y subtareas correspondientes se priorizan y documentan en un formato adecuado para la implementación progresiva. Un plan de implementación del SSP, junto con el desarrollo de un documento (exposición) de alto nivel del SSP, proporciona la base para que un Estado alcance la mejora progresiva de los procesos de gestión de seguridad operacional, administración y vigilancia. Estos dos documentos clave deben estar disponibles fácilmente para todo el personal pertinente dentro de la organización, con el fin de facilitar la toma de conciencia del SSP y el progreso relacionado con su implementación. En la Sección 4.4 y en el Apéndice 7 de este capítulo podrá encontrar una guía detallada sobre el desarrollo de un plan de implementación del SSP.

4.3.5 Indicadores de seguridad operacional

Nivel aceptable de rendimiento en materia de seguridad operacional

4.3.5.1 El concepto de nivel aceptable de rendimiento en materia de seguridad operacional (ALoSP) complementa el enfoque tradicional de vigilancia de la seguridad operacional que se centra principalmente en el cumplimiento reglamentario prescriptivo con un enfoque basado en rendimiento que define los niveles de rendimiento en materia de seguridad operacional dentro de un marco de trabajo de SSP prescrito. Para fines de este manual, ALoSP es el nivel aceptable del rendimiento en materia de seguridad operacional de un Estado, como lo definen los indicadores de seguridad operacional del SSP y sus niveles de objetivos y alertas asociados. El ALoSP de un Estado debe ser pertinente a su política y objetivos de seguridad operacional.

4.3.5.2 Los criterios de ALoSP del Estado pueden variar según el contexto específico de cada sistema de aviación del Estado y la madurez de su sistema de vigilancia de seguridad operacional. El enfoque principal es lograr el cumplimiento de los requisitos de la OACI y reducir los eventos de alto impacto cuando tales problemas son evidentes. El enfoque progresará hacia donde el Estado muestre preocupación, con una mejora continua en el rendimiento en materia de seguridad operacional. El ALoSP de un SSP dado, una vez desarrollado, es una manifestación de lo que el Estado considera como adecuado dentro del contexto de su propio sistema de aviación. El ALoSP de un Estado también expresa los objetivos de seguridad operacional mínimos aceptables para la autoridad de vigilancia que deberán lograr los proveedores de servicios colectivos según su autoridad.

4.3.5.3 Para propósitos de un SSP, el ALoSP se identifica y establece mediante los indicadores de seguridad operacional colectivos del Estado. Los indicadores de seguridad operacional del Estado usados para este propósito son aquellos que tienen una configuración de objetivos y alertas incorporada, donde corresponda. Por lo tanto, el ALoSP es el concepto dominante, mientras que los indicadores de seguridad operacional junto a sus niveles de objetivos y alertas correspondiente (configuración de límites de rendimiento) son las métricas reales del ALoSP. El punto hasta donde se logran los objetivos del indicador de seguridad operacional es la medición del rendimiento de aquellos indicadores. En el Apéndice 4 se ofrecen ejemplos ilustrativos sobre el desarrollo de indicadores de seguridad operacional de ALoSP.

4.3.5.4 Un proceso de control y medición de ALoSP completamente desarrollado, siguiendo una base constante:

a) identificará todos los sectores esenciales de seguridad operacional y los indicadores de seguridad operacional que definen el nivel de seguridad operacional en estas áreas;

b) identificará los objetivos que definen el nivel que se debe mantener o la mejora deseada que se debe lograr para los indicadores relevantes en cada sector con una visión para lograr una mejora continua en todo el sistema de aviación;

c) identificará alertas que indicarán un problema de rendimiento en materia de seguridad operacional real o en desarrollo en un indicador o sector de seguridad operacional en particular; y

d) revisará el rendimiento en materia de seguridad operacional del SSP para determinar si se necesitan modificaciones o adiciones a indicadores, objetivos o alertas existentes para lograr la mejora continua.

4.3.5.5 El establecimiento de indicadores de seguridad operacional, objetivos y alertas de ALoSP para un SSP no cambia ni reemplaza la necesidad de que los Estados implementen todos los SARPS correspondientes ni exime a los Estados de sus obligaciones acerca del Convenio sobre Aviación Civil Internacional y sus disposiciones relacionadas.

Configuración de alertas/objetivos

4.3.5.6 Los indicadores de seguridad operacional son herramientas de control y medición tácticas del rendimiento en materia de seguridad operacional del Estado. Durante el desarrollo y la implementación inicial de un SSP, el nivel del rendimiento en materia de seguridad operacional se representa normalmente mediante indicadores de seguridad operacional relacionados con los resultados de alto impacto (como tasas de accidentes e incidentes graves) y resultados de la evaluación del sistema de alto nivel (como la implementación eficaz de los SARPS de la OACI). A medida que madura el SSP, el nivel del rendimiento en materia de seguridad operacional puede complementarse mediante indicadores que representan resultados del sistema de bajo impacto o eventos de desviación. Los indicadores de rendimiento en materia de seguridad operacional se controlan generalmente mediante herramientas básicas de tendencia de datos cuantitativos que generan gráficos o diagramas que incorporan niveles de alertas/objetivos usados comúnmente en sistemas de control técnico, de calidad o confiabilidad.

4.3.5.7 Los objetivos definen metas de rendimiento en materia de seguridad operacional del SSP a largo plazo. Se expresan en términos numéricos y deben ser concretos, medibles, aceptables, confiables y pertinentes. Los objetivos también necesitan contener fechas de finalización con hitos, si se debe alcanzar el objetivo en etapas o en un período de tiempo extendido. Los objetivos proporcionan una forma medible de garantizar y demostrar la eficacia de un SSP. La configuración del objetivo (cantidad) debe considerar factores como el nivel de riesgos de la seguridad operacional correspondiente, los costos y beneficios relacionados con las mejoras al sistema de aviación, así como también, las expectativas sobre la seguridad operacional de la industria de aviación del Estado. La configuración de los objetivos de mejora deseados deben determinarse después de considerar lo que es de verdad alcanzable para el sector de aviación asociado. Debe considerar el rendimiento histórico reciente del indicador de seguridad operacional en particular, donde estén disponibles los datos de tendencia histórica.

4.3.5.8 Se identifica un nivel de alerta correspondiente para cada indicador de rendimiento en materia de seguridad operacional, lo que cuantifica el umbral de rendimiento inaceptable (tasa de sucesos anormal) durante un período de control especificado. El uso de criterios basados en datos objetivos para configurar los niveles de alertas es esencial para facilitar los análisis de tendencia o de punto de referencia coherentes. Una configuración del nivel de alerta separa lo aceptable de las regiones de rendimiento inaceptables de un diagrama del indicador de seguridad operacional y es el primer activador (campana de precaución o alarma) o medida correctiva relacionado con un indicador de seguridad operacional en particular. Una violación del nivel de alerta garantiza una investigación de seguimiento acerca de la causa de la alerta y posterior medida correctiva o de mitigación, donde sea necesario.

Las medidas de seguimiento implican la coordinación con los proveedores de servicios afectados para identificar las causas de origen, los peligros y los riesgos asociados, según corresponda.

4.3.5.9 Al igual que con las prácticas de métricas de seguridad operacional genéricas, el uso de la desviación estándar de la población (STDEVP) proporciona un método objetivo básico para configurar los criterios de alertas. Este método deriva el valor de desviación estándar (SD) basado en los puntos de datos históricos anteriores de un indicador de seguridad operacional determinado. Este valor de SD más el valor promedio (medio) del conjunto de datos históricos forma el valor de alerta básico para el siguiente período de control. El principio de SD (una función de MS Excel básica) ajusta los criterios del nivel de alerta según el rendimiento histórico real del indicador determinado (conjunto de datos), como su volatilidad (fluctuaciones del punto de datos). Un conjunto de datos históricos más volátil producirá valores del nivel de alerta más altos (más generosos) para el siguiente período de control. En el Apéndice 4 podrá encontrar guías sobre la configuración del nivel de alerta mediante los criterios de SD.

4.3.5.10 Los indicadores de seguridad operacional básicos (ALoSP inicial) de un Estado constan generalmente de indicadores de seguridad operacional de alto impacto, como tasas de accidentes o incidentes graves para cada sector. Es importante que tales datos se expresen normalmente en términos de índices en lugar de números de incidentes absolutos. Posteriormente, en una etapa ALoSP madura, se podrán desarrollar los indicadores de seguridad operacional de bajo impacto para complementar el paquete de ALoSP. (Los indicadores de bajo impacto se denominan a veces indicadores "proactivos/predictivos").

4.3.5.11 Luego de identificar un paquete de configuración de indicadores de seguridad operacional, objetivos y alertas del Estado, es posible compilar un resumen de resultados de rendimiento de cada indicador de seguridad operacional regularmente. Entonces, puede revisarse el estado de rendimiento (logro) respectivo del nivel de objetivos y alertas para cada indicador. Posteriormente se puede compilar un resumen consolidado del resultado del rendimiento de objetivos/alertas general de todo el paquete de indicadores de seguridad operacional de ALoSP para ese año o período de control en particular. Si lo desea, se puede asignar un valor cuantitativo a cada “objetivo alcanzado” y a cada “nivel de alerta no violado” (puntos positivos). Entonces, esto puede proporcionar una medición numérica o porcentual del rendimiento de ALoSP. El rendimiento de ALoSP de un año o período de control determinado puede compararse con el rendimiento anterior o futuro. Los Estados tienen permitido mejorar aún más estos criterios de medición del rendimiento básico de ALoSP con otros factores o procesos complementarios, según se encuentre necesario.

4.3.5.12 Para garantizar que los indicadores de seguridad operacional de ALoSP sigan eficaces y adecuados con el paso del tiempo, se deben revisar periódicamente para determinar si es necesario realizar alguna modificación o adición a los indicadores, los objetivos y las alertas existentes. Esta revisión periódica de ALoSP y cualquier cambio resultante puede abordarse a nivel de la plataforma de coordinación del SSP, donde corresponda. En el Apéndice 4 de este capítulo podrá encontrar más información sobre el desarrollo de criterios para los indicadores de seguridad operacional y la configuración de objetivos y alertas. En los Capítulos 2 y 5 podrá encontrar una guía paralela sobre los indicadores de rendimiento en materia de seguridad operacional del SMS.

4.4 IMPLEMENTACIÓN DEL SSP — ENFOQUE EN ETAPAS

4.4.1 La implementación del SSP se facilita al identificar los procesos asociados con cada uno de los cuatro componentes y los elementos relacionados del marco de trabajo del SSP. La implementación progresiva o en etapas de un SSP gestiona eficazmente la carga de trabajo y las expectativas asociadas dentro de un marco de tiempo realista. La secuenciación o priorización real de las tareas relacionadas con la implementación de los diversos elementos del SSP variarán entre los Estados. El enfoque en etapas, como se describe en este capítulo, supone que los once elementos del SSP requerirán algún grado de implementación adicional. Donde ciertos elementos o procesos ya están implementados satisfactoriamente, estos pueden integrarse o vincularse al marco de trabajo del SSP, como corresponda.

4.4.2 En esta sección ofrecemos un enfoque de cuatro etapas para la implementación del SSP. Este enfoque implica cierta reorganización de los once elementos del SSP en las cuatro etapas. El motivo de este marco de trabajo en etapas es facilitar la implementación de los elementos y procesos de forma progresiva. En la Tabla 4-1 se incluye una descripción general de las cuatro etapas y sus elementos incluidos.

Etapa 1

4.4.3 Responsabilidades de seguridad operacional estatal — Elemento 1.2 (i)

a) Identificar la organización apoderada del SSP y el ejecutivo responsable del SSP. El ejecutivo responsable del SSP del Estado debe tener, como mínimo:

   1) autoridad y responsabilidad, en nombre del Estado, de la implementación y el mantenimiento del SSP en todo su sistema de aviación, con la excepción de la organización de investigación de accidentes del Estado;

   2) autoridad en temas de recursos humanos relacionados con la organización apoderada del SSP;

   3) autoridad en temas financieros importantes relacionados con la organización apoderada del SSP;

   4) autoridad en la certificación del proveedor de servicios y la vigilancia de la seguridad operacional mediante la organización apoderada del SSP; y

   5) responsabilidad de la coordinación de todos los temas relacionados con el SSP del Estado.

b) Establecer el equipo de implementación del SSP. El equipo debe componerse de representantes de las organizaciones reglamentarias y administrativas de la aviación pertinentes del Estado. El papel del equipo es impulsar la implementación del SSP desde la etapa de planificación hasta su finalización. La organización apoderada del SSP, junto con el departamento/oficina responsables de la administración del SSP, debe tomar control del equipo de implementación del SSP luego de la implementación. Otras funciones del equipo de implementación deben incluir, entre otros:

   1) coordinar el proceso de análisis de brechas;

   2) desarrollar el plan de implementación del SSP;

   3) garantizar una capacitación de SSP adecuada y experiencia técnica del equipo para establecer una implementación eficaz de los elementos del SSP y procesos relacionados;

   4) controlar y notificar el progreso de la implementación del SSP, proporcionar actualizaciones regulares, coordinar con el ejecutivo responsable del SSP y garantizar que las actividades dentro de cada etapa se cumplan según el cronograma definido.

   Para garantizar la ejecución correcta del plan de implementación, en especial para los Estados con múltiples organizaciones, el ejecutivo responsable debe garantizar que se ofrezca un respaldo adecuado de la autoridad y la administración al equipo de implementación.

Tabla 4-1. Un ejemplo de las cuatro etapas de la implementación del SSP

Etapa 1 (12 meses)	*Etapa 2 (12 meses)*	*Etapa 3 (24 meses)*	*Etapa 4 (24 meses)*
1. Elemento 1.2 del SSP (i): a) identificar la organización apoderada del SSP y al ejecutivo responsable; b) establecer el equipo de implementación del SSP; c) realizar un análisis de brechas del SSP; d) desarrollar un plan de implementación del SSP; e) establecer un mecanismo de coordinación del SSP; f) desarrollar la documentación del SSP necesaria, incluido el marco de trabajo del SSP del Estado, sus componentes y elementos.	1. Elemento 1.1 del SSP: Establecer un marco de trabajo de seguridad operacional legislativo. 2. Elemento 1.2 del SSP (ii): a) identificar, definir y documentar las responsabilidades de la gestión de seguridad operacional; b) definir y documentar la política y los objetivos de la seguridad operacional del Estado. 3. Elemento 1.3 del SSP: Establecer un proceso de investigación de accidentes e incidentes graves. 4. Elemento 1.4 del SSP (i): Establecer una legislación de cumplimiento (sanciones) básica. 5. Elemento 3.1 del SSP (i): Supervisión estatal de la seguridad operacional y vigilancia de sus proveedores de servicios. 6. Elemento 2.1 del SSP (i): Facilitar y promover la educación del SMS para los proveedores de servicios.	1. Elemento 1.4 del SSP (ii): Promulgar la política/ legislación de cumplimiento que incluya: a) disposiciones para los proveedores de servicios que operan bajo un SMS a fin de que aborden y resuelvan desviaciones de seguridad operacional y calidad de forma interna; b) condiciones y circunstancias en las cuales un Estado puede intervenir las desviaciones de seguridad operacional; c) disposiciones para evitar el uso o la divulgación de datos de seguridad operacional para propósitos que no sean la mejora de la seguridad operacional; d) disposiciones para proteger las fuentes de información obtenidas desde los sistemas de notificación voluntaria/ confidencial. 2. Elemento 2.1 del SSP (ii): Desarrollar reglamentos armonizados que requieran de la implementación de SMS. 3. Elemento 3.2 del SSP (i): a) establecer sistemas de recopilación e intercambio de datos; b) establecer indicadores de rendimiento en materia de seguridad operacional del Estado de alto impacto y niveles de objetivos/ alertas.	1. Elemento 2.2 del SSP: Revisar y acordar los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios. 2. Elemento 3.1 del SSP (ii): Incorporar el SMS y los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios en el programa de vigilancia de rutina. 3. Elemento 3.2 del SSP (ii): a) implementar sistemas de notificación de seguridad operacional voluntaria/confidencial; b) establecer indicadores de seguridad operacional/calidad de bajo impacto con control del nivel de objetivos/alertas, según corresponda; c) promover el intercambio de información de seguridad operacional con los proveedores de servicios y otros Estados, y entre ellos. 4. Elemento 3.3 del SSP: Priorizar inspecciones y auditorías basadas en el análisis de riesgos de seguridad operacional o datos de calidad, donde corresponda. 5. Elemento 3.1 del SSP (iii) Establecer un mecanismo de revisión interna que aborde el SSP para garantizar la eficacia y mejora continuas.

Nota 1.— Los Elementos 4.1 y 4.2 del SSP (SSP interno y capacitación de SMS; promoción de capacitación de SMS externa; y comunicación y diseminación interna y externa de información de seguridad operacional) se implementan progresivamente mediante las Etapas 1 a 4.

Nota 2.— El marco de tiempo para cada etapa (por ejemplo, 12 meses para la Etapa 1) es solo un aproximado. El período de implementación real dependerá del alcance/complejidad del sistema de aviación de un Estado, las brechas reales dentro de cada elemento y la estructura institucional.

c) Realizar un análisis de brechas del SSP. Para desarrollar un plan de implementación del SSP, se debe realizar un análisis de brechas de las estructuras y los procesos existentes en el Estado, en comparación con el marco de trabajo del SSP de la OACI. Esto permitirá que el Estado evalúe la existencia y madurez de los elementos del SSP. Luego de terminar y documentar el análisis de brechas, los componentes/elementos/procesos identificados como faltantes o deficientes, junto con aquellos existentes, formarán la base del plan de implementación del SSP. En el Apéndice 7 de este capítulo podrá encontrar un ejemplo de una lista de verificación del análisis de brechas de un SSP.

d) Desarrollar un plan de implementación del SSP. El plan servirá como una guía sobre cómo se desarrollará e integrará el SSP en las actividades de gestión de la seguridad operacional. El plan debe:

1) establecer claramente las actividades (elementos/procesos) que se desarrollarán o completarán según sus hitos o fases asignadas respectivas. Estas actividades se basan en los resultados del análisis de brechas; y

2) determinar un cronograma realista, que incluya hitos, para cumplir cada actividad o etapa. Según la complejidad del SSP del Estado, se podrá compilar un plan de implementación de SSP como una simple tabla de Word/Excel o, si fuera necesario, al usar una herramienta de gestión de proyectos, como un diagrama Gantt. En el Apéndice 7 de este capítulo podrá encontrar un formato de muestra de un plan de implementación de SSP básico.

e) Establecer una plataforma de coordinación de seguridad operacional de la aviación de un Estado. Si no existe, comience a establecer un mecanismo de coordinación de SSP, con participación de todas las organizaciones reglamentarias y administrativas de aviación del Estado. Este mecanismo puede estar en la forma de un directorio o comité. Su función es coordinar la implementación y posterior administración del SSP entre diversas organizaciones reglamentarias y administrativas de aviación del Estado. Esto garantizará que el desarrollo, la revisión periódica y la creación de políticas y toma de decisiones, relacionados con las actividades del SSP, como política de seguridad operacional, indicadores de seguridad operacional, política de cumplimiento, protección y distribución de datos de seguridad operacional, requisitos reglamentarios del SMS y revisión y hallazgos internos del SSP, se lleven a cabo de forma integrada y coordinada. Esta plataforma de SSP constante debe implicar la administración superior de diversas organizaciones, con el ejecutivo responsable del SSP como el coordinador.

f) Establecer la documentación del SSP. El proceso para redactar un documento de SSP debe comenzar desde el principio del ejercicio de implementación del SSP. A medida que los componentes y elementos del SSP se definen progresivamente, la descripción de cada elemento y sus procesos asociados pueden redactarse progresivamente en este documento de alto nivel. Vease el Apéndice 8 para un ejemplo ilustrativo de cómo se debe estructurar un documento de SSP y su contenido. Establezca un sistema de documentación del SSP (biblioteca/gabinete/carpeta) dentro de la organización apoderada del SSP, que sirva como el repositorio central para materiales como el documento del SSP, los SOP relacionados, los formularios, las minutas de las reuniones y los registros asociados con la implementación y operación continua del SSP. Estos documentos sirven como registros y evidencia de las actividades reales y la operación continua de los elementos individuales del SSP. Es posible que algunos registros, como informes confidenciales o informes de sucesos, puedan mantenerse en un sistema computacional por separado o residir en otra organización reglamentaria o administrativa. En tales casos, se deben mantener muestras o extractos en la biblioteca, según corresponda. Un índice maestro de la documentación del SSP debe ayudar a explicar toda la documentación relevante. Un sistema de documentación consolidado facilitará obtener una fácil trazabilidad, actualización, referencia y auditoría interna/externa del sistema.

Etapa 2

4.4.4 Marco de trabajo legislativo estatal de la seguridad operacional — Elemento 1.1

a) Revisar, desarrollar y promulgar, según sea necesario, un marco de trabajo legislativo nacional y reglamentos específicos, en cumplimiento de normas internacionales y nacionales, que definen cómo el Estado gestionará y regulará la seguridad operacional de la aviación en todo el sistema de la aviación.

b) Establecer un marco de tiempo para revisar periódicamente la legislación de seguridad operacional y los reglamentos de operación específicos, a fin de garantizar que sigan siendo relevantes y adecuados para el Estado.

4.4.5 Responsabilidades estatales de seguridad operacional — Elemento 1.2 (ii)

a) Definir y establecer las responsabilidades de gestión de la seguridad operacional de las organizaciones reglamentarias respectivas. Dentro del documento SSP se debe incluir una descripción o ilustración de la estructura e integración institucional existente de las diversas organizaciones reglamentarias y administrativas. En el documento mencionado se incluirá una referencia cruzada que respaldará la documentación en términos de las responsabilidades de la seguridad operacional en detalle.

b) Desarrollar e implementar una política estatal de seguridad operacional y los medios necesarios para garantizar que se entienda, implemente y respete la política en todos los niveles dentro de las organizaciones del Estado. En el Apéndice 1 de este capítulo se describe una guía sobre el desarrollo de una política estatal de seguridad operacional.

c) Desarrollar o incluir amplios objetivos de seguridad operacional estatal, que sean coherentes con la política estatal de seguridad operacional. Tales objetivos de seguridad operacional pueden ser independientes o parte de la declaración de misión general de la organización, según la complejidad y los papeles de la organización. Estos objetivos de seguridad operacional se deben considerar entonces durante el desarrollo posterior de los indicadores de seguridad operacional de ALoSP del Estado. Deben existir indicadores que sirvan como una métrica para evaluar el estado de logro de los objetivos de la seguridad operacional.

4.4.6 Investigación de accidentes e incidentes — Elemento 1.3

El Estado debe:

a) garantizar que el marco de trabajo legislativo nacional incluya disposiciones para el establecimiento de un proceso de investigación de accidentes e incidentes independiente, que se administre mediante una organización, departamento, comisión u otra entidad independiente;

b) establecer una organización, departamento, comisión u otra entidad de investigación de accidentes e incidentes, que sea independiente del resto de organizaciones de aviación del Estado. En los Estados donde no sea práctico establecer una entidad de investigación de accidentes, se podrá asignar una comisión o un directorio de investigación de accidentes competente para cada accidente que deba ser investigado. O bien, tales Estados podrán considerar los servicios de una RAIO (Véase el Doc 9946);

c) establecer mecanismos para garantizar que el único objetivo del proceso de investigación de accidentes e incidentes sea la prevención de accidentes e incidentes, en respaldo a la gestión de la seguridad operacional en el Estado, y no la de encontrar culpables o responsables.

4.4.7 Política de cumplimiento — Elemento 1.4 (i)

El Estado debe garantizar o establecer disposiciones legislativas fundamentales para la medida (sanción) de cumplimiento reglamentario, lo que incluye la suspensión o revocación de certificados.

4.4.8 Vigilancia de la seguridad operacional — Elemento 3.1 (i)

El Estado debe garantizar o establecer un programa de vigilancia de la seguridad operacional básico para supervisar a los proveedores de servicios. Esto debe incluir un programa de vigilancia que garantice el cumplimiento reglamentario de los proveedores de servicios durante las operaciones de rutina, como, entre otras:

a) inspecciones del sitio, estación o productos; y

b) auditorías institucionales o del sistema.

4.4.9 Requisitos de seguridad operacional para el SMS del proveedor de servicios — Elemento 2.1 (i)

a) Donde corresponda, durante la etapa de educación y promoción de la implementación del SMS, el Estado debe preparar a los proveedores de servicios y a los accionistas de la industria para los requisitos de implementación del SMS mediante las actividades educativas y promocionales del SMS, como foros, seminarios, sesiones informativas o talleres de SMS.

b) Desarrollar material guía del SMS, pertinente a los proveedores de servicios, en anticipación o junto con el desarrollo de reglamentos del SMS. Véase el Apéndice 9 de este capítulo para ver un ejemplo de regulación de SMS de un Estado.

Etapa 3

4.4.10 Política de cumplimiento — Elemento 1.4 (ii)

En un entorno de SSP-SMS, la política y los procedimientos de cumplimiento reglamentario del Estado debe establecer:

a) las condiciones y circunstancias en las cuales los proveedores de servicios tienen permitido abordar y resolver eventos que impliquen ciertas desviaciones de seguridad operacional, de forma interna, dentro del contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios y a la satisfacción de la autoridad estatal correspondiente;

b) las condiciones y circunstancias en las cuales las desviaciones de seguridad operacional se abordan mediante procedimientos de cumplimiento establecidos;

c) los procedimientos para garantizar que ninguna información obtenida mediante los sistemas de notificación voluntaria/confidencial o un sistema de control de datos operacionales restringido equivalente, que funciona según un SMS, se usará para una medida de cumplimiento;

d) un proceso para proteger las fuentes de información obtenidas a partir de sistemas de notificación voluntaria y confidencial.

En este capítulo, en el Apéndice 10 se describe una muestra de política de cumplimiento del Estado y en el Apéndice 11 se entrega una muestra de procedimientos de cumplimiento estatales.

4.4.11 Requisitos de SMS para los proveedores de servicios — Elemento 2.1 (ii)

a) Establecer reglamentos, material de guía y requisitos de implementación de SMS para todos los proveedores de servicios correspondientes y garantizar que todo el marco de trabajo reglamentario del SMS esté armonizado en todos los sectores de aviación y que sea congruente con el marco de trabajo del SMS de la OACI. La adopción del marco de trabajo de SMS armonizado de la OACI facilitará el reconocimiento mutuo entre los Estados.

b) Establecer un proceso para aceptar el SMS de un proveedor de servicios individual, con el fin de garantizar que su marco de trabajo de SMS sea congruente con el marco de trabajo reglamentario del SMS del Estado. Dicha revisión y aceptación inicial puede manifestarse mediante la aprobación o aceptación del manual de SMS de la organización. Donde un Estado adopte tal enfoque de implementación de SMS en etapas, dicho proceso de aceptación podrá llevarse a cabo en etapas, donde corresponda. Consulte el Apéndice 12 para ver un ejemplo de la lista de verificación de evaluación/aceptación reglamentaria de un SMS.

Nota.— Se promueve la aceptación o el reconocimiento del SMS de una organización extranjera (por ejemplo, AMC extranjera) donde dicho SMS haya sido debidamente aceptado por la autoridad local de esa organización y donde el marco de trabajo de SMS de la organización esté en armonía con el marco de trabajo de SMS de la OACI.

4.4.12 Recopilación, análisis e intercambio de datos de seguridad operacional — Elemento 3.2 (i)

El Estado debe:

a) configurar mecanismos y procedimientos para recopilar y analizar datos de sucesos con notificación obligatoria a nivel de todos los Estados. Esto requeriría que el Estado:

1) establezca un procedimiento de suceso con notificación obligatoria para que los proveedores de servicios certificados/aprobados de cada sector de la aviación informen (base obligatoria) accidentes e incidentes graves. Esto debe incluir informes obligatorios de defectos (MDR) o informes importantes, donde corresponda. Véase en el Apéndice 3 un ejemplo de un procedimiento de notificación obligatoria de un Estado;

2) establezca requisitos para que los proveedores de servicios tengan un proceso interno de investigación y resolución de sucesos que documente los resultados de la investigación y haga que los informes estén disponibles para la organización reglamentaria respectiva;

3) garantice que existe una integración, consolidación y adición adecuada de datos recopilados desde diversos sectores de la aviación a nivel del SSP. Los datos de seguridad operacional no deberían existir como bases de datos independientes solo a nivel del sector individual. Este aspecto de la integración también debe abordarse para las bases de datos de seguridad operacional respectivas de CAA y aquellas de la autoridad de investigación de accidentes independiente, como aquellos Estados donde ciertas funciones de gestión de la seguridad operacional se llevaron a cambo mediante una RSOO o una RAIO en nombre del Estado;

b) establecer los indicadores de seguridad operacional de alto impacto básicos (ALoSP inicial) y la configuración de objetivos y alertas asociada. Entre los ejemplos de indicadores de seguridad operacional de alto impacto se incluyen tasas de accidentes, tasas de incidentes graves y el control de resultados de alto riesgo, reglamentarios y de no cumplimiento (por ejemplo, hallazgos de la

auditoría de la OACI). El desarrollo y la selección de indicadores de seguridad operacional deben ser congruentes con los objetivos de seguridad operacional del Estado y la política de seguridad operacional. Deben ser adecuados y pertinentes al alcance y complejidad de las actividades de aviación del Estado. La selección de indicadores de seguridad operacional de bajo impacto puede abordarse en una etapa posterior. Se debe realizar el control periódico de tendencias indeseables, violaciones a nivel de alerta y el logro de objetivos en los indicadores de seguridad operacional. Consulte el Apéndice 4 en busca de guías sobre el desarrollo y control de indicadores de seguridad operacional.

Etapa 4

4.4.13 Acuerdo sobre el rendimiento en materia de seguridad operacional del proveedor de servicios — Elemento 2.2

El Estado debe establecer un procedimiento de vinculación con los proveedores de servicios en su desarrollo de un conjunto de indicadores de rendimiento en materia de seguridad operacional (SPI), objetivos y alertas realistas, donde sea posible, según la envergadura y complejidad de la organización. Los indicadores de seguridad operacional, los objetivos y las alertas deben ser:

a) una combinación de SPI de alto y bajo impacto, según corresponda;

b) pertinentes a las actividades de aviación del proveedor de servicios;

c) consistentes con otros proveedores de servicios del mismo sector/categoría;

d) congruentes con los indicadores de seguridad operacional colectivos del SSP del Estado para el sector/categoría del proveedor de servicios.

Luego de que los indicadores de seguridad operacional, los objetivos y las alertas se han implementado, se deben documentar los planes de medidas del proveedor de servicios, en relación con el logro de los objetivos y sus planes de medidas correctivas en caso de llegar a un nivel de alerta. El proceso de revisión periódica posterior del regulador sobre el rendimiento en materia de seguridad operacional del proveedor de servicios debe ser transparente para el proveedor de servicios durante la implementación de los requisitos de rendimiento.

4.4.14 Vigilancia de la seguridad operacional — Elemento 3.1 (ii)

El Estado debe incorporar la vigilancia del SMS de los proveedores de servicios como parte del programa de vigilancia de rutina que incluye:

a) configurar la revisión periódica de los requisitos del SMS de los proveedores de servicios y el material guía relacionado, para garantizar que sigan siendo pertinentes y adecuados para ellos;

b) medir el rendimiento en materia de seguridad operacional del SMS del proveedor de servicios individual mediante revisiones periódicas del rendimiento en materia de seguridad operacional acordado y garantizar que los SPI y la configuración de objetivos y alertas sigan siendo pertinentes para el proveedor de servicios;

c) garantizar que los procesos de identificación de peligros y gestión de riesgos de la seguridad operacional del proveedor de servicios sigan requisitos reglamentarios establecidos y que los controles de riesgos de seguridad operacional se integren adecuadamente en el SMS del proveedor de servicios.

4.4.15 Vigilancia de la seguridad operacional — Elemento 3.1 (iii)

El Estado debe desarrollar un mecanismo interno de revisión o evaluación que aborde al SSP y su política de seguridad operacional para garantizar el cumplimiento y mejora continuos del SSP. Al igual que con un mecanismo de revisión interno eficaz, también debe haber un nivel adecuado de independencia en el proceso de revisión y responsabilidad para realizar una medida de seguimiento.

4.4.16 Recopilación, análisis e intercambio de datos de seguridad operacional — Elemento 3.2 (ii)

El Estado debe:

a) establecer un sistema de notificación voluntaria a nivel del Estado, que incluya disposiciones para la protección de información de seguridad operacional. Véase el Apéndice 5 para guía sobre la protección de la información de seguridad operacional. Este sistema de notificación voluntaria debe constituir parte del sistema de recopilación y procesamiento de datos de seguridad operacional del SSP. La base de datos de este sistema de notificación voluntaria debe ser parte del SDCPS del SSP y debe estar disponible para la CAA del Estado, así como también, para la autoridad de investigación de accidentes. Véase el Apéndice 2 para guía sobre el sistema de notificación voluntaria del Estado;

b) establecer indicadores de seguridad operacional o calidad de bajo impacto con un control de objetivos y alertas adecuado (ALoSP maduro). La selección y el desarrollo de los indicadores de seguridad operacional deben ser congruentes con los objetivos de seguridad operacional y la política de seguridad operacional del Estado, y deben ser relevantes para el alcance y la complejidad de las actividades de aviación del Estado. Se debe realizar el control periódico de tendencias indeseables, violaciones a nivel de alerta y el logro de objetivos en los indicadores de seguridad operacional. Véase el Apéndice 4 para guía sobre el desarrollo y control de los indicadores de seguridad operacional;

c) promover el intercambio y la distribución de información de seguridad operacional entre las organizaciones reglamentarias y administrativas del Estado y los proveedores de servicios, así como también, con otros Estados y organizaciones de la industria.

4.4.17 Enfoque basado en datos de seguridad operacional de la vigilancia de áreas de mayor preocupación o necesidad — Elemento 3.3

El Estado debe revisar los programas de vigilancia y auditoría existentes para incorporar disposiciones para la calibración de la frecuencia y alcance de la vigilancia o auditoría de un proveedor de servicios individual, según los resultados de rendimiento pertinentes y las entradas de datos de seguridad operacional. Véase la Sección 4.2, Elemento 3.3, 4.2.36 y 4.2.37 del SSP para guía sobre el concepto de vigilancia basada en datos de seguridad operacional.

4.4.18 Capacitación interna, comunicación y distribución de información de seguridad operacional — Elemento 4.1 (Etapas 1 a 4)

El Estado debe:

a) desarrollar una política y procedimientos de capacitación internos;

b) desarrollar un programa de capacitación de SSP y SMS para el personal correspondiente. Se debe dar prioridad al personal de investigación de SSP-SMS y a los inspectores operacionales/de campo que participan en el SMS del proveedor de servicios;

c) incluir procesos de SSP específicos del Estado y su relevancia con los elementos genéricos del marco de trabajo de la OACI en el material de capacitación y educación posterior a la implementación de SSP y SMS;

d) desarrollar medios para comunicar información relacionada con la seguridad operacional, como documentación del SSP del Estado y políticas y procedimientos de seguridad operacional/ cumplimiento, a las organizaciones reglamentarias y administrativas del Estado mediante tales mecanismos como folletos informativos, boletines y sitios web.

4.4.19 Capacitación externa, comunicación y distribución de información de seguridad operacional — Elemento 4.2 (Etapas 1 a 4)

El Estado debe:

a) establecer un proceso para comunicar la información reglamentaria y relacionada con el SSP y SMS a los proveedores de servicios;

b) desarrollar, para los proveedores de servicios, material guía sobre la implementación del SMS;

c) establecer los medios para comunicar problemas relacionados con la seguridad operacional de forma externa, como políticas y procedimientos de seguridad operacional, mediante mecanismos como folletos informativos, boletines o sitios web;

d) promover el intercambio de información de seguridad operacional con proveedores de servicios y otros Estados, y entre ellos;

e) facilitar la capacitación o familiarización del SMS para los proveedores de servicios, donde corresponda.

Nota.— Los elementos en 4.4.18 y 4.4.19 se desarrollan e implementan progresivamente mediante todas las etapas de implementación.

Apéndice 1 del Capítulo 4

GUÍA SOBRE EL DESARROLLO DE UNA DECLARACIÓN DE POLÍTICA ESTATAL DE SEGURIDAD OPERACIONAL

1. GENERALIDADES

1.1 La declaración de política estatal de seguridad operacional debe considerar, entre otros, los siguientes compromisos:

a) desarrollar e implementar estrategias y procesos para garantizar que todas las actividades y operaciones de aviación alcancen el más alto nivel de rendimiento en materia de seguridad operacional;

b) desarrollar y promulgar un marco de trabajo legislativo nacional de seguridad operacional y reglamentos de operación correspondientes para la gestión de la seguridad operacional del Estado, la que se basa en el análisis integral del sistema de aviación del Estado. También cumple con los requisitos y las normas internacionales de seguridad operacional y, cuando es posible, los supera;

c) consultar con los segmentos relevantes de la industria de la aviación sobre temas acerca del desarrollo reglamentario;

d) asignar los recursos necesarios para las organizaciones de aviación del Estado, a fin de garantizar que el personal esté correctamente capacitado y para permitirles descargar sus responsabilidades;

e) respaldar la gestión de la seguridad operacional mediante la promoción de sistemas de notificación voluntaria y confidencial a nivel del proveedor de servicios y del Estado;

f) realizar actividades de vigilancia basada en datos y riesgos y priorizadas, que se basen en rendimiento y en cumplimiento, y garantizar que tales actividades de vigilancia reglamentaria y administrativa se lleven a cabo según las normas y mejores prácticas internacionales, según corresponda;

g) promover y educar a la industria de la aviación en los conceptos y principios de gestión de la seguridad operacional, y supervisar la implementación y operación del SMS mediante los proveedores de servicios del Estado;

h) establecer disposiciones para la protección de los sistemas de recopilación y procesamiento de datos de seguridad operacional, para alentar a que el personal y las organizaciones proporcionen información esencial relacionada con la seguridad operacional y que exista un flujo e intercambio continuo de datos de la gestión de la seguridad operacional entre el Estado y los proveedores de servicios;

i) garantizar la interacción eficaz con los proveedores de servicios en la resolución de las preocupaciones de seguridad operacional;

j) mantener una política y procedimientos de cumplimiento que complementen la protección de la información que derivada de los sistemas de recopilación y procesamiento de datos de seguridad operacional;

k) establecer un mecanismo para el control y la medición del rendimiento de SSP mediante indicadores de seguridad operacional y la configuración del nivel de objetivos y alertas respectiva;

l) promover la adopción de las mejores prácticas y una cultura de seguridad operacional positiva dentro de las organizaciones del proveedor de servicios.

1.2 El ejecutivo responsable del SSP o un funcionario de la oficina a nivel de Estado correspondiente, responsable de supervisar las organizaciones reglamentarias y administrativas del Estado, debe firmar la declaración de la política estatal de seguridad operacional.

2. ILUSTRACIÓN DE UNA DECLARACIÓN BÁSICA DE LA POLÍTICA DE SEGURIDAD OPERACIONAL

La siguiente es una ilustración de la declaración básica de la política de seguridad operacional:

[Nombre de la organización reglamentaria del Estado] promueve y regula la seguridad operacional de la aviación en [Nombre del Estado]. Estamos comprometidos a desarrollar e implementar estrategias, marcos de trabajo reglamentarios y procesos eficaces para garantizar que las actividades de aviación, bajo nuestra vigilancia, alcancen el más alto nivel viable de seguridad operacional.

Para este fin:

1) configuraremos normas nacionales que estén en línea con las normas, métodos recomendados y procedimientos de la Organización de Aviación Civil Internacional;

2) adoptaremos un enfoque basado en datos y en rendimiento para las actividades de regulación y vigilancia industrial de la seguridad operacional, donde corresponda;

3) identificaremos las tendencias de seguridad operacional dentro de la industria de aviación y adoptaremos un enfoque basado en riesgos para abordar las áreas de mayor preocupación o necesidad de la seguridad operacional;

4) controlaremos y mediremos el rendimiento en materia de seguridad operacional de nuestro sistema de aviación continuamente mediante los indicadores de seguridad operacional colectivos del Estado, así como también, los indicadores de rendimiento en materia de seguridad operacional de los proveedores de servicios;

5) colaboraremos y consultaremos con la industria para abordar los temas de seguridad operacional y mejoraremos continuamente la seguridad operacional de la aviación;

6) promoveremos las buenas prácticas de seguridad operacional y una cultura de seguridad operacional institucional positiva dentro de la industria basada en principios sólidos de la gestión de la seguridad operacional;

7) alentaremos la recopilación, el análisis y el intercambio de información de seguridad operacional entre todas las organizaciones industriales y proveedores de servicios pertinentes, con la intención de que tal información se use solo para propósitos de gestión de la seguridad operacional;

8) asignaremos suficientes recursos financieros y humanos para la gestión y vigilancia de la seguridad operacional; y

9) equiparemos al personal con habilidades y experiencia adecuadas para descargar de forma competente sus responsabilidades de vigilancia y gestión de la seguridad operacional.

(Firmado) _____
DGAC [ejecutivo responsable de SSP o un funcionario de la oficina a nivel de Estado responsable de la aviación civil]

Apéndice 2 del Capítulo 4

GUÍA SOBRE EL SISTEMA DE NOTIFICACIÓN VOLUNTARIA Y CONFIDENCIAL DE UN ESTADO

[Véase el Elemento 3.2 del SSP y el Capítulo 4, 4.4.16 a)]

Un sistema de notificación voluntario y confidencial de un Estado debe, como mínimo, definir:

a) el objetivo del sistema de notificación;

Ejemplo:

El objetivo clave del sistema de notificación voluntaria y confidencial de [nombre del Estado] es mejorar la seguridad operacional de la aviación mediante la recopilación de informes sobre deficiencias reales o posibles de la seguridad operacional que, de lo contrario, podrían no informarse mediante otros canales. Tales informes pueden implicar los sucesos, los peligros o las amenazas pertinentes a la seguridad operacional de la aviación. Este sistema no elimina la necesidad de la notificación obligatoria de accidentes e incidentes con aeronaves a las autoridades pertinentes, según los reglamentos de aviación existentes. Se alienta a que los notificadores usen el sistema de notificación voluntaria del SMS interno de su organización, donde corresponda, a menos que no tengan acceso a tal sistema o el incidente o peligro se considere que va más allá del alcance del ámbito de la organización.

El [nombre del sistema] es un sistema de notificación voluntaria, no punitivo, confidencial que establece [Nombre de la organización reglamentaria/administrativa]. Proporciona un canal para la notificación voluntaria de sucesos o peligros de aviación mientras protege la identidad de los notificadores.

b) el alcance de los sectores/áreas de aviación que aborda el sistema;

Ejemplo:

El [Nombre del sistema] abarca áreas como:

a) Operaciones de vuelo:

i) salida/en ruta/acercamiento y aterrizaje;
ii) operaciones en la cabina de la aeronave;
iii) eventos de proximidad aérea;
iv) peso, equilibrio y rendimiento.

b) Operaciones en el aeródromo:

i) operaciones de la aeronave en tierra;
ii) movimiento en el aeródromo;
iii) operaciones de abastecimiento de combustible;
iv) condiciones o servicios del aeródromo;
v) carga de cargamento.

c) Gestión del tránsito aéreo:

i) operaciones de ATC;
ii) equipo del ATC y ayudas para la navegación;
iii) comunicaciones de la tripulación y del ATC.

d) Mantenimiento de la aeronave:

i) actividades de mantenimiento y reparación de la aeronave/motor/componentes.

e) Diseño y fabricación:

i) actividades de diseño o producción de aeronaves/motores/componentes.

f) Organizaciones de capacitación probadas:

i) actividades de capacitación que implican operaciones de vuelo.

g) Misceláneo:

i) operaciones de control de pasajeros relacionadas con la seguridad operacional;
ii) etc.

c) quien pueda hacer un informe voluntario;

Ejemplo:

Si pertenece a alguno de estos grupos, puede contribuir con la mejora de la seguridad operacional de la aviación mediante [Nombre del sistema] al notificar sucesos, peligros o amenazas en el sistema de la aviación:

a) miembros de la tripulación de vuelo y de la cabina;

b) controladores de tránsito aéreo;

c) ingenieros, técnicos o mecánicos de aeronaves con licencia;

d) empleados de organizaciones de mantenimiento, diseño y fabricación;

e) explotadores de servicios de escala del aeródromo;

f) empleados del aeródromo;

g) personal de aviación general;

h) etc.

d) cuándo se debe hacer dicho informe;

Ejemplo:

Debe hacer un informe cuando:

a) desee que otros aprendan y se beneficien del informe de sucesos o peligros, pero está preocupado de proteger su identidad;

b) no existe otro procedimiento o canal de notificación adecuado;

c) ha probado con otro procedimiento o canal de notificación sin que el problema se haya abordado.

e) cómo se procesan los informes;

Ejemplo:

El [Nombre del sistema] presta particular atención a la necesidad de proteger la identidad del notificador cuando se procesan todos los informes. El administrador leerá y validará cada informe. El administrador puede comunicarse con el notificador para asegurarse de que comprenda la naturaleza y las circunstancias del suceso/peligro informado o para obtener información y clarificación adicional necesaria.

Cuando el administrador esté satisfecho con que la información obtenida es completa y coherente omitirá la identidad de quien entrega la información e ingresará los datos en la base de datos del [Nombre del sistema]. En caso que se deba buscar aportes de cualquier tercero, solo se usarán datos no identificados.

El formulario del [Nombre del sistema], con la fecha de retorno anotada, será devuelta finalmente al notificador. El administrador intentará completar el procesamiento dentro de 10 días hábiles si no se necesita información adicional. En los casos donde el administrador debe conversar con el notificador o consultar a un tercero, se necesitará más tiempo.

Si el administrador no está en su oficina por un tiempo prolongado, el administrador suplente procesará el informe. Los notificadores pueden estar tranquilos de que el administrador o el administrador suplente leerá y seguirá cada informe de [Nombre del sistema].

Retroalimentación a la comunidad de la aviación

Se pueden compartir informes y extractos sin identificación relevantes con la comunidad de aviación mediante publicaciones periódicas, para que todos puedan aprender de las experiencias. Las autoridades y partes relevantes también pueden revisar su política y planificar las mejoras.

Si el contenido de un informe de [Nombre del sistema] sugiere una situación o condición que represente una amenaza inmediata o urgente para la seguridad operacional de la aviación, el informe se tratará con prioridad y se derivará, luego de eliminar la identidad del notificador, a las organizaciones pertinentes lo antes posible, para permitirles tomar las medidas de seguridad operacional necesarias.

f) cómo comunicarse con el administrador de [Nombre del sistema];

Ejemplo:

Si lo desea, puede llamar a [Nombre de la organización reglamentaria/administrativa] para consultar sobre [Nombre del sistema] o para solicitar un análisis preliminar con el administrador de [Nombre del sistema] antes de hacer un informe. Puede comunicarse con el administrador y el administrador suplente durante horas de oficina de lunes a viernes en los siguientes números de teléfono:

Administrador del [Nombre del sistema]	Administrador suplente
El Sr. ABC	El Sr. XYZ
Tel.:	Tel.:

Apéndice 3 del Capítulo 4

EJEMPLO DEL PROCEDIMIENTO DE NOTIFICACIÓN OBLIGATORIA DE UN ESTADO

El siguiente es un ejemplo ilustrativo del procedimiento de notificación obligatoria de un Estado, el que aborda los sistemas de notificación de incidentes obligatorio. Este procedimiento corresponde a la notificación obligatoria y oportuna de accidentes, incidentes graves, incidentes y otros sucesos que pueden ser notificados por los accionistas pertinentes. Tales accionistas pueden, según los reglamentos del Estado, abordar a las organizaciones de aviación certificadas/aprobadas, al personal licenciado/autorizado independiente (por ejemplo, pilotos, miembros de la tripulación de la cabina, controladores de tránsito aéreo, personal de mantenimiento) y miembros del público.

Nota 1.— Si un Estado lo prefiere, la notificación obligatoria de accidentes e incidentes graves, así como también, de defectos, malfuncionamientos, dificultades de servicio, etc. pueden abordarse en procedimientos separados, de lo contrario, pueden abordarse en su procedimiento de notificación obligatoria (tal como es el caso en este ejemplo ilustrativa).

Nota 2.— En algunos casos, se ha proporcionado un "Comentario" en corchetes [ ]. Esta es una guía administrativa para la consideración de los Estados en el curso o redacción de sus propios procedimientos de notificación obligatoria.

1. NOTIFICACIÓN OBLIGATORIA

1.1 En conformidad con [Referencias de reglamentos], es obligatorio que [Accionistas nombrados] informen accidentes, incidentes graves, incidentes u otros sucesos relacionados con la seguridad operacional en la aviación (como defectos/malfuncionamiento/dificultades de servicio) a [Nombre de la autoridad/entidad y departamento].

1.2 En el Anexo A de este procedimiento se incluye la lista de sucesos que pueden notificarse (aparte de los accidentes) y las cronologías de notificación. [*Comentario:* aunque el Anexo A consta principalmente de ejemplos de incidentes graves, se promueve que los Estados incluyan otros sucesos que pueden notificarse según este sistema de notificación obligatoria].

1.3 La notificación de los sucesos obligatorios se lleva a cabo mediante el Informe obligatorio [Formulario XYZ]. Todos los informes obligatorios están firmados por el signatario autorizado de la organización aprobada y certificada, donde corresponda. [*Comentario:* también se debe desarrollar un procedimiento para abordar las notificaciones recibidas mediante las comunicaciones verbales y vía telefónica].

1.4 En caso de accidentes e incidentes graves, se debe iniciar una coordinación inmediata con [Nombre de la autoridad de investigación de accidentes del Estado] al momento de recibir dicha notificación, para determinar si se debe activar el proceso de investigación independiente. [*Comentario:* el proceso de notificación e información real para la CAA del Estado o la autoridad de investigación de accidentes dependerá de la naturaleza de los requisitos y acuerdos de notificación obligatoria del Estado. Tales detalles específicos deben reflejarse entonces coherentemente en esta sección de este procedimiento].

2. PROCESAMIENTO DE INFORMES OBLIGATORIOS

2.1 Al momento de la recepción de un informe obligatorio, se validará para garantizar que el notificador ha proporciona toda la información esencial.

2.2 El informe se clasificará entonces en las siguientes categorías:

a) accidente;

b) incidente grave;

c) incidente;

d) otro suceso.

2.3 Luego de la clasificación, el registro del informe se cargará en la base de datos correspondiente con un número de referencia de suceso asignado.

2.4 El estado de cada informe se categorizará y actualizará de la siguiente forma:

a) Notificación inicial: para evaluación/seguimiento/información como se anotó.

b) Bajo investigación: investigación del [autoridad de investigación de accidentes/CAA/proveedor de servicios] en progreso como se anotó.

c) Investigación completada: resultados/datos de la investigación recibidos y actualizados.

d) Cerrado: sin medidas posteriores necesarias.

Nota.— La notificación y envío de informes de datos de accidentes e incidentes graves a la OACI es responsabilidad de [Nombre de la autoridad de investigación de accidentes].

[*Comentario:* los Estados con múltiples autoridades y responsabilidades de la regulación de la seguridad operacional (por ejemplo, la CAA, autoridad de investigación de accidentes) deben establecer una coordinación adecuada y accesibilidad a la base de datos].

3. CLASIFICACIÓN DE ACCIDENTE/INCIDENTE GRAVE/INCIDENTE

3.1 La clasificación de accidente, incidente grave y otro tipo de incidente se basará en las definiciones del Anexo 13 de la OACI.

3.2 Los sucesos que se clasifican como accidentes o incidentes graves pueden requerir investigaciones independientes de [Nombre de la autoridad de investigación de accidentes]. En tales casos, el representante asignado de la CAA rastrea los resultados del proceso de investigación independiente y proporciona actualizaciones a [Nombre de la base de datos de CAA], según sea necesario.

3.3 Para los incidentes y otros sucesos (como defectos/malfuncionamientos/dificultades de servicio) que no son el objeto del proceso de investigación independiente del Estado, el representante asignado de la CAA se vinculará con la parte pertinente para la investigación de seguimiento y envío del informe necesario, según corresponda.

4. SEGUIMIENTO/INVESTIGACIÓN

4.1 Para los sucesos que requieren de medidas de seguimiento o la investigación de la función de seguridad operacional/calidad del proveedor de servicios, el representante pertinente de la CAA se vinculará con el representante autorizado de seguridad operacional/calidad del proveedor de servicio para garantizar el seguimiento y cierre oportunos del suceso, según corresponda.

4.2 El representante asignado de la CAA controla y determina si es necesario la intervención de la CAA antes, durante o después del proceso de investigación y resolución interna de sucesos del proveedor de servicios.

4.3 Al terminar y recibir el informe de seguimiento/investigación, el representante de la CAA ingresa toda la información pertinente recibida en la base de datos pertinente. En caso de informes de investigación emitidos por [Nombre de la autoridad de investigación de accidentes], el representante de la CAA se vincula con esa autoridad para la carga necesaria de tales informes de datos a la base de datos.

4.4 Donde se considere necesaria la medida administrativa (cumplimiento) de la CAA después de la conclusión de un informe de investigación de suceso, el inspector pertinente reenvía tales recomendaciones al DGAC para su aprobación, de acuerdo con la referencia xxx del procedimiento de cumplimiento de la CAA. En el caso de informes de investigación emitidos por [Nombre de la autoridad de investigación de accidentes], se debe considerar adecuadamente el objetivo de la investigación establecida en el Anexo 13.

ANEXO A

PARTE I. CRONOGRAMAS DE NOTIFICACIÓN (EJEMPLO)

	*Notificación a la CAA o a la autoridad de investigación de accidentes**	*Envío del informe obligatorio (Formulario XYZ) a la CAA o a la autoridad de investigación de accidentes***	*Informe de investigación a la CAA****
Accidente	Inmediato/lo antes posible	Dentro de 24 horas	90 días
Incidente grave	Inmediato/lo antes posible	Dentro de 48 horas	60 días
Incidente	N/A	Dentro de 72 horas	30 días (donde sea necesario)

* El teléfono, fax o correo electrónico constituirá, en la mayoría de los casos, los medios más adecuados y rápidos para enviar una notificación.
** Esta columna no se aplica a los miembros del público.
*** Esta columna no se aplica a los informes de investigación de la autoridad de investigación de accidentes del Estado.

PARTE II. EJEMPLOS DE SUCESOS QUE PUEDEN NOTIFICARSE

Nota.— La siguiente lista no es exhaustiva y no incluye accidentes.

Explotador aéreo

- cuasicolisión que requiere de una maniobra de prevención para evitar una colisión o situación insegura, o cuando una medida de prevención podría haber sido adecuada;

- vuelo controlado hacia tierra evitado solo de forma marginal;
- despegues interrumpidos en una pista cerrada u ocupada, en una calle de rodaje[1] o pista sin asignar;
- despegues desde una pista cerrada u ocupada, desde una calle de rodaje[1] o pista sin asignar;
- aterrizajes o intento de aterrizaje en una pista cerrada u ocupada, en una calle de rodaje[1] o pista sin asignar;
- falla total para lograr el performance predicho durante el despegue o ascenso inicial;
- incendios y humo en el compartimiento de pasajeros o de cargamento, o incendios del motor, incluso si tales incendios se extinguieron con agentes extintores;
- eventos que requieren el uso de emergencia de oxígeno por parte de la tripulación de vuelo;
- averías estructurales de la aeronave o desintegraciones del motor, como averías del motor de la turbina no contenidas, no clasificadas como un accidente;
- malfuncionamiento múltiple de uno o más sistemas de aeronaves que afectan gravemente la operación de la aeronave;
- incapacitación en vuelo de la tripulación de vuelo;
- cantidad de combustible que requiere que el piloto declare una emergencia;
- incursiones en la pista clasificadas con gravedad A. El *Manual sobre la prevención de incursiones en la pista* (Doc 9870) contiene información sobre las clasificaciones de gravedad;
- incidentes en el despegue o aterrizaje como entrada corta, prolongación de la pista o salir por los lados de la pista;
- averías del sistema, fenómenos climáticos, operaciones fuera del envolvente de vuelo aprobado u otros sucesos que podrían haber causado dificultades al controlar la aeronave;
- averías de más de un sistema en un sistema de redundancia obligatorio para la guía y navegación de vuelo;
- [*Comentario:* incluir cualquier otro incidente o suceso que puede ser notificado por el Estado bajo este sistema de notificación obligatoria].

Organización de mantenimiento

- cualquier defecto/malfuncionamiento/daño a células de aeronave, motores, hélices, componentes o sistemas encontrados durante las actividades de mantenimiento (células de aeronave, motores, componentes) programadas o no programadas de la aeronave, que pueden generar un accidente operacional o incidente grave de la aeronave (si no se rectifica oportunamente);
- [*Comentario:* incluir cualquier otro incidente o suceso que puede ser notificado por el el Estado bajo este sistema de notificación obligatoria].

1. Exclusión de operaciones autorizadas de los helicópteros.

Organizaciones de diseño y fabricación

- cualquier deficiencia, defecto o malfuncionamiento relacionado con el diseño o la fabricación de productos o servicios, encontrados por la organización de diseño/fabricación, o informados a esta, que se considera que garantiza el posible problema de una directriz de aeronavegabilidad de emergencia (EAD), directriz de aeronavegabilidad (AD) o boletín de servicio de alerta (ASB);

- [*Comentario:* incluir cualquier otro incidente o suceso que puede ser notificado por el Estado bajo este sistema de notificación obligatoria].

Explotador del aeródromo

- incursión en la pista (sin implicación de ATC);

- excursión en la pista/aterrizaje largo (sin implicación de ATC);

- avería o malfuncionamiento importante de la iluminación del aeropuerto;

- daños a la aeronave o el motor, que generan el contacto o ingestión de objetos extraños o suciedad en la pista o calle de rodaje;

- incidentes dentro del límite del aeródromo que implican daños a la aeronave o con posible impacto en la seguridad operacional del movimiento en la superficie de la aeronave;

- [*Comentario*: incluir cualquier otro incidente o suceso considerado que puede ser notificado por el Estado bajo este sistema de notificación obligatoria].

Proveedor de ANS/CNS

- cualquier defecto, malfuncionamiento o daño del equipo o sistema relacionado con ANS/CNS, descubierto durante la operación o el mantenimiento del equipo, que podría generar un accidente operacional o incidente grave de la aeronave;

- entrada no autorizada de espacio aéreo;

- cuasi CFIT de la aeronave;

- incidentes de salidas de nivel de suelo importantes;

- incidentes de pérdida de separación;

- incursión en la pista (implica las comunicaciones de ATC);

- excursión/aterrizaje largo en la pista (implica las comunicaciones de ATC);

- cualquier otra deficiencia, defecto o malfuncionamiento relacionados con ANS, notificado al explotador de ANS/CNS (y verificado por este) y que se considere que tiene un impacto en la seguridad operacional de la navegación aérea;

- [*Comentario:* incluir cualquier otro incidente o suceso que puede ser notificado por el Estado bajo este sistema de notificación obligatoria].

Nota.— Donde existan otros sistemas de notificación obligatoria específica del sector o del proveedor de servicios dentro de un Estado, según el Anexo 8, Parte II, 4.2.3 f) y 4.2.4 (notificación continua de aeronavegabilidad), puede que se deba abordar la correlación o integración necesarias con este procedimiento de notificación obligatoria relacionado con SSP a nivel del Estado.

Apéndice 4 del Capítulo 4

INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DEL SSP

1. Las Tablas 4-A4-1 a 4-A4-4 (ejemplos de indicadores de seguridad operacional) proporcionan ejemplos ilustrativos de los indicadores de rendimiento en materia de seguridad operacional (SPI) colectivos del Estado y sus criterios de configuración de alertas y objetivos correspondientes. Los SPI del SMS en el lado derecho de las tablas aparecen para indicar la correlación necesaria entre los indicadores de seguridad operacional del SSP y el SMS. El Estado puede compilar dicha tabla de resumen y se podrá completar de acuerdo con la mayor cantidad de indicadores de seguridad operacional existentes o viables como sea posible. Los proveedores de servicios deberán desarrollar los SPI del SMS en relación con las expectativas de los indicadores de seguridad operacional del SSP del Estado. Para garantizar la congruencia entre los indicadores de SSP y SMS, el Estado deberá hacer participar activamente a los proveedores de servicios en el desarrollo de los SPI del SMS. Se puede esperar que los SPI del SMS sean más integrales que los indicadores de seguridad operacional del SSP. A partir de este banco de indicadores de seguridad operacional, el Estado puede seleccionar un paquete adecuado de indicadores para el propósito de control y medición del ALoSP de su SSP. Es posible que ciertos indicadores de seguridad operacional/calidad se hayan mantenido (por el Estado o los proveedores de servicios) para propósitos complementarios y, por tanto, no necesitan incluirse para propósitos de control y medición del nivel del SSP (o el SMS). Por lo general, estos serían indicadores de nivel inferior o específicos de otros procesos dentro de la organización.

2. La Tabla 4-A4-5 (ejemplo de un diagrama del indicador de seguridad operacional del SSP) es un ejemplo de cómo luce un diagrama del indicador de rendimiento en materia de seguridad operacional de alto impacto del SSP. En este caso, es el conjunto de todas las tasas de incidentes con notificación obligatoria de los explotadores del Estado. El diagrama de la izquierda es el rendimiento del año anterior, mientras que el diagrama de la derecha es la tendencia de datos progresiva del año actual. La configuración del nivel de alerta se basa en criterios de desviación estándar de la métrica de seguridad operacional básica. La fórmula de la hoja de cálculo Excel es “=STDEVP”. Para propósitos del cálculo de desviación estándar manual, la fórmula es:

$$\sigma = \sqrt{\frac{\Sigma\,(x-\mu)^2}{N}}$$

donde “X” es el valor de cada punto de datos, “N” es el número de puntos de datos y “μ” es el valor promedio de todos los puntos de datos.

3. La configuración de objetivos es una mejora porcentual deseada (en este caso el 5%) en el promedio del punto de datos del año anterior. Se debe considerar que el intervalo de punto de datos real y el denominador de la tasa de sucesos se deberán determinar según la naturaleza de cada conjunto de datos, para garantizar la viabilidad del indicador de seguridad operacional. Por ejemplo, para los sucesos de muy baja frecuencia, el intervalo del punto de datos tendría que ser una actualización anual en lugar de trimestral. De igual forma, el denominador de la tasa de sucesos, por ejemplo, tendría que ser cada 100 000 movimientos aéreos en lugar de cada 1 000 movimientos aéreos. Este diagrama se genera con la hoja de datos de la Tabla 4-A4-6.

4. La hoja de datos de la Tabla 4-A6 (hoja de datos para muestra de un diagrama del indicador de seguridad operaciona) se usa para generar el diagrama del indicador de seguridad operacional que aparece en la Tabla 4-A4-5. Lo mismo puede usarse para generar cualquier otro diagrama del indicador de seguridad operacional con la entrada de datos adecuada y la personalización del descriptor del indicador de seguridad operacional. Las tres líneas de alerta y líneas de objetivos se generan automáticamente según la configuración respectiva en esta hoja de datos.

5. La Tabla 4-A4-7 (ejemplo de un resumen del rendimiento de ALoSP del SSP) es un resumen de todos los indicadores de seguridad operacional del SSP del Estado, con sus resultados respectivos del nivel de alertas y objetivos anotados. Tal resumen podrá compilarse al final de cada período de control para proporcionar una descripción general del rendimiento de ALoSP del SSP. Si se desea una medición del resumen del rendimiento más cuantitativa, se pueden asignar puntos adecuados para cada respuesta Sí/No por cada resultado de objetivos y alertas. Por ejemplo:

Indicadores de alto impacto:

Nivel de alerta no violado	[Sí (4), No (0)]
Objetivo alcanzado	[Sí (3), No (0)]

Indicadores de bajo impacto:

Nivel de alerta no violado	[Sí (2), No (0)]
Objetivo alcanzado	[Sí (1), No (0)]

Gracias a esto se puede obtener una puntuación (o porcentaje) de resumen para indicar el rendimiento general de los indicadores de seguridad operacional de ALoSP al final de cualquier período de control determinado.

Tabla 4-A4-1. Indicadores de rendimiento en materia de seguridad operacional para los explotadores aéreos

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores aéreos (solo explotadores aéreos del Estado)											
Tasa de accidentes/ incidentes graves mensual/trimestral del explotador aéreo colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador aéreo colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa de incidentes graves mensual de la flota individual del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes mensual de la flota combinada del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
Tasa de incidentes de IFSD trimestral del motor del explotador aéreo colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la inspección de la estación de línea del explotador aéreo colectivo de CAA (hallazgos por inspección)	Consideración	Consideración	Tasa de incidentes graves mensual de la flota combinada del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador (hallazgos por auditoría)	Consideración	Consideración
			% de LEI promedio anual de la inspección de vigilancia de la plataforma del explotador aéreo extranjero de CAA (para cada explotador extranjero)	Consideración	Consideración	Tasa de incidentes de IFSD del motor del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros voluntario del explotador (por ejemplo, cada 1 000 FH)	Consideración	Consideración
			Tasa del informe de incidentes de DGR del explotador colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa del informe de incidentes de DGR del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
etc.											

Tabla 4-A4-2. Indicadores de rendimiento en materia de seguridad operacional para los explotadores de aeródromos

Indicadores de rendimiento en materia de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores de aeródromos											
Tasa de incidentes graves/ accidentes en tierra mensual/ trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador del aeródromo colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa de incidentes graves/accidentes en tierra trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador del aeródromo (hallazgos por auditoría)	Consideración	Consideración
Tasa de incidentes en la excursión en pista mensual/ trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa de incidentes en la excursión en pista trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros de objetos extraños/suciedad trimestral del explotador del aeródromo (por ejemplo, cada 10.000 movimientos en tierra)	Consideración	Consideración
Tasa de incidentes en la incursión en pista mensual/ trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa de incidentes en la incursión en pista trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros voluntario del explotador (por personal de operaciones por trimestre)	Consideración	Consideración

Indicadores de rendimiento en materia de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
									Tasa trimestral del informe de incidentes de daños por objetos extraños en la aero-nave del explotador del aeródromo — Implica daños a la aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
etc.											

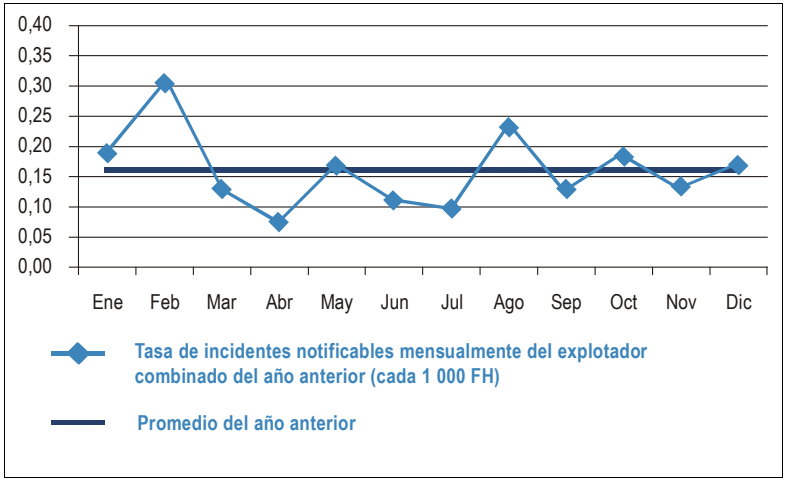
Tabla 4-A4-3. Indicadores de rendimiento en materia de seguridad operacional para los explotadores de ATS

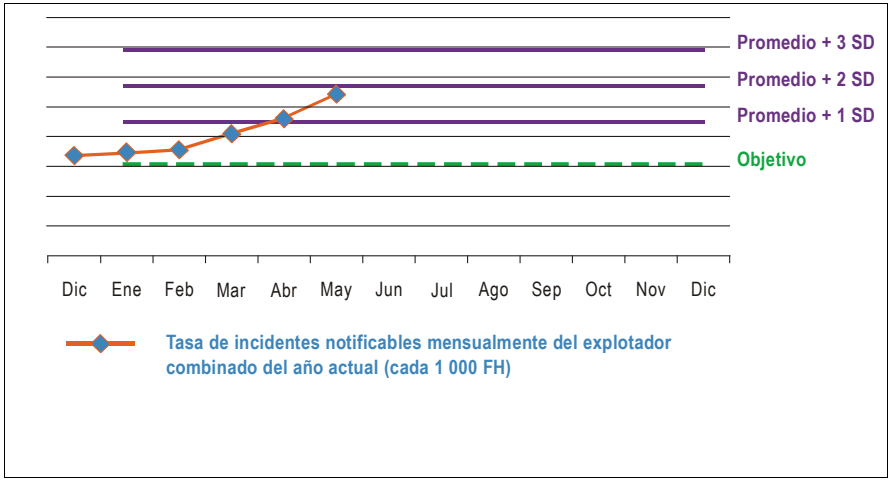
Indicadores de rendimiento en materia de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores de ATS											
Tasa de incidentes graves (espacio aéreo) de FIR trimestral de ATS colectivos de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes trimestral del RA de los TCAS de la FIR de ATS colectivos de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes graves de FIR trimestral del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes trimestral del RA de los TCAS de la FIR del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
			Tasa de incidentes trimestral (LOS) de salidas de nivel de suelo de FIR de ATS colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes de cuasicolisión trimestral/anual del explotador de ATS (por ejemplo, cada 100 000 movimientos en vuelo)	Suponiendo que el promedio anual histórico es 3, la tasa de alerta posible podría ser 5.	Suponiendo que el promedio anual histórico es 3, la tasa de objetivo posible podría ser 2.	Tasa de incidentes trimestral (LOS) de salidas de nivel de suelo de FIR del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
			Tasa de% o hallazgos de LEI anual de la auditoría de vigilancia del explotador de ATS colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración				Tasa de% o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador de ATS (hallazgos por auditoría)	Consideración	Consideración
etc.											

Tabla 4-A4-4. ORGANIZACIONES DE POA/DOA/MRO

Indicadores de rendimiento en materia de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Organizaciones de DOA/POA/MRO											
Informes obligatorios de defectos (MDR) trimestrales de la MRO colectiva de CAA recibidos	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia de MRO/POA/DOA colectivas de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa trimestral de MRO/POA de reclamos de la garantía técnica de los componentes	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna de MRO/POA/DOA (hallazgos por auditoría)	Consideración	Consideración
Tasa trimestral de POA/DOA colectiva de CAA de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración				Tasa trimestral de POA/DOA de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración	Tasa de averías/rechazos trimestral de la inspección final/pruebas de MRO/POA/DOA (debido a problemas de calidad interna)	Consideración	Consideración
						Tasa trimestral de MRO/POA de los informes obligatorios/ importantes de defectos de componentes emitidos (debido a problemas de calidad interna)	Consideración	Consideración	Tasa de informes de peligros voluntarios de MRO/POA/DOA (por personal de operaciones por trimestre)	Consideración	Consideración
etc.											

Tabla 4-A4-5. Ejemplo de un diagrama del indicador de rendimiento en materia de seguridad operacional del SSP (con la configuración del nivel de alerta y objetivo)





a) Configuración de nivel de alerta:

El nivel de alerta de un nuevo período de control (año actual) se basa en el rendimiento del período anterior (año anterior), es decir, su promedio de datos y desviación estándar. Las tres líneas de alerta son el promedio + 1 SD, promedio + 2 SD y promedio + 3 SD.

b) Activador del nivel de alerta:

Se indica una alerta (tendencia anormal/inaceptable) si cualquiera de las siguientes condiciones se cumple en el período de control actual (año actual):

— cualquier punto único está sobre la línea 3 SD
— 2 puntos consecutivos están sobre la línea 2 SD
— 3 puntos consecutivos están sobre la línea 1 SD.

Cuando se activa una alerta (posible situación de alto riesgo o fuera de control), se espera una medida de seguimiento correspondiente, como un análisis posterior para determinar la fuente y causa de origen de la tasa de incidente anormal y cualquier medida necesaria para abordar la tendencia inaceptable.

c) Configuración del nivel de objetivo (mejora planificada):

La configuración del nivel de objetivo puede estar menos estructurada que la configuración del nivel de alerta, por ejemplo, tenga como objetivo la nueva tasa promedio del período de control (año actual) para que indique ser un 5% inferior (mejor) que el valor promedio del período anterior.

d) Logro del objetivo:

Al final del año actual, si la tasa promedio del año actual es inferior en al menos un 5% o más que la tasa promedio del año anterior, el objetivo establecido de 5% de mejora se considera como logrado.

e) Niveles de alerta y objetivo — Período de validez:

Los niveles de alerta y objetivo deben revisarse/restablecerse para cada nuevo período de control, según la tasa promedio y SD del período anterior equivalente, según corresponda.

Tabla 4-A4-6. Hoja de datos de muestra usada para generar un diagrama de alto impacto del indicador de seguridad operacional del SSP (con criterios de la configuración de alerta y objetivo)

Mes	*Todo el FH total del explotador*	*Todos los incidentes del explotador*	*Tasa de incidentes**	*Promedio*
Enero	51 837	10,00	0,19	0,16
Febrero	48 406	15,00	0,31	0,16
Marzo	53 354	7,00	0,13	0,16
Abril	52 513	4,00	0,08	0,16
Mayo	54 037	9,00	0,17	0,16
Junio	52 673	6,00	0,11	0,16
Julio	54 086	5,00	0,09	0,16
Agosto	54 043	13,00	0,24	0,16
Septiembre	52 383	7,00	0,13	0,16
Octubre	53 042	10,00	0,19	0,16
Noviembre	51 353	7,00	0,14	0,16
Diciembre	53 006	9,00	0,17	0,16
		Promedio	0,16	
		SD	0,06	

Promedio + 1 SD	Promedio + 2 SD	Promedio + 3 SD
0,23	0,29	0,35

Los criterios de configuración del nivel de alerta del año actual se basan en el año anterior (Promedio + 1/2/3 SD)

	Año actual						
Mes	*Todo el FH total del explotador*	*Todos los incidentes del explotador*	*Tasa de incidentes**	*Promedio del año anterior + 1 SD*	*Promedio del año anterior + 2 SD*	*Promedio del año anterior + 3 SD*	*Promedio del objetivo del año actual*
Diciembre	53 006	9,00	0,17				
Enero	51 635	9,00	0,17	0,23	0,29	0,35	0,15
Febrero	44 295	8,00	0,18	0,23	0,29	0,35	0,15
Marzo	48 323	10,00	0,21	0,23	0,29	0,35	0,15
Abril	47 176	11,00	0,23	0,23	0,29	0,35	0,15
Mayo	47 469	13,00	0,27	0,23	0,29	0,35	0,15
Junio				0,23	0,29	0,35	0,15
Julio				0,23	0,29	0,35	0,15
Agosto				0,23	0,29	0,35	0,15
Septiembre				0,23	0,29	0,35	0,15
Octubre				0,23	0,29	0,35	0,15
Noviembre				0,23	0,29	0,35	0,15
Diciembre				0,23	0,29	0,35	0,15
		Promedio					
		SD					

El objetivo del año actual indica una tasa de mejora promedio del 5% sobre la tasa promedio del año anterior, la que es:	0,15

* Cálculo de la tasa (cada 1 000 FH).

Tabla 4-A4-7. Ejemplo de resumen de ALoSP del SSP del Estado "X" (digamos, para el año 2010)

Indicadores de seguridad operacional de bajo impacto					
Descripción de SI		*Criterios del nivel de alerta de SI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios del nivel de objetivo de SI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Tasa de incidentes graves/ accidentes mensual del explotador aéreo colectivo de CAA (cada 1 000 FH)	Tasa promedio de 2009 + 1/2/3 SD (restablecimiento anual)	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No
2	Tasa de incidentes graves/accidentes en tierra mensual del aeródromo colectivo de CAA — Implica cualquier aeronave (cada 10.000 movimientos en tierra)	Tasa promedio de 2009 + 1/2/3 SD (restablecimiento anual)	Sí	3% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
3	Tasa de incidentes graves mensual de FIR de los ATS de CAA — Implica cualquier aeronave (cada 100.000 movimientos aéreos)	Tasa promedio de 2009 + 1/2/3 SD (restablecimiento anual)	No	4% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No

Indicadores de seguridad operacional de bajo impacto					
Descripción de SI		*Criterios del nivel de alerta de SI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios del nivel de objetivo de SI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Resultados de la vigilancia/auditoría anual de la organización del explotador aéreo colectivo de CAA	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	Sí	Menos del 10% del LEI promedio y menos de 1 hallazgo de Nivel 2 por auditoría	No
2	% de LEI promedio anual de la inspección de vigilancia de la estación de línea del explotador aéreo de CAA (para cada explotador)	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	Sí	Menos del 10% de LEI promedio	Sí
3	Programa de inspección anual de muestreo de la plataforma del explotador aéreo extranjero de CAA	Más del 25% de LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría o menos del 25% de los explotadores extranjeros inspeccionados	Sí	No menos del 50% de los explotadores extranjeros por inspeccionar	No
4	Resultados de la vigilancia/auditoría anual de la organización del explotador de aeródromo colectivo de CAA	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	No	Menos del 10% del LEI promedio y menos de 1 hallazgo de Nivel 2 por auditoría	No

Indicadores de seguridad operacional de bajo impacto					
Descripción de SI		*Criterios/nivel de alerta de SI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios/nivel de objetivo de SI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Resultados de la vigilancia/auditoría anual de la organización del explotador de ATS colectivo de CAA	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	Sí	Menos del 10% del LEI promedio y menos de 1 hallazgo de Nivel 2 por auditoría	Sí
2	Tasa de incidentes trimestral del RA de los TCAS de la FIR de ATS colectivos de CAA — Implica cualquier aeronave (cada 100.000 movimientos en vuelo)	Tasa promedio de 2009 + 1/2/3 SD (restablecimiento anual)	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No
3	Resultados de la vigilancia/auditoría anual de D&M/MRO colectivo de CAA	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	Sí	Menos del 10% del LEI promedio y menos de 1 hallazgo de Nivel 2 por auditoría	Sí
4	Tasa trimestral de AMO (MRO) colectivo de CAA de los reclamos de la garantía de componentes debido a defectos técnicos (importantes)	Tasa promedio de 2009 + 1/2/3 SD (restablecimiento anual)	No	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No

Nota 1.— Otros indicadores del proceso. Además de los indicadores de seguridad operacional del nivel de SSP mencionado anteriormente, puede que haya otros indicadores del nivel de sistema dentro de cada área operacional. Entre los ejemplos se incluyen indicadores de control específicos del proceso o del sistema en AIR, OPS o AGA, o indicadores asociados con programas basados en performance, como la gestión de riesgos por fatiga o la gestión de combustible. Tales indicadores específicos del proceso o del sistema deben administrarse correctamente como parte del sistema o proceso de interés. Pueden verse como indicadores de nivel específicos del sistema o proceso, lo que afianza los indicadores de seguridad operacional de control de mayor nivel del SSP. Deben abordarse dentro de los manuales/SOP del sistema o proceso respectivos, según corresponda. Sin embargo, los criterios para configurar los niveles de alertas u objetivos para tales indicadores deben, de preferencia, alinearse con aquellos de los indicadores de seguridad operacional del nivel de SSP, donde corresponda.

Nota 2.— Selección de indicadores y configuración. El Estado debe seleccionar la combinación (o paquete) de indicadores de seguridad operacional de alto y bajo impacto, de acuerdo con el alcance de su sistema de aviación. Para aquellos indicadores donde los criterios sugeridos de la configuración del nivel de alerta u objetivo no sean aplicables, el Estado puede considerar cualquier criterio alternativo, según corresponda. La guía general es configurar las alertas y los objetivos que consideran el performance reciente histórico o actual.

Apéndice 5 del Capítulo 4

PROTECCIÓN DE LA INFORMACIÓN DE LA SEGURIDAD OPERACIONAL

1.1 El excepcional registro de seguridad operacional de la aviación civil internacional se debe, entre otros, a un factor clave: un proceso de aprendizaje continuo basado en el desarrollo e intercambio libre de información de seguridad operacional. Por mucho tiempo se ha reconocido que las actividades orientadas a mejorar la seguridad operacional de la aviación civil contemporánea deben basarse en datos objetivos. Existen muchas fuentes de dichos datos disponibles en la aviación civil. En combinación, proporcionan la base de una sólida comprensión de fortalezas y debilidades de las operaciones de aviación.

1.2 De manera histórica, la información de las investigaciones de accidentes e incidentes han formado la columna vertebral de las actividades orientadas a mejorar el diseño del equipo, los procedimientos de mantenimiento, la capacitación de la tripulación de vuelo, los sistemas de control de tránsito aéreo, el diseño y las funciones del aeródromo, los servicios meteorológicos y otros aspectos fundamentales para la seguridad operacional del sistema de transporte aéreo. En los últimos años, la disponibilidad de los medios tecnológicos ha generado un desarrollo acelerado de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS).

1.3 Los SDCPS han permitido que la comunidad de la aviación civil obtenga una comprensión más profunda de los errores operacionales: por qué ocurren, qué puede hacerse para minimizar su ocurrencia y cómo contener su impacto negativo en la seguridad operacional. No hay duda de que los peligros generan errores operacionales en la aviación, siendo accidentales la gran mayoría de estos. Las personas bien capacitadas y bien intencionadas cometen errores mientras realizan mantenimiento, operan o controlan equipo bien diseñado. Para aquellas situaciones extrañas donde los actos considerados, según la ley, como conductas con intención para causar daño o conductas con conocimiento de que podría generarse un daño, equivalentes a conducta imprudente, negligencia grave o conducta impropia deliberada, los sistemas de cumplimiento implementados garantizan que la cadena de responsabilidad permanezca intacta. Este enfoque doble, que combina la comprensión mejorada de errores operacionales accidentales con el cumplimiento adecuado de la ley mediante la autoridad correspondiente, donde corresponda, ha servido bien a la aviación civil en términos de seguridad operacional, mientras garantiza que no se da asilo a los infractores.

1.4 Sin embargo, en años recientes se ha demostrado una tendencia en la aviación civil, cuando se trata con errores operacionales que generan sucesos, que señala que se ha usado información del SDCPS para propósitos disciplinarios y de cumplimiento. En algunos casos, también se ha admitido como evidencia en procesos judiciales, lo que ha generado en cargos penales en contra de las personas involucradas en tales sucesos. Presentar cargos penales en los sucesos de aviación que se produzcan por errores operacionales accidentales pueden entorpecer la notificación eficaz de tales eventos, lo que, por tanto, evita el desarrollo e intercambio libre de información de seguridad operacional que es fundamental para mejorar la seguridad operacional de la aviación.

1.5 Varias iniciativas dentro de la comunidad de la aviación civil internacional han intentado abordar la protección del SDCPS. Sin embargo, dada la sensibilidad del asunto actual, es fundamental contar con un marco de trabajo que ofrezca la unidad de los propósitos y coherencia en los esfuerzos de la comunidad de aviación civil. Los esfuerzos para garantizar la protección de la información de la seguridad operacional deben llegar a un equilibrio muy delicado entre la necesidad de proteger la información de la seguridad operacional, la necesidad de control de calidad, la necesidad de gestión de riesgos de la seguridad operacional y la aplicación adecuada de la justicia. Se debe tomar

un enfoque precavido acerca de esto para evitar hacer propuestas que puedan ser incompatibles con las leyes relacionadas con la aplicación de la justicia en los Estados contratantes.

1.6 Para abordar este tema, la OACI desarrolló el Adjunto E del Anexo 13, el que proporciona una guía legal para ayudar a que los Estados promulguen leyes y reglamentos nacionales para proteger la información reunida del SDCPS, mientras se permite la correcta aplicación de la justicia. El objetivo es evitar el uso inadecuado de la información recopilada solamente para mejorar la seguridad operacional de la aviación. Al considerar que los Estados deben tener la flexibilidad de redactar sus leyes y reglamentos de acuerdo con las políticas y prácticas nacionales, la guía legal toma la forma de la siguiente serie de principios que puedan adaptarse para satisfacer las necesidades particulares del Estado al promulgar leyes y reglamentos para proteger la información de la seguridad operacional.

1.7 La guía legal incluye principios generales que señalan que:

a) el único propósito de la protección de la información de seguridad operacional contra el uso incorrecto es garantizar su disponibilidad continua para que se puedan tomar medidas preventivas adecuadas y oportunas y se pueda mejorar la seguridad operacional de la aviación;

b) el propósito de la protección de la información de seguridad operacional no es interferir con la correcta aplicación de la justicia en los Estados;

c) las leyes y los reglamentos nacionales que protegen a la información de seguridad operacional deben garantizar que se llegue a un equilibrio entre la necesidad de protección de la información de seguridad operacional para mejorar la seguridad operacional de la aviación, y la necesidad de la correcta aplicación de la justicia;

d) las leyes y los reglamentos nacionales que protegen la información de la seguridad operacional deben evitar su uso inadecuado; y

e) proporcionar protección a la información de seguridad operacional calificada según las condiciones especificadas, es parte de las responsabilidades de seguridad operacional de un Estado.

1.8 La guía incluye los siguientes principios de protección:

a) la información de la seguridad operacional debe calificar para la protección contra el uso incorrecto de acuerdo con condiciones especificadas que deben incluir, entre otros, que: la recopilación de la información se llevó a cabo para propósitos de seguridad operacional explícita y la divulgación de la información inhibiría su disponibilidad continuada;

b) la protección debe ser específica para cada SDCPS, según la naturaleza de la información de la seguridad operacional que contiene;

c) un procedimiento formal debe establecerse para proporcionar protección para la información de seguridad operacional calificada, de acuerdo con las condiciones especificadas;

d) la información de seguridad operacional no debe usarse para fines distintos para los que fue recopilada; y

e) el uso de información de seguridad operacional en procesos disciplinarios, civiles, administrativos y penales se llevará a cabo solo bajo resguardos adecuados.

1.9 Las siguientes son circunstancias recomendadas donde la información de seguridad operacional podría no calificar para incluirse en la protección:

a) existe evidencia de que el suceso se originó por un acto considerado, de acuerdo con la ley, como conducta con intención para causar daño o conductas con conocimiento de que podría generarse un daño, equivalentes a conducta imprudente, negligencia grave o conducta impropia deliberada;

b) una autoridad considera que las circunstancias indican razonablemente que el suceso puede haberse originado por una conducta con intención para causar daño o conductas con conocimiento de que podría generarse un daño, equivalentes a conducta imprudente, negligencia grave o conducta impropia deliberada; o

c) la revisión de una autoridad adecuada determina que la comunicación de la información de seguridad operacional es necesaria para la correcta aplicación de la justicia y que su comunicación supera con creces el impacto adverso doméstico o internacional que tal comunicación podría tener en la futura disponibilidad de la información de la seguridad operacional.

1.10 La guía también aborda el tema de divulgación pública, la que propone que, al estar sujeta a los principios de protección y excepción descritos anteriormente, cualquier persona que busque la divulgación de la información de la seguridad operacional debe justificar su comunicación. Se deben establecer criterios formales para la divulgación de la información de la seguridad operacional y esta debe incluir, entre otros, lo siguiente:

a) la divulgación de la información de la seguridad operacional es necesaria para corregir las condiciones que componen la seguridad operacional o para cambiar las políticas y reglamentos;

b) la divulgación de la información de la seguridad operacional no inhibe su futura disponibilidad para mejorar la seguridad operacional;

c) la divulgación de información personal pertinente incluida en la información de seguridad operacional cumple con las leyes de privacidad correspondientes; y

d) la divulgación de la información de la seguridad operacional se hace de forma no identificada, resumida o colectiva.

1.11 La guía aborda la responsabilidad del custodio de la información de seguridad operacional, que propone que cada SDCPS debe tener un custodio designado. Es responsabilidad del custodio de la información de la seguridad operacional aplicar toda la protección posible sobre la divulgación de la información, a menos que:

a) el custodio de la información de la seguridad operacional tenga el consentimiento del originador de la información para su divulgación; o

b) el custodio de la información de la seguridad operacional está satisfecho con que la comunicación de la información de seguridad operacional está de acuerdo con los principios de excepción.

1.12 Por último, la guía presenta la protección de la información registrada y, al considerar que las grabaciones ambientales del lugar de trabajo necesarias según la legislación, como los registradores de la voz en el puesto de pilotaje (CVR), pueden percibirse como si constituyeran una invasión de la privacidad del personal de operaciones a la que otras profesiones no están expuestas, propone que:

a) sujeto a los principios de protección y excepción anteriores, las leyes y los reglamentos nacionales deben considerar a las grabaciones ambientales del lugar de trabajo necesarias según la legislación como información protegida privilegiada, es decir, información que merece una protección mejorada; y

b) las leyes y los reglamentos nacionales deben proporcionar medidas específicas de protección a dichas grabaciones en cuanto a su confidencialidad y acceso para el público. Tales medidas específicas de protección de las grabaciones del lugar de trabajo necesarias según la legislación pueden incluir la emisión de órdenes de divulgación no pública.

1.13 Aunque la guía para la protección de SDCPS se adoptó como un adjunto del Anexo 13 el 3 de marzo de 2006, la comunidad de aviación ha recomendado que la OACI realice otras actividades de progreso sobre la protección de los datos e información de seguridad operacional para garantizar su disponibilidad para la mejora de la seguridad operacional. Por lo tanto, durante su 37ª sesión, la Asamblea instruyó al Consejo para considerar mejorar las disposiciones de la protección de información de la seguridad operacional. El 7 de diciembre de 2010, la Comisión de Aeronavegación aprobó el establecimiento de la Safety Information Protection Task Force (SIP TF), la cual, el 5 de mayo de 2011, comenzó a trabajar en recomendaciones para las disposiciones y el material guía nuevos o mejorados relacionados con la protección de la información de la seguridad operacional.

Apéndice 6 del Capítulo 4

GUÍA SOBRE LA NOTIFICACIÓN E INFORMACIÓN DE ACCIDENTES E INCIDENTES

1. INTRODUCCIÓN

1.1 De acuerdo con el Anexo 13 — *Investigación de accidentes e incidentes de aviación*, se requiere que los Estados informen a la OACI la información sobre todos los accidentes de aeronaves que impliquen a aeroplanos de turborreactor o aeronaves que tengan una masa máxima de despegue certificada sobre los 2 250 kg. La organización también reúne información sobre incidentes de aeronaves considerados importantes para la seguridad operacional y la prevención de accidentes. Para facilitar la referencia, el término "suceso" incluye tanto a accidentes como a incidentes.

1.2 En toda esta guía, las normas del Anexo 13 se citan en un cuadro de texto gris.

2. ACCIDENTES E INCIDENTES — NOTIFICACIÓN E INFORMES

2.1 Generalidades

2.1.1 El sistema de notificación de datos sobre accidentes e incidentes (ADREP) de la OACI recopila datos de los Estados para mejorar la seguridad operacional mediante el análisis, ya sea con la validación de problemas de seguridad operacional conocidos o la identificación de tendencias de seguridad operacional emergentes, que produzcan recomendaciones para propósitos de prevención de accidentes .

2.1.2 Existen cuatro etapas diferentes en las cuales la información se envía a la OACI después de un suceso. Estas son:

a) notificación;

b) informe preliminar (ADREP);

c) informe final; y

d) informe de datos (ADREP).

Estas cuatro etapas se analizan con más detalle en las Secciones 2.2 a 2.5, y la Tabla 4-A6-1 muestra un resumen secuencial de una lista de verificación de notificación e información, de acuerdo con el Anexo 13, Adjunto B.

2.1.3 Para facilitar la notificación, los Estados pueden ahora usar el sitio del portal seguro en línea de la OACI para enviar notificaciones e informes ADREP mediante un formato electrónico o mediante un formato compatible con ADREP (por ejemplo, ECCAIRS). En 3 se proporciona una guía más detallada sobre los formatos -electrónicos de la OACI.

2.2 Notificación

Una notificación se usa para la distribución inmediata de información sobre accidentes e incidentes. Según el Anexo 13, Capítulo 4, la siguiente información debe enviarse a la OACI:

4.1 El Estado del suceso deberá reenviar la notificación de un accidente o incidente grave, con un mínimo de retraso y mediante los medios más adecuados y rápidos disponibles, al:

a) Estado de matrícula;

b) Estado del explotador;

c) Estado de diseño;

d) Estado de fabricación; y

e) la Organización de Aviación Civil Internacional, cuando la aeronave involucrada tiene una masa máxima de más de 2 250 kg o es un aeroplano de turborreactor.

Sin embargo, cuando el Estado de suceso no está consciente de un incidente grave, el Estado de matrícula o el Estado del explotador, según corresponda, deberá reenviar una notificación de tal incidente al Estado de diseño, al Estado de fabricación y al Estado de suceso.

. . .

4.2 La notificación deberá estar redactada de manera sencilla y contener toda la siguiente información que esté fácilmente disponible, pero su despacho no podrá retrasarse debido a la falta de información completa:

a) para los accidentes, la abreviatura identificadora ACCID, para los incidentes graves, INCID;

b) el fabricante, el modelo, la nacionalidad y las marcas de registro, y el número de serie de la aeronave;

c) el nombre del propietario, el explotador y el contratante, si existe, de la aeronave;

d) la calificación del piloto al mando y la nacionalidad de la tripulación y los pasajeros;

e) la fecha y hora (hora local o UTC) del accidente o incidente grave;

f) el último punto de salida y punto de aterrizaje previsto de la aeronave;

g) la posición de la aeronave en referencia a un punto geográfico fácilmente definido y latitud y longitud;

h) la cantidad de tripulación y pasajeros; a bordo, muertos o gravemente heridos; otros, muertos y gravemente heridos;

i) la descripción del accidente o incidente grave y el grado de daño conocido de la aeronave;

j) un indicio de hasta qué punto se realizará la investigación o se propone que delegue el Estado de suceso;

k) las características físicas del área del accidente o incidente grave, así como también, un indicio de dificultades de acceso o requisitos especiales para llegar al sitio;

l) la identificación de la autoridad originadora y los medios para comunicarse con el investigador a cargo y la autoridad de investigación de accidentes del Estado de suceso en cualquier momento; y

m) la presencia y descripción de mercancías peligrosas a bordo de la aeronave.

2.3 Informe preliminar

2.3.1 El informe preliminar es la comunicación usada para la rápida distribución de datos obtenidos durante las primeras etapas de la investigación. Es un informe i*nterino* que contiene información adicional que faltaba o no estaba disponible al momento de enviar la notificación. Los informes preliminares no son obligatorios para los incidentes. También puede encontrar la información necesaria que debe enviarse para un Informe preliminar en el sitio web http://www.icao.int/Safety/reporting.

2.3.2 El Anexo 13, Capítulo 7, 7.1 y 7.2, estipula:

Accidentes de aeronaves sobre 2 250 kg

7.1 Cuando la aeronave implicada en un accidente tiene una masa máxima de más de 2 250 kg, el Estado que realiza la investigación deberá enviar el Informe preliminar al:

a) Estado de matrícula o al Estado de suceso, según corresponda;

b) Estado del explotador;

c) Estado de diseño;

d) Estado de fabricación;

e) cualquier Estado que proporcionó información pertinente, instalaciones importantes o expertos; y

f) la Organización de Aviación Civil Internacional.

Accidentes en aeronaves de 2 250 kg o menos

7.2 Cuando una aeronave, no incluida en 7.1, está involucrada en un accidente y cuando se trate de la aeronavegabilidad o los asuntos considerados como de interés para otros Estados, el Estado que realiza la investigación deberá reenviar el Informe preliminar al:

a) Estado de matrícula o al Estado de suceso, según corresponda;

b) Estado del explotador;

c) Estado de diseño;

d) Estado de fabricación; y

e) cualquier Estado que proporcionó información pertinente, instalaciones importantes o expertos.

2.3.3 El Anexo 13, Capítulo 7, 7.4, estipula:

Despacho

7.4 El Informe preliminar deberá enviarse por fax, correo electrónico o correo aéreo dentro de 30 días a partir de la fecha del accidente a menos que el Informe de datos de accidentes/incidentes se haya enviado en ese período. Cuando existen asuntos que afectan directamente la seguridad operacional, se deberá enviar la información tan pronto como esté disponible y mediante los medios más adecuados y rápidos disponibles.

2.4 Informe final

2.4.1 El Anexo 13, Capítulo 6, 6.5 a 6.7, contiene las siguientes normas acerca del Informe final:

Comunicación del Informe final

6.5 En el interés de la prevención de accidentes, el Estado que realiza la investigación de un accidente o incidente deberá hacer el Informe final disponible públicamente lo antes posible y, si fuera posible, dentro de doce meses.

. . .

6.6 Si el informe no puede estar disponible públicamente dentro de doce meses, el Estado que realiza la investigación deberá dejar disponible una declaración interina públicamente en cada aniversario del suceso, detallando el progreso de la investigación y cualquier problema de seguridad operacional identificado.

6.7 Cuando el Estado que ha realizado una investigación en un accidente o incidente, que implique una aeronave de una masa máxima de más de 5 700 kg, ha comunicado un Informe final, el Estado deberá enviar a la Organización de Aviación Civil Internacional una copia del Informe final.

2.4.2 La guía detallada del formato, contenido y envío del Informe final se incluye en el *Manual de investigación de accidentes e incidentes de aviación* (Doc 9756), Parte IV — *Redacción de informes*.

2.5 Informe de datos

2.5.1 Cuando se ha completado la investigación y el Informe final se ha aprobado, se puede compilar un Informe de datos de accidentes o incidentes. Si se reabre una investigación, la información previamente informada debe enmendarse como corresponde. El propósito del Informe de datos es proporcionar información precisa y completa en un formato estándar.

2.5.2 Puede encontrar la información necesaria para completar el Informe de datos en el sitio web http://www.icao.int/Safety/reporting.

2.5.3 Además, el Anexo 13, Capítulo 7, 7.5, requiere:

Accidentes de aeronaves sobre 2 250 kg

7.5 Cuando la aeronave involucrada en un accidente tiene una masa máxima de más de 2.250 kg, el Estado que realiza la investigación deberá enviar, lo antes posible como sea práctico después de la investigación, el Informe de datos de accidentes a la Organización de Aviación Civil Internacional.

3. INSTRUCCIONES GENERALES PARA LA COMPILACIÓN

3.1 Opciones para notificar sucesos a la OACI

Los sucesos pueden informarse a la OACI mediante una de las siguientes opciones:

a) Administrador de informes de sucesos de la OACI disponible en el portal seguro de iSTARS en el sitio web http://www.icao.int/Safety;

b) un informe de la base de datos compatible de ADREP (por ejemplo, ECCAIRS);

c) informes en papel enviados a la OACI.

3.2 Administrador de informes de sucesos

El formulario de Notificación y del Informe preliminar de ADREP pueden ahora completarse de forma electrónica mediante el Administrador de informes de sucesos de la OACI disponible en el portal seguro de iSTARS. Los miembros de iSTARS pueden acceder a los formularios del Informe de suceso al visitar iSTARS y luego seguir el vínculo a las instrucciones de notificación de sucesos. Las nuevas inscripciones en el portal seguro de iSTARS pueden solicitar acceso mediante iSTARS en línea o mediante correo electrónico en adrep@icao.int.

3.3 Reglas básicas

La validez de la información de seguridad operacional que la OACI proporciona a los Estados depende del detalle y cuidado con que se informan los sucesos. Por tanto, es de particular interés para los Estados informar datos precisos y completos de acuerdo con el Anexo 13 y la guía de este manual. Algunas reglas básicas que puede seguir al completar el Formulario de notificación de accidentes e incidentes en línea de la OACI o el registro (por ejemplo, ECCAIRS) del formato compatible con ADREP del suceso son:

a) Determinar la clasificación y categorización de sucesos adecuada, es decir, si es un accidente, incidente grave o incidente, según el nivel de lesiones, daños a la aeronave y otra información disponible.

b) Completar los datos básicos como la fecha, hora, Estado y ubicación del suceso, aeropuerto, gravedad, tipo de aeronave, explotador, tipo de explotador y etapa de vuelo.

c) Elija las unidades de campo adecuadas antes de ingresar valores, por ejemplo, pies, MSL o FL para altitud.

d) Si más de una aeronave está implicada en un suceso, proporcione la información acerca de la otra aeronave. Cuando se ingresan tipos de eventos por más de una aeronave, asegúrese de seleccionar la aeronave adecuada (1 o 2). Todos los eventos deben estar en una secuencia de tiempo y se debe tener cuidado de no excluir eventos vitales.

e) Alinee los eventos con las categorías de sucesos.

f) Use entradas "Desconocidas" solo si se establece después de investigar que no se encontró la información.

g) Use entradas en "Blanco" para indicar que la investigación está en progreso para encontrar la información que actualmente no está disponible.

3.4 Notificaciones

3.4.1 En caso de emitir una notificación mediante el Administrador de informes de sucesos de iSTARS, toda la información necesaria, según el Anexo 13, Capítulo 4, 4.2, se incluye en los formularios de notificación electrónica, ahora disponibles en línea, y deben completarse según las instrucciones que aparecen en el formulario.

3.4.2 Ciertos campos en los formularios de notificación son identificadores clave que ayudarán a la OACI a identificar informes en la base de datos. Por lo tanto, en el caso de la emisión electrónica, estos campos deben completarse para enviar una notificación inicial. Estos campos son:

a) notificación del Estado;

b) número de archivo del Estado;

c) organización de notificación;

d) clase de suceso; y

e) fecha de suceso.

3.4.3 Cuando se ingresen los datos de suceso básicos, como el nivel de lesiones o el daño a la aeronave, se debe tener cuidado de alinear estas selecciones con la clase de suceso. Por ejemplo, si el suceso se clasificó como un "accidente", entonces el nivel de lesión debe ser grave, fatal o desconocido, y el daño a la aeronave debe ser importante, destruido o desconocido.

3.5 Taxonomía de ADREP

La OACI desarrolló la taxonomía de ADREP y contiene definiciones y terminología para los sistemas de notificación de accidentes e incidentes de la aviación. Los documentos de taxonomía están disponibles en http://www.icao.int/Safety/reporting y deben consultarse cada vez que tenga dudas sobre la terminología de los formularios de notificación e informes.

3.6 Despacho de los informes

3.6.1 Cuando tenga información del suceso disponible en un formato compatible con ADREP (por ejemplo, formato ECCAIRS), se debe adjuntar una copia del archivo electrónico (por ejemplo, .E4F) al correo electrónico de notificación y enviarlo a adrep@icao.int.

3.6.2 Los formularios de informes en línea enviados de forma electrónica mediante el portal seguro de iSTARS los recibe la OACI directamente. Los informes que se completan en papel se deben enviar a la OACI a adrep@icao.int a la siguiente dirección:

Organización de Aviación Civil Internacional
999 University Street
Montreal, Quebec H3C 5H7
Canadá
Fax: + 1 (514) 954-6077

3.6.3 La notificación y los informes deben estar redactados de manera sencilla y cuando sea posible, sin causar retraso indebido, deben prepararse en uno de los idiomas de trabajo de la OACI, considerando los idiomas de los destinatarios.

4. INSTRUCCIONES ESPECIALES PARA LA COMPILACIÓN

4.1 Codificación de la categoría de suceso

4.1.1 La taxonomía de la categoría de suceso de ADREP es parte del sistema de notificación de accidentes e incidentes de la OACI. Las categorías de suceso son un conjunto de términos usados por la OACI para categorizar accidentes e incidentes para realizar un análisis de tendencia de la seguridad operacional. La meta de dicho análisis es tomar medidas preventivas con el fin de evitar que ocurran accidentes o incidentes parecidos en el futuro.

4.1.2 La mayoría de las secuencias de accidentes e incidentes implican múltiples eventos. Por lo tanto, codificar estrictamente un accidente o incidente bajo una sola categoría puede resultar difícil. Por ejemplo, una maniobra abrupta (AMAN) también puede generar una pérdida del control en vuelo (LOC-I). En este caso, el evento se codifica en dos categorías, AMAN y LOC-I. La filosofía de codificación de la categoría de suceso de la OACI permite que los notificadores codifiquen múltiples categorías para un solo accidente o incidente, a fin de que la OACI considere o estudie todos los eventos que produjeron al accidente o incidente. Puede encontrar las definiciones detalladas de la categoría de suceso y la guía sobre codificación de categorías múltiples en http://www.icao.int/Safety/reporting.

4.2 Codificación del tipo de evento

4.2.1 Para determinar por qué sucedió un accidente o incidente, es fundamental estudiar factores que los genera, durante y después del suceso. Por lo tanto, es vital que todos los datos de evento conocidos al momento de la notificación se incluyan con precisión.

4.2.2 Para describir con mayor detalle un evento, puede ingresar "factores descriptivos" para cada uno de ellos. Los factores descriptivos describen, en detalle, lo que sucedió durante un evento al enumerar todos los fenómenos presentes. Si fuera posible, los factores descriptivos deben codificarse en orden cronológico debajo de cada tipo de evento.

4.2.3 Para explicar un evento, puede ingresar “factores explicativos” para cada factor descriptivo. Estos factores explican por qué el evento sucedió e incluyen aspectos de factores humanos en la codificación de los eventos. Se usan para determinar qué medida preventiva puede necesitarse. El conjunto completo de tipos de evento y los factores descriptivos y explicativos, con sus descripciones detalladas, pueden encontrarse en la página web de la taxonomía de ADREP de la OACI.

4.2.4 Entre las consideraciones generales al notificar eventos se incluyen:

a) *Ser tan específico como sea posible sin especular en los detalles*. Por ejemplo, si no se extendió el tren de aterrizaje delantero, use el evento "evento relacionado con el tren de aterrizaje delantero/trasero" y no el evento "evento relacionado con el tren de aterrizaje".

b) *Alinee las categorías de suceso con los eventos.* Por ejemplo, si la categoría de suceso es SCF-NP, entonces debe existir un evento de avería de un componente/sistema que no sea de la planta eléctrica.

c) *Alinee los eventos y los factores descriptivos.* Los eventos y factores descriptivos describen lo que salió mal, lo que no funcionó, qué había de diferente y qué contribuyó con el suceso. Por ejemplo, el evento "evento relacionado con la advertencia central" puede usarse para eventos donde el sistema tuvo un malfuncionamiento y el factor descriptivo "computadoras centrales" puede usarse para especificar el evento.

d) *Complete la secuencia de eventos en orden cronológico*. Un suceso se debe describir según la forma en que está codificado. En esencia, la codificación del evento debe proporcionar una imagen similar de la secuencia de suceso, como se encuentra en la narrativa.

4.3 Narrativa

4.3.1 La narrativa proporciona una breve descripción del suceso, como las circunstancias de emergencia, los hechos significativos y otra información pertinente. La narrativa no deberá superar las 200 palabras. Es importante que los eventos se describan en orden (hora) cronológico y que sean breves y específicos.

4.3.2 El estudio y análisis de la secuencia de eventos que generó el suceso pueden ayudar a comprender mejor la naturaleza del mismo. Por lo tanto, las narrativas deben incluir un resumen conciso de todos los eventos para proporcionar información acerca de los eventos que produjeron el suceso. La información provista en la narrativa del Informe preliminar no debe repetirse en un Informe de datos. Sin embargo, cualquier nueva información obtenida posteriormente al envío del Informe preliminar debe incluirse en el Informe de datos. En conjunto, las dos narrativas deben proporcionar toda la historia del vuelo y las conclusiones de la investigación.

4.3.3 Cuando no se ha enviado un Informe preliminar (en caso de un accidente o cuando una investigación de accidentes se ha completado dentro de 30 días), la narrativa en el Informe de datos debe proporcionar la historia de vuelo y la descripción y análisis de cómo y por qué ocurrió el evento, las conclusiones de la investigación, los hallazgos y la causa probable. En tales casos, se debe usar idealmente un total de 400 palabras en el Informe de datos enviado.

4.4 Recomendaciones de seguridad operacional

El notificador debe correlacionar las recomendaciones o medidas de seguridad operacional con los hallazgos pertinentes, donde corresponda. Los campos bajo la recomendación de la seguridad operacional en el Informe de datos deben incluir cualquier medida correctiva tomada o considerada. Si es posible, la recomendación debe especificar cómo esta medida correctiva resolverá el problema de la seguridad operacional identificada. Incluya un resumen de cualquier medida correctiva ya tomada.

Tabla 4-A6-1. Lista de verificación de notificación e información

En esta lista de verificación, los términos tienen los siguientes significados:

Accidentes internacionales. Accidentes e incidentes graves que suceden en el territorio de un Estado contratante a aeronaves registradas en otro Estado contratante.

Accidentes nacionales. Accidentes e incidentes graves que suceden en el territorio del Estado de matrícula.

Otros accidentes. Accidentes e incidentes graves que ocurren en el territorio de un Estado no contratante o fuera del territorio de cualquier Estado.

Notificación de accidentes e incidentes graves

Desde	*Informe*	*Hacia*	*Para*	*Mediante*
Estado de suceso	Notificación	Estado de matrícula Estado del explotador Estado de diseño Estado de fabricación	Accidentes internacionales: Todas las aeronaves	Con un mínimo de retraso
		OACI	Aeronave sobre los 2 250 kg o aeroplanos de turborreactor	
Estado de matrícula	Notificación	Estado del explotador Estado de diseño Estado de fabricación	Accidentes nacionales y otros	
		OACI	Aeronave sobre los 2 250 kg o aeroplanos de turborreactor	

Informe preliminar de ADREP

Desde	*Categoría*	*Informe*	*Hacia*	*Para*	*Mediante*
Estado que realiza la investigación	Accidente	Preliminar	Estado de matrícula Estado de suceso Estado del explotador Estado de fabricación Estado de diseño Cualquier Estado que proporcione información, instalaciones importantes o expertos. OACI	Aeronave sobre los 2 250 kg	30 días*
			Lo mismo que lo anterior, salvo la OACI	Accidentes a aeronaves de 2 250 kg o menos si está involucrada la aeronavegabilidad o los asuntos de interés	
	Incidente	Preliminar	No se requiere		

*Si, dentro de 30 días, el Informe de datos de accidentes se compiló y envió a la OACI, no se requiere un Informe preliminar.

Informe final — Accidentes e incidentes donde sea que hayan ocurrido

Desde	*Informe*	*Hacia*	*Para*	*Mediante*
Estado que realiza la investigación	Informe final	Estado que instituye la investigación Estado de matrícula Estado del explotador Estado de diseño Estado de fabricación Estado que tiene interés a causa de las fatalidades Estados que proporcionan información, instalaciones importantes o expertos	Todas las aeronaves	Con un mínimo de retraso
		OACI	Aeronave sobre los 5 700 kg	

Informe de datos de ADREP

Desde	*Categoría*	*Informe*	*Hacia*	*Para*	*Mediante*
Estado que realiza la investigación	Accidente	Datos	OACI	Aeronave sobre los 2 250 kg	Cuando la investigación se ha completado
Estado que realiza la investigación	Incidente	Datos	OACI	Aeronave sobre los 5 700 kg	Cuando la investigación se ha completado

Apéndice 7 del Capítulo 4

LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHAS Y PLAN DE IMPLEMENTACIÓN DEL SSP

1. LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHAS INICIAL (TABLA 4-A7-1)

1.1 La lista de verificación del análisis de brechas inicial en la Tabla 4-A7-1 puede usarse como una plantilla para realizar el primer paso de un análisis de brechas del SSP. Este formato con sus respuestas generales "Sí/No/Parcial" proporcionará una indicación inicial del amplio alcance de las brechas y, por lo tanto, la carga de trabajo general que puede esperarse. Esta información inicial debe ser útil para que la administración superior anticipe la escala del esfuerzo de implementación del SSP y, por lo tanto, los recursos que se proporcionarán. Esta lista de verificación inicial necesitaría de seguimiento con un plan de implementación adecuado, según las Tablas 4-A7-2 y 4-A7-3.

1.2 Una respuesta "Sí" indica que el Estado satisface o supera las expectativas de la pregunta en cuestión. Una respuesta "No" indica una brecha importante en el sistema existente, en relación con la expectativa de la pregunta. Una respuesta "Parcial" indica que se requiere una posterior mejora o trabajo de desarrollo para un proceso existente a fin de satisfacer las expectativas de la pregunta.

Nota.— El SMM hace referencia en corchetes [ ] al material guía en este manual, en relación con la pregunta del análisis de brechas.

Tabla 4-A7-1. Lista de verificación del análisis de brechas

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
Componente 1 — POLÍTICAS Y OBJETIVOS ESTATALES DE LA SEGURIDAD OPERACIONAL			
Elemento 1.1 — Marco de trabajo legislativo estatal de la seguridad operacional			
1.1-1	¿Ha promulgado [Estado] un marco de trabajo legislativo de seguridad operacional nacional y reglamentos específicos que definen la gestión de la seguridad operacional en el Estado? [4.2.1, Elemento 1.1; 4.3.2; 4.4.4]	☐ Sí ☐ No ☐ Parcial	
1.1-2	¿Se revisan periódicamente el marco de trabajo legislativo y los reglamentos específicos para garantizar que sigan siendo pertinentes para el Estado? [4.2.1, Elemento 1.1; 4.4.4 b)]	☐ Sí ☐ No ☐ Parcial	
	Elemento 1.2 — Responsabilidades de la seguridad operacional estatal		
1.2-1	¿Ha identificado [Estado] una organización apoderada del SSP y un ejecutivo responsable de la implementación y coordinación del SSP? [4.2.1, Elemento 1.2; 4.4.3 a)]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
1.2-2	¿Ha establecido [Estado] un equipo de implementación del SSP? [4.2.1, Elemento 1.2; 4.4.3 b)]	☐ Sí ☐ No ☐ Parcial	
1.2-3	¿Ha definido [Estado] los requisitos y las responsabilidades del Estado, acerca del establecimiento y mantenimiento del SSP? [4.2.1, Elemento 1.2; 4.4.3]	☐ Sí ☐ No ☐ Parcial	
1.2-4	¿Tiene implementado [Estado] un plan de implementación del SSP, que incluye un marco de tiempo para la implementación de las medidas y brechas, como se identificaron mediante el análisis de brechas? [4.3; 4.4.3 d)]	☐ Sí ☐ No ☐ Parcial	
1.2-5	¿Existe una declaración documentada acerca de la disposición de los recursos necesarios para la implementación y el mantenimiento del SSP? [4.2.1, Elemento 1.2; Capítulo 4, Apéndice 1, Parte 1, 1.1 d)]	☐ Sí ☐ No ☐ Parcial	
1.2-6	¿Tiene el ejecutivo responsable del SSP de [Estado] el control de los recursos necesarios para la implementación del SSP? [4.4.3 a)]	☐ Sí ☐ No ☐ Parcial	
1.2-7	¿Ha definido [Estado] las actividades y responsabilidades específicas relacionadas con la gestión de la seguridad operacional en el Estado, las que son responsabilidad de cada organización reglamentaria de la aviación según el SSP? [4.4.5 a)]	☐ Sí ☐ No ☐ Parcial	
1.2-8	¿Tiene [Estado] un mecanismo o una plataforma para la coordinación de la implementación del SSP y posteriores actividades de control continuo del SSP que involucran a todas las organizaciones reglamentarias del Estado? [4.4.3 e)]	☐ Sí ☐ No ☐ Parcial	
1.2-9	¿Coordina el ejecutivo responsable del SSP de [Estado], según corresponda, las actividades de las diferentes organizaciones de aviación del Estado según el SSP? [4.2.1, Elemento 1.2; 4.4.3 a)]	☐ Sí ☐ No ☐ Parcial	
1.2-10	¿Ha establecido [Estado] una política de seguridad operacional? [4.2.1, Elemento 1.2; 4.4.5 b)]	☐ Sí ☐ No ☐ Parcial	
1.2-11	¿Está firmada la política de seguridad operacional de [Estado] por un ejecutivo responsable del SSP de [Estado] o una autoridad adecuada de [Estado]? [Capítulo 4, Apéndice 1]	☐ Sí ☐ No ☐ Parcial	
1.2-12	¿Se revisa periódicamente la política de seguridad operacional de [Estado]? [4.4.15]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
1.2-13	¿Se comunica la política de seguridad operacional de [Estado] a los empleados en todas las organizaciones de aviación de [Estado] con la intención de que tomen conciencia de sus responsabilidad individuales en la seguridad operacional? [4.4.5 b)]	☐ Sí ☐ No ☐ Parcial	
1.2-14	¿Ha iniciado [Estado] un documento de SSP unificado como parte del plan de implementación del SSP para describir sus componentes y elementos del marco de trabajo del SSP? [4.2.1, Elemento 1.2; 4.4.3 f); Apéndice 8]	☐ Sí ☐ No ☐ Parcial	
1.2-15	¿Se ha completado, aprobado y firmado el documento del SSP por un ejecutivo responsable del SSP y se comunicó o dejó disponible para todos los accionistas al momento de la implementación total del SSP? [4.4.3 f)]	☐ Sí ☐ No ☐ Parcial	
1.2-16	¿Tiene [Estado] un sistema de documentación que garantiza un almacenamiento, archivo, protección y recuperación adecuados de todos los documentos relacionados con las actividades del SSP? [4.2.1, Elemento 1.2; 4.4.3 f)]	☐ Sí ☐ No ☐ Parcial	
1.2-17	¿Tiene [Estado] un mecanismo de revisión interno periódico para garantizar la mejora y eficacia continuas de su SSP? [4.2.1, Elemento 3.1; 4.4.15]	☐ Sí ☐ No ☐ Parcial	
Elemento 1.3 — Investigación de accidentes e incidentes			
1.3-1	¿Ha establecido [Estado] un proceso de investigación de accidentes e incidentes independiente, cuyo único objetivo es evitar accidentes e incidentes y no encontrar culpables o responsables? [4.2.1, Elemento 1.3; 4.4.6]	☐ Sí ☐ No ☐ Parcial	
1.3-2	¿Es funcionalmente independiente la organización/autoridad para la investigación de accidentes? (véase el *Manual de investigación de accidentes e incidentes de aviación* (Doc 9756, Parte I, 2.1)? [4.4.6 b)]	☐ Sí ☐ No ☐ Parcial	
Elemento 1.4 — Política de cumplimiento			
1.4-1	¿Ha promulgado [Estado] una política de cumplimiento? [4.2.1, Elemento 1.4; 4.4.10; Apéndices 10 y 11]	☐ Sí ☐ No ☐ Parcial	
1.4-2	¿Proporciona [Estado] una legislación de aviación primaria para el cumplimiento de la legislación y los reglamentos correspondientes? [4.4.7]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
1.4-3	¿Considera la política de cumplimiento que a los proveedores de servicios se les permite abordar y resolver desviaciones de seguridad operacional o calidad de rutina de forma interna, dentro del alcance de sus procedimientos de SMS/QMS aprobados? [4.4.10 a)]	☐ Sí ☐ No ☐ Parcial	
1.4-4	¿Establece la política de cumplimiento las condiciones y circunstancias en las cuales el Estado puede abordar las desviaciones de seguridad operacional directamente mediante sus procedimientos de investigación y cumplimiento establecidos? [4.2.1, Elemento 1.4; 4.4.10 b)]	☐ Sí ☐ No ☐ Parcial	
1.4-5	¿Incluye la política de cumplimiento del SSP disposiciones para evitar el uso o la divulgación de datos de seguridad operacional para propósitos que no sean la mejora de la seguridad operacional? [4.2.1, Elemento 1.4; 4.4.10 c)]	☐ Sí ☐ No ☐ Parcial	
1.4-6	¿Incluye la política de cumplimiento del SSP disposiciones para proteger las fuentes de información obtenidas de sistemas de notificación de incidentes voluntarios? [4.4.10 d); Apéndices 2 y 10]	☐ Sí ☐ No ☐ Parcial	
Componente 2 — GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL ESTATAL			
Elemento 2.1 — Requisitos de seguridad operacional para el SMS del proveedor de servicios			
2.1-1	¿Ha promulgado [Estado] reglamentos armonizados para exigir que los proveedores de servicios implementen un SMS? 4.2.1, Elemento 2.1; 4.4.9; Apéndice 9]	☐ Sí ☐ No ☐ Parcial	
2.1-2	¿Se revisan periódicamente estos requisitos de SMS y el material guía relacionado para garantizar que siguen siendo pertinentes y adecuados para los proveedores de servicios? [4.2.1, Elemento 2.1; 4.4.14 a)]	☐ Sí ☐ No ☐ Parcial	
Elemento 2.2 — Acuerdo sobre el rendimiento en materia de seguridad operacional del proveedor de servicios			
2.2-1	¿Ha acordado/aceptado [Estado] de forma individual los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios y sus niveles de alertas/objetivos respectivos? [4.2.1, Elemento 2.2; 4.4.13]	☐ Sí ☐ No ☐ Parcial	
2.2-2	¿Son los indicadores de rendimiento en materia de seguridad operacional acordados/aceptados proporcionales al alcance/complejidad del contexto operacional específico del proveedor de servicios individual? [4.4.13]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
2.2-3	¿Se revisan periódicamente los indicadores de rendimiento en materia de seguridad operacional acordados por [Estado] para garantizar que sigan siendo pertinentes y adecuados para el proveedor de servicios? [4.4.14 b)]	☐ Sí ☐ No ☐ Parcial	
Componente 3 — ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL ESTATAL			
Elemento 3.1 — Vigilancia de la seguridad operacional			
3.1-1	¿Ha establecido [Estado] un programa de vigilancia formal para garantizar un cumplimiento satisfactorio de los reglamentos y requisitos de seguridad operacional del Estado por parte de los proveedores de servicios? [4.2.1, Elemento 3.1]	☐ Sí ☐ No ☐ Parcial	
3.1-2	¿Ha establecido [Estado] un proceso para la revisión y aceptación inicial de un SMS del proveedor de servicios individual? [4.2.1, Elemento 2.2; 4.4.11 b)]	☐ Sí ☐ No ☐ Parcial	
3.1-3	¿Ha establecido [Estado] procedimientos para la revisión de indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios individual y sus niveles de alertas/objetivos pertinentes? [4.2.1, Elemento 2.2; 4.4.13]	☐ Sí ☐ No ☐ Parcial	
3.1-4	¿Incluye el programa de vigilancia de seguridad operacional del [Estado] una evaluación periódica del SMS de un proveedor de servicios individual? [4.2.1, Elemento 3.1; 4.4.14]	☐ Sí ☐ No ☐ Parcial	
3.1-5	¿Incluye el programa de vigilancia periódica del SMS de [Estado] una evaluación de los procesos de investigación de peligros y gestión de riesgos de seguridad operacional del proveedor de servicios? [4.4.14 c)]	☐ Sí ☐ No ☐ Parcial	
3.1-6	¿Incluye el programa de vigilancia periódica del SMS de [Estado] una evaluación de los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios y sus niveles de alertas/objetivos pertinentes? [4.4.14 b)]	☐ Sí ☐ No ☐ Parcial	
3.1-7	¿Tiene [Estado] un mecanismo de revisión interno periódico para el aseguramiento del cumplimiento eficaz del SSP y sus funciones de vigilancia relacionadas? [4.4.15]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
Elemento 3.2 — Recopilación, análisis e intercambio de datos de seguridad operacional			
3.2-1	¿Ha establecido [Estado] mecanismos para garantizar la notificación, la evaluación y el procesamiento obligatorios de datos de accidentes e incidentes graves a nivel del Estado colectivo? [4.2.1, Elemento 3.2; 4.4.12]	☐ Sí ☐ No ☐ Parcial	
3.2-2	¿Ha establecido [Estado] un sistema de notificación voluntaria para facilitar la recopilación de datos sobre peligros y riesgos de seguridad operacional conocidos que podrían no recopilarse con un sistema de notificación de incidentes obligatoria? [4.4.16 a)]	☐ Sí ☐ No ☐ Parcial	
3.2-3	¿Ha establecido [Estado] mecanismos para desarrollar información a partir de los datos guardados y para promover el intercambio de información de seguridad operacional con proveedores de servicios u otros Estados, según corresponda? [4.2.1, Elemento 3.2; 4.4.16]	☐ Sí ☐ No ☐ Parcial	
3.2-4	¿Ha establecido [Estado] un nivel aceptable de rendimiento en materia de seguridad operacional (ALoSP) como lo definen los indicadores de seguridad operacional seleccionados con niveles de objetivos y alertas correspondientes, según corresponda? [4.4.12 b); 4.4.16 b)]	☐ Sí ☐ No ☐ Parcial	
3.2-5	¿Son adecuados y pertinentes los indicadores de seguridad operacional de ALoSP para el alcance y la complejidad de las actividades de aviación? [4.4.12 b); 4.4.16 b)]	☐ Sí ☐ No ☐ Parcial	
3.2-6	¿Tiene [Estado] un mecanismo para el control periódico de los indicadores de seguridad operacional del SSP, a fin de garantizar que se tomen medidas correctivas y de seguimiento para cualquier tendencia indeseada, violaciones del nivel de alerta o no cumplimiento de objetivos de mejora? [4.4.12 b); 4.4.16 b)]	☐ Sí ☐ No ☐ Parcial	
Elemento 3.3 — Enfoque basado en datos de seguridad operacional de la vigilancia de áreas de mayor preocupación o necesidad			
3.3-1	¿Ha desarrollado [Estado] procedimientos para priorizar inspecciones, auditorías y estudios hacia aquellas áreas de mayor preocupación o necesidad de seguridad operacional? [4.2.1, Elemento 3.3; 4.4.17]	☐ Sí ☐ No ☐ Parcial	
3.3-2	¿Está la priorización de las inspecciones y auditorías asociadas con el análisis de datos de seguridad operacional o calidad internas o externas pertinentes? [4.2.1, Elemento 3.3; 4.4.17]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
Componente 4 — PROMOCIÓN DE LA SEGURIDAD OPERACIONAL ESTATAL			
Elemento 4.1 — Capacitación interna, comunicación y distribución de información de seguridad operacional			
4.1-1	¿Existe un proceso para identificar requisitos de capacitación relacionados con la gestión de la seguridad operacional, como capacitación de SSP y SMS, para el personal pertinente de las organizaciones reglamentarias/administrativas? [4.4.18]	☐ Sí ☐ No ☐ Parcial	
4.1-2	¿Existen registros para demostrar que el personal involucrado en la implementación de SSP y su operación participó en la capacitación o familiarización adecuada de SSP/SMS? [4.2.1, Elemento 4.1; 4.4.18]	☐ Sí ☐ No ☐ Parcial	
4.1-3	¿Mantiene [Estado] un mecanismo para la consolidación, comunicación y distribución de información de seguridad operacional entre sus organizaciones reglamentarias y administrativas implicadas en el SSP? [4.4.18 d)]	☐ Sí ☐ No ☐ Parcial	
4.1-4	¿Incluye la información de seguridad operacional interna/distribución de datos, informes de sucesos, investigación y peligros de todos los sectores de aviación del Estado? [4.4.16 c)]	☐ Sí ☐ No ☐ Parcial	
Elemento 4.2 — Capacitación externa, comunicación y distribución de información de seguridad operacional			
4.2-1	¿Facilita [Estado] la educación, comunicación y distribución continuas de la información de seguridad operacional con sus proveedores de servicios y entre ellos? [4.2.1, Elemento 4.2; 4.4.19]	☐ Sí ☐ No ☐ Parcial	
4.2-2	¿Participan las organizaciones reglamentarias de [Estado] en la distribución y el intercambio regional y global de información de seguridad operacional de aviación, y facilitan la participación de sus proveedores de servicios respectivos de la misma forma? [4.4.19 d)]	☐ Sí ☐ No ☐ Parcial	
4.2-3	¿Existe un proceso formal para la distribución externa de documentos e información reglamentaria a los proveedores de servicios y un medio para garantizar la eficacia de este proceso? [4.4.19 a)]	☐ Sí ☐ No ☐ Parcial	
4.2-4	¿Se incluye el documento del SSP de [Estado] y su política de seguridad operacional, política de cumplimiento e indicadores de seguridad operacional colectivos asociados en el proceso de comunicación y distribución de información de seguridad operacional del Estado? [4.4.19 a)]	☐ Sí ☐ No ☐ Parcial	

2. ANÁLISIS DE BRECHAS DETALLADO Y PLAN DE IMPLEMENTACIÓN (TABLA 4-A7-2).

La lista de verificación del análisis de brechas inicial en la Tabla 4-A7-1 debe seguirse mediante el "plan de identificación del análisis de brechas y tarea de implementación" descrito en la Tabla 4-A7-2. Una vez completada, esta tabla debe proporcionar un análisis de seguimiento sobre los detalles de las brechas y ayudar a traducir esto en tareas y subtareas necesarias reales en el contexto específico del entorno, los procesos y la terminología del Estado. Cada tarea se asignará en conformidad a las personas adecuadas o grupos de acción. Es importante que en la Tabla 4-A7-2 se proporcione la correlación del desarrollo del elemento/tarea individuales con sus apoderados descriptivos en el documento del SSP para activar la actualización progresiva del documento de SSP borrador a medida que se implementa o mejora cada elemento. (Las críticas iniciales del elemento en los documentos del SSP tienden a ser anticipativos en lugar de ser declarativos).

3. PROGRAMA DE IMPLEMENTACIÓN DE MEDIDAS/TAREAS (TABLA 4-A7-3).

La Tabla 4-A7-3 mostrará los hitos (fechas de inicio y fin) programados para cada tarea/medida. Para un enfoque de implementación en etapas, estas tareas/acciones se deberán organizar de acuerdo con la asignación de la etapa de sus elementos relacionados. Véase la Sección 4.4 de este capítulo, según corresponda. La Tabla 4-A7-3 puede ser una consolidación por separado de todas las acciones/tareas pendientes o, si se prefiere, ser una continuación de la Tabla 4-A7-2 en la forma de una hoja de cálculo.

Tabla 4-A7-2. Ejemplo de un plan de identificación de análisis de brechas y tareas de implementación

Referencia de GAQ	*Pregunta del análisis de brechas*	*Respuesta (Sí/No/Parcial)*	*Descripción de la brecha*	*Medida/tarea necesaria para completar la brecha*	*Grupo/persona de tarea asignada*	*Referencia del documento de SSP*	*Estado de la medida/tarea (abierta/WIP/cerrada)*
1.1-1	¿Ha promulgado [Estado] un marco de trabajo legislativo de seguridad operacional nacional y reglamentos específicos que definen la gestión de la seguridad operacional en el Estado?	Parcial	No hay una definición o asignación clara de los papeles de la gestión de seguridad operacional dentro de las organizaciones reglamentarias existentes	Tarea #1 — Departamento legal para revisar el marco de trabajo legislativo	Grupo de tareas A	Capítulo 2, Sección 1	WIP
1.1-2	¿Se revisan periódicamente el marco de trabajo legislativo y los reglamentos específicos para garantizar que sigan siendo pertinentes para el Estado?	Parcial	Solo revisión Ad hoc o fragmentada. Sin SOP para el proceso de revisión periódica	Tarea #3 — Desarrollo de SOP para la revisión periódica de todos los reglamentos de operaciones	Grupo de tareas B	Capítulo 2, Sección 3	Abierto
etc.							

Nota.— Todas las preguntas del análisis de brechas o solo aquellas preguntas con respuestas “No/Parcial” pueden abordarse en esta tabla, según corresponda.

Tabla 4-A7-3. Ejemplo de programa de implementación de medidas/tareas

Medidas/tareas necesarias para completar la brecha	*Referencia de GAQ*	*Grupo/persona de tarea asignada*	*Estado de medidas/tareas*	*Programa/cronología (inicio y fin)*												
				1Q10	*2Q10*	*3Q10*	*4Q10*	*1Q11*	*2Q11*	*3Q11*	*4Q11*	*1Q12*	*2Q12*	*3Q12*	*4Q12*	*etc.*
Tarea #1 — Departamento legal para revisar el marco de trabajo legislativo	1.1-1	Grupo de tareas A	WIP													
Tarea #2 — Definición del alcance del SMS		Grupo 3														
etc.																

Nota.— La Tabla 4-A7-3 puede ser una consolidación por separado o una continuación de la Tabla 4-A7-2 (hoja de cálculo) si se prefiere. Donde sea necesaria la priorización de la implementación de tareas, véase la Sección 4.4 de este capítulo.

Apéndice 8 del Capítulo 4

CONTENIDO DE MUESTRA DE UN DOCUMENTO DEL SSP

ÍNDICE

Página

Página

Apéndice 9 del Capítulo 4

EJEMPLO DE UN REGLAMENTO DE SMS ESTATAL

1. BASE REGLAMENTARIA

El reglamento del SMS debe promulgarse según la autoridad reglamentaria de la autoridad de aviación civil correspondiente del Estado.

2. ALCANCE DEL REGLAMENTO DEL SMS

2.1 El reglamento especifica el requisito que señala que los proveedores de servicios deben implementar un sistema de gestión de la seguridad operacional (SMS) que funcione de acuerdo con el Anexo 1 — *Licencias al personal*; el Anexo 6 — *Operación de aeronaves;* el Anexo 8 — *Aeronavegabilidad;* el Anexo 11 — *Servicios de tránsito aéreo;* y el Anexo 14 — *Aeródromos,* Volumen I — *Diseño y operaciones de aeródromos.*

2.2 Dentro del contexto de este reglamento, el término "proveedor de servicios" hará referencia normalmente a las organizaciones aprobadas/certificadas que ofrezcan servicios de aviación. El término hace referencia a organizaciones de capacitación aprobadas que están expuestas a riesgos de seguridad operacional durante la entrega de sus servicios, explotadores de aeronave, organizaciones de mantenimiento aprobados, organizaciones responsables del diseño o fabricación de la aeronave, proveedores de servicios de tránsito aéreo y aeródromos certificados, según corresponda.

2.3 El reglamento aborda los procesos, los procedimientos y las actividades del proveedor de servicios relacionados con la seguridad operacional de la aviación, en lugar de actividades de la seguridad operacional ocupacional, protección ambiental u otras relacionadas con la aviación.

2.4 El reglamento establece los requisitos mínimos del marco de trabajo del SMS. El proveedor de servicios puede establecer requisitos internos más estrictos.

3. EJEMPLO DE UNA CLÁUSULA DE REGLAMENTO/REQUISITO DE UN SMS

3.1 En vigencia [Fecha(s)], el [Tipo de proveedor de servicios] tendrá implementado un sistema de gestión de la seguridad operacional (SMS) aceptable para [Nombre de CAA] y que aborde cuatro objetivos de seguridad operacional de alto nivel, de la siguiente manera:

a) identifica peligros de seguridad operacional;

b) garantiza la implementación de la medida correctiva necesaria para mantener el rendimiento en materia de seguridad operacional acordado;

c) proporciona un control continuo y evaluación regular del rendimiento en materia de seguridad operacional; y

d) tiene como objetivo la mejora continua del rendimiento general del sistema de gestión de la seguridad operacional.

3.2 El marco de trabajo de este SMS deberá, como mínimo, incluir los siguientes componentes y elementos:

1. Política y objetivos de seguridad operacional

    1.1 Compromiso y responsabilidad de la gestión
    1.2 Responsabilidades de la seguridad operacional
    1.3 Nombramiento de personal de seguridad operacional clave
    1.4 Coordinación de la planificación de respuesta ante emergencias
    1.5 Documentación del 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 Control y medición del rendimiento en materia de la seguridad operacional
    3.2 La gestión de cambio
    3.3 Mejora continua del SMS

4. Promoción de la seguridad operacional

    4.1 Capacitación y educación
    4.2 Comunicación de seguridad operacional.

Nota.— Un reglamento sobre el SMS también debe incluir la disposición de una guía de SMS o material de asesoramiento del Estado. Tal material guía también debe incluir cualquier disposición de un enfoque de implementación de SMS en etapas. En tales requisitos o material guía también se debe dejar claro el proceso de aceptación, por parte de CAA, del SMS de un proveedor de servicios individual y el acuerdo sobre su rendimiento en materia de seguridad operacional, según corresponda.

Apéndice 10 del Capítulo 4

MUESTRA DE LA POLÍTICA DE CUMPLIMIENTO ESTATAL

Esta política de cumplimiento se promulga según la autoridad reglamentaria en [los reglamentos de aviación civil, las órdenes de aeronavegación o las normas reglamentarias correspondientes del Estado].

1. OBJETIVO

1.1 La política de cumplimiento de [CAA del Estado] está orientada a promover el cumplimiento de los reglamentos y requisitos de seguridad operacional de la aviación mediante funciones de cumplimiento en forma equitativa.

1.2 La implementación de los sistemas de gestión de la seguridad operacional (SMS) requiere que [CAA del Estado] tenga un enfoque de cumplimiento justo y discrecional para respaldar el marco de trabajo de SSP-SMS.

1.3 Las políticas y los procedimientos de cumplimiento de [CAA del Estado] permiten que los proveedores de servicios aborden y solucionen ciertos eventos que implican desviaciones de seguridad operacional, de forma interna, dentro del contexto del SMS del proveedor de servicios y a la satisfacción de la autoridad. Las contravenciones intencionales de [Ley de aviación civil del Estado] y de [Reglamentos de aviación civil del Estado] se investigarán y estarán sujetas a la medida de cumplimiento convencional, donde corresponda. Debe haber disposiciones claras de una debida consideración en el marco de trabajo de cumplimiento para distinguir entre infracciones premeditadas y errores o desviaciones accidentales.

1.4 La declaración de la política de cumplimiento y los procedimientos de cumplimiento asociados se aplican a los proveedores de servicios que operan de acuerdo con el Anexo 1 — *Licencias al personal;* el Anexo 6 — *Operación de aeronaves*, Parte I — *Transporte aéreo comercial internacional — Aviones* y Parte III — *Operaciones internacionales — Helicópteros;* el Anexo 8 — *Aeronavegabilidad;* el Anexo 11 — *Servicios de tránsito aéreo* y el Anexo 14 — *Aeródromos*, Volumen I — *Diseño y operaciones de aeródromos* de la OACI.

2. POLÍTICA

2.1 [Todos los proveedores de servicios correspondientes] establecen, mantienen y respetan un SMS que es proporcional a la envergadura, naturaleza y complejidad de las operaciones autorizadas para realizarse según su aprobación/certificación.

2.2 Para mantener esta política de cumplimiento que respalde la implementación del SMS, los inspectores de [CAA del Estado] mantendrán un canal de comunicación abierto con los proveedores de servicios.

2.3 No se usará información derivada de los sistemas de recopilación y procesamiento de datos de seguridad operacional (establecidos según un SMS), en relación con los informes clasificados como confidenciales, voluntarios o categoría equivalente, como la base para la medida de cumplimiento.

2.4 Cuando un proveedor de servicios que funciona según un SMS contraviene accidentalmente [los reglamentos de aviación civil o la ley de aviación civil], se deben usar procedimientos de revisión específicos. Estos procedimientos permiten que el inspector de [CAA del Estado] responsable de la vigilancia del proveedor de servicios tenga la oportunidad de entrar en conversaciones con la organización aprobada por SMS. El objetivo de este diálogo es llegar a un acuerdo sobre las medidas correctivas propuestas y un plan de acción que aborde correctamente las deficiencias que produjeron la contravención, y para asignarle al proveedor de servicios un tiempo razonable para implementarlos. Este enfoque apunta a nutrir y mantener una notificación eficaz de la seguridad operacional, mediante la cual los empleados de los proveedores de servicios puedan notificar deficiencias de seguridad operacional y peligros sin miedo a recibir medidas punitivas. Por lo tanto, un proveedor de servicios, sin encontrar culpables y sin miedo a medidas punitivas, podrá analizar el evento y los factores institucionales o humanos que puedan haberlo generado, para incorporar medidas correctivas que ayudarán de mejor forma a evitar que suceda de nuevo.

2.5 [CAA del Estado], mediante el inspector responsable de la vigilancia del proveedor de servicios, evaluará las medidas correctivas propuestas por el proveedor de servicios o los sistemas actualmente implementados para abordar el evento subyacente a la contravención. Si las medidas correctivas propuestas (incluida cualquier medida disciplinaria interna) se consideran satisfactorias y es probable que eviten la recurrencia y promuevan un cumplimiento futuro, la revisión de la infracción debe concluirse sin ninguna medida de cumplimiento punitivo por parte del regulador. En los casos donde las medidas correctivas o los sistemas implementados se consideran inadecuados, [CAA del Estado] seguirá interactuando con el proveedor de servicios para encontrar una resolución satisfactoria que pudiera evitar una medida de cumplimiento punitivo. Sin embargo, en los casos donde el proveedor de servicios se niega a abordar el evento y proporcionar medidas correctivas eficaces, [CAA del Estado] considerará tomar medidas de cumplimiento u otras medidas administrativas consideradas adecuadas.

2.6 Las violaciones a los reglamentos de aviación pueden ocurrir por muchas razones distintas, desde una genuina confusión de los reglamentos hasta una despreocupación de la seguridad operacional de la aviación. [CAA del Estado] cuenta con una gama de procedimientos de cumplimiento para abordar eficazmente las obligaciones de la seguridad operacional según la [Ley estatal correspondiente], teniendo en cuenta diferentes circunstancias. Estos procedimientos pueden producir varias medidas, como:

a) asesoría;

b) capacitación correctiva; o

c) modificación, suspensión o cancelación de las autorizaciones.

2.7 Las decisiones de cumplimiento no deben verse influenciadas por:

a) conflictos personales;

b) ganancias personales;

c) consideraciones como género, raza, religión, visiones o afiliaciones políticas; o

d) poderío personal, político o financiero de aquellos implicados.

3. PROPORCIONALIDAD DE LAS RESPUESTAS

Las decisiones de cumplimiento deben ser proporcionales a las brechas identificadas y los riesgos de seguridad operacional a los que subyacen, según tres principios:

a) [CAA del Estado] tomará medidas contra aquellos que operan constante y deliberadamente fuera de los reglamentos de aviación civil;

b) [CAA del Estado] buscará educar y promover la capacitación o supervisión de aquellos que muestren un compromiso para resolver las deficiencias de seguridad operacional; y

c) [CAA del Estado] dará una debida y justa consideración para distinguir las infracciones premeditadas de los errores o las desviaciones accidentales.

4. JUSTICIA NATURAL Y RESPONSABILIDAD

Las decisiones de cumplimiento deben:

a) ser justas y seguir un debido proceso;

b) ser transparentes para aquellos implicados;

c) considerar las circunstancias del caso y las medidas/actitudes del proveedor de servicios o la persona cuando se considera una medida;

d) ser medidas/decisiones constantes para circunstancias parecidas o iguales; y

e) estar sujetas a una revisión interna y externa adecuada.

5. EXCEPCIONES

5.1 Esta política no se aplica si existe evidencia de un esfuerzo deliberado para ocultar el no cumplimiento.

5.2 Esta política no corresponde si el proveedor de servicios no puede mantener un SMS aceptable o su rendimiento en materia de seguridad operacional acordado.

5.3 Esta política no corresponde si la autoridad considera al proveedor de servicios como un infractor recurrente.

5.4 En las circunstancias anteriores, la autoridad puede abordar dicho no cumplimiento o infracción de acuerdo con los procedimientos de cumplimiento establecidos, según se determine correcto.

(Firmado) _____
Ejecutivo responsable del SSP

Apéndice 11 del Capítulo 4

GUÍA SOBRE LOS PROCEDIMIENTOS DE CUMPLIMIENTO DEL ESTADO EN UN ENTORNO DE SSP-SMS

1. GENERALIDADES

En el programa estatal de seguridad operacional (SSP) de [Estado], [CAA del Estado] es responsable de supervisar a los titulares de certificados que operan en un entorno de SMS. Los procedimientos de cumplimiento proporcionan una guía sobre la respuesta adecuada ante errores o infracciones para aquellos responsables de la vigilancia de los proveedores de servicios que operan en un entorno de SMS. Los procedimientos de cumplimiento juegan una función de respaldo en el proceso. No obstante, la decisión final acerca de cualquier problema de cumplimiento del SSP es la responsabilidad del ejecutivo responsable del CAA o SSP.

2. APLICABILIDAD

2.1 Estos procedimientos se aplican a contravenciones que podrían haber cometido personas o proveedores de servicios que llevan a cabo actividades en un entorno de SSP-SMS.

2.2 Estos procedimientos están vigentes a partir de [Fecha].

2.3 Estos procedimientos se usarán para los proveedores de servicios que tienen un SMS aceptado por la CAA o siguen un "enfoque de implementación de SMS en etapas" con un plan de implementación aceptado por la CAA.

2.4 Donde los proveedores de servicios o las personas no han demostrado que operan en un entorno de SMS, pueden aplicarse medidas de cumplimiento sin las ventajas de los procedimientos explicados en el párrafo 3.

3. PROCEDIMIENTOS

3.1 Con el fin de determinar si se debe realizar un proceso de evaluación de cumplimiento o investigación bajo un entorno de cumplimiento de SSP-SMS, será necesario que el grupo de investigación/cumplimiento determine el estado de implementación del SMS del proveedor de servicios específico. Esta determinación se tomaría inicialmente mediante la comunicación entre el grupo de cumplimiento y el inspector principal, quien es responsable de vigilar y certificar al proveedor de servicios bajo investigación. La deliberación del cumplimiento siempre se debe llevar a cabo mediante un panel de funcionarios designado o asignado en lugar de un funcionario individual.

3.2 El inspector principal asegurará si el proveedor de servicios cumple con los criterios antes mencionados para los procedimientos de cumplimiento del SMS. Para facilitar la evaluación inicial, [CAA del Estado] debe tener una lista del estado de implementación del SMS de los proveedores de servicios. Dejar esta lista disponible para el personal de investigación/cumplimiento de aviación ayudará a que los investigadores tomen una decisión acerca de la aplicabilidad del proceso de evaluación de investigación/cumplimiento.

3.3 Durante el “enfoque en etapas” de la implementación del SMS del proveedor de servicios, [CAA del Estado] puede aplicar los procedimientos de cumplimiento del SMS a los proveedores de servicios que aún no tienen un SMS implementado o aceptado por completo, siempre y cuando se cumplan ciertas condiciones.

3.4 [CAA del Estado] requerirá, como mínimo, que se cumplan las siguientes tres condiciones antes de poder aplicar los procedimientos de cumplimiento del SMS:

a) el proveedor de servicios tiene un proceso interno de notificación de peligros y mitigación de riesgos eficaz;

b) el proveedor de servicios tiene un proceso de medida correctiva e investigación de sucesos eficaz proporcional a la envergadura y complejidad de sus operaciones y adecuados para determinar los factores de origen y desarrollar medidas correctivas;

c) los datos o la información de seguridad operacional sobre el evento bajo investigación están disponibles para el panel de investigación/cumplimiento y el proveedor de servicios o la persona ofrecen total cooperación al grupo de investigación/cumplimiento.

Informe inicial de infracción

3.5 El personal de cumplimiento de aviación debe llevar a cabo un análisis preliminar en todos los casos donde se detecte contravención o donde se reciba información acerca una posible contravención. Si la infracción notificada es el resultado o la recomendación de un informe oficial, el grupo de cumplimiento necesitará decidir si el informe de sucesos es adecuado para respaldar la medida de cumplimiento.

Evaluación preliminar

3.6 Deben considerarse las siguientes preguntas según la información recibida:

a) ¿Existen fundamentos razonables para creer que una persona u organización que lleva a cabo actividades según un SMS puede haber cometido una contravención?

b) ¿Es el evento de tal naturaleza (por ejemplo, no cumplimiento total/recurrente) que se debe considerar una medida de cumplimiento?

c) ¿Existe más información o evidencia, como condiciones latentes, factores institucionales/humanos, que deben asegurarse para facilitar la toma de decisiones de la medida de cumplimiento?

Cuando se responden estas preguntas de manera positiva, el inspector principal debe notificar a su concurrencia que siga con la evaluación de la medida de cumplimiento, donde corresponda.

Evaluación y recomendación de la medida de cumplimiento

3.7 El proceso del grupo de cumplimiento para determinar una medida administrativa, o punitiva, adecuada, justa y eficaz debe basarse en un proceso objetivo que considere todas las condiciones subyacentes, circunstanciales, ambientales o latentes. Estas deben incluir factores institucionales, humanos y de escalada, donde corresponda. También se deben considerar otros factores, como si la medida de no cumplimiento constituye un error accidental o una medida deliberada, según corresponda.

3.8 Luego de tomar una decisión de la medida de cumplimiento correspondiente, el grupo de cumplimiento debe hacer la recomendación necesaria para la aprobación del ejecutivo responsable y notificar a partir de ahí a las partes de interés.

Apéndice 12 del Capítulo 4

EJEMPLO DE UNA LISTA DE VERIFICACIÓN DE ACEPTACIÓN/EVALUACIÓN REGLAMENTARIA DEL SMS

1. La Tabla 4-A12-1 es una lista de verificación reglamentaria para la evaluación del SMS, de muestra, (85 preguntas) que puede usarse para la evaluación y aceptación iniciales del SMS de un proveedor de servicios. Para un proceso de aceptación inicial, las preguntas de evaluación deben ser integrales para abordar adecuadamente todos los elementos del SMS de la organización. Esto garantizará que todos los elementos y sus procesos relacionados estén implementados dentro de la organización. Los aspectos operacionales del SMS serían abordados de manera más adecuada durante la evaluación de rutina/anual posterior del SMS.

2. El procedimiento de rendimiento aceptable mínimo ilustrado proporciona criterios de puntuación aceptable mínima de tres etapas. Este procedimiento puede facilitar la evaluación progresiva por parte del regulador del proceso de implementación del SMS del proveedor de servicios, en lugar de realizar una auditoría solo después de haber implementado completamente el SMS de un proveedor de servicios o que sea maduro. Dicho protocolo de evaluación progresiva también garantizará que el regulador esté involucrado activamente en el control de la implementación del SMS de la industria desde las primeras etapas.

3. Donde se adopte un enfoque de implementación del SMS del elemento en etapas, como se analizó en el Capítulo 5 de este documento, las preguntas en la lista de verificación deberán reconfigurarse y adaptarse para alinearse con la gama específica de elementos en todas las etapas pertinentes, como lo podrá determinar el Estado.

4. Se ofrece un procedimiento ilustrativo del aviso de medida correctiva (CAN) al final de la lista de verificación.

5. La Tabla 4-A12-2 es una lista de verificación reglamentaria para la evaluación del SMS, de muestra, (39 preguntas) que puede usarse para una evaluación del SMS de rutina posterior. Después de que el SMS de una organización haya completado el proceso de evaluación y aceptación iniciales del regulador, quedarán muchas preguntas de la evaluación de la lista de verificación de evaluación inicial que ya no serán apropiadas o necesarias para propósitos de la evaluación de rutina. Una lista de verificación de evaluación de SMS de rutina solo necesita concentrarse en los aspectos operacionales de un SMS y en la evidencia de la implementación satisfactoria de sus procesos de respaldo.

6. Se puede realizar una evaluación del SMS de rutina de forma independiente o incorporada como parte de una auditoría de la organización/sistemas de rutina. En caso de lo último, tales preguntas de la evaluación de rutina de SMS pueden incorporarse en conformidad como una sección dentro de la lista de verificación de la auditoría institucional normal. El auditor que realiza una auditoría de QMS-SMS integrada debe capacitarse para una auditoría de SMS, según corresponda. El protocolo de aviso de medida correctiva (CAN) normal del regulador también puede aplicarse a la evaluación de SMS de rutina.

Tabla 4-A12-1. Lista de verificación de la evaluación de SMS— Aceptación de SMS inicial

Lista de verificación de evaluación de SMS — Aceptación inicial			Lista de verificación de auditoría de SMS_rutina/18 de agosto de 2011	
Columna de entrada: anotar "S" para Sí," N " para No, "N/A" para No corresponde				
Nombre de la organización:	Fecha de la evaluación:		Evaluado por POI/PMI:	Ref.:

Elemento del SMS	Nivel 1	Entrada	Ref./ comen-tarios del Doc	Nivel 2	Entrada	Ref./ comen-tarios del Doc	Nivel 3	Entrada	Ref./ comen-tarios del Doc
Compromiso y responsabilidades de la gestión [1.1]	**Componente 1 del SMS. Política y objetivos de seguridad operacional**								
	1.1 /N1/1			1.1 /N2/1			1.1 /N3/1		
	Existe una declaración de política de seguridad operacional documentada.	S		Existe evidencia de que la política de seguridad operacional se comunica a todos los empleados con la intención de crear conciencia de sus obligaciones de seguridad operacional individuales.	N		Existe una revisión periódica de la política de seguridad operacional por parte de la administración superior o el comité de seguridad operacional.	N	
	1.1 /N1/2			1.1 /N2/2			1.1 /N3/2		
	La política de seguridad operacional es pertinente para la seguridad operacional de la aviación.	S		La política de seguridad operacional recibe el respaldo del gerente responsable.	S		Las atribuciones del gerente responsable indican su responsabilidad general para todos los problemas de seguridad operacional.	N	
	1.1 /N1/3			1.1 /N2/3					
	La política de seguridad operacional es pertinente para el alcance y la complejidad de las operaciones de la organización.	N		La política de seguridad operacional aborda la entrega de los recursos humanos y financieros necesarios para su implementación.	N		–		
Responsabilidades de la seguridad operacional [1.2]	1.2 /N1/1			1.2 /N2/1					
	Existe una responsabilidad de la seguridad operacional documentada (SMS) dentro de la organización que comienza con el gerente responsable.	S		Las atribuciones del gerente responsable indican su responsabilidad final para la gestión de la seguridad operacional de su organización.	N		–		
	1.2 /N1/2			1.2 /N2/2					
	El ejecutivo responsable tiene autoridad final sobre todas las actividades de aviación de su organización.	N		La autoridad final del gerente responsable sobre todas las operaciones realizadas bajo los certificados de su organización se indica en sus atribuciones.	N		–		

Elemento del SMS	Nivel 1	Entrada	Ref./ comen-tarios del Doc	Nivel 2	Entrada	Ref./ comen-tarios del Doc	Nivel 3	Entrada	Ref./ comen-tarios del Doc
Responsabilidades de la seguridad operacional [1.2]	1.2 /N1/3			1.2 /N2/3			1.2 /N3/1		
	Existe un comité de seguridad operacional (o mecanismo equivalente) que revisa el SMS y su rendimiento en materia de seguridad operacional.	S		Para una gran organización, existen grupos de acción de la seguridad operacional por departamento o sección que trabajan en conjunto con el comité de seguridad operacional.	N/A		El comité de seguridad operacional lo lidera el gerente responsable o (para organizaciones muy grandes) un delegado asignado de forma adecuada, debidamente confirmado en el manual del SMS.	S	
	1.2 /N1/4			1.2 /N2/4			1.2 /N3/2		
	El comité de seguridad operacional incluye líderes de departamento u operacionales pertinentes, según corresponda.	N		Existe un coordinador de seguridad operacional asignado (SMS) dentro del grupo de acción de seguridad operacional.	N/A		Los grupos de acción de seguridad operacional los dirigen líderes de departamentos o sección, donde corresponda.	N/A	
Nombramiento del personal de seguridad operacional clave [1.3]	1.3 /N1/1			1.3 /N2/1			1.3 /N3/1		
	Existe un gerente que desempeña el papel de administrar el SMS.	S		El gerente responsable de administrar el SMS no tiene otra responsabilidad que pueda entrar en conflicto o perjudicar su papel como gerente de SMS.	N		El gerente de SMS tiene acceso o notificación directos al gerente responsable encargado de la implementación y operación del SMS.	N	
	1.3 /N1/2						1.3 /N3/2		
	El gerente que desempeña el papel de SMS tiene funciones de SMS pertinentes incluidas en sus atribuciones.	N		–			El gerente de SMS es un puesto administrativo superior que no es inferior jerárquicamente o subordinado a otros puestos operacionales o de producción.	N	
Planificación de respuesta ante emergencias [1.4]	1.4 /N1/1			1.4 /N2/1			1.4 /N3/1		
	Existe un ERP documentado o un procedimiento de contingencia operacional equivalente.	S		El ERP incluye procedimientos para la producción, la entrega y el respaldo seguros y continuos de los productos o servicios de la aviación durante tales emergencias o contingencias.	N		El ERP aborda la integración relevante con organizaciones del cliente o el subcontratista, donde corresponda.	N	
	1.4 /N1/2			1.4 /N2/2			1.4 /N3/2		
	El ERP es adecuado para la envergadura, naturaleza y complejidad de la organización.	S		Existe un plan para ensayos o ejercicios en relación con el ERP.	S		Existe un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continuas.	N	
	1.4 /N1/3			1.4 /N2/3					
	El plan de emergencia aborda escenarios de emergencia/crisis posibles o probables relacionados con las entregas de productos o servicios de la aviación de la organización.	N		Los ensayos o ejercicios del ERP se llevan a cabo de acuerdo con el plan y el resultado de los ensayos efectuados se documentan.	N		–		

Elemento del SMS	Nivel 1	Entrada	Ref./ comen-tarios del Doc	Nivel 2	Entrada	Ref./ comen-tarios del Doc	Nivel 3	Entrada	Ref./ comen-tarios del Doc
Documentación del SMS [1.5]	1.5 /N1/1			1.5 /N2/1			1.5 /N3/1		
	El gerente responsable aprueba el documento o exposición de SMS y la CAA lo acepta.	S		La autoridad de aviación nacional de la organización acepta o respalda el documento de SMS.	S		Los procedimientos de SMS reflejan la correcta integración con otros sistemas de gestión pertinentes dentro de la organización, como QMS, OSHE, seguridad de la aviación, según corresponda.	N	
	1.5 /N1/2			1.5 /N2/2			1.5 /N3/2		
	El documento de SMS proporciona una descripción general o exposición del marco de trabajo y los elementos de SMS de la organización.	S		La exposición de cada elemento del SMS del documento de SMS incluye referencias cruzadas a procedimientos, manuales o sistemas de respaldo o relacionados, según corresponda.	S		Los procedimientos de SMS reflejan la coordinación o integración pertinentes con organizaciones de cliente o subcontratista externo, donde corresponda.	N	
	1.5 /N1/3			1.5 /N2/3			1.5 /N3/3		
	El documento de SMS es un documento controlado independiente o un documento respaldado/aprobado por la CAA existente.	S		Se mantienen registros acerca de las actas del comité de seguridad operacional/reunión de SAG (o equivalente).	S		Existe un proceso para revisar periódicamente la exposición de SMS y la documentación de respaldo para garantizar su continua relevancia.	N	
	1.5 /N1/4			1.5 /N2/4					
	Todos los componentes y elementos de los requisitos reglamentarios de SMS se abordan en el documento de SMS.	S		Están disponibles los registros acerca de la revisión periódica de evaluaciones de seguridad operacional/riesgos o revisión especial existentes, junto con los cambios pertinentes.	N		–		
	1.5 /N1/5								
	Se mantienen registros acerca de las evaluaciones de los riesgos de seguridad operacional realizadas.	S		–			–		
	1.5 /N1/6								
	Se mantienen registros acerca de peligros/amenazas identificadas o notificadas.	S		–			–		

Elemento del SMS	Nivel 1	Entrada	Ref./ comen-tarios del Doc	Nivel 2	Entrada	Ref./ comen-tarios del Doc	Nivel 3	Entrada	Ref./ comen-tarios del Doc
Identificación de peligros [2.1]	**Componente 2 del SMS. Gestión de riesgos de seguridad operacional**								
	2.1 /N1/1			2.1 /N2/1			2.1 /N3/1		
	Existe un procedimiento para la notificación de peligros/amenazas voluntaria de todos los empleados.	S		En el sistema de identificación de peligros, existe una clara definición y distinción entre peligros y consecuencias.	N		Existe un procedimiento para identificar peligros/amenazas de informes de investigación internos de incidentes/accidentes para la mitigación de riesgos de seguimiento, donde corresponda.	N	
	2.1 /N1/2			2.1 /N2/2			2.1 /N3/2		
	Existe un procedimiento para la notificación de incidentes/ accidentes por parte del personal de operaciones o producción.	S		El sistema de notificación de peligros es confidencial y tiene disposiciones para proteger la identidad del notificador.	N		Existe un procedimiento para revisar los peligros/amenazas del servicio industrial pertinente o de los informes de incidentes/ accidentes para la mitigación de riesgos, donde corresponda.	N	
	2.1 /N1/3			2.1 /N2/3			2.1 /N3/3		
	Existe un procedimiento para la investigación de incidentes/ accidentes relacionados con la calidad o seguridad operacional.	S		Los procedimientos disciplinarios y de investigación internos de la organización distinguen entre infracciones premeditadas y deliberadas y errores y equivocaciones accidentales.	N		Existe un procedimiento para la revisión periódica de los registros de análisis de riesgos existentes.	N	
Evaluación y mitigación de riesgos de seguridad operacional [2.2]	2.2 /N1/1			2.2 /N2/1					
	Existe un procedimiento de HIRM documentado que implica el uso de herramientas de análisis de riesgos objetivas.	S		Los gerentes de departamento han aprobado los informes de evaluación de riesgos o se han aprobado en un nivel superior, donde corresponda.	N		–		
	2.2 /N1/2			2.2 /N2/2					
	Existe un procedimiento para la identificación de operaciones, procesos, instalaciones y equipos que se consideran pertinentes para HIRM (por la organización).	N		Las medidas de mitigación recomendadas, que requieren la decisión o aprobación de la administración superior, están consideradas y documentadas.	N		–		
	2.2 /N1/3			2.2 /N2/3			2.2 /N3/1		
	Existe un programa para el rendimiento de HIRA progresivo de todas las operaciones, los procesos, las instalaciones y los equipos relacionados con la seguridad operacional de la aviación, como lo identifica la organización.	N		Existe un procedimiento para priorizar el rendimiento de HIRA para las operaciones, los procesos, las instalaciones y los equipos con peligros/riesgos fundamentales para la seguridad operacional identificados o conocidos.	N		Existe evidencia de cumplimiento y mantenimiento progresivos del programa de rendimiento de HIRA de la organización.	N	

Elemento del SMS	Nivel 1	Entrada	Ref./ comen-tarios del Doc	Nivel 2	Entrada	Ref./ comen-tarios del Doc	Nivel 3	Entrada	Ref./ comen-tarios del Doc
Control y medición del rendimiento en materia de seguridad operacional [3.1]	**Componente 3 del SMS. Aseguramiento de la seguridad operacional**								
	3.1 /N1/1			3.1 /N2/1			3.1 /N3/1		
	Existen indicadores de rendimiento en materia de seguridad operacional identificados para medir y controlar el rendimiento en materia de seguridad operacional de la organización.	S		Hay indicadores de rendimiento en materia de seguridad operacional de bajo impacto (por ejemplo, no cumplimiento, eventos de desviación).	N		Existe un procedimiento para una medida correctiva o de seguimiento que puede tomarse cuando no se logran los objetivos o se violan los niveles de alerta.	N	
	3.1 /N1/2			3.1 /N2/2			3.1 /N3/2		
	Existen indicadores de rendimiento en materia de seguridad operacional basados en datos de alto impacto (por ejemplo, tasas de incidentes graves y accidentes).	S		Existe una configuración de nivel de alertas u objetivos dentro de los indicadores de rendimiento en materia de seguridad operacional, donde corresponda.	N		Los indicadores de rendimiento en materia de seguridad operacional se revisan mediante un comité de seguridad operacional en busca de niveles de alertas y tendencias que se han excedido y el logro de objetivos, donde corresponda.	S	
La gestión de cambio [3.2]	3.2 /N1/1			3.2 /N2/1			3.2 /N3/1		
	Existe un procedimiento para la revisión de instalaciones y equipos existentes relacionados con la seguridad operacional de la aviación (incluidos los registros de HIRA) cada vez que haya cambios pertinentes a aquellas instalaciones y equipos.	N		Existe un procedimiento para revisar las nuevas instalaciones y los equipos relacionados con la seguridad operacional de la aviación en busca de peligros/riesgos antes de ponerlos en servicio.	N		Existe un procedimiento para revisar las instalaciones, los equipos, las operaciones o los procesos existentes pertinentes (incluidos los registros de HIRM) cada vez que existan cambios pertinentes que sean externos a la organización, como normas reglamentarias/industriales, mejores prácticas o tecnología.	N	
	3.2 /N1/2			3.2 /N2/2					
	Existe un procedimiento para revisar las operaciones y los procesos de aviación existentes y pertinentes (incluidos los registros de HIRA) cada vez que haya cambios pertinentes para aquellas operaciones o procesos.	N		Existe un procedimiento para revisar las nuevas operaciones y los procesos relacionados con la seguridad operacional de la aviación en busca de peligros/riesgos antes de implementarlos.	N		–		

Elemento del SMS	Nivel 1	Entrada	Ref./ comen-tarios del Doc	Nivel 2	Entrada	Ref./ comen-tarios del Doc	Nivel 3	Entrada	Ref./ comen-tarios del Doc
Mejora continua del SMS [3.3]	3.3 /N1/1			3.3 /N2/1			3.3 /N3/1		
	Existe un procedimiento para la evaluación/auditoría interna periódica del SMS.	S		Existe un procedimiento de seguimiento para abordar las medidas correctivas de la auditoría.	S		La evaluación/auditoría de SMS se llevó a cabo de acuerdo con el plan.	N	
	3.3 /N1/2			3.3 /N2/2			3.3 /N3/2		
	Existe un plan actual de la auditoría/evaluación de SMS interna.	N		–			Existe un proceso para que los informes de auditoría/evaluación de SMS puedan enviarse o destacarse para la atención del gerente responsable, cuando sea necesario.	N	
	3.3 /N1/3			3.3 /N2/3			3.3 /N3/3		
	Existe un procedimiento de auditoría/evaluación de SMS interno documentado.	N		El plan de auditoría de SMS incluye la toma de muestras de las evaluaciones de seguridad operacional completadas.	N		El plan de auditoría de SMS aborda los papeles de SMS/aportes de los contratistas, donde corresponda.	N	
Capacitación y comunicación [4.1, 4.2]	**Componente 4 del SMS. Promoción de la seguridad operacional**								
	4.1 /N1/1			4.1 /N2/1			4.1 /N3/1		
	Existe una política de capacitación/familiarización de SMS documentada para el personal.	S		Al personal que participa en la evaluación de riesgos se le brinda capacitación o familiarización adecuadas de la gestión de riesgos.	N		Existe evidencia de esfuerzos de educación o toma de conciencia del SMS a nivel de la organización.	N	
	4.1 /N1/2			4.1 /N2/2			4.1 /N3/2		
	El gerente responsable de la administración de SMS ha tomado un curso de capacitación de SMS adecuado.	S		El personal directamente involucrado en el SMS (comité de seguridad operacional/miembros de SAG) ha tomado un curso de capacitación o familiarización de SMS adecuado.	N		Existe evidencia de una publicación, una circular o un canal de seguridad operacional (SMS) para comunicar la seguridad operacional y asuntos de SMS a los empleados.	N	
	4.1 /N1/3								
	El gerente responsable ha tomado un curso de familiarización, una sesión informativa o una capacitación de SMS adecuado.	S		–			–		

SUBTOTAL	CATEGORÍA 1
S	23
N	11
N/A	0
Cantidad de preguntas completadas	34

CATEGORÍA 2
6
21
2
29

CATEGORÍA 3
2
19
1
22

MONTO TOTAL*	
S	31
N	51
N/A	3
Cantidad de preguntas completadas	85

RESULTADO DE LA EVALUACIÓN (% DE SÍ):
38,7%

PROCEDIMIENTO DE AVISO DE MEDIDA CORRECTIVA (CAN)

1) Rendimiento aceptable mínimo general (implementación de SMS en etapas):

   Primer año/etapa de la evaluación (por ejemplo, 2012) — 45%.
   Segundo año/etapa de la evaluación (por ejemplo, 2013) — 65%.
   Tercer año/etapa de la evaluación (por ejemplo, 2014) y de ahí en adelante — 85%.
   Noventa (90) días para que la medida correctiva obtenga menos del 45% de rendimiento general.

2) Rendimiento de línea base (preguntas de Nivel 1) (durante cualquier año/etapa de evaluación) posterior a la fecha de aplicabilidad necesaria del SMS del Estado:

   El aviso de medida correctiva (CAN) se emitirá para respuestas “No” a cualquier pregunta de Nivel 1 (durante cualquier año/etapa de la evaluación).
   (Sesenta (60) días para que la medida correctiva obtenga una respuesta "Sí" a las preguntas pertinentes).

Tabla 4-A12-2. Lista de verificación de la evaluación del SMS — Evaluación del SMS de rutina

Elemento del SMS		*Pregunta de evaluación*
Compromiso y responsabilidades de la gestión [1.1]	1	La política de seguridad operacional es pertinente para el alcance y la complejidad de las operaciones de la organización.
	2	Existe evidencia de que la política de seguridad operacional se comunica a todos los empleados con la intención de crear conciencia de sus obligaciones de seguridad operacional individuales.
	3	Existe una revisión periódica de la política de seguridad operacional por parte de la administración superior o el comité de seguridad operacional.
	4	Las atribuciones del gerente responsable indican su responsabilidad general para todos los problemas de seguridad operacional.
Responsabilidades de la seguridad operacional [1.2]	1	Existe un comité de seguridad operacional (o mecanismo equivalente) que revisa el SMS y su rendimiento en materia de seguridad operacional.
	2	La autoridad final del gerente responsable sobre todas las operaciones realizadas bajo los certificados de su organización se indica en sus atribuciones.
Nombramiento del personal de seguridad operacional clave [1.3]	1	El gerente que desempeña el papel de SMS tiene funciones de SMS pertinentes incluidas en sus atribuciones.
	2	El gerente responsable de administrar el SMS no tiene otra responsabilidad que pueda entrar en conflicto o perjudicar su papel como gerente de SMS.
	3	El gerente de SMS tiene acceso o notificación directos al gerente responsable encargado de la implementación y operación del SMS.
	4	El gerente de SMS es un puesto administrativo superior que no es inferior jerárquicamente o subordinado a otros puestos operacionales o de producción.
Planificación de respuesta ante emergencias [1.4]	1	El ERP aborda escenarios de emergencia/crisis posibles o probables relacionados con las entregas de servicios de aviación.
	2	El ERP incluye procedimientos para la producción, la entrega y el respaldo seguros y continuos de sus productos o servicios de la aviación durante tales emergencias o contingencias.
	3	Los ensayos o ejercicios del ERP se llevan a cabo de acuerdo con el plan y el resultado de los ensayos efectuados se documentan.
	4	El ERP aborda la integración relevante con organizaciones del cliente o el subcontratista, donde corresponda.
	5	Existe evidencia de una revisión periódica del ERP para garantizar su relevancia y eficacia continuas.

Elemento del SMS		*Pregunta de evaluación*
Documentación del SMS [1.5]	1	Los componentes y elementos del SMS de la organización se manifiestan adecuadamente en el documento del SMS.
	2	Los componentes y elementos del SMS documentados de la organización están en línea con los requisitos de SMS de la autoridad de la aviación.
	3	Existe evidencia de una coordinación o integración de SMS pertinente con las organizaciones de cliente o subcontratista externos, donde corresponda.
	4	Existe evidencia de procedimientos de revisión periódica del documento de SMS y la documentación de respaldo para garantizar su continua relevancia.
	5	Se dispone de los registros acerca de la revisión periódica de las evaluaciones de seguridad operacional/riesgos existentes.
Identificación de peligros [2.1]	1	La cantidad o tasa de informes de peligros registrados/recopilados de la organización es proporcional a la envergadura y el alcance de las operaciones de la organización.
	2	El sistema de notificación de peligros es confidencial y tiene disposiciones para proteger la identidad del notificador.
	3	Existe evidencia de que los peligros/amenazas descubiertos durante el proceso de investigación de incidentes/accidentes están registrados con el sistema HIRM.
	4	Existe evidencia de que los peligros registrados se procesan sistemáticamente para la mitigación de riesgos, donde corresponda.
Evaluación y mitigación de riesgos de seguridad operacional [2.2]	1	Existe evidencia de que las operaciones, los procesos, las instalaciones y los equipos con implicaciones de la seguridad operacional de la aviación se someten progresivamente al proceso HIRM de la organización.
	2	Un nivel adecuado de gestión aprueba los informes de evaluación de riesgos completada.
	3	Existe un procedimiento para la revisión periódica de los registros de mitigación de riesgos completados.

Elemento del SMS		*Pregunta de evaluación*
Control y medición del rendimiento en materia de seguridad operacional [3.1]	1	Los indicadores de rendimiento en materia de seguridad operacional del SMS de la organización se han acordado con la autoridad de aviación nacional pertinente.
	2	Existen indicadores de rendimiento en materia de seguridad operacional basados en datos de alto impacto (por ejemplo, tasas de incidentes graves y accidentes).
	3	Hay indicadores de rendimiento en materia de seguridad operacional de bajo impacto (por ejemplo, no cumplimiento, eventos de desviación).
	4	Existe una configuración de nivel de alertas u objetivos dentro de los indicadores de rendimiento en materia de seguridad operacional, donde corresponda.
	5	El procedimiento de gestión de cambio de la organización incluye el requisito que señala que se realice una evaluación de riesgos de la seguridad operacional, donde corresponda.
	6	Existe evidencia de una medida correctiva o de seguimiento tomada cuando no se logran los objetivos o se violan los niveles de alerta.
La gestión de cambio [3.2]	1	Existe evidencia de que hay procesos y operaciones relacionados con la seguridad operacional de aviación pertinentes que se han sometido al proceso HIRM de la organización, según corresponda.
	2	El procedimiento de gestión de cambio de la organización incluye el requisito que señala que se realice una evaluación de riesgos de la seguridad operacional, donde corresponda.
Mejora continua del SMS [3.3]	1	Existe evidencia de que se ha planificado y llevado a cabo una auditoría/evaluación interna del SMS.
Capacitación, educación y comunicación [4.1, 4.2]	1	Existe evidencia de que todo el personal implicado en las operaciones de SMS han tomado un curso de capacitación o familiarización de SMS adecuado.
	2	Al personal que participa en la evaluación de riesgos se le brinda capacitación o familiarización adecuadas de la gestión de riesgos.
	3	Existe evidencia de una publicación, una circular o un canal de seguridad operacional (SMS) para comunicar la seguridad operacional y asuntos de SMS a los empleados.

Capítulo 5

SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

5.1 INTRODUCCIÓN

5.1.1 Un SMS es un sistema que sirve para garantizar la operación segura de la aeronave mediante una gestión de riesgos de seguridad operacional eficaz. Este sistema 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 busca contener o mitigar proactivamente los riesgos antes de que produzcan accidentes e incidentes de aviación. Es un sistema proporcional a las obligaciones y metas de seguridad operacional de la organización.

5.1.2 El SMS es necesario para que una organización de aviación identifique peligros y gestione los riesgos encontrados durante la entrega de sus productos o servicios. Un SMS incluye elementos clave que son fundamentales para la identificación de peligros y la gestión de riesgos de seguridad operacional al garantizar que:

a) esté disponible la información necesaria;

b) estén disponibles las herramientas adecuadas para el uso de la organización;

c) las herramientas son adecuadas para la tarea;

d) las herramientas son proporcionales a las necesidades y limitaciones de la organización; y

e) las decisiones se toman basándose en la consideración total de los riesgos de seguridad operacional.

5.2 ALCANCE

El SMS aborda las actividades de aviación de un proveedor de servicios de aviación que se relacionan con la operación segura de la aeronave. El alcance de un SMS puede incluir indirectamente otras actividades institucionales que respaldan el desarrollo operacional o de productos, como finanzas, recursos humanos y aspectos legales. Por tanto, es fundamental hacer partícipe a todos los accionistas internos y externos del sistema de aviación que tengan un posible impacto en el rendimiento en materia de seguridad operacional de la organización. Es más, se debe considerar cualquier entrada potencial en una etapa primaria de la implementación de SMS y en todas las evaluaciones internas futuras del SMS. Los siguientes accionistas pueden proporcionar entradas a los proveedores de servicios, según sus posibles impactos en el rendimiento en materia de seguridad operacional:

a) profesionales de la aviación;

b) autoridades reglamentarias y administrativas de la aviación;

c) agrupaciones empresariales de la industria;

d) agrupaciones y federaciones de profesionales;

e) organizaciones de aviación internacional;

f) subcontratistas o directores de un proveedor de servicios; y

g) el público pasajero en vuelos.

5.3 MARCO DE TRABAJO DEL SMS

5.3.1 Esta sección introduce un marco de trabajo para la implementación de SMS por parte de los proveedores de servicios de aviación pertinentes. Se debe tener presente que la implementación del marco de trabajo debe ser proporcional a la envergadura de la organización y la complejidad de los productos o servicios proporcionados.

5.3.2 El marco de trabajo incluye cuatro componentes y doce elementos, los que representan los requisitos mínimos para la implementación del SMS. Los cuatro componentes de un SMS son:

a) política y objetivos de seguridad operacional;

b) gestión de riesgos de seguridad operacional;

c) aseguramiento de la seguridad operacional; y

d) promoción de la seguridad operacional.

5.3.3 Las políticas y objetivos de seguridad operacional crean el marco de referencia para el SMS. El objetivo del componente de gestión de riesgos de seguridad operacional es identificar peligros, evaluar los riesgos relacionados y desarrollar mitigaciones adecuadas en el contexto de la entrega de los productos y servicios de la organización. Se logra el aseguramiento de la seguridad operacional mediante procesos constantes que controlan el cumplimiento de las normas internacionales y los reglamentos nacionales. Es más, el proceso de aseguramiento de la seguridad operacional proporciona confianza en que el SMS funciona como fue diseñado y es eficaz. La promoción de la seguridad operacional proporciona la toma de conciencia y capacitación necesarias.

5.3.4 Los cuatro componentes y los doce elementos que componen el marco de trabajo del SMS de la OACI son los siguientes:

1. Política y objetivos de seguridad operacional

   1.1 Compromiso y responsabilidad de la gestión
   1.2 Responsabilidades de la seguridad operacional
   1.3 Nombramiento de personal de seguridad operacional clave
   1.4 Coordinación de la planificación de respuesta ante emergencias
   1.5 Documentación del 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 Control y medición del rendimiento en materia de la seguridad operacional
   3.2 La gestión de cambio
   3.3 Mejora continua del SMS

4. Promoción de la seguridad operacional

   4.1 Capacitación y educación
   4.2 Comunicación de seguridad operacional.

5.3.5 A continuación se entregan detalles adicionales acerca de cada uno de los cuatro componentes y lo doce elementos. Se proporciona un resumen de alto nivel de cada uno de los componentes, y le sigue el texto del marco de trabajo del SMS para cada elemento. Luego se presentan estrategias de guía/implementación generales para cada elemento.

Componente 1 del SMS. Política y objetivos de la seguridad operacional

5.3.6 La política de seguridad operacional describe los principios, procesos y métodos del SMS de la organización para lograr los resultados deseados de la seguridad operacional. La política establece el compromiso de la administración superior para incorporar y mejorar continuamente la seguridad operacional en todos los aspectos de sus actividades. La administración superior desarrolla objetivos de seguridad operacional a nivel de la organización medibles y asequibles que puedan alcanzarse.

Elemento 1.1 del SMS Compromiso y responsabilidad de la gestión

El proveedor de servicios deberá definir su política de seguridad operacional de acuerdo con requisitos internacionales y nacionales. La política de seguridad operacional deberá:

a) reflejar el compromiso institucional acerca de la seguridad operacional;

b) incluir una clara declaración sobre la disposición de los recursos necesarios para la implementación de la política de seguridad operacional;

c) incluir procedimientos de notificación de seguridad operacional;

d) indicar claramente qué tipos de comportamientos son inaceptables, en relación con las actividades de aviación del proveedor de servicios e incluir las circunstancias según las cuales no se aplicaría una medida disciplinaria;

e) tener la firma de un ejecutivo responsable de la organización;

f) comunicarse, con un respaldo visible, en toda la organización; y

g) revisarse periódicamente para garantizar que sigue siendo pertinente y adecuado para el proveedor de servicios.

Guía general

5.3.7 En cualquier organización, la administración controla las actividades del personal y el uso de los recursos para la entrega de un producto o servicio. La exposición de la organización a peligros de seguridad operacional es una consecuencia de estas actividades. La administración mitiga los riesgos relacionados con la seguridad operacional al:

a) configurar las prioridades y tareas institucionales;

b) prescribir procedimientos sobre cómo realizar actividades o procesos;

c) contratar, capacitar y supervisar empleados;

d) procurar equipo para respaldar las actividades de entrega de servicios;

e) usar las habilidades de su personal; y

f) asignar los recursos necesarios.

5.3.8 La administración debe garantizar que:

a) hayan directrices y controles de seguridad operacional incorporados en los procedimientos operacionales normalizados (SOP);

b) los empleados respeten los SOP y las directrices de seguridad operacional; y

c) el equipo siga en condiciones de recibir mantenimiento.

5.3.9 La principal responsabilidad de la administración para garantizar una operación segura y eficiente se logra al garantizar que se respeten los SOP (cumplimiento de seguridad operacional) y al establecer y mantener un SMS dedicado que establezca los controles de riesgos de la seguridad operacional necesarios (rendimiento en materia de seguridad operacional).

Estrategia de implementación

5.3.10 La administración superior desarrolla y apoya la política de seguridad operacional, la cual está firmada por un ejecutivo responsable. (Véase el Apéndice 1 para un análisis sobre la aceptación y el uso de las firmas electrónicas en una política de seguridad operacional y otra documentación relacionada con el SMS). En la Figura 5-1 se muestra un ejemplo de una declaración de política de seguridad operacional.

5.3.11 Luego de haber desarrollado una política de seguridad operacional, la administración superior deberá:

a) respaldar visiblemente la política;

b) comunicar la política a todo el personal correspondiente;

c) establecer objetivos de rendimiento en materia de seguridad operacional para el SMS y la organización; y

d) establecer objetivos de seguridad operacional que identifiquen lo que intenta alcanzar la organización en términos de gestión de la seguridad operacional.

DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD OPERACIONAL

La seguridad operacional es una de nuestras funciones comerciales centrales. Estamos comprometidos a desarrollar, implementar, mantener y mejorar constantemente las estrategias y los procesos para garantizar que todas nuestras actividades de aviación se lleven a cabo a partir de una correcta asignación de recursos institucionales, orientados a alcanzar el más alto nivel de rendimiento en materia de seguridad operacional y cumplir con requisitos reglamentarios, mientras prestamos nuestros servicios.

Todos los niveles de administración y todos los empleados son responsables de proporcionar el más alto nivel de rendimiento en materia de seguridad operacional, comenzando con [Funcionario ejecutivo principal director ejecutivo/o lo que corresponda para la organización].

Nuestro compromiso es para:

- *respaldar* la gestión de la seguridad operacional mediante la disposición de los recursos correspondientes que generarán una cultura institucional que fomenta prácticas seguras, alienta una notificación y comunicación eficaces de la seguridad operacional y gestiona activamente la seguridad operacional con la misma atención a los resultados como la atención a los resultados de otros sistemas de gestión de la organización;
- *garantizar* que la gestión de la seguridad operacional sea una de las responsabilidades principales de todos los gerentes y empleados;
- *definir claramente,* para todo el personal, gerentes y empleados por igual, sus responsabilidades para la entrega del rendimiento en materia de seguridad operacional de la organización y el rendimiento de nuestro sistema de gestión de la seguridad operacional;
- *establecer y operar* los procesos de identificación de peligros y gestión de riesgos, incluido un sistema de notificación de peligros, para eliminar o mitigar los riesgos de seguridad operacional de las consecuencias de peligros que se generen de nuestras operaciones o actividades, para alcanzar una mejora continua en nuestro rendimiento en materia de seguridad operacional;
- *garantizar* que no se tome ninguna medida en contra de ningún empleado que divulgue una preocupación de seguridad operacional mediante el sistema de notificación de peligros, a menos que dicha divulgación indique, más allá de cualquier duda razonable, una negligencia grave o una despreocupación deliberada o consciente de los reglamentos y procedimientos;
- *cumplir* con y, cuando sea posible, superar los requisitos y las normas reglamentarias y legislativas;
- *garantizar* que estén disponibles suficientes recursos humanos cualificados y capacitados para implementar las estrategias y los procesos de seguridad operacional;
- *garantizar* que todo el personal disponga de información y capacitación adecuadas y correspondientes de la seguridad operacional de la aviación, sea competente en asuntos de seguridad operacional y tengan asignadas solo tareas proporcionales a sus habilidades;
- *establecer y medir* nuestro rendimiento en materia de seguridad operacional en contraste con indicadores de rendimiento en materia de seguridad operacional realistas y objetivos de rendimiento en materia de seguridad operacional;
- *mejorar continuamente* nuestro rendimiento en materia de seguridad operacional mediante un control y una medición continuos, revisión y ajuste regulares de los objetivos y las metas de seguridad operacional y el logro diligente de estos; y
- *garantizar* que se implementen los sistemas y servicios suministrados de forma externa para respaldar nuestras operaciones y que cumplan nuestras normas de rendimiento en materia de seguridad operacional.

(Firmado)

_____

Director ejecutivo/o quien corresponda

Figura 5-1. Ejemplo de una declaración de la política de seguridad operacional

5.3.12 La política de seguridad operacional debe incluir un compromiso para:

a) lograr las más altas normas de seguridad operacional;

b) cumplir con todos los requisitos reglamentarios correspondientes;

c) cumplir normas internacionales;

d) adoptar las mejores prácticas comprobadas adecuadas para la actividad;

e) proporcionar todos los recursos necesarios;

f) garantizar que la seguridad operacional es una de las principales responsabilidades de todos los gerentes;

g) seguir la política disciplinaria; y

h) garantizar que se entiende, implementa y mantiene la política de seguridad operacional en todos los niveles.

5.3.13 Las normas de seguridad operacional logradas son un indicio de la conducta institucional y también son una medida del rendimiento del SMS. Es más, los objetivos de la seguridad operacional y las normas del rendimiento en materia de seguridad operacional deben vincularse con:

a) indicadores del rendimiento en materia de seguridad operacional;

b) objetivos del rendimiento en materia de seguridad operacional; y

c) medidas de mitigación del SMS.

5.3.14 La política disciplinaria se usa para determinar si ha ocurrido una infracción que requiere de una medida que vaya más allá de los requisitos del análisis de los sistemas de gestión de riesgos. Por lo tanto, es fundamental garantizar que las personas responsables de tomar dicha determinación tengan la experiencia técnica necesaria para considerar completamente el contexto relacionado con el informe, con lo que se disminuye la probabilidad de que dicho personal y el proveedor de servicios puedan estar expuestos a procesos "disciplinarios/judiciales" injustos o inadecuados. Un enfoque que puede usarse para tomar esta determinación es el algoritmo de actos inseguros de James Reason para ayudar a que los gerentes de primera línea determinen la responsabilidad de las personas implicadas en un incidente.[1] Otro recurso acerca de esto es el libro de Sidney Dekker titulado *Just Culture: Balancing Safety and Accountability* (Tan solo cultura: equilibrio de la seguridad operacional y la responsabilidad).[2]

1. James Reason, *Managing the Risks of Organizational Accidents* (Gestión de riesgos de los accidentes institucionales), 1997.
2. Sidney Dekker, *Just Culture: Balancing Safety and Accountability* (Tan solo cultura: equilibrio de la seguridad operacional y la responsabilidad), segunda edición, 2012.

5.3.15 Una política para proteger adecuadamente los datos de la seguridad operacional, así como también, los notificadores de tales datos, puede tener un efecto positivo importante en la cultura de notificación. Luego que queda claro que un informe no implica una infracción, el proveedor de servicios y el Estado deben permitir la eliminación de la identidad de los notificadores y la incorporación de los informes como para realizar un análisis de seguridad operacional significativo sin implicar al personal o a los proveedores de servicios específicos. Dado que los sucesos importantes pueden invocar procesos y procedimientos fuera del SMS del proveedor de servicios, la autoridad estatal pertinente podría no permitir la eliminación temprana de la identidad de los informes en todas las circunstancias. Sin embargo, una política que permita la eliminación de identidad adecuada de los informes puede mejorar drásticamente la calidad de los datos recopilados.

Elemento 1.2 del SMS Responsabilidades de la seguridad operacional

El proveedor de servicios deberá:

a) identificar al ejecutivo responsable quien, sin importar otras funciones, tiene la responsabilidad final, en nombre de la organización, de implementar y mantener al SMS;

b) definir claramente líneas de responsabilidad de la seguridad operacional en toda la organización, lo que incluye una responsabilidad directa de la seguridad operacional por parte de la administración superior;

c) identificar las responsabilidades de todos los miembros de la administración, sin importar otras funciones, así como también, de los empleados, en relación con el rendimiento en materia de seguridad operacional del SMS;

d) documentar y comunicar las responsabilidades de la seguridad operacional y las autoridades en toda la organización; y

e) definir los niveles de administración con la autoridad para tomar decisiones acerca de la tolerabilidad de los riesgos de seguridad operacional.

Guía general

5.3.16 En el contexto de SMS, responsabilidad significa ser el responsable final del rendimiento en materia de la seguridad operacional, ya sea a nivel de SMS general (ejecutivo responsable) o a niveles específicos del producto/proceso (miembros del equipo de gestión). Esto incluye ser responsable de garantizar que se tomen medidas correctivas adecuadas para abordar los peligros y errores notificados, así como también, responder ante accidentes e incidentes.

5.3.17 De forma histórica, en la mayoría de las organizaciones, la oficina de seguridad operacional gestionó todo el proceso de seguridad operacional dentro de la organización. El funcionario de seguridad operacional era la persona a cargo de identificar los problemas de seguridad operacional, proporcionar soluciones, participar en la implementación de las soluciones y controlar la eficacia de las soluciones. Esta práctica ubicó al propietario del proceso de seguridad operacional por completo en la oficina de seguridad operacional, lo que elimina a los ejecutivos y gerentes de línea del proceso de toma de decisiones sobre la seguridad operacional. Esto creó la percepción de que los asuntos de seguridad operacional no eran la responsabilidad del gerente de línea; los problemas de seguridad operacional se consideraban responsabilidad de la oficina de seguridad operacional y del funcionario de seguridad operacional. Adicionalmente, este enfoque descuidó la valiosa entrada que podían incluir las unidades de producción y operaciones al proceso de toma de decisiones sobre seguridad operacional de la organización.

5.3.18 Al exigir que el proveedor de servicios identifique al ejecutivo responsable, la responsabilidad del rendimiento en materia de seguridad operacional general se ubica en un nivel en la organización que tenga la autoridad para tomar medidas a fin de garantizar que el SMS sea eficaz. Al definir las responsabilidades específicas de la seguridad operacional de todos los miembros del equipo de gestión se clarifica el marco de trabajo de la responsabilidad en toda la organización. Estos marcos de trabajo de la responsabilidad necesitan incluir la responsabilidad del rendimiento en materia de seguridad operacional del subproducto o de los proveedores de servicios subcontratados que no requieren de forma separada una certificación o aprobación de seguridad operacional. Estas responsabilidades y autoridades de la seguridad operacional deben documentarse y comunicarse a toda la organización y necesitan identificar los niveles de gestión con la autoridad para tomar decisiones acerca de la tolerabilidad de los riesgos de la seguridad operacional. Además, las responsabilidades de seguridad operacional de los gerentes deben incluir la asignación de los recursos humanos, técnicos, financieros o de otro tipo necesarios para el rendimiento eficaz y eficiente del SMS.

Nota.— En el contexto del SMM, el término "responsabilidades" puede considerarse como aquellas responsabilidades que no pueden delegarse.

Estrategia de implementación

5.3.19 La gestión de la seguridad operacional puede ser una función principal para cualquier proveedor de servicios de la aviación. La definición de las responsabilidades de todo el personal implicado en las tareas relacionadas con la seguridad operacional servirán para garantizar la entrega de productos y operaciones seguras, así como también, una asignación de recursos equilibrada de forma correcta.

5.3.20 El ejecutivo responsable que identificó el proveedor de servicios es la única persona con total responsabilidad del SMS, incluida la responsabilidad de proporcionar los recursos esenciales para su implementación y mantenimiento. Las autoridades y responsabilidades del ejecutivo responsable incluyen, entre otras:

a) la disposición y asignación de recursos humanos, técnicos, financieros y de otro tipo necesarios para el rendimiento eficaz y eficiente del SMS;

b) la responsabilidad directa de la conducta de los asuntos de la organización;

c) la autoridad final sobre las operaciones con certificación/aprobación de la organización;

d) el establecimiento y la promoción de la política de seguridad operacional;

e) el establecimiento de los objetivos de seguridad operacional de la organización;

f) actuar como promotor de la seguridad operacional de la organización;

g) tener la responsabilidad final para la resolución de todos los problemas de seguridad operacional; y

h) el establecimiento y mantenimiento de la competencia de la organización para aprender del análisis de los datos recopilados mediante sus sistema de notificación de seguridad operacional.

Nota.— Las responsabilidades descritas anteriormente no deben delegarse.

5.3.21 Según la envergadura, estructura y complejidad de la organización, el ejecutivo responsable puede ser:

a) el funcionario ejecutivo principal de la organización del proveedor de servicios;

b) el presidente del consejo de directores;

c) un socio; o

d) el propietario.

5.3.22 Asimismo, el nombramiento de un ejecutivo responsable, quien cuenta con las autoridades y responsabilidades necesarias, requiere que la persona tenga los atributos necesarios para desempeñar su función. El ejecutivo responsable tendrá muchas funciones en la organización. Sin embargo, la función del ejecutivo responsable será inculcar la seguridad operacional como un valor institucional principal y garantizar que el SMS se implemente y mantenga de forma correcta mediante la asignación de recursos y tareas.

5.3.23 Todos los puestos, las responsabilidades y las autoridades relacionadas con la seguridad operacional de la aviación deben definirse, documentarse y comunicarse en toda la organización. Las responsabilidades de la seguridad operacional de cada gerente superior (líder de departamento o persona responsable de una unidad funcional) son componentes integrales de sus descripciones laborales. Dado que la gestión de la seguridad operacional es una función comercial principal, cada gerente superior tiene un grado de participación en la operación del SMS. Esta participación es ciertamente más profunda para aquellos gerentes directamente responsables de las unidades funcionales que ofrecen productos o servicios de la organización (operaciones, fabricación, mantenimiento, ingeniería, capacitación y despacho, de aquí en adelante se conocerán con el término genérico “gerentes de línea”) que para aquellos responsables de respaldar las funciones (recursos humanos, administración, legal y financiero).

5.3.24 Un proveedor de servicios es responsable del rendimiento en materia de seguridad operacional de los productos o servicios que proporcionan los subcontratistas que no requieren una certificación o aprobación de seguridad operacional por separado. Si bien es cierto que no se requiere que todos los subcontratistas tengan necesariamente un SMS, sigue siendo la responsabilidad del proveedor de servicios garantizar que se cumplan sus propios requisitos de rendimiento en materia de seguridad operacional. En cualquier caso, es fundamental que el SMS del proveedor de servicios interactúe lo más perfectamente posible que se pueda con los sistemas de seguridad operacional o los subcontratistas que proporcionan productos o servicios pertinentes para la operación segura de la aeronave. La interfaz entre el SMS de la organización y aquel del sistema de seguridad operacional del proveedor de subproductos o subservicios debe abordar la identificación de peligros, la evaluación de riesgos y el desarrollo de estrategias de mitigación de riesgos, donde corresponda. El proveedor de servicios debe garantizar que:

a) haya una política que establezca claramente un flujo de responsabilidad y autoridad de seguridad operacional entre el proveedor de servicios y el subcontratista;

b) el subcontratista tenga un sistema de notificación de seguridad operacional proporcional a su envergadura y complejidad, que facilite la identificación temprana de peligros y averías sistémicas de interés para el proveedor de servicios;

c) el consejo de revisión de seguridad operacional del proveedor de servicios incluya la representación del subcontratista, donde corresponda;

d) se hayan creado indicadores de seguridad operacional/calidad para controlar el rendimiento del subcontratista, donde corresponda;

e) el proceso de promoción de la seguridad operacional del proveedor de servicios garantiza que los empleados del subcontratista cuenten con las comunicaciones de seguridad operacional correspondientes de la organización; y

f) se haya desarrollado y probado cualquier papel, responsabilidad y función del subcontratista pertinente para el plan de respuesta ante emergencias del proveedor de servicios.

5.3.25 Las responsabilidades y autoridades relacionadas con SMS de todos los gerentes superiores correspondientes deben describirse en la documentación del SMS de la organización. Las funciones de seguridad operacional obligatorias que realiza el gerente de seguridad operacional, la oficina de seguridad operacional, los grupos de acción de seguridad operacional, etc., pueden incorporarse en las descripciones, los procesos y los procedimientos de trabajo existentes.

5.3.26 La función del gerente de seguridad operacional se describe en detalle en la siguiente sección. A partir de una perspectiva de responsabilidad, la persona que realiza la función del gerente de seguridad operacional es responsable del rendimiento del SMS ante el ejecutivo responsable y de la entrega de servicios de seguridad operacional a los otros departamentos en la organización.

Elemento 1.3 del SMS. Nombramiento del personal de seguridad operacional clave

El proveedor de servicios deberá asignar un gerente de seguridad operacional que sea responsable de la implementación y mantenimiento de un SMS eficaz.

Guía general

5.3.27 El nombramiento de un gerente de seguridad operacional calificado es clave para la implementación y el funcionamiento eficaces de una oficina de servicios de seguridad operacional. El gerente de seguridad operacional puede identificarse con diferentes cargos en las organizaciones, pero para propósitos de este manual, usaremos el término genérico "gerente de seguridad operacional".

Estrategia de implementación

5.3.28 En la mayoría de las organizaciones, el gerente de seguridad operacional es la persona responsable del desarrollo y mantenimiento de un SMS eficaz. El gerente de seguridad operacional también aconseja al ejecutivo responsable y a los gerentes de línea sobre los asuntos de gestión de la seguridad operacional y es responsable de coordinar y comunicar temas de seguridad operacional dentro de la organización, así como también, con accionistas externos. Las funciones del gerente de seguridad operacional incluyen, entre otras:

a) gestionar el plan de implementación del SMS en nombre del ejecutivo responsable;

b) realizar/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 la seguridad operacional de la organización;

e) mantener registros y documentación de la seguridad operacional;

f) planificar y facilitar una capacitación de seguridad operacional para el personal;

g) proporcionar consejos independientes 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;

i) coordinarse y comunicarse (en nombre del ejecutivo responsable) con la autoridad de vigilancia del Estado y otras entidades estatales, según sea necesario, sobre temas relacionados con la seguridad operacional; y

j) coordinarse y comunicarse (en nombre del ejecutivo responsable) con organizaciones internacionales sobre temas relacionados con la seguridad operacional.

5.3.29 Los criterios de selección de un gerente de seguridad operacional deben incluir, entre otros, los siguientes:

a) experiencia de gestión de seguridad operacional/calidad;

b) experiencia operacional;

c) antecedentes técnicos para comprender los sistemas que respaldan las operaciones;

d) habilidades para relacionarse con las personas;

e) habilidades analíticas y de solución de problemas;

f) habilidades de gestión de proyectos; y

g) habilidades de comunicaciones oral y escrita.

Nota.— El Apéndice 2 de este capítulo contiene una muestra de descripción de trabajo de un gerente de seguridad operacional. Para las organizaciones pequeñas, puede ser viable combinar las funciones de gestión de calidad y seguridad operacional dentro de la misma oficina.

5.3.30 Por lo general, el gerente de seguridad operacional recibe el respaldo de personal adicional. Esto dependerá de la envergadura de la organización y la naturaleza y complejidad de la organización. El gerente de seguridad operacional se vincula directamente con los gerentes de línea o sus delegados, como cuando las unidades operacionales reciben el respaldo de funcionarios de seguridad operacional dedicados.

5.3.31 El gerente de seguridad operacional es la persona responsable de la recopilación y el análisis de los datos de seguridad operacional y la distribución de información de seguridad operacional asociada a los gerentes de línea. La distribución de la información de seguridad operacional mediante la oficina de servicios de seguridad operacional es el primer paso en el proceso de gestión de riesgos de seguridad operacional. Esta información la deberán usar los gerentes de línea para mitigar los riesgos de seguridad operacional, que inevitablemente requieren la asignación de los recursos. Los recursos necesarios podrían estar disponibles fácilmente para los gerentes de línea para este propósito.

5.3.32 Además, se requiere de un proceso formal para evaluar la eficacia y eficiencia de cualquier estrategia de mitigación usada para lograr los objetivos de rendimiento en materia de seguridad operacional acordados de la organización. Un posible proceso incluye la creación de un comité de revisión de seguridad operacional (SRC). El SRC proporciona la plataforma para lograr los objetivos de la asignación de recursos y para evaluar la eficacia y eficiencia de las estrategias de mitigación de riesgos. El SRC es un comité de muy alto nivel, liderado por un ejecutivo responsable y se compone de gerentes superiores, lo que incluye gerentes de línea responsables de las áreas funcionales, así como también, de aquellos departamentos administrativos pertinentes. El gerente de seguridad operacional participa en el SRC solo en una función de asesoría. El SRC puede reunirse con poca frecuencia, a menos que circunstancias excepcionales indiquen lo contrario. El SRC:

a) controla la eficacia del SMS;

b) controla que se tome cualquier medida correctiva necesaria de forma oportuna;

c) controla el rendimiento en materia de seguridad operacional en comparación con la política y los objetivos de seguridad operacional de la organización;

d) controla la eficacia de los procesos de gestión de seguridad operacional de la organización, la que respalda la prioridad empresarial declarada de la gestión de seguridad operacional como otro proceso comercial principal;

e) controla la eficacia de la supervisión de seguridad operacional de las operaciones subcontratadas; y

f) garantiza que los recursos correspondientes estén asignados para lograr el rendimiento en materia de seguridad operacional más allá de lo que requiere el cumplimiento reglamentario.

5.3.33 El SRC es estratégico y aborda temas de alto nivel relacionados con políticas, la asignación de recursos y el control del rendimiento institucional. Luego que el SRC desarrolla una dirección estratégica, se deben coordinar las estrategias de seguridad operacional en toda la organización. Esto puede lograrse al crear un grupo de acción de seguridad operacional (SAG). Los SAG se componen de gerentes de línea y personal de primera línea, y los lidera normalmente un gerente de línea designado. Los SAG son entidades tácticas que abordan problemas de implementación específicos según la dirección del SRC. 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 gestión de riesgos de seguridad operacional correspondientes, con participación del personal, según sea necesario, para generar conciencia de la seguridad operacional;

b) coordinan la resolución de las estrategias de mitigación para las consecuencias de peligros identificadas y garantizan que existan disposiciones satisfactorias para la captura de los datos de seguridad operacional y los comentarios del empleado;

c) evalúan el impacto de la seguridad operacional relacionado con la introducción de cambios operacionales o nuevas tecnologías;

d) coordinan la implementación de planes de medidas correctivas y garantizan que se tome la medida correctiva de forma oportuna;

e) revisan la eficacia de las recomendaciones de seguridad operacional anteriores; y

f) supervisan las actividades de promoción de la seguridad operacional, según sea necesario, para aumentar la conciencia de los empleados sobre temas de seguridad operacional y para garantizar que se les proporcione oportunidades adecuadas para participar en las actividades de la gestión de seguridad operacional.

Elemento 1.4 del SMS Coordinación de la planificación de respuesta ante emergencias

El proveedor de servicios deberá garantizar que un plan de respuesta ante emergencias esté coordinado correctamente con los planes de respuesta ante emergencias de aquellas organizaciones con las que deben establecer una interfaz, durante la entrega de sus servicios.

Estrategia de implementación

5.3.34 Un plan de respuesta ante emergencias (ERP) documenta las medidas que deberá tomar todo el personal responsable durante las emergencias relacionadas con la aviación. El propósito de un ERP es 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. En el plan también se incluye la autorización de las medidas realizadas por personal clave, así como también, los medios para coordinar esfuerzos necesarios para hacer frente a la emergencia. El objetivo general es salvar vidas, la continuación segura de las operaciones y el retorno a las operaciones normales, lo antes posible.

5.3.35 La aplicabilidad de la planificación de respuesta ante emergencias se extiende a los proveedores de productos de aviación que pueden atribuirse al suceso de seguridad operacional de la aviación o verse afectado por él. Por lo general, los procesos del proveedor de productos se conocen como "respaldo de producto de contingencia" e incluyen la medida de aeronavegabilidad de emergencia, los servicios de alerta y el respaldo en terreno para los accidentes de la aeronave. El proveedor de servicios no necesita cambiar el nombre de estos procesos de respaldo al producto a procesos de ERP; sin embargo, se debe dejar una constancia adecuada en la documentación de SMS de la organización. Véase el Apéndice 3 para guía detallada sobre ERP.

Elemento 1.5 del SMS Documentación del SMS

1.5.1 El proveedor de servicios deberá desarrollar un plan de implementación de SMS, formalmente respaldado por la organización, que defina el enfoque de la organización acerca de la gestión de la seguridad operacional en una forma que cumpla los objetivos de seguridad operacional de la organización.

1.5.2 El proveedor de servicios deberá desarrollar y mantener la documentación de SMS que describa:

a) la política y los objetivos de la seguridad operacional;

b) los requisitos de SMS;

c) los procesos y procedimientos de SMS;

d) las responsabilidades y autoridades para los procesos y procedimientos de SMS; y

e) los resultados de SMS.

1.5.3 El proveedor de servicios deberá desarrollar y mantener un manual de SMS como parte de su documentación de SMS.

Guía general

5.3.36 La documentación de SMS debe incluir un documento de descripción (exposición) de alto nivel, que describa al SMS de la organización de acuerdo con sus componentes y elementos. Tal documento facilita la administración, la comunicación y el mantenimiento internos del SMS de la organización. Al mismo tiempo, sirve como la comunicación (declaración) de SMS de la organización a la autoridad pertinente (CAA) para propósitos de aceptación,

evaluación y posterior vigilancia reglamentarias del SMS. Este documento de SMS de alto nivel puede ser un documento independiente o puede ser una "sección/capítulo del SMS" distinto dentro del documento aprobado por la organización existente (o CAA). Donde los detalles de los procesos de SMS de la organización ya estén abordados en los documentos existentes, es suficiente contar con referencias cruzadas adecuadas a dichos documentos. Este documento de SMS se deberá mantener actualizado y donde se piense hacer o se han hecho enmiendas importantes, se podría necesitar la concurrencia de CAA, donde sea necesario. En el Apéndice 4 encontrará una guía para la compilación de un documento de SMS.

5.3.37 Otro aspecto de la documentación de SMS es la compilación y el mantenimiento de registros que corroboran la existencia y operación continua del SMS. Tales registros deben organizarse de acuerdo con los elementos de SMS respectivos y los procesos asociados. Para ciertos procesos, puede que sea suficiente un sistema de documentación de SMS para incluir copias o muestras de registros mantenidos dentro de otros sistemas de documentación de la organización (como el departamento de registros técnicos y la biblioteca central). Durante la etapa de implementación inicial, la documentación de SMS puede incluir un registro del análisis de brechas y el plan de implementación en etapas.

Estrategia de implementación

5.3.38 La documentación de SMS aborda todos los elementos y procesos del SMS y normalmente incluye:

a) una descripción consolidada de los componentes y elementos de SMS, como por ejemplo:

   1) gestión de documentos y registros;

   2) requisitos del SMS reglamentario;

   3) marco de trabajo, alcance e integración;

   4) política y objetivos de seguridad operacional;

   5) responsabilidades de la seguridad operacional y personal clave;

   6) sistema de notificación de peligros voluntaria;

   7) procedimientos de notificación e investigación de incidentes;

   8) procesos de identificación de peligros y evaluación de riesgos;

   9) indicadores de rendimiento en materia de seguridad operacional;

   10) capacitación y comunicación de seguridad operacional;

   11) mejora continua y auditoría de SMS;

   12) gestión de cambio; y

   13) planificación de contingencia de emergencia u operaciones;

b) una compilación de registros y documentos relacionados con SMS actuales, como por ejemplo:

   1) registro del informe de peligros y muestras de los informes reales;

2) indicadores de rendimiento en materia de seguridad operacional y gráficos relacionados;

3) registro de evaluaciones de seguridad operacional completadas o en progreso;

4) registros de revisión o auditoría internas de SMS;

5) registros de promoción de seguridad operacional;

6) registros de capacitación de SMS/seguridad operacional del personal;

7) actas de la reunión del comité de SMS/seguridad operacional; y

8) plan de implementación del SMS (durante el proceso de implementación).

Componente 2 del SMS. Gestión de riesgos de la seguridad operacional

Guía general

5.3.39 Los proveedores de servicios deben garantizar que los riesgos de seguridad operacional encontrados en las actividades de aviación están bajo control para alcanzar sus objetivos de eficacia de la seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional e incluye la identificación de peligros, la evaluación de riesgos de seguridad operacional y la implementación de medidas de solución adecuadas. El proceso de gestión de riesgos de seguridad operacional se ilustra en la Figura 5-2.

5.3.40 El componente de la gestión de riesgos de seguridad operacional identifica sistemáticamente los peligros que existen dentro del contexto de la entrega de sus productos o servicios. Puede que los peligros sean el resultado de los sistemas que son deficientes en su diseño, función técnica, interfaz humana o interacciones con otros procesos y sistemas. También pueden producirse a partir 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 durante las etapas de planificación, diseño e implementación puede identificar posibles peligros antes de que el sistema quede operativo.

5.3.41 También es fundamental comprender el sistema y su entorno de operación para lograr un alto rendimiento en materia de seguridad operacional. Se pueden descubrir peligros durante el ciclo de la vida operacional, mediante los informes de empleados o investigaciones de incidentes. El análisis de estos peligros se debe hacer en el contexto del sistema. Este contexto es clave para evitar atribuir los eventos a "errores humanos", donde puedan omitirse los defectos en el sistema, quedando latentes para eventos futuros o posiblemente más graves que podrían suceder. En 5.3.42 a 5.3.61, al igual que en el Capítulo 2, 2.14 y 2.15, respectivamente, podrá encontrar una guía que aborda los procedimientos y formatos de identificación de peligros y evaluación de riesgos.

Elemento 2.1 del SMS Identificación de peligros

2.1.1 El proveedor de servicios deberá desarrollar y mantener un proceso formal que garantice que los peligros asociados con sus productos o servicios de aviación están identificados.

2.1.2 La identificación de peligros deberá basarse en una combinación de métodos reactivos, proactivos y predictivos de recopilación de datos de seguridad operacional.

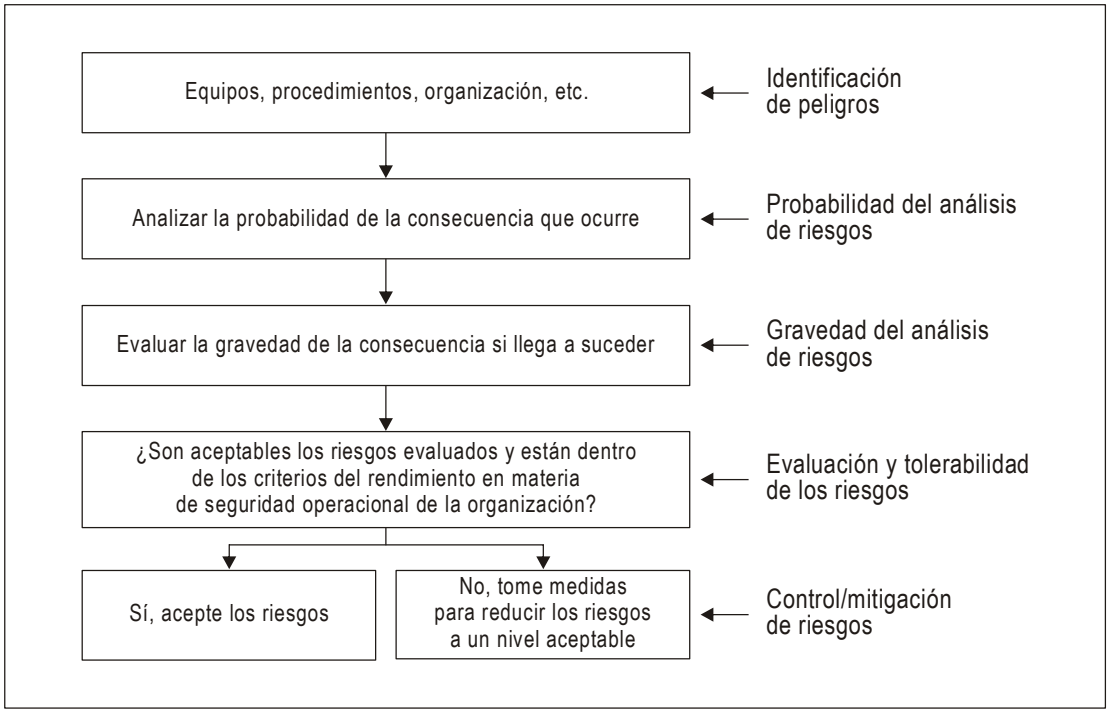


Figura 5-2. El proceso de gestión de riesgos de la seguridad operacional

Guía general

5.3.42 La gestión de riesgos de seguridad operacional requiere que el proveedor de servicios desarrolle y mantenga un proceso formal para identificar peligros que pueden contribuir con los sucesos relacionados con la aviación. Los peligros pueden existir en las actividades de aviación continuas o introducirse accidentalmente en una operación cada vez que se producen cambios al sistema de aviación. En este caso, la identificación de peligros es una parte integral de los procesos de la gestión de cambio, como se describió en el Elemento 3.2 del SMS — La gestión de cambio.

5.3.43 La identificación de peligros se basa en una combinación de métodos de recopilación de datos de seguridad operacional reactivos, proactivos y predictivos, como se analizó en el Capítulo 2. La identificación de peligros es el primer paso en el proceso de gestión de riesgos de la seguridad operacional. Los riesgos de seguridad operacional correspondientes se evalúan dentro del contexto de las consecuencias potencialmente dañinas relacionadas con el peligro. Donde se evalúe que los riesgos de seguridad operacional son inaceptables, se deben incorporar controles de riesgos de seguridad operacional adicionales en el sistema.

5.3.44 En los sistemas de gestión de seguridad operacional maduros, la identificación de peligros es continua y es parte integral de los procesos institucionales del proveedor de servicios. Varias condiciones activan actividades de identificación de peligros más en profundidad y de largo alcance, y pueden incluir:

a) instancias donde la organización experimenta un inexplicable aumento en los eventos relacionados con la seguridad operacional o el no cumplimiento reglamentario;

b) cambios operaciones importantes, como cambios anticipados para el personal clave u otros componentes importantes del sistema; y

c) cambios institucionales importantes, como crecimiento y contracción anticipados, fusiones empresariales o adquisiciones.

5.3.45 Un enfoque estructurado para la identificación de peligros puede incluir el uso de sesiones de intercambio de ideas en grupo, en las cuales los expertos en los temas explican escenarios de análisis detallados. Las sesiones de identificación de peligros requieren una gama de personal de operaciones y técnico con experiencia y los gestiona un facilitador. Se puede usar el mismo grupo para evaluar los riesgos de seguridad operacional correspondientes.

5.3.46 El sistema de gestión de la información de la seguridad operacional del proveedor de servicios debe incluir la documentación de la evaluación de seguridad operacional que contiene descripciones de peligros, las consecuencias relacionadas, la probabilidad evaluada y la gravedad de los riesgos de seguridad operacional, además de los controles de riesgos de la seguridad operacional necesarios. Las evaluaciones de la seguridad operacional existentes deben revisarse cada vez que se identifican peligros nuevos y se anticipan propuestas para otros controles de riesgos de la seguridad operacional.

5.3.47 La Figura 5-3 ilustra la documentación de peligros y el proceso de gestión de riesgos de seguimiento. Los peligros se identifican constantemente mediante varias fuentes de datos. Se espera que el proveedor de servicios identifique peligros, elimine estos peligros o mitigue los riesgos asociados. En el caso de peligros identificados en los productos o servicios suministrados mediante subcontratistas, una mitigación podría ser el requisito del proveedor de servicios para que tales organizaciones tengan un SMS o un proceso equivalente para la identificación de peligros y la gestión de riesgos.

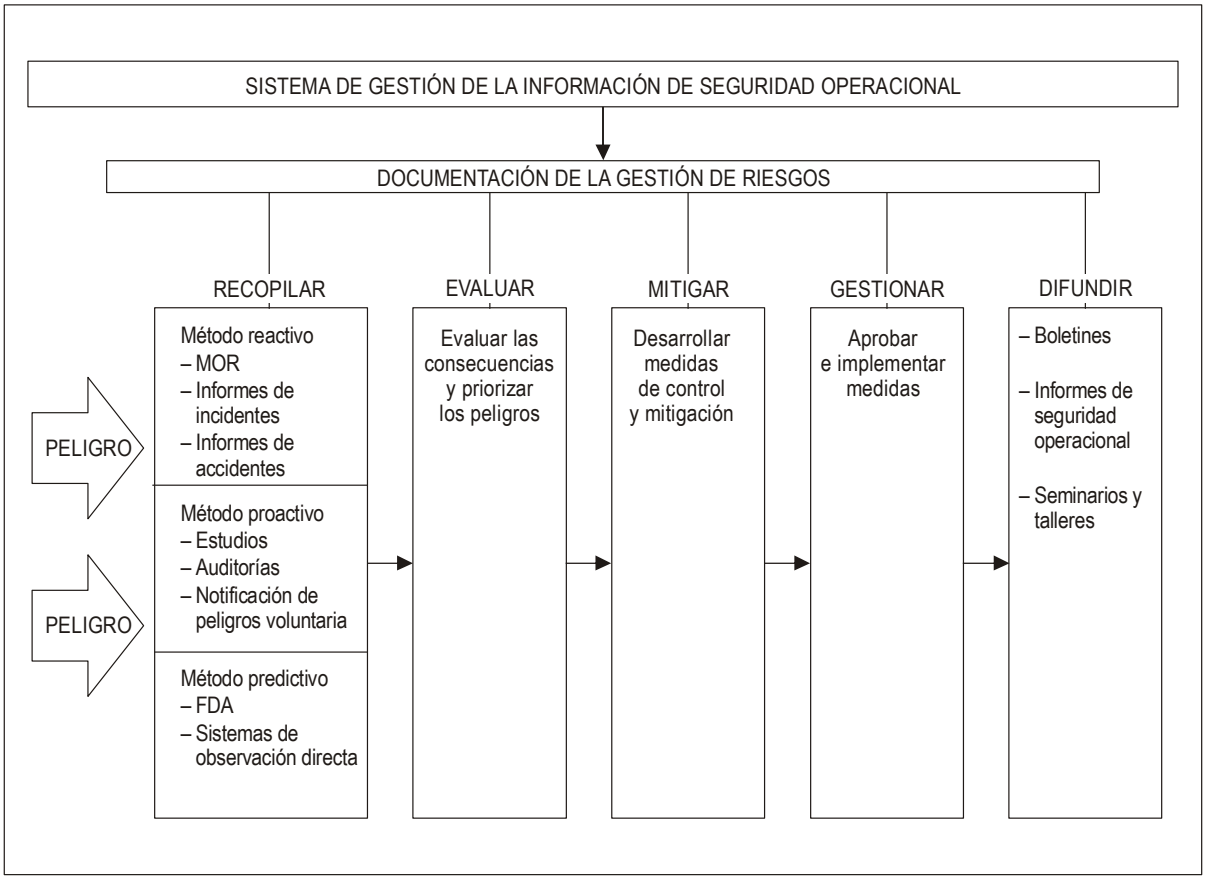


Figura 5-3. Documentación de peligros y seguimiento del proceso de gestión de riesgos

5.3.48 El sistema de información de la gestión de seguridad operacional se convierte en una fuente de conocimientos de seguridad operacional que se usará como referencia en los procesos de toma de decisiones de la seguridad operacional institucional. Este conocimiento de la seguridad operacional proporciona el material para el análisis de tendencia de la seguridad operacional, así como también, para la educación de la seguridad operacional. En el Apéndice 5 podrá encontrar una guía sobre los sistemas de notificación voluntaria y confidencial de peligros.

Estrategia de implementación

5.3.49 Lo siguiente podrá considerarse mientras se participa en el proceso de identificación de peligros:

a) factores de diseño, como el diseño del equipo y las tareas;

b) limitaciones del desempeño humano (por ejemplo, fisiológico, sicológico y cognitivo);

c) procedimientos y prácticas de operación, como su documentación y las listas de verificación bajo condiciones de operación reales;

d) factores de comunicación, como medios, terminología e idioma;

e) factores institucionales, como aquellos relacionados con el reclutamiento, capacitación y retención de personal, la compatibilidad de metas de producción y seguridad operacional, la asignación de los recursos, las presiones de operación y la cultura de seguridad operacional empresarial;

f) factores relacionados con el entorno operacional del sistema de aviación (por ejemplo, ruido ambiental y vibración, temperatura, iluminación y la disponibilidad de equipo y ropa de protección);

g) factores de vigilancia reglamentaria, como la aplicabilidad y ejecutabilidad de los reglamentos y la certificación del equipo, el personal y los procedimientos;

h) sistemas de control de rendimiento que pueden detectar desviaciones de la práctica o desviaciones operacionales; e

i) factores de la interfaz humano-máquina.

5.3.50 Los peligros pueden identificarse mediante las metodologías proactivas y predictivas o como resultado de investigaciones de accidentes o incidentes. Existe una variedad de fuentes de datos de identificación de peligros que pueden ser internos o externos a la organización. Entre los ejemplos de fuentes de datos de la identificación de peligros internos se incluyen:

a) diagramas de control de operación normal (por ejemplo, análisis de datos en vuelo para los explotadores de aeronaves);

b) sistemas de notificación voluntaria y obligatoria;

c) estudios de seguridad operacional;

d) auditorías de seguridad operacional;

e) comentarios de la capacitación; y

f) investigación e informes de seguimiento sobre accidentes/incidentes.

5.3.51 Entre los ejemplos de fuentes de datos externos para la identificación de peligros se incluyen:

a) informes de accidentes industriales;

b) sistemas de notificación de incidentes obligatoria estatal;

c) sistemas de notificación de incidentes voluntaria estatal;

d) auditorías de vigilancia estatal; y

e) sistemas de intercambio de información.

5.3.52 El tipo de tecnologías usadas en el proceso de identificación de peligros dependerá de la envergadura y complejidad del proveedor de servicios y sus actividades de aviación. En todos los casos, el proceso de identificación de peligros del proveedor de servicios se describe claramente en la documentación de SMS/seguridad operacional de la organización. El proceso de identificación de peligros considera todos los peligros posibles que puedan existir dentro del alcance de las actividades de aviación del proveedor de servicios, como las interfaces con otros sistemas, tanto dentro como fuera de la organización. Luego de identificar los peligros, sus consecuencias (es decir, cualquier evento o resultado específico) se deben determinar. Véase el Apéndice 5 para guía sobre el sistema de notificación voluntaria y confidencial de una organización.

Elemento 2.2 del SMS Evaluación y mitigación de riesgos de la seguridad operacional

El proveedor de servicios deberá desarrollar y mantener un proceso que garantiza el análisis, la evaluación y el control de los riesgos de seguridad operacional asociados con los peligros identificados.

Guía general

5.3.53 La Figura 5-4 presenta el proceso de gestión de riesgos de seguridad operacional por completo. El proceso comienza con la identificación de los peligros y sus posibles consecuencias. Los riesgos de seguridad operacional se evalúan en términos de probabilidad y gravedad, para definir el nivel de riesgos de seguridad operacional (índice de riesgo de seguridad operacional). Si los riesgos de seguridad operacional evaluados se consideran tolerables, se debe tomar una medida adecuada y la operación puede continuar. La identificación de peligros completada y el proceso de evaluación y mitigación de riesgos de seguridad operacional se documenta y aprueba como corresponda y forma parte del sistema de gestión de información de seguridad operacional.

5.3.54 Si los riesgos de seguridad operacional se evalúan como intolerables, las siguientes preguntas son pertinentes:

a) ¿Pueden eliminarse los peligros y riesgos de seguridad operacional relacionados? Si la respuesta es Sí, se toma y documenta una medida correspondiente. Si la respuesta es No, la siguiente pregunta es:

b) *¿Pueden mitigarse los riesgos de seguridad operacional?* Si la respuesta es No, las actividades relacionadas deben cancelarse. Si la respuesta es Sí, se toma una medida de mitigación correspondiente y la siguiente pregunta es:

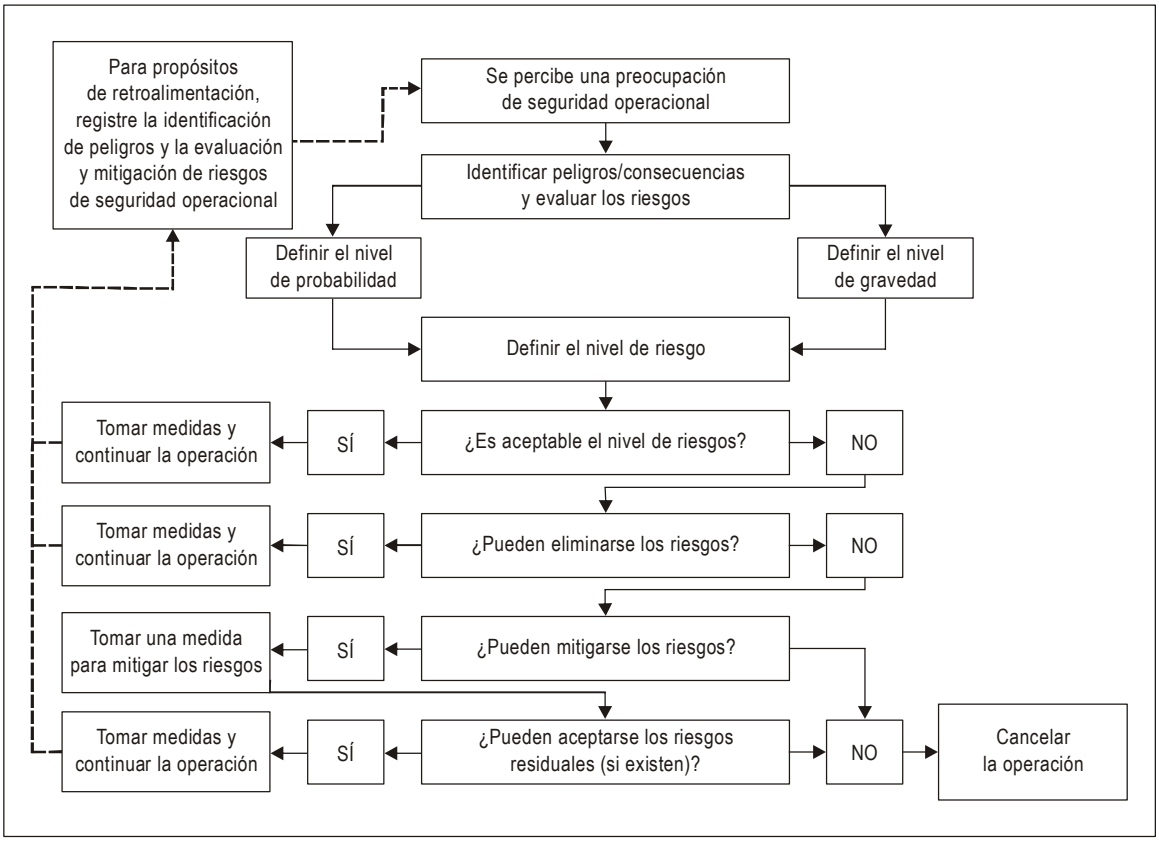


Figura 5-4. El proceso de gestión de riesgos de la seguridad operacional

b) *¿Existe algún riesgo de seguridad operacional residual?* Si la respuesta es Sí, los riesgos residuales deben evaluarse para determinar su nivel de tolerabilidad, así como también, si pueden eliminarse o mitigarse según sea necesario, para garantizar un nivel aceptable de rendimiento en materia de seguridad operacional.

5.3.55 La evaluación de riesgos de seguridad operacional implica un análisis de peligros identificados que incluye dos componentes:

a) la gravedad de un resultado de seguridad operacional; y

b) la probabilidad que sucederá.

En el Capítulo 2 se proporciona una guía sobre cómo se debe analizar la información de seguridad operacional en organizaciones complejas y grandes. Luego de que los riesgos se han evaluado, el proveedor de servicios entrará al proceso de toma de decisiones para determinar la necesidad de implementar medidas de mitigación de riesgos. Este proceso de toma de decisiones implica el uso de una herramienta de categorización de riesgos que puede estar en forma de una matriz de evaluación. En la Figura 5-5 se ofrece un ejemplo de una matriz de evaluación (índice) de riesgos de seguridad operacional.

Probabilidad del riesgo		Gravedad del riesgo				
		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

Figura 5-5. Ejemplo de una matriz de evaluación (índice) de riesgos de seguridad operacional

5.3.56 Al usar esta matriz, los riesgos pueden categorizarse de acuerdo con una evaluación de su posible gravedad y probabilidad. Mientras se recomienda una metodología de matriz de evaluación, están disponibles otros métodos equivalentes de descripción de la tolerancia de riesgos. La matriz de evaluación de riesgos puede personalizarse para reflejar el contexto de cada estructura institucional y actividades de aviación del proveedor de servicios y puede estar sujeta al acuerdo de su autoridad reglamentaria. Según este ejemplo de matriz, los riesgos reflejados como inaceptables (categorías roja y amarilla) deben mitigarse para reducir su gravedad o probabilidad. El proveedor de servicios debe considerar la suspensión de cualquier actividad que siga exponiendo la organización a riesgos de seguridad operacional intolerables en la ausencia de medidas de mitigación que reduzcan los riesgos a un nivel aceptable. En el Capítulo 2 de este documento se incluye información adicional sobre la probabilidad, la gravedad y la matriz de tolerabilidad de riesgos.

5.3.57 Después de evaluar los riesgos de seguridad operacional, se pueden implementar medidas de mitigación adecuadas. Entre las medidas de mitigación se pueden incluir varias alternativas como, entre otras, las modificaciones a los procedimientos de operación existentes, los programas de capacitación o el equipo usado en el suministro de productos o servicios de aviación. Las alternativas adicionales pueden incluir la introducción de nuevos procedimientos de operación, programas de capacitación, tecnologías o controles de vigilancia. Casi de forma invariable, estas alternativas implicarán el desarrollo o nuevo desarrollo de las tres defensas de seguridad operacional de aviación tradicionales: tecnología, capacitación y regulación. Se debe hacer una determinación de cualquier consecuencia accidental, particularmente la introducción de nuevos peligros, antes de la implementación de cualquier medida de mitigación de riesgos.

5.3.58 Los tres enfoques genéricos de mitigación de riesgos de la seguridad operacional incluyen:

a) *Prevención.* La actividad se suspende a causa de que los riesgos de seguridad operacional asociados son intolerables o se consideran inaceptables en comparación con los beneficios asociados.

b) *Reducción.* Se acepta cierta exposición de riesgos de seguridad operacional, aunque la gravedad o probabilidad asociada con los riesgos se aminora, posiblemente mediante medidas que mitigan las consecuencias relacionadas.

c) *Segregación de la exposición.* Medida tomada para aislar la posible consecuencia relacionada con el peligro o para establecer varias capas de defensas contra ella.

5.3.59 Una estrategia de mitigación de riesgos puede implicar uno de los enfoques descritos anteriormente o puede incluir múltiples enfoques. Es importante considerar toda la gama de posibles medidas de control para encontrar una solución óptima. La eficacia de cada estrategia alternativa debe evaluarse antes de poder tomar una decisión. Cada alternativa de mitigación de riesgos de seguridad operacional propuesta debe examinarse a partir de las siguientes perspectivas:

a) *Eficacia.* El grado hasta donde las alternativas reducen o eliminan los riesgos de seguridad operacional. La eficacia puede determinarse en términos de defensas técnicas, de capacitación y reglamentarias que pueden reducir o eliminar los riesgos de seguridad operacional.

b) *Costo/beneficio.* El grado hasta donde los beneficios percibidos de la mitigación exceden los costos.

c) *Practicidad.* El grado hasta donde la mitigación puede implementarse y cuán adecuado es en términos de tecnología disponible, recursos financieros y administrativos, legislación y reglamentos, voluntad política, etc.

d) *Aceptabilidad.* El grado hasta donde la alternativa es coherente con los paradigmas del accionista.

e) *Ejecutabilidad.* El grado hasta donde el cumplimiento de nuevas reglas, reglamentos o procedimientos de operación pueden supervisarse.

f) *Durabilidad.* El grado hasta donde la mitigación será sostenible y eficaz.

g) *Riesgos de seguridad operacional residual.* El grado de los riesgos de seguridad operacional que sigue siendo secundario a la implementación de la mitigación inicial y que podría necesitar medidas de control de riesgos adicionales.

h) *Consecuencias accidentales.* La introducción de nuevos peligros y riesgos de seguridad operacional relacionados que estén asociados con la implementación de cualquier alternativa de mitigación.

5.3.60 Luego de aprobar e implementar la mitigación, cualquier impacto asociado con el rendimiento en materia de seguridad operacional proporciona retroalimentación para el proceso de aseguramiento de la seguridad operacional del proveedor de servicios. Esto es necesario para garantizar la integridad, eficiencia y eficacia de las defensas según las nuevas condiciones operacionales.

5.3.61 Cada ejercicio de mitigación de riesgos se documentará de manera progresiva. Esto puede lograrse al usar una variedad de aplicaciones, desde hojas de cálculo o tablas básicas hasta software personalizado de mitigación de riesgos comercial. Los documentos de mitigación de riesgos completos deben recibir la aprobación del nivel correspondiente de la administración. Para conocer un ejemplo de una hoja de cálculo de mitigación de riesgos de peligros básica, véase el Apéndice 2 del Capítulo 2.

Componente 3 del SMS. Aseguramiento de la seguridad operacional

5.3.62 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. El proveedor de servicios controla continuamente sus procesos internos, así como también, su entorno de operación para detectar cambios o desviaciones que puedan introducir riesgos de seguridad operacional emergentes o la degradación de los controles de riesgos existentes. Tales cambios o desviaciones podrían abordarse entonces con el proceso de gestión de riesgos de seguridad operacional.

5.3.63 El proceso de aseguramiento de la seguridad operacional complementa aquel del aseguramiento de la calidad; cada uno de estos procesos requiere de análisis, documentación, auditoría y revisiones de la gestión para garantizar que se cumplan ciertos criterios de rendimiento. Si bien es común que el aseguramiento de la calidad se centre en el cumplimiento de requisitos reglamentarios por parte de la organización, el aseguramiento de la seguridad operacional controla específicamente la eficacia de los controles de riesgos de la seguridad operacional.

5.3.64 La relación complementaria entre el aseguramiento de la seguridad operacional y el aseguramiento de la calidad permite la integración de ciertos procesos de respaldo. Tal integración puede servir para lograr sinergias a fin de garantizar que se cumplan los objetivos de seguridad operacional, calidad y comerciales del proveedor de servicios.

5.3.65 Finalmente, las actividades del aseguramiento de seguridad operacional deben incluir el desarrollo y la implementación de medidas correctivas en respuesta a los hallazgos de deficiencias sistémicas que podrían tener un impacto en la seguridad operacional. La responsabilidad institucional del desarrollo e implementación de medidas correctivas debe residir con los departamentos citados en los hallazgos.

Elemento 3.1 del SMS Control y medición del rendimiento en materia de seguridad operacional

3.1.1 El proveedor de servicios desarrollará y mantendrá los medios para verificar el rendimiento en materia de seguridad operacional de la organización y para validar la eficacia de los controles de riesgos de la seguridad operacional.

3.1.2 El rendimiento en materia de seguridad operacional del proveedor de servicios se verificará en referencia a los indicadores de rendimiento en materia de seguridad operacional y los objetivos de rendimiento en materia de seguridad operacional del SMS.

Estrategia de implementación

5.3.66 La información usada para medir el rendimiento en materia de seguridad operacional de la organización se genera mediante sus sistemas de notificación de la seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional se analizan en detalle en la sección 5.4.5 y en el Apéndice 6 de este capítulo.

5.3.67 Existen dos tipos de sistemas de notificación:

a) sistemas de notificación de incidentes obligatoria; y

b) sistemas de notificación de incidentes voluntaria.

5.3.68 Los *sistemas de notificación de incidentes obligatoria* requieren ciertos tipos de eventos (por ejemplo, incidentes graves, incursiones en la pista). Esto necesita la implementación de reglamentos detallados que identifiquen los criterios de notificación y el alcance de sucesos que pueden notificarse. Los sistemas de notificación obligatoria tienden a recopilar más información relacionada con averías técnicas de alto impacto que otros aspectos de las actividades operacionales.

5.3.69 Los *sistemas de notificación voluntaria* permiten el envío de información relacionada con los peligros observados o errores accidentales sin un requisito legal o administrativo asociado para hacerlo. En estos sistemas, las agencias reglamentarias o las organizaciones pueden ofrecer un incentivo para realizar un informe. Por ejemplo, se puede omitir una medida de cumplimiento para los informes de errores o infracciones accidentales. En estas circunstancias, la información notificada solo se usará para respaldar la mejora de la seguridad operacional. Tales sistemas se consideran “no punitivos” dado que ofrecen protección a los notificadores, con lo que se garantiza una disponibilidad continua de dicha información para respaldar las mejoras constantes en el rendimiento en materia de seguridad operacional. Si bien la naturaleza y el grado de las políticas no punitivas de los proveedores de servicios pueden variar, la intención es promover una cultura de notificación eficaz e identificación proactiva de las deficiencias potenciales de la seguridad operacional.

5.3.70 Los sistemas de notificación voluntaria pueden ser confidenciales, lo que requiere que cualquier información que dé la identidad del notificador la sepan solo los "puntos de entrada” para permitir una medida de seguimiento. Los sistemas de notificación de incidentes confidencial facilitan la divulgación de peligros que generan errores humanos, sin miedo a retribuciones o dificultades Los informes de incidentes voluntarios pueden archivarse y su identidad eliminarse luego de haber tomado cualquier medida de seguimiento necesaria. Los informes sin identidad pueden respaldar futuros análisis de tendencias para rastrear la eficacia de la mitigación de riesgos y para identificar los peligros emergentes.

5.3.71 Para ser eficaces, las herramientas de notificación de seguridad operacional debe estar accesible fácilmente para el personal operacional. El personal de operaciones debe aprender sobre los beneficios de los sistemas de notificación de la seguridad operacional y se les debe entregar retroalimentación acerca de las medidas correctivas tomadas en respuesta al informe. La alineación de los requisitos, las herramientas de análisis y los métodos del sistema de notificación pueden facilitar el intercambio de información de seguridad operacional, así como también, comparaciones de ciertos indicadores de seguridad operacional. En el Apéndice 5 de este capítulo podrá encontrar una guía sobre los sistemas de notificación voluntaria y confidencial.

5.3.72 Otras fuentes de información de seguridad operacional para respaldar el control y la medición del rendimiento en materia de seguridad operacional pueden incluir:

a) *El estudio de seguridad operacional* es un análisis usado para obtener una comprensión de los amplios temas de seguridad operacional o aquellos de una naturaleza global. Por ejemplo, la industria de las líneas aéreas puede producir recomendaciones de seguridad operacional e implementar medidas para reducir accidentes e incidentes durante las etapas de acercamiento y aterrizaje. Los proveedores de servicios individuales pueden encontrar que estas recomendaciones globales mejoran el rendimiento en materia de seguridad operacional en el contexto de sus actividades de aviación.

b) *Las revisiones de seguridad operacional* son un componente fundamental de la gestión de cambio. Estas se llevan a cabo durante la introducción de nuevas tecnologías, nuevos procedimientos o cambios sistémicos que afectan las operaciones de la aviación. Las revisiones de seguridad operacional tienen un objetivo claramente definido que se vincula con el cambio en consideración. Las revisiones de seguridad operacional garantizan que el rendimiento en materia de seguridad operacional se mantenga a niveles adecuados durante los períodos de cambio.

c) *Los estudios de seguridad operacional* examinan los procedimientos o procesos relacionados con una operación específica. Los estudios de seguridad operacional implican el uso de listas de verificación, cuestionarios y entrevistas confidenciales e informales. Los estudios de seguridad operacional proporcionan generalmente información cualitativa que puede requerir de validación para determinar una medida correctiva correspondiente. Sin embargo, los estudios pueden proporcionar una fuente económica de información de seguridad operacional importante.

d) *Las auditorías* se centran en la integridad del SMS de la organización y en sus sistemas de respaldo. Las auditorías proporcionan una evaluación de los controles de riesgos de seguridad operacional y los procesos de aseguramiento de la calidad relacionados. Las auditorías pueden realizarse mediante entidades externas al proveedor de servicios o con un proceso de auditoría interna que cuente con las políticas y los procedimientos necesarios para garantizar su independencia y objetividad. Las auditorías tienen como fin proporcionar el aseguramiento de las funciones de la gestión de la seguridad operacional, lo que incluye al personal, el cumplimiento de reglamentos aprobados, niveles de competencia y capacitación.

e) *Las investigaciones internas* se llevan a cabo para ciertos eventos de seguridad operacional que pueden notificarse, de acuerdo con los requisitos internos o reglamentarios. Los accidentes e incidentes graves que investiga el Estado correspondiente o las autoridades regionales también pueden proporcionar el estímulo para llevar a cabo investigaciones internas mediante las organizaciones del proveedor de servicios.

5.3.73 El resultado final del control y la medición del rendimiento en materia de seguridad operacional es el desarrollo de indicadores de rendimiento en materia de seguridad operacional, basado en el análisis de los datos recopilados mediante las fuentes nombradas anteriormente. El proceso de control y medición implica el uso de indicadores de rendimiento en materia de seguridad operacional seleccionados y niveles de objetivos y alertas del rendimiento en materia de seguridad operacional correspondientes. En la Sección 5.4.5 y el Apéndice 6 podrá encontrar una guía sobre el desarrollo de indicadores de rendimiento en materia de seguridad operacional y su configuración de objetivos y alertas.

Elemento 3.2 del SMS La gestión de cambio

El proveedor de servicios deberá desarrollar y mantener un proceso formal para identificar los cambios que podrían afectar el nivel de riesgos de seguridad operacional asociados con sus productos o servicios de aviación, y para identificar y gestionar los riesgos de seguridad operacional que puedan emerger de aquellos cambios.

Estrategia de implementación

5.3.74 La experiencia de los proveedores de servicios de aviación cambia debido a varios factores, los que incluyen entre otros:

a) expansión o contracción institucional;

b) cambios a los sistemas, procesos o procedimientos internos que respaldan la entrega de productos y servicios; y

c) cambios al entorno de operación de la organización.

5.3.75 El cambio puede afectar la relevancia o eficacia de las estrategias de mitigación de riesgos de la seguridad operacional. Además, los nuevos peligros y los riesgos de seguridad operacional relacionados pueden introducirse accidentalmente en una operación cada vez que ocurre un cambio. Tales peligros deben identificarse para permitir la evaluación y el control de cualquier riesgo de seguridad operacional relacionado. Las revisiones de seguridad operacional, como se analizaron en el control y la medición del rendimiento en materia de seguridad operacional, pueden ser fuentes valiosas de información para respaldar los procesos de toma de decisiones y gestionar el cambio eficazmente.

5.3.76 El proceso de gestión de cambio de la organización debe considerar las siguientes tres consideraciones:

a) *Criticidad.* Las evaluaciones de criticidad determinan los sistemas, los equipos o las actividades que son fundamentales para la operación segura de la aeronave. Aunque la criticidad se evalúa normalmente durante el proceso de diseño del sistema, también es relevante durante una situación de cambio. Los sistemas, los equipos y las actividades que tengan una criticidad de seguridad operacional más alta deben revisarse después del cambio para asegurarse de que las medidas correctivas se tomaron para controlar los riesgos de seguridad operacional potencialmente emergentes.

b) *Estabilidad de los sistemas y entornos operacionales.* Los cambios pueden ser planificados y estar bajo el control directo de la organización. Dichos cambios incluyen el crecimiento y la contracción institucional, la expansión de los productos o servicios suministrados o la introducción de nuevas tecnologías. Los cambios no planificados pueden incluir aquellos relacionados con ciclos económicos, descontento laboral, así como también, cambios en los entornos políticos, reglamentarios u operacionales.

c) *Rendimiento pasado.* El rendimiento pasado de los sistemas críticos y el análisis de tendencias en el proceso de aseguramiento de la seguridad operacional debe usarse para anticipar y controlar el rendimiento en materia de seguridad operacional bajo situaciones de cambio. El control del rendimiento pasado también garantiza la eficacia de las medidas correctivas tomadas para abordar deficiencias de seguridad operacional identificadas como resultado de auditorías, evaluaciones, investigaciones o informes.

5.3.77 A medida que evolucionan los sistemas, los cambios incrementales pueden acumularse, lo que requiere enmiendas a la descripción inicial del sistema. Por lo tanto, la gestión de cambio necesita de revisiones periódicas de la descripción del sistema y el análisis de peligros de línea base para determinar su validez continua.

Elemento 3.3 del SMS Mejora continua del SMS

El proveedor de servicios deberá controlar y evaluar la eficacia de sus procesos de SMS para permitir la mejora continua del rendimiento general del SMS.

Estrategia de implementación

5.3.78 La medida continua se mide mediante el control de los indicadores de rendimiento en materia de seguridad operacional de la organización y se relaciona con la madurez y eficacia de un SMS. Los procesos del aseguramiento de la seguridad operacional respaldan las mejoras al SMS mediante la verificación continua y las medidas de seguimiento. Estos objetivos se logran mediante la aplicación de evaluaciones internas y auditorías independientes del SMS.

5.3.79 Las evaluaciones internas implican la evaluación de las actividades de aviación del proveedor de servicios que pueden proporcionar información útil a los procesos de toma de decisiones de la organización. Es aquí donde se realiza la actividad clave del SMS, la identificación de peligros y mitigación de riesgos (HIRM). Las evaluaciones realizadas a raíz de este requisito deben realizarlas personas u organizaciones que sean funcionalmente independientes de los procesos técnicos evaluados. La evaluación interna incluye la evaluación de las funciones de la gestión de la seguridad operacional, el diseño de políticas, la gestión de riesgos de la seguridad operacional, el aseguramiento de la seguridad operacional y la promoción de la seguridad operacional en toda la organización.

5.3.80 Las auditorías internas implican la examinación sistemática y programada de las actividades de aviación del proveedor de servicios, lo que incluye aquellas específicas para la implementación del SMS. Para lograr la máxima eficacia, las auditorías internas las llevan a cabo personas o departamentos que son independientes de las funciones que se evalúan. Tales auditorías proporcionan al ejecutivo responsable, así como también, a los funcionarios de administración superior responsables del SMS, la capacidad de rastrear la implementación y eficacia del SMS, al igual que sus sistemas de respaldo.

5.3.81 Las autoridades pertinentes, responsables de la aceptación del SMS del proveedor de servicios, puede realizar las auditorías externas del SMS. Además, las auditorías pueden realizarlas asociaciones industriales u otros terceros que selecciona el proveedor de servicios. Estas auditorías externas mejoran el sistema de auditoría interna, así como también, proporcionan vigilancia independiente.

5.3.82 En resumen, los procesos de evaluación y auditoría contribuyen con la capacidad del proveedor de servicios de lograr una mejora continua en el rendimiento en materia de seguridad operacional. El control continuo del SMS, sus controles de seguridad operacional relacionados y los sistemas de respaldo garantizan que el proceso de gestión de la seguridad operacional logre sus objetivos.

Componente 4 del SMS. Promoción de la seguridad operacional

5.3.83 La promoción de la seguridad operacional alienta una cultura de seguridad operacional positiva y crea un entorno que propicia el logro de los objetivos de seguridad operacional del proveedor de servicios. Una cultura de seguridad operacional positiva se caracteriza por tener valores, actitudes y conductas que se comprometen con los esfuerzos de seguridad operacional de la organización. Esto se logra mediante la combinación de competencias técnicas que mejoran continuamente con la capacitación y educación, las comunicaciones eficaces y la distribución de información. La administración superior proporciona el liderazgo para promover la cultura de seguridad operacional en toda la organización.

5.3.84 Un esfuerzo de seguridad operacional institucional no puede tener éxito por sí solo siguiendo una orden o adherencia estricta de las políticas. La promoción de la seguridad operacional afecta la conducta tanto de personas como de organizaciones y complementa las políticas, los procedimientos y los procesos de la organización, lo que proporciona un sistema de valor que respalda los esfuerzos de la seguridad operacional.

5.3.85 El proveedor de servicios debe establecer e implementar procesos y procedimientos que faciliten la comunicación eficaz en todos los niveles de la organización. Los proveedores de servicios deben comunicar sus objetivos de seguridad operacional, así como también, el estado actual de cualquier actividad o evento relacionado. Los proveedores de servicios también deben alentar la comunicación "jerárquica ascendente", lo que ofrece un entorno que permite a la administración superior recibir comentarios abiertos y constructivos del personal de operaciones.

Elemento 4.1 del SMS Capacitación y educación

4.1.1 El proveedor de servicios deberá desarrollar y mantener un programa de capacitación de seguridad operacional que garantice que el personal está capacitado y es competente para realizar sus tareas de SMS.

4.1.2 El alcance del programa de capacitación de la seguridad operacional deberá ser adecuado para la participación de cada persona en el SMS.

Estrategia de implementación

5.3.86 El gerente de seguridad operacional debe proporcionar información actual y facilitar la capacitación pertinente para los temas de seguridad operacional específicos que encuentran las unidades institucionales. La entrega de la capacitación al personal adecuado, sin importar su nivel en la organización, es un indicio del compromiso de la gestión con un SMS eficaz. El programa de capacitación y educación de seguridad operacional debe constar de lo siguiente:

a) políticas de seguridad operacional institucional, metas y objetivos;

b) funciones de seguridad operacional institucional y responsabilidades relacionadas con la seguridad operacional;

c) principios básicos de la gestión de riesgos de la seguridad operacional;

d) sistemas de notificación de la seguridad operacional;

e) respaldo de la gestión de la seguridad operacional (lo que incluye los programas de evaluación y auditoría);

f) líneas de comunicación para la diseminación de información de seguridad operacional;

g) un proceso de validación que mide la eficacia de la capacitación; y

h) adoctrinamiento inicial documentado y requisitos de capacitación recurrente.

5.3.87 Los requisitos de capacitación coherentes con las necesidades y la complejidad de la organización deben documentarse para cada área de actividad. Se debe desarrollar un archivo de capacitación para cada empleado, incluida la administración.

5.3.88 La capacitación de seguridad operacional dentro de una organización debe garantizar que el personal sea competente para realizar tareas relacionadas con la seguridad operacional. Los procedimientos de capacitación deben especificar normas de capacitación de seguridad operacional iniciales y recurrentes para el personal de operaciones, los gerentes y supervisores, los gerentes superiores y el ejecutivo responsable. La cantidad de capacitación de seguridad operacional debe ser adecuada para la responsabilidad y participación de la persona en el SMS. La documentación de capacitación del SMS también debe especificar las responsabilidades para el desarrollo del contenido y programación de la capacitación, así como también, la gestión de los registros de la capacitación.

5.3.89 La capacitación debe incluir la política de seguridad operacional y las funciones y responsabilidades de la seguridad operacional de la organización, los principios de SMS relacionados con la gestión de riesgos de la seguridad

operacional y el aseguramiento de la seguridad operacional, así como también, el uso y los beneficios de los sistemas de notificación de seguridad operacional de la organización.

5.3.90 La capacitación de la seguridad operacional para los gerentes superiores debe incluir el contenido relacionado con el cumplimiento de los requisitos de seguridad operacional nacionales e institucionales, la asignación de recursos y la promoción activa del SMS, lo que incluye la comunicación eficaz de seguridad operacional entre los departamentos. Además, la capacitación de seguridad operacional para los gerentes superiores debe incluir material acerca del establecimiento de niveles de objetivos y alertas del rendimiento en materia de seguridad operacional.

5.3.91 Finalmente, el programa de capacitación de la seguridad operacional puede incluir una sesión diseñada específicamente para el ejecutivo responsable. Esta sesión de capacitación debe estar en un alto nivel, dándole al ejecutivo responsable una comprensión del SMS y su relación con la estrategia comercial general de la organización.

Elemento 4.2 del SMS Comunicación de la seguridad operacional

El proveedor de servicios deberá desarrollar y mantener medios formales para la comunicación de seguridad operacional que:

a) garantice que el personal está consciente del SMS hasta un grado proporcional a sus cargos;

b) transfiera información fundamental de seguridad operacional;

c) explique por qué se toman medidas de seguridad operacional en particular; y

d) explique por qué se introducen y cambian procedimientos de seguridad operacional.

Estrategia de implementación

5.3.92 El proveedor de servicios debe comunicar los objetivos y procedimientos del SMS de la organización a todo el personal de operaciones. El gerente de seguridad operacional debe comunicar regularmente información sobre las tendencias de rendimiento en materia de seguridad operacional y temas de seguridad operacional específicos mediante los boletines y las sesiones informativas. El gerente de seguridad operacional también debe garantizar que las lecciones aprendidas a partir de las investigaciones, las historias de casos o las experiencias, ya sean internas o de otras organizaciones, se distribuyan ampliamente. El rendimiento en materia de seguridad operacional será más eficiente si se alienta activamente para que el personal de operaciones identifique e informe los peligros. Por lo tanto, la comunicación de la seguridad operacional apunta a:

a) garantizar que el personal esté totalmente consciente del SMS;

b) transmitir información fundamental de seguridad operacional;

c) tomar conciencia de las medidas correctivas; y

d) proporcionar información acerca de procedimientos nuevos o enmendados de seguridad operacional.

5.3.93 Entre los ejemplos de iniciativas de comunicación institucional se incluye:

a) la diseminación del manual del SMS;

b) los procesos y procedimientos de seguridad operacional;

c) los folletos informativos, las noticias y los boletines de seguridad operacional; y

d) sitios web o correo electrónico.

5.4 PLANIFICACIÓN DE LA IMPLEMENTACIÓN DEL SMS

5.4.1 Descripción del sistema

Una revisión y descripción del sistema de los elementos de SMS y su interfaz con los sistemas y los procesos existentes es el primer paso en la definición del alcance y aplicabilidad del SMS. Este ejercicio proporciona una oportunidad para identificar cualquier brecha relacionada con los componentes y elementos de SMS del proveedor de servicios. La descripción del sistema incluye las interfaces de SMS dentro de la organización, así como también, las interfaces pertinentes con otras organizaciones externas, como subcontratistas. Una descripción general del sistema y su estructura de responsabilidad y notificación debe incluirse en la documentación del SMS. Para las organizaciones grandes y complejas, los detalles de los sistemas básicos y los procedimientos institucionales se abordan en la exposición pertinente o los manuales administrativos del proveedor de servicios. En tales casos, una breve descripción junto con un diagrama institucional con referencias cruzadas adecuadas podría ser suficiente para el propósito de la descripción del sistema.

5.4.2 Integración de los sistemas de gestión

5.4.2.1 Según los contextos institucionales, operacionales y reglamentarios, un proveedor de servicios puede implementar un SMS integrado. La integración tiene el potencial de proporcionar sinergias al gestionar riesgos de seguridad operacional en varias áreas de las actividades de la aviación. Por ejemplo, un proveedor de servicios puede implementar un solo SMS para su organización de diseño, de producción y el departamento de vuelo de aviación corporativa. O bien, puede que haya situaciones donde sea adecuado solo un SMS para cada tipo de actividad de aviación. La organización puede definir los mejores medios para integrar o segregar su SMS como se adapte a su modelo comercial o institucional, siempre y cuando el Estado quede satisfecho de que se llevan a cabo correctamente todas las tareas de SMS en todas las funciones del proveedor de servicios. El SMS del proveedor de servicios también puede integrarse con sistemas de seguridad de la aviación y gestión sobre cuestiones de salud y seguridad en el trabajo.

Integración de SMS y QMS

5.4.2.2 Por lo general, los proveedores de servicios de aviación implementan sistemas de gestión a nivel empresarial. El rendimiento en materia de seguridad operacional institucional depende de la integración eficaz de estos sistemas para respaldar el suministro de productos y servicios. En el contexto de SMS, el aspecto más importante de la integración es el sistema de gestión de la calidad (QMS) del proveedor de servicios. El QMS se define generalmente como la estructura institucional y las responsabilidades, los recursos, los procesos y los procedimientos asociados que son necesarios para establecer y promover un sistema de aseguramiento y mejora de la calidad continuos mientras se suministra un producto o servicio. El QMS es un requisito reglamentario de la aviación existente para la mayoría de los proveedores de servicios, que incluye la aprobación de producción (Anexo 8), las organizaciones de mantenimiento (Anexo 6, Parte I) y los proveedores de servicios de datos meteorológicos y aeronáuticos (Anexos 3 y 15, respectivamente).

5.4.2.3 El QMS y SMS son complementarios. El QMS se centra en el cumplimiento de reglamentos y requisitos prescriptivos para satisfacer las expectativas y obligaciones contractuales del cliente, mientras que el SMS se centra en el rendimiento en materia de seguridad operacional. Los objetivos de un SMS son identificar peligros relacionados con la seguridad operacional, evaluar el riesgo asociado 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. Sin embargo, tanto el SMS como el QMS:

a) deben planificarse y gestionarse;

b) dependen de la medición y el control de los indicadores de rendimiento;

c) implican todas las funciones institucionales relacionadas con el suministro de productos y servicios de aviación; y

d) buscan una mejora continua.

5.4.2.4 El SMS y QMS usan procesos de gestión de riesgos y aseguramiento similares. El objetivo del SMS es identificar peligros relacionados con la seguridad operacional que la organización debe enfrentar, y controlar los riesgos asociados. El SMS está diseñado para gestionar riesgos de seguridad operacional y medir el rendimiento en materia de seguridad operacional durante el suministro de los productos y servicios. El proceso de gestión de riesgos de la seguridad operacional elimina los peligros o proporciona controles eficaces para mitigar los riesgos de seguridad operacional al mantener un equilibrio adecuado en la asignación de recursos entre la producción y protección para cumplir con requisitos de rendimiento en materia de seguridad operacional.

5.4.2.5 Un QMS proporciona coherencia en el suministro de los productos y servicios para cumplir con normas de rendimiento, así como también, con las expectativas del cliente. El QMS también tiene una función de aseguramiento independiente que usa un ciclo de retroalimentación para garantizar el suministro de productos y servicios que sean “aptos para el propósito” y estén libres de defectos o errores. La función de aseguramiento de la calidad identifica los procesos y procedimientos ineficaces que deben rediseñarse en cuanto a eficiencia y eficacia.

5.4.2.6 Es más, el SMS y QMS usan herramientas parecidas. Los profesionales de la seguridad operacional y la calidad se centran básicamente en la misma meta para proporcionar productos y servicios seguros y confiables a los clientes. Los profesionales de calidad y seguridad operacional están capacitados en diversos métodos de análisis, los que incluyen el análisis de la causa de origen y el análisis de tendencias estadísticas.

5.4.2.7 Dados los aspectos complementarios de SMS y QMS, es posible establecer una relación sinérgica entre los sistemas que pueden resumirse de la siguiente forma:

a) un SMS recibe el respaldo de los procesos de QMS como auditorías, inspección, análisis de causa de origen, diseño del proceso, análisis estadístico y medidas preventivas;

b) un QMS puede anticipar problemas de seguridad operacional que existan a pesar del cumplimiento de normas y especificaciones de la organización; y

c) los principios, las políticas y las prácticas de calidad están vinculadas a los objetivos de la gestión de seguridad operacional.

5.4.2.8 La relación entre el SMS y QMS produce contribuciones complementarias de cada sistema con el logro de las metas de seguridad operacional y calidad de la organización. En la Tabla 5-1 se ofrece una comparación de resumen de los dos sistemas.

Tabla 5-1. Comparación de resumen de QMS y SMS

QMS	*SMS*
Calidad	Seguridad operacional
Aseguramiento de la calidad	Aseguramiento de la seguridad operacional
Control de la calidad	Identificación de peligros y control de riesgos
Cultura de calidad	Cultura de seguridad operacional
Cumplimiento de requisitos	Nivel aceptable de rendimiento en materia de seguridad operacional
Prescriptivo	Basado en rendimiento
Normas y especificaciones	Factores institucionales y humanos
Reactivo > Proactivo	Proactivo > Predictivo

5.4.3 Análisis de brechas

5.4.3.1 Un análisis de brechas compara los procesos y procedimientos existentes de la gestión de seguridad operacional del proveedor de servicios con los requisitos que se incluyen en el marco de trabajo del SMS. Los proveedores de servicios de la aviación habrán implementado normalmente varias funciones de SMS a causa de su cumplimiento con reglamentos nacionales o la adopción de las mejores prácticas industriales. El desarrollo de un SMS debe basarse en las estructuras y los sistemas de control institucionales existentes. El análisis de brechas facilita el desarrollo de un plan de implementación de SMS al identificar las brechas que deben abordarse para implementar completamente un SMS. Luego que se complete el análisis de brechas y quede totalmente documentado, los recursos y procesos que se identificaron como faltantes o inadecuados formarán la base del plan de implementación del SMS.

5.4.3.2 En el Apéndice 7 de este capítulo se ofrece una lista de las preguntas del análisis de brechas para facilitar que los proveedores de servicios evalúen sistemáticamente sus procesos existentes. A partir de una respuesta objetiva hasta cada pregunta del análisis de brechas, es aparente que se necesita aplicar mejoras o medidas.

5.4.4 Plan de implementación del SMS

5.4.4.1 Un plan de implementación de SMS se desarrolla con el asesoramiento del ejecutivo responsable y los gerentes responsables del suministro de productos y servicios relacionados con la operación segura de la aeronave o en respaldo de esta. Luego de completarse, el ejecutivo responsable apoya el plan. El plan de implementación del SMS incluye cronologías e hitos coherentes con los requisitos identificados en el proceso de análisis de brechas, la envergadura del proveedor de servicios y la complejidad de sus productos o servicios. El plan debe abordar la coordinación con organizaciones o contratistas externos, donde corresponda.

5.4.4.2 El plan de implementación del proveedor de servicios puede documentarse de diferentes formas, lo que varía de una simple hoja de cálculos hasta software especializado de gestión de proyectos. El plan de implementación debe abordar brechas mediante la finalización de medidas e hitos específicos de acuerdo con la cronología determinada. La asignación de cada tarea garantiza una responsabilidad en todo el proceso de implementación. El plan

debe revisarse y actualizarse regularmente, según sea necesario. En el Apéndice 7 de este capítulo se muestra un ejemplo de formato de un plan/programa de implementación del SMS.

5.4.4.3 la completa implementación de todos los componentes y elementos del marco de trabajo del SMS puede demorar hasta cinco años, según la madurez y complejidad de la organización. La implementación de SMS, incluida una guía para un enfoque en etapas, se analiza en la Sección 5.5.

5.4.5 Indicadores de rendimiento en materia de seguridad operacional

5.4.5.1 Un SMS define los resultados del rendimiento medible para determinar si el sistema funciona verdaderamente en acuerdo con las expectativas de diseño y no cumplen simplemente con requisitos reglamentarios. Los indicadores de rendimiento en materia de seguridad operacional se usan para controlar los riesgos de seguridad operacional conocidos, detectar riesgos de seguridad operacional emergentes y para determinar cualquier medida correctiva necesaria.

5.4.5.2 Los indicadores de rendimiento en materia de seguridad operacional también proporcionan evidencia objetiva para que el regulador evalúe la eficacia del SMS del proveedor de servicios y controle el logro de sus objetivos de seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios consideran factores como la tolerancia de los riesgos de seguridad operacional de la organización, el costo/beneficios que conlleva la implementación de las mejoras al sistema, los requisitos reglamentarios y las expectativas públicas. Se deben seleccionar y desarrollar indicadores de rendimiento en materia de seguridad operacional con el asesoramiento de la autoridad reglamentaria del proveedor de servicios. Este proceso es necesario para facilitar la agregación del regulador y la armonización de los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios para el mismo sector de aviación.

5.4.5.3 Los indicadores de rendimiento en materia de seguridad operacional y los objetivos asociados debe aceptarlos el Estado responsable de la autorización, certificación o designación del proveedor de servicios. Los indicadores de rendimiento en materia de seguridad operacional son complementarios a cualquier requisito legal o reglamentario y no exime a los proveedores de servicios de sus obligaciones reglamentarias.

5.4.5.4 En la práctica, el rendimiento en materia de seguridad operacional de un SMS se expresa mediante indicadores de rendimiento en materia de seguridad operacional y sus valores de alertas y objetivos correspondientes. El proveedor de servicios debe controlar el rendimiento de los indicadores actuales en el contexto de tendencias históricas para identificar cambios anormales en el rendimiento en materia de seguridad operacional. De igual forma, la configuración de objetivos y alertas debe considerar el rendimiento histórico reciente para un indicador determinado. Los objetivos de mejora deseados deben ser realistas y alcanzables para el proveedor de servicios y el sector de aviación asociado.

5.4.5.5 El establecimiento de un nivel de alerta para un indicador de seguridad operacional es pertinente desde una perspectiva de control de riesgos. Un nivel de alerta es un criterio común para delinear las regiones de rendimiento aceptable de aquellas inaceptables para un indicador de seguridad operacional particular. Según los libros de métricas genéricas de seguridad operacional, un método objetivo básico para ajustar los criterios de alertas fuera de control (OOC) es el uso del principio de desviación estándar. Este método considera la desviación estándar y los valores promedio de los puntos de datos históricos previos para un indicador de seguridad operacional determinado. Estos dos valores se usan entonces para establecer el nivel de alerta para el siguiente período de control del indicador.

5.4.5.6 Una gama de indicadores de rendimiento en materia de seguridad operacional de alto y bajo impacto proporcionan una comprensión más integral acerca del rendimiento en materia de seguridad operacional del proveedor de servicios. Esto garantiza que se aborden los resultados de alto impacto (por ejemplo, accidentes e incidentes graves), así como también, los eventos de bajo impacto (por ejemplo, incidentes, informes de no cumplimiento, desviaciones). Los indicadores de rendimiento en materia de seguridad operacional son básicamente diagramas de tendencias de datos que

rastrean los sucesos en términos de tasas de eventos (por ejemplo, cantidad de incidentes cada 1 000 horas de vuelo). Los indicadores de alto impacto deben abordarse primero, mientras que los indicadores de bajo impacto pueden desarrollarse en una etapa más madura de la implementación del SMS.

5.4.5.7 Luego de definir los indicadores de rendimiento en materia de seguridad operacional y su configuración de objetivos y alertas correspondiente, el resultado del rendimiento de cada indicador debe actualizarse y controlarse de forma regular. Puede rastrearse el estado de rendimiento respectivo del nivel de objetivos y alertas para cada indicador. También se puede compilar/agregar un resumen consolidado del resultado de rendimiento general de objetivos y alertas de todo el paquete de indicadores de rendimiento en materia de seguridad operacional para un período de control determinado. Se pueden asignar valores cualitativos (satisfactorio/insatisfactorio) para cada “objetivo logrado” y cada “nivel de alerta no violado”. O bien, se pueden usar valores numéricos (puntos) para proporcionar una medición cuantitativa del rendimiento general del paquete de indicadores. En el Apéndice 6 de este capítulo se ofrecen ejemplos de los indicadores de rendimiento en materia de seguridad operacional y sus criterios de configuración de objetivos y alertas.

5.5 ENFOQUE DE IMPLEMENTACIÓN EN ETAPAS

5.5.1 Generalidades

5.5.1.1 El objetivo de esta sección es introducir un ejemplo de las cuatro etapas de implementación de SMS. La implementación de un SMS es un proceso sistemático. Sin embargo, este proceso puede resultar ser una tarea bastante desafiante dependiendo de los factores, como la disponibilidad del material guía y recursos necesarios para la implementación, así como también, el conocimiento preexistente del proveedor de servicios de los procesos y procedimientos del SMS.

5.5.1.2 Entre los motivos para un enfoque en etapas para la implementación de SMS se incluyen:

a) la disposición de una serie de pasos gestionables que se deban seguir para la implementación de un SMS, como la asignación de recursos;

b) la necesidad de permitir la implementación de elementos del marco de trabajo de SMS en varias secuencias, según los resultados de cada análisis de brechas del proveedor de servicios;

c) la disponibilidad inicial de los datos y procesos analíticos para respaldar las prácticas de gestión de la seguridad operacional reactiva, proactiva y predictiva; y

d) la necesidad de un proceso metodológico para garantizar la implementación de SMS eficaz y sustentable.

5.5.1.3 El enfoque en etapas reconoce que la implementación de un SMS completamente maduro es un proceso que toma varios años. Un enfoque de implementación en etapas permite que el SMS sea mucho más sólido a medida que se completa cada etapa de implementación. Se completan los procesos de gestión de la seguridad operacional fundamentales antes de pasar a etapas sucesivas que impliquen procesos de mayor complejidad.

5.5.1.4 Se proponen cuatro etapas de implementación para un SMS. Cada etapa se asocia con varios elementos (o subelementos) según el marco de trabajo del SMS de la OACI. Resulta aparente que la configuración particular de los elementos en este material guía no esté diseñada para ser absoluta. Los Estados y proveedores de servicios pueden elegir hacer estos ajustes como mejor se considere según las circunstancias. En la Tabla 5-2 se muestra un resumen de las cuatro etapas de la implementación del SMS y sus elementos correspondientes.

5.5.2 Etapa 1

5.5.2.1 El objetivo de la Etapa 1 de la implementación de SMS es proporcionar un plano de cómo se cumplirán los requisitos de SMS y se integrarán en los sistemas de control de la organización, así como también, un marco de trabajo de responsabilidad para la implementación del SMS.

5.5.2.2 Durante la Etapa 1, se establece una planificación básica y la asignación de responsabilidades. Un aspecto central en la Etapa 1 es el análisis de brechas. A partir del análisis de brechas, una organización puede determinar el estado de sus procesos de gestión de la seguridad operacional existentes y puede comenzar a planificar el desarrollo de otros procesos de gestión de la seguridad operacional. El resultado importante de la Etapa 1 es el plan de implementación del SMS.

5.5.2.3 Al finalizar la Etapa 1, se deben finalizar las siguientes actividades de tal forma que cumplan las expectativas de la autoridad de vigilancia de la aviación civil, como se establece en los requisitos y el material guía pertinentes:

Compromiso y responsabilidad de la gestión — Elemento 1.1 (i)

a) Identificar al ejecutivo responsable y las responsabilidades de seguridad operacional de los gerentes. Esta actividad se basa en los Elementos 1.1 y 1.2 del marco de trabajo del SMS de la OACI.

b) Establecer un plan de implementación del SMS. El equipo debe componerse de representantes de los departamentos pertinentes. El papel del equipo es impulsar la implementación de SMS desde la etapa de planificación hasta la implementación final. Otras funciones del equipo de implementación incluirán, entre otros:

   1) desarrollar el plan de implementación de SMS;

   2) garantizar la capacitación adecuada de SMS y experiencia técnica del equipo para implementar eficazmente los elementos del SMS y los procesos relacionados; y

   3) controlar y notificar el progreso de la implementación del SMS, proporcionar actualizaciones regulares y coordinar con el ejecutivo responsable de SMS.

c) Definir el alcance de las actividades de la organización (departamentos/divisiones) según el cual el SMS será aplicable. El alcance de la aplicabilidad del SMS de la organización se deberá describir posteriormente en el documento del SMS, según corresponda. Esta actividad se basa en el Elemento 1.5 del marco de trabajo del SMS de la OACI. En 5.4.1 de este capítulo podrá encontrar una guía sobre la descripción del sistema.

d) Realizar un análisis de brechas de los sistemas y procesos actuales de la organización en relación con los requisitos del marco de trabajo del SMS de la OACI (o los requisitos reglamentarios de SMS pertinentes). En el Apéndice 7 de este capítulo se encuentra una guía sobre un análisis de brechas de SMS para un proveedor de servicios.

Plan de implementación del SMS — Elemento 1.5 (i)

a) Desarrollar un plan de implementación del SMS acerca de cómo la organización implementará el SMS sobre la base del sistema identificado y las brechas del proceso que se generan del análisis de brechas. En el Apéndice 7 de este capítulo se muestra un ejemplo de un plan de implementación de SMS básico.

Tabla 5-2. Cuatro etapas de la implementación del SMS

Etapa 1 (12 meses)*	*Etapa 2 (12 meses)*	*Etapa 3 (18 meses)*	*Etapa 4 (18 meses)*
1. Elemento 1.1 del SMS (i): a) identificar al ejecutivo responsable del SMS; b) establecer un equipo de implementación del SMS; c) definir el alcance del SMS; d) realizar un análisis de brechas de SMS. 2. Elemento 1.5 del SMS (i): a) desarrollar un plan de implementación del SMS. 3. Elemento 1.3 del SMS: a) establecer una persona/oficina clave responsable de la administración y el mantenimiento del SMS. 4. Elemento 4.1 del SMS (i): a) establecer un programa de capacitación de SMS para el personal, con prioridad para el equipo de implementación del SMS. 5. Elemento 4.2 del SMS (i): a) iniciar canales de comunicación del SMS/seguridad operacional.	1. Elemento 1.1 del SMS (ii): a) establecer la política y los objetivos de seguridad operacional, 2. Elemento 1.2 del SMS: a) definir las responsabilidades de la gestión de la seguridad operacional en los departamentos pertinentes de la organización; b) establecer un mecanismo/comité de coordinación de SMS/ seguridad operacional; c) establecer SAG por departamento/divisional, donde corresponda. 3. Elemento 1.4 del SMS: a) establecer un plan de respuesta ante emergencias. 4. Elemento 1.5 del SMS (ii): a) iniciar el desarrollo progresivo de un documento/manual de SMS y otra documentación de respaldo.	1. Elemento 2.1 del SMS (i): a) establecer un procedimiento de notificación de peligros voluntaria. 2. Elemento 2.2 del SMS: a) establecer procedimientos de gestión de riesgos de la seguridad operacional. 3. Elemento 3.1 del SMS (i): a) establecer procedimientos de notificación e investigación de sucesos; b) establecer un sistema de recopilación y procesamiento de datos de seguridad operacional para los resultados de alto impacto; c) desarrollar SPI de alto impacto y una configuración de objetivos y alertas asociada. 4. Elemento 3.2 del SMS: a) establecer un procedimiento de gestión de cambio que incluye la evaluación de riesgos de seguridad operacional. 5. Elemento 3.3 del SMS (i): a) establecer un programa interno de auditoría de la calidad; b) establecer un programa externo de auditoría de la calidad.	1. Elemento 1.1 del SMS (iii): a) mejorar el procedimiento disciplinario/la política existentes con una debida consideración de los errores o las equivocaciones accidentales de las infracciones deliberadas o graves. 2. Elemento 2.1 del SMS (ii): a) integrar los peligros identificados a partir de los informes de investigación de sucesos con el sistema de notificación de peligros voluntaria; b) integrar procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o el cliente, donde corresponda. 3. Elemento 3.1 del SMS (ii): a) mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto; b) desarrollar SPI de bajo impacto y una configuración de objetivos/alertas asociada. 4. Elemento 3.3 del SMS (ii): a) establecer programas de auditoría de SMS o integrarlos en programas de auditoría internos y externos existentes; b) establecer otros programas de revisión/estudio de SMS operacional, donde corresponda. 5. Elemento 4.1 del SMS (ii): a) garantizar que se haya completado el programa de capacitación de SMS para todo el personal pertinentes. 6. Elemento 4.2 del SMS (ii): a) promover la distribución e intercambio de información de la seguridad operacional de forma interna y externa.
Elemento 1.5 del SMS: documentación del SMS (Etapas 1 a 4) >>			
Elementos 4.1 y 4.2 del SMS: capacitación, educación y comunicación de SMS (Etapas 1 y posteriores) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			

Nota 1.— El período de implementación indicado es una aproximación. El período de implementación real depende del alcance de las medidas necesarias para cada elemento asignado y la envergadura/complejidad de la organización.

Nota 2.— Los números de elementos del SMS indicados corresponden a los números de elementos del SMS de la OACI. Los sufijos como a), b) y c) indican que el elemento se ha subdividido para facilitar el enfoque de implementación en etapas.

Nombramiento del personal de seguridad operacional clave — Elemento 1.3

a) Identificar la persona de SMS clave (seguridad operacional/calidad/función) dentro de la organización que será responsable de administrar el SMS en nombre del ejecutivo responsable.

b) Establecer la oficina de servicios de seguridad operacional.

Capacitación y educación — Elemento 4.1 (i)

a) Realizar un análisis de las necesidades de capacitación.

b) Organizar y configurar programas para la capacitación correcta de todo el personal, de acuerdo con sus responsabilidades individuales y su participación en el SMS.

c) Desarrollar la capacitación de la seguridad operacional, considerando:

1) la capacitación inicial (seguridad operacional general) específica del trabajo; y

2) la capacitación recurrente.

d) Identificar los costos asociados con la capacitación.

e) Desarrollar un proceso de validación que mide la eficacia de la capacitación.

f) Establecer un sistema de registros de capacitación de la seguridad operacional.

Comunicación de la seguridad operacional — Elemento 4.2 (i)

a) Iniciar un mecanismo o medio para una comunicación de seguridad operacional.

b) Establecer un medio para transferir información de seguridad operacional mediante cualquiera de las siguientes opciones:

1) folletos informativos, noticias y boletines de seguridad operacional;

2) sitios web;

3) correo electrónico.

5.5.3 Etapa 2

El objetivo de la Etapa 2 es implementar procesos de gestión de seguridad operacional fundamentales, mientras que al mismo tiempo de corrigen las posibles deficiencias en los procesos de gestión de seguridad operacional existentes. La mayoría de las organizaciones tendrán implementadas ciertas actividades de gestión de seguridad operacional básicas, en diferentes niveles de implementación. Esta etapa está orientada a consolidar las actividades existentes y desarrollar aquellas que todavía no existen.

Compromisos y responsabilidades de la gestión — Elemento 1.1 (ii)

a) Desarrollar una política de seguridad operacional.

b) Solicitar que el ejecutivo responsable firme la política de seguridad operacional.

c) Comunicar la política de seguridad operacional en toda la organización.

d) Establecer un programa de revisión de la política de seguridad operacional para garantizar que sigue siendo pertinente y adecuada para la organización.

e) Establecer objetivos de seguridad operacional para el SMS mediante el desarrollo de normas de rendimiento en materia de seguridad operacional en términos de:

   1) indicadores de rendimiento en materia de seguridad operacional;

   2) niveles de objetivos y alertas de rendimiento en materia de seguridad operacional; y

   3) planes de acción.

f) Establecer los requisitos del SMS para los subcontratistas:

   1) establecer un procedimiento para escribir requisitos de SMS en el proceso contratante; y

   2) establecer los requisitos de SMS en la documentación de licitación.

Responsabilidades de la seguridad operacional — Elemento 1.2

a) Definir las responsabilidades de la seguridad operacional y comunicarlas en toda la organización.

b) Establecer el grupo de acción de seguridad operacional (SAG).

c) Establecer el comité de coordinación de la seguridad operacional/SMS.

d) Definir las funciones claras para el SAG y el comité de coordinación de la seguridad operacional/SMS.

e) Establecer líneas de comunicación entre la oficina de servicios de seguridad operacional, el ejecutivo responsable, el SAG y el comité de coordinación de la seguridad operacional/SMS.

f) Asignar un ejecutivo responsable como el líder del comité de coordinación de seguridad operacional/SMS.

g) Desarrollar un programa de reuniones para la oficina de servicios de seguridad operacional para reunirse con el comité de coordinación de seguridad operacional/SMS y el SAG, según sea necesario.

Coordinación de la planificación de respuesta ante emergencias — Elemento 1.4

a) Revisar la descripción del ERP relacionado con la delegación de autoridad y asignación de responsabilidades de emergencia.

c) Establecer procedimientos de coordinación para medidas mediante el personal clave durante la emergencia y volver a las operaciones normales.

c) Identificar entidades externas que interactuarán con la organización durante situaciones de emergencia.

d) Evaluar los ERP respectivos de las entidades externas.

e) Establecer la coordinación entre los diferentes ERP.

f) Incorporar información acerca de la coordinación entre los diferentes ERP en la documentación de SMS de la organización.

Nota.— Véase el Apéndice 3 para una guía detallada sobre ERP.

Documentación del SMS — Elemento 1.5 (ii)

a) Crear un sistema de documentación de SMS para describir, guardar, recuperar y archivar toda la información y los registros relacionados con SMS al:

1) desarrollar un documento de SMS que sea un manual independiente o una sección distinta dentro de un manual institucional controlado existente (véase el Apéndice 4 para una guía sobre el desarrollo de un manual de SMS);

2) establecer un sistema de archivo de SMS para recopilar y mantener los registros actuales en relación con los procesos de SMS constantes de la organización;

3) mantener registros para proporcionar una referencia histórica, así como también, el estado actual de todos los procesos de SMS, como por ejemplo: un registro de peligros; un índice de evaluaciones de seguridad operacional completadas; registros de capacitación de SMS/ seguridad operacional; los SPI actuales y los objetivos de seguridad operacional asociados; informes de auditoría interna de SMS; actas de la reunión del comité de SMS/seguridad operacional y el plan de implementación de SMS;

4) mantener registros que servirán como evidencia de la operación de SMS y las actividades durante la evaluación o auditoría internas o externas del SMS.

5.5.4 Etapa 3

El objetivo de la Etapa 3 es establecer procesos de gestión de riesgos de la seguridad operacional. Hacia el final de la Etapa 3, la organización estará lista para recopilar datos de seguridad operacional y realizar los análisis de seguridad operacional basados en la información obtenida mediante diversos sistemas de notificación.

Identificación de peligros — Elemento 2.1 (i)

a) Establecer un procedimiento de notificación voluntaria. Véase el Apéndice 5 para guía.

b) Establecer un programa/plan para la revisión sistemática de todos los procesos/equipos relacionados con la seguridad operacional de aviación aplicables que sean idóneos para el proceso de HIRM.

c) Establecer un proceso para la priorización y asignación de peligros identificados para la mitigación de riesgos.

Evaluación y mitigación de riesgos de seguridad operacional — Elemento 2.2

a) Establecer un procedimiento de gestión de riesgos de la seguridad operacional que incluya su aprobación y un proceso de revisión periódico.

b) Desarrollar y adoptar matrices de riesgos de seguridad operacional pertinentes para los procesos operacionales y de producción de la organización.

c) Incluir matrices de riesgos de seguridad operacional adoptados e instrucciones asociadas en el material de capacitación de la gestión de riesgos o SMS de la organización.

Control y medición del rendimiento en materia de seguridad operacional — Elemento 3.1 (i)

a) Establecer un procedimiento interno de notificación e investigación de sucesos. Esto puede incluir informes obligatorios de defectos (MDR) o informes importantes, donde corresponda.

b) Establecer la recopilación, el procesamiento y el análisis de los datos de seguridad operacional de los resultados de alto impacto.

c) Establecer indicadores de seguridad operacional de alto impacto (ALoSP inicial) y su configuración de objetivos y alertas asociados. Entre los ejemplos de indicadores de seguridad operacional de alto impacto se incluyen tasas de accidentes, tasas de incidentes graves y el control de los resultados de no cumplimiento de alto riesgo. Véase el Apéndice 6 para guía sobre los indicadores de rendimiento en seguridad operacional.

d) Lograr un acuerdo con la autoridad de vigilancia del Estado sobre los indicadores de rendimiento en materia de seguridad operacional y objetivos de rendimiento en materia de seguridad operacional.

La gestión de cambio — Elemento 3.2

a) Establecer un proceso formal para la gestión de cambio que considera:

   1) la vulnerabilidad de los sistemas y actividades;

   2) la estabilidad de los sistemas y entornos operacionales;

   3) rendimiento pasado;

   4) cambios reglamentarios, industriales y tecnológicos.

b) Garantizar que los procedimientos de la gestión de cambio aborden el impacto de los registros existentes de rendimiento en materia de seguridad operacional y de mitigación de riesgos antes de implementar nuevos cambios.

c) Establecer procedimientos para garantizar que se lleve a cabo (o se considere) la evaluación de seguridad operacional de las operaciones, los procesos y los equipos relacionados con la seguridad operacional de la aviación, según corresponda, antes de ponerlos en servicio.

Mejora continua del SMS — Elemento 3.3 (i)

a) Desarrollar formularios para las evaluaciones internas.

b) Definir un proceso de auditoría interna.

c) Definir un proceso de auditoría externa.

d) Definir un programa para la evaluación de instalaciones, equipos, documentación y procedimientos que se deben completar mediante auditorías y estudios.

e) Desarrollar documentación pertinente para el aseguramiento de la seguridad operacional.

5.5.5 Etapa 4

La Etapa 4 es la etapa final de la implementación de SMS. Esta etapa implica la implementación madura de la gestión de riesgos de la seguridad operacional y el aseguramiento de la seguridad operacional. En esta etapa, el aseguramiento de la seguridad operacional se evalúa mediante la implementación de control periódico, retroalimentación y una medida correctiva continua para mantener la eficacia de los controles de riesgos de seguridad operacional.

Compromiso y responsabilidad de la gestión — Elemento 1.1 (iii)

a) Mejorar el procedimiento disciplinario/la política existentes con una debida consideración de errores/equivocaciones accidentales de las infracciones deliberadas/graves.

Identificación de peligros — Elemento 2.1 (ii)

a) Integrar los peligros identificados en los informes de investigación de sucesos con el sistema de notificación voluntaria.

b) Integrar los procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o del cliente, donde corresponda.

c) Si fuera necesario, desarrollar un proceso para priorizar peligros recopilados para la mitigación de riesgos según las áreas de mayor necesidad o preocupación. Véase el Apéndice 3 del Capítulo 2 para guía.

Control y medición del rendimiento en materia de seguridad operacional — Elemento 3.1 (ii)

a) Mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto.

b) Establecer indicadores de seguridad operacional/calidad de bajo impacto con el control del nivel de objetivos/alertas, según corresponda (ALoSP maduro).

. c) Lograr un acuerdo con la autoridad de vigilancia del Estado sobre indicadores de rendimiento en materia de seguridad operacional de bajo impacto y niveles de objetivos/alertas de rendimiento en materia de seguridad operacional.

Mejora continua del SMS — Elemento 3.3 (ii)

a) Establecer auditorías de SMS o integrarlas en los programas de auditoría interna o externa existentes.

b) Establecer otros programas de revisión/estudio de SMS operacional, donde corresponda.

Capacitación y educación — Elemento 4.1 (ii)

a) Completar un programa de capacitación de SMS para todo el personal pertinente.

Comunicación de seguridad operacional — Elemento 4.2 (ii)

a) Establecer mecanismos para promover la distribución y el intercambio de información de seguridad operacional de forma interna y externa.

5.5.6 Elementos del SMS implementados progresivamente a través de las Etapas 1 a 4

En la implementación del enfoque en etapas, los siguientes tres elementos clave se implementan progresivamente en cada una de las etapas:

Documentación del SMS — Elemento 1.5

A medida que el SMS madura progresivamente, el manual del SMS pertinente y la documentación de la seguridad operacional deben revisarse y actualizarse en conformidad. Esta actividad será inherente a todas las etapas de la implementación del SMS y también deberá mantenerse después de la implementación.

Capacitación y educación — Elemento 4.1 y comunicación de la seguridad operacional — Elemento 4.2

Al igual que con la documentación de SMS, la capacitación, la educación y la comunicación de seguridad operacional son actividades continuas importantes en todas las etapas de la implementación del SMS. A medida que evoluciona el SMS, pueden entrar en vigencia nuevos procesos, procedimientos o reglamentos o los procedimientos existentes pueden cambiar para proveer los requisitos del SMS. Para garantizar que todo el personal que participa en las tareas relacionadas con la seguridad operacional comprenden e implementan realmente estos cambios, es vital que la capacitación y comunicación sigan siendo actividades continuas en toda la implementación del SMS y luego de completarse.

Apéndice 1 del Capítulo 5

FIRMAS ELECTRÓNICAS

Nota.— Este apéndice consta de extractos de la circular de asesoramiento (AC) de la Administración Federal de Aviación de los Estados Unidos (FAA) Nº 120-78 "Acceptance and Use of Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manuals" (Aceptación y uso de firmas electrónicas, sistemas de registro electrónico y manuales electrónicos), del 29 de octubre de 2002.[1] Se debe entender que la siguiente información es tan solo ilustrativa y no tiene como fin ser limitante de ninguna manera. Este apéndice no debe considerarse ni utilizarse como el único conjunto de información necesario para el uso de firmas electrónicas. Nada en este apéndice afectará el derecho de los Estados contratantes de desarrollar o usar sus propio material sobre firmas electrónicas.

1. ¿Cuál es el propósito de esta circular de asesoramiento (AC)?

a) Esta AC no es obligatoria ni constituye un reglamento. Esta AC proporciona una guía sobre la aceptación y el uso de firmas electrónicas para satisfacer ciertos requisitos operacionales y de mantenimiento. Esta AC también proporciona una guía sobre la aceptabilidad de los sistemas de registro electrónico y los manuales de mantenimiento electrónico, lo que incluye los manuales de procedimientos de inspección, el aseguramiento de la calidad, los manuales de operaciones y los manuales de capacitación que requiere el Título 14 del Code of Federal Regulations (14 CFR).

b) Esta AC describe un medio aceptable, pero no el único medio, de cumplir con los requisitos operacionales y de mantenimiento de la FAA. Específicamente, las firmas a mano, los registros y las marcas mecánicas siguen siendo aceptables. Sin embargo, si usa los medios electrónicos descritos en la AC, debe cumplir con sus disposiciones en todos los aspectos importantes.

2. ¿A quién se aplica esta AC?

- Transportistas aéreos según el 14 CFR partes 121, 129 o 135
- Explotadores según el 14 CFR partes 91, 125, 133 o 137
- Personas que realicen la certificación de personal técnico aeronáutico según el 14 CFR partes 61, 63, 65, 141 y 142
- Personas que realicen el mantenimiento o el mantenimiento preventivo según el 14 CFR parte 43
- Estaciones de reparación según el 14 CFR parte 145
- Escuelas técnicas de mantenimiento de la aviación según el 14 CFR parte 147

1. El texto completo de la AC de la FAA AC Nº 120-78 podrá encontrarlo en el sitio web de la FAA: http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/23224.

3. Definiciones

. . .

d) ***Firma digital.*** Datos generados de forma criptográfica que identifican al signatario (firmante) del documento y certifican que el documento no se ha alterado. La tecnología de firma digital es la base para una variedad de productos de seguridad de la aviación, negocio electrónico y comercio electrónico. Esta tecnología se basa en la criptografía de clave pública o privada, la tecnología de firma digital usada en la mensajería segura, la infraestructura de clave pública (PKI), la red privada virtual (VPN), las normas de la web para transacciones seguras y las firmas digitales electrónicas.

e) ***Firma electrónica.*** El equivalente en línea de una firma a mano. Es un sonido, símbolo o proceso electrónico adjunto o asociado de manera lógica con un contrato u otro registro y que ejecuta o adopta una persona. Identifica y autentica de forma electrónica que una persona ingresa, verifica o realiza una auditoría a los registros computacionales. Una firma electrónica combina funciones criptográficas con la imagen de la firma escrita de una persona o alguna otra marca visible considerada aceptable en un proceso de firma tradicional. Autentica los datos con un algoritmo hash y proporciona una autenticación de usuario permanente y segura.

. . .

5. ¿Qué es una firma electrónica aceptable?

a) ***General.*** Antes de los cambios recientes para permitir el uso de firmas electrónicas, las firmas a mano se usaban en cualquier registro, entrada de registro o documento necesario. El propósito de la firma electrónica es idéntico al de una firma a mano o cualquier otra forma de firma aceptada actualmente por la FAA. La firma a mano se acepta universalmente ya que tiene ciertas cualidades y atributos (por ejemplo, subpárrafo c) 4) d) a continuación, acerca del despido de un empleado) que se deben preservar en cualquier firma electrónica. Por lo tanto, una firma electrónica debe representar aquellas cualidades y atributos que garanticen la autenticidad de una firma a mano.

b) ***Formas de firmas electrónicas.***

1) Una firma electrónica podría estar en los siguientes formatos.

- Una firma digital
- Una imagen digitalizada de una firma en papel
- Una nota escrita
- Un código electrónico
- Cualquier otra forma única de identificación individual que pueda usarse como medio para autenticar un registro, una entrada de registro o un documento

2) No toda la información de identificación que se encuentre en un sistema electrónico podría constituir una firma. Por ejemplo, la entrada del nombre de una persona en un sistema electrónico podría no constituir una firma electrónica. Se deben proporcionar otras garantías iguales a las que tiene una firma a mano.

c) ***Atributos de una firma electrónica aceptable.*** Antes que nada, una firma electrónica debe ser parte de un programa bien diseñado. Este programa debe, como mínimo, considerar lo siguiente.

1) ***Unicidad.*** Una firma electrónica debe conservar las cualidades de una firma a mano que garanticen su unicidad. Una firma debe identificar a una persona específica y debe ser difícil de duplicar. Una firma única proporciona evidencia de que una persona acepta una declaración. Un sistema electrónico no puede proporcionar una identificación única con una certeza razonable, a menos que sea difícil que una persona no autorizada duplique la identificación.

2) ***Importancia.*** Una persona que usa una firma electrónica debe tomar una medida deliberada y reconocible para adjuntar su firma. Las medidas aceptables y deliberadas para crear una firma electrónica digital incluyen, entre otras, las siguientes:

- Deslizar una tarjeta
- Firmar un documento electrónico con un lápiz
- Presionar teclas específicas
- Usar una firma digital

3) ***Alcance.*** El alcance de la información que se afirma con la firma electrónica debe ser claro para el signatario y para los posteriores lectores del registro, la entrada del registro o el documento. Los documentos escritos a mano colocan la firma cerca de la información para identificar aquellos elementos autenticados por el signatario. Sin embargo, los documentos electrónicos podrían no colocar una firma de la misma manera. Por lo tanto, es importante identificar claramente las secciones específicas de un registro o documento que serán afirmadas con una firma y aquellas que no lo serán. Entre los métodos aceptables para marcar las áreas afectadas se incluyen, entre otros, destacar, invertir el contraste o usar límites o caracteres parpadeantes. Además, el sistema debe notificar al signatario que la firma se ha adjuntado.

4) ***Seguridad de la firma.*** Se mantiene la seguridad de una firma a mano de una persona al garantizar que sea difícil para otra persona duplicarla o alterarla. Una firma electrónica debe mantener un nivel de seguridad equivalente. Un sistema electrónico que produce firmas debe restringir que otras personas adjunten la firma de otra persona en un registro, entrada de registro o documento.

5) ***No rechazo.*** Una forma electrónica debe evitar que un signatario rechace el hecho de haber adjuntado una firma en un registro, entrada de registro o documento específicos. Mientras más difícil sea duplicar una firma, más probable es que el signatario haya creado la firma. Las características de seguridad del sistema que dificultan que otros dupliquen las firmas o alteren los documentos firmados, por lo general, garantizan que un signatario ha creado en realidad la firma.

6) ***Trazabilidad.*** Una firma electrónica debe proporcionar una trazabilidad hacia la persona que firmó el registro, la entrada de registro o cualquier otro documento.

d) ***Otros formatos aceptables de firma/identificación.*** Aunque esta AC aborda específicamente las firmas electrónicas, otros tipos de firmas, como una marca mecánica, podrían ser aceptables para la FAA. Si se usa un tipo de identificación que no sea una firma a mano, el acceso a la identificación debe limitarse solo a la persona nombrada.

e) ***Cumplimiento de otros registros reglamentarios.*** Aunque la FAA ahora permite el uso de firmas electrónicas para cumplir con ciertos requisitos operacionales y de mantenimiento de la FAA, cualquier hardware computacional usado para generar los documentos y registros necesarios debe seguir cumpliendo los requisitos reglamentarios actuales. Una firma correcta adjunta a un documento creado inadecuadamente sigue siendo un documento que no cumple con requisitos reglamentarios. Por lo tanto, los métodos y procedimientos usados para generar una firma electrónica deben cumplir todos los requisitos reglamentarios para que los propietarios, explotadores o el personal de mantenimiento puedan usar un sistema de registro. Además, las firmas electrónicas deben usarse solo para satisfacer los requisitos de mantenimiento y operacionales relacionados con esta AC. Las firmas electrónicas podrían no considerarse aceptables en otras áreas que aborda el 14 CFR que tengan una aplicabilidad más específica (es decir, disposiciones legales y diversas otras aplicaciones). Aunque la aceptación de las firmas electrónicas fomentará el uso de sistemas de registro electrónico, la FAA sigue aceptando documentos en papel para satisfacer los requisitos reglamentarios actuales.

Apéndice 2 del Capítulo 5

MUESTRA DE DESCRIPCIÓN DEL TRABAJO DE UN GERENTE DE SEGURIDAD OPERACIONAL

1. PROPÓSITO GENERAL

El gerente de seguridad operacional es responsable ante el ejecutivo responsable de proporcionar una guía e instrucciones para la planificación, implementación y operación del sistema de gestión de la seguridad operacional (SMS) de la organización. El gerente de seguridad operacional proporciona servicios relacionados con el SMS a áreas de la organización certificadas, no certificadas y de terceros que se incluyen en el SMS y podría haber delegado responsabilidades en nombre de las personas que están en los cargos que requieren los reglamentos.

2. FUNCIONES CLAVE

Defensor de la seguridad operacional

- Demuestra una excelente conducta y actitud de seguridad operacional, sigue las prácticas y reglas reglamentarias, reconoce e informa los peligros y promueve la notificación eficaz de la seguridad operacional.

Líder

- Modela y promueve una cultura institucional que impulsa las prácticas de seguridad operacional mediante un liderazgo eficaz.

Comunicador

- Actúa como un conducto de información para llevar temas de seguridad operacional a la atención de la administración y para entregar información de seguridad operacional al personal, los contratistas o los accionistas de la organización.

- Proporciona y articula la información acerca de temas de seguridad operacional dentro de la organización.

Desarrollador

- Ayuda en la mejora continua de los diagramas de la evaluación de identificación de peligros y gestión de riesgos de seguridad operacional y el SMS de la organización.

Creador de relaciones

- Construye y mantiene una excelente relación de trabajo con el grupo de acción de seguridad operacional (SAG) de la organización y dentro de la oficina de servicios de seguridad operacional (SSO).

Embajador

- Representa a la organización ante comités industriales, gubernamentales y de organizaciones internacionales (por ejemplo, OACI, IATA, CAA, AIB, etc.).

Analista

- Analiza datos técnicos en busca de tendencias relacionadas con peligros, eventos y sucesos.

Gestión del proceso

- Usa eficazmente los procesos y procedimientos correspondientes para satisfacer las funciones y responsabilidades.
- Investiga las oportunidades de aumentar la eficiencia de los procesos.
- Mide la eficacia y busca mejorar continuamente la calidad de los procesos.

3. RESPONSABILIDADES

Entre otras tareas, el gerente de seguridad operacional es responsable de:

- gestionar la operación del sistema de gestión de seguridad operacional;
- recopilar y analizar la información de la seguridad operacional de forma oportuna;
- administrar cualquier estudio relacionado con la seguridad operacional;
- controlar y evaluar los resultados de las medidas correctivas;
- garantizar que las evaluaciones de riesgos se lleven a cabo cuando corresponda;
- controlar la industria en busca de preocupaciones de seguridad operacional que pudiesen afectar a la organización;
- participar en las respuestas ante emergencias reales o prácticas;
- participar en el desarrollo y actualización del plan y procedimientos de respuesta ante emergencias; y
- garantizar que la información relacionada con la seguridad operacional, como las metas y los objetivos institucionales, esté disponible para todo el personal mediante los procesos de comunicación establecidos.

4. NATURALEZA Y ALCANCE

El gerente de seguridad operacional debe interactuar con el personal de operaciones, los gerentes superiores y los líderes de departamento en toda la organización. El gerente de seguridad operacional también debe fomentar relaciones positivas con las autoridades, las agencias y los proveedores de servicios y productos reglamentarios fuera de la organización. Otros contactos se establecerán en niveles de trabajo, según sea necesario.

5. CALIFICACIONES

Para calificar como gerente de seguridad operacional, una persona debe tener:

- experiencia de tiempo completo en la seguridad operacional de la aviación, en capacidad de un investigador de seguridad operacional de la aviación, gerente de seguridad operacional/calidad o gerente de riesgos de la seguridad operacional;
- conocimientos sólidos de las operaciones, procedimientos y actividades de la organización;
- un amplio conocimiento técnico de aviación;
- un extenso conocimiento de los sistemas de gestión de la seguridad operacional (SMS) y haber completado la capacitación de SMS correspondiente;
- una comprensión de los principios y las técnicas de la gestión de riesgos para respaldar al SMS;
- experiencia en la implementación o gestión de un SMS;
- experiencia y calificaciones en la investigación de accidentes/incidentes de la aviación y factores humanos;
- experiencia y calificaciones en la realización de auditorías e inspecciones de seguridad operacional/ calidad;
- un conocimiento sólido de los marcos de trabajo reglamentarios de la aviación, incluidas las normas y métodos recomendados (SARPS) de la OACI y los reglamentos de aviación civil pertinentes;
- la capacidad de comunicarse en todos los niveles tanto dentro como fuera de la empresa;
- la capacidad de tener una postura firme, promover una “cultura justa e imparcial” y aun así fomentar una atmósfera abierta y no punitiva para la notificación;
- la capacidad y confianza de comunicarse directamente con el ejecutivo responsable como su asesor o confidente;
- habilidades de comunicación bien desarrolladas y habilidades interpersonales demostradas de alto orden, con la capacidad de vincularse con una variedad de personas y representantes institucionales, como aquellos de diferentes entornos culturales;
- alfabetización computacional y habilidades analíticas superiores.

6. AUTORIDAD

6.1 Acerca de los temas de seguridad operacional, el gerente de seguridad operacional tiene acceso directo con el ejecutivo responsable y la administración superior y de cargo medio correspondiente.

6.2 El gerente de seguridad operacional tiene autorización, según las instrucciones del ejecutivo responsable, de realizar auditorías de seguridad operacional, estudios e inspecciones de cualquier aspecto de la operación, de acuerdo con los procedimientos especificados en la documentación del sistema de gestión de seguridad operacional.

6.3 El gerente de seguridad operacional tiene autorización, según las instrucciones del ejecutivo responsable, de realizar investigaciones de los eventos de seguridad operacional internos, de acuerdo con los procedimientos especificados en la documentación del SMS de la organización.

6.4 El gerente de seguridad operacional no debe tener otros cargos ni responsabilidades que puedan entrar en conflicto o perjudicar su función como un gerente de seguridad operacional de SMS. Este debe ser un cargo administrativo superior que no sea inferior jerárquicamente o subordinado a las funciones de producción u operacionales de la organización.

Apéndice 3 del Capítulo 5

PLANIFICACIÓN DE LA RESPUESTA ANTE EMERGENCIAS

1. Tal vez, dado que los accidentes de aviación son eventos raros, pocas organizaciones están preparadas cuando uno sucede. Muchas organizaciones no tienen planes eficaces implementados para gestionar eventos durante o después de una emergencia o crisis. La forma en que una organización lidia con las consecuencias de un accidente u otra emergencia puede depender de cuán bien controla las primeras horas o días después de un evento de seguridad operacional importante. Un plan de respuesta ante emergencias (ERP) describe por escrito lo que se debe hacer después de un accidente o una crisis de aviación y quién es responsable de cada medida. Entre los diferentes proveedores de productos y servicios, tal planificación de emergencia podría conocerse con diferentes términos, como plan de contingencia, plan de gestión de crisis y plan de respaldo de la aeronavegabilidad continua. En este manual, el término genérico "plan de respuesta ante emergencias (ERP)" se usa para abordar los planes de contingencia pertinentes que se esperan de los proveedores de servicios de la aviación, cuyos productos/servicios podrían tener un impacto en la seguridad operacional de la aviación.

2. Si bien existe una tendencia para pensar que la planificación de respuesta ante emergencias se relaciona con las operaciones de la aeronave o el aeródromo, por lo general, a causa de un accidente de aeronave, la expectativa puede aplicarse de igual forma a otros proveedores de servicios de aviación. En el caso de proveedores de ATS, esto puede incluir un importante corte eléctrico o pérdida del radar, las comunicaciones u otras instalaciones importantes. Para una organización de mantenimiento, podría implicar una grave violación de los requisitos de aeronavegabilidad que producen el aterrizaje de una flota (AOG). Para una organización de diseño y fabricación, una grave deficiencia de diseño podría generar un AOG global que requiera de medidas de rediseño, modificación, producción y modernización de emergencia (directrices de aeronavegabilidad de la emergencia) para abordar tales crisis. Donde exista la posibilidad de que las operaciones o actividades de aviación de la organización estén comprometidas a causa de otras crisis o emergencias que se originan de fuentes externas, como emergencias de salud/pandémicas, estos casos también deben abordarse en este ERP de aviación, según corresponda. Por lo tanto, un ERP es básicamente un componente integral del procedimiento de gestión de riesgos de seguridad operacional de una organización para abordar todas las emergencias, las crisis o los eventos posibles relacionados con la seguridad operacional o la calidad con los cuales este producto o servicio pueda contribuir o asociarse. El ERP debe abordar todos los escenarios posibles/probables y tener medidas o procesos de mitigación adecuados implementados para que la organización, sus clientes, el público o la industria en toda su extensión puedan tener un mejor nivel de aseguramiento de la seguridad operacional, así como también, la continuidad de servicio.

3. Una respuesta satisfactoria ante una emergencia comienza con la planificación eficaz. Un ERP representa la base de un enfoque sistemático para gestionar los asuntos de la organización durante las consecuencias de un evento no planificado importante, en el peor de los casos, un accidente importante.

4. El propósito de un plan de respuesta ante emergencias es para garantizar:

a) la delegación de la autoridad de emergencia;

b) la asignación de responsabilidades de emergencia;

c) la documentación de procedimientos y procesos de emergencia;

d) la coordinación de esfuerzos de emergencia de forma interna y con partes externas;

e) la continuación segura de las operaciones fundamentales, mientras se gestiona la crisis;

f) la identificación proactiva de todos los posibles eventos/escenarios de emergencia y sus medidas de mitigación correspondientes, etc.

5. Para ser eficaz, un ERP debe:

a) ser adecuado según la envergadura, naturaleza y complejidad de la organización;

b) estar fácilmente accesible para todo el personal pertinente y otras organizaciones, donde corresponda;

c) incluir listas de verificación y procedimientos pertinentes a las situaciones de emergencia específicas;

d) tener detalles de contacto de referencia rápida de todo el personal pertinente;

e) probarse regularmente mediante ejercicios;

f) revisarse y actualizarse periódicamente cuando cambian los detalles, etc.

Contenido del ERP

6. Un ERP normalmente estaría documentado en el formato de un manual que debiera establecer las responsabilidades, las funciones y las medidas de las diversas agencias y el personal que participan abordando emergencias específicas. Un ERP debe considerar lo siguiente:

a) *Políticas gobernantes.* El ERP debe proporcionar las instrucciones para responder a emergencias, como leyes y reglamentos gobernantes para las investigaciones, acuerdos con autoridades locales, políticas empresariales y prioridades.

b) *Organización.* El ERP debe describir las intenciones de la gestión en relación con las organizaciones que dan respuesta al:

1) designar quién liderará y quién estará asignado a los equipos de respuesta;

2) definir las funciones y responsabilidades del personal asignado a los equipos de respuesta;

3) clarificar las líneas de notificación de la autoridad;

4) configurar un centro de gestión de emergencia (EMC);

5) establecer procedimientos para recibir una gran cantidad de solicitudes para la información, especialmente durante los primeros días después de un accidente importante;

6) designar al vocero empresarial para tratar con los medios;

7) definir qué recursos estarán disponibles, lo que incluye a las autoridades financieras para actividades inmediatas;

8) designar al representante de la empresa para cualquier investigación formal que lleven a cabo los funcionarios del Estado;

9) definir un plan de llamada para el personal clave.

Se podría usar un diagrama institucional para mostrar las funciones institucionales y las relaciones de la comunicación.

c) *Notificaciones.* El plan debe especificar a quién, en la organización, se le notificará de una emergencia, quién realizará las notificaciones externas y mediante qué medios. Se deben considerar las necesidades de notificación de lo siguiente:

1) la gestión;

2) las autoridades del Estado (búsqueda y salvamento, la autoridad reglamentaria, el consejo de investigación de accidentes, etc.);

3) los servicios de respuesta ante emergencias locales (autoridades del aeródromo, bomberos, policía, ambulancia, instituciones médicas, etc.);

4) los familiares de las víctimas (un tema delicado que, en muchos Estados, está a cargo de la policía);

5) el personal de la empresa;

6) los medios de comunicación; y

7) el área legal, contabilidad, aseguradores, etc.

d) *Respuesta inicial.* Dependiendo de las circunstancias, un equipo de repuesta inicial puede despacharse al sitio del accidente o crisis para aumentar los recursos locales y supervisar los intereses de la organización. Entre los factores que deben considerarse para dicho equipo se incluyen:

1) ¿Quién debe liderar el equipo de respuesta inicial?

2) ¿Quién debe incluirse en el equipo de respuesta inicial?

3) ¿Quién debe hablar en nombre de la organización en el sitio del accidente?

4) ¿Qué se necesitará en cuanto a equipo especial, ropa, documentación, transporte, hospedaje, etc.?

e) *Ayuda adicional.* Los empleados con una capacitación y experiencia adecuadas puede proporcionar un respaldo útil durante la preparación, el ejercicio y la actualización del ERP de una organización. Su experiencia puede resultar útil en la planificación y ejecución de tales tareas como:

1) actuar como pasajeros o clientes en los ejercicios;

2) abordar a los supervivientes o partes externas;

3) hablar con el familiar más cercano, las autoridades, etc.

f) *Centro de gestión de emergencia (EMC).* Un EMC (normalmente en modo de espera) puede establecerse en la sede de la organización luego de cumplir los criterios de activación. Además, se

puede establecer un puesto de mando (CP) cerca o en el sitio de la crisis. El ERP debe abordar cómo se cumplirán los siguientes requisitos:

1) personal (tal vez por 24 horas al día, los 7 días de la semana, durante el período de respuesta inicial);

2) equipo de comunicaciones (teléfonos, fax, Internet, etc.);

3) requisitos de documentación, mantenimiento de los registros de actividad de emergencia;

4) incautar los registros empresariales relacionados;

5) muebles y suministros de oficina; y

6) documentos de referencia (como listas de verificación y procedimientos de respuesta ante emergencias, manuales de la empresa, planes de emergencia del aeródromo y listas telefónicas).

Una línea aérea u otra organización especialista puede contratar los servicios de un centro de crisis para que resguarde los intereses del proveedor de servicios ante una crisis lejos de la base de domicilio. Por lo general, el personal de la empresa complementaría dicho centro contratado lo antes posible.

g) *Registros.* Además de la necesidad de la organización de mantener registros de los eventos y las actividades, la organización también necesitará proporcionar información a cualquier equipo de investigación del Estado. El ERP debe abordar los siguientes tipos de información que requieran los investigadores:

1) todos los registros pertinentes acerca del producto o servicio de interés;

2) listas de puntos de contacto y cualquier personal asociado con el suceso;

3) notas de cualquier entrevista (o declaración) con alguien asociado con el evento;

4) cualquier evidencia fotográfica o de otro tipo.

h) *Sitio del accidente.* Para un accidente importante, los representantes de muchas jurisdicciones tienen motivos legítimos para acceder al sitio: por ejemplo, la policía; bomberos; médicos; autoridades del aeródromo; forenses (funcionarios encargados de examen médico) para abordar las fatalidades; investigadores de accidentes del Estado; agencias de ayuda como la Cruz Roja e incluso los medios de comunicación. Aunque la coordinación de las actividades de estos accionistas es la responsabilidad de la autoridad de investigación o la policía del Estado, el proveedor de servicios debe clarificar los siguientes aspectos de las actividades en el sitio del accidente:

1) nominar a un representante superior de la empresa en el sitio del accidente si:

— se está en la base de domicilio;

— se está lejos de la base de domicilio;

— se está en mar abierto o en un Estado extranjero;

2) gestión de las víctimas supervivientes;

3) las necesidades de los familiares de las víctimas;

4) la seguridad de los restos de la aeronave;

5) manipulación de los restos humanos y la propiedad personal de los fallecidos;

6) preservación de la evidencia;

7) disposición de ayuda (según sea necesario) a las autoridades de la investigación;

8) retiro y eliminación de los restos de la aeronave; etc.

i) *Medios de prensa.* La forma como responde la empresa a los medios de comunicación puede afectar cuán bien la empresa se recupera del evento. Se requiere una clara instrucción acerca de, por ejemplo:

1) qué información está protegida por un estatuto (datos de FDR, registros de CVR y ATC, declaraciones de testigos, etc.);

2) quién puede hablar en nombre de la organización matriz en la oficina principal y en el sitio del accidente (gerente de relaciones públicas, funcionario ejecutivo principal u otro ejecutivo superior, gerente, propietario);

3) declaraciones preparadas para obtener una respuesta inmediata a las consultas de los medios de comunicación;

4) qué información puede divulgarse (qué debe evitarse);

5) la sincronización y el contenido de la declaración inicial de la empresa;

6) disposiciones de actualizaciones regulares a los medios de comunicación.

j) *Investigaciones formales.* Se debe proporcionar una guía acerca del personal de la empresa que trata con los investigadores del accidente y la policía del Estado.

k) *Ayuda para la familia.* El ERP también debe incluir una guía sobre el enfoque de la organización para ayudar a las víctimas de las crisis o las organizaciones del cliente. Esta guía puede incluir factores como:

1) Requisitos del Estado para la disposición de servicios de ayuda;

2) arreglos de viajes y hospedaje para visitar el sitio de la crisis;

3) coordinador del programa y puntos de contacto para las víctimas/clientes;

4) disposición de información actualizada;

5) ayuda temporal a las víctimas y los clientes.

Nota.— La Circular 285 de la OACI, Orientación sobre asistencia a las víctimas de accidentes de aviación y sus familiares*, proporciona una guía detallada sobre este tema.*

l) *Revisión posterior al suceso.* Se deben proporcionar instrucciones para garantizar que, después de una emergencia, el personal clave realice una sesión informativa completa y el registro de todas las lecciones significativas aprendidas, que pueden producir enmiendas al ERP y procedimientos asociados.

Listas de verificación

7. Todos los que participan en la respuesta inicial a un evento de aviación importante sufrirán de algún grado de desorientación. Por lo tanto, el proceso de respuesta ante emergencias se presta para el uso de las listas de verificación. Estas listas de verificación pueden formar una parte integral del manual de operaciones de la empresa o el manual de respuesta ante emergencias. Para ser eficaces, las listas de verificación deben regularmente:

a) revisarse y actualizarse (por ejemplo, la actualidad de las listas de llamada y los detalles de contacto); y

b) probarse mediante ejercicios realistas.

Capacitación y ejercicios

8. Un ERP es un indicio de intento en papel. Con suerte, gran parte del ERP no se probará nunca bajo condiciones reales. Se requiere de capacitación para garantizar que estas intenciones reciban el respaldo de capacidades operacionales. Dado que la capacitación tiene una corta “vida útil”, se recomienda llevar a cabo ensayos regulares y ejercicios. Algunas partes del ERP, como el plan de llamadas y comunicaciones, pueden probarse mediante ejercicios de "escritorio". Otros aspectos, como las actividades "en terreno" que implican a otras agencias, necesitan practicarse en intervalos regulares. Tales ejercicios tienen la ventaja de demostrar deficiencias en el plan, las que pueden rectificarse antes de una emergencia real. Para ciertos proveedores de servicios, como aeropuertos, puede que sea obligatorio usar pruebas periódicas de la idoneidad del plan y la conducta de un ejercicio de emergencia a escala completa.

Apéndice 4 del Capítulo 5

GUÍA SOBRE EL DESARROLLO DE UN MANUAL DE SMS

1. GENERALIDADES

1.1 Este apéndice sirve para guiar a las organizaciones en su compilación de un manual (o documento) de SMS de alto nivel para definir su marco de trabajo de SMS y sus elementos asociados. Puede ser un manual de SMS independiente o puede integrarse como una sección/capítulo de SMS consolidada dentro de un manual aprobado correspondiente de la organización (por ejemplo, el manual de exposición o el manual de la empresa de la organización). La configuración real puede depender de la expectativa reglamentaria.

1.2 Al usar el formato sugerido y los elementos del contenido en este apéndice y adaptarlos como corresponda, es una forma en que la organización puede desarrollar su propio manual de SMS de nivel superior. Los elementos del contenido real dependerán del marco de trabajo de SMS específico y los elementos de la organización. La descripción debajo de cada elemento será proporcional al alcance y la complejidad de los procesos de SMS de la organización.

1.3 El manual servirá para comunicar el marco de trabajo de SMS de la organización de forma interna, así como también, con las organizaciones externas pertinentes. El manual puede someterse al respaldo o aprobación de la CAA como evidencia de la aceptación del SMS.

Nota.— Se debe hacer una distinción entre un manual de SMS y sus registros y documentos de respaldo operacional. El último hace referencia a registros y documentos históricos y actuales generados durante la implementación y operación de los diversos procesos del SMS. Estos constituyen evidencia documental de las actividades constantes de SMS de la organización.

2. FORMATO DEL MANUAL DE SMS

2.1 El manual de SMS puede asumir un formato de la siguiente manera:

a) encabezado de sección;

b) objetivo;

c) criterios;

d) documentos de referencia cruzada.

2.2 Debajo de cada “encabezado de sección” numerado se incluye una descripción del “objetivo” de esa sección, seguido de sus “criterios” y “documentos de referencia cruzada”. El “objetivo” es lo que intenta lograr la organización al hacer lo que se describe en esa sección. Los "criterios" definen el alcance de lo que se debe considerar al escribir esa sección. Los “documentos de referencia cruzada” vinculan la información con otros manuales pertinentes o SOP de la organización, los que contienen detalles del elemento o proceso, según corresponda.

3. CONTENIDO DEL MANUAL

3.1 Entre los contenidos del manual se pueden incluir las siguientes secciones:

1. Control de documentos;
2. Requisitos reglamentarios del SMS;
3. Alcance e integración del sistema de gestión de la seguridad operacional;
4. Política de seguridad operacional;
5. Objetivos de seguridad operacional;
6. Responsabilidades de la seguridad operacional y personal clave;
7. Notificación de seguridad operacional y medidas correctivas;
8. Identificación de peligros y evaluación de riesgos;
9. Control y medición del rendimiento en materia de seguridad operacional;
10. Investigaciones relacionadas con la seguridad operacional y medidas correctivas;
11. Capacitación y comunicación de seguridad operacional;
12. Mejora continua y auditoría de SMS;
13. Gestión de los registros de SMS;
14. Gestión de cambio; y
15. Plan de respuesta ante emergencias/contingencia.

3.2 A continuación se indica un ejemplo del tipo de información que puede incluirse en cada sección mediante el formato descrito en 2.2.

1. Control de documentos

Objetivo

Describir cómo los manuales se mantendrán actualizados y cómo garantizará la organización que el personal que participa en las tareas relacionadas con la seguridad operacional tenga la versión más actual.

Criterios

a) Copia impresa o medio electrónico controlado y lista de distribución.

b) La correlación entre el manual de SMS y otros manuales existentes, como el manual de control de mantenimiento (MCM) o el manual de operaciones.

c) El proceso de revisión periódica del manual y sus formularios/documentos relacionados para garantizar su sustentabilidad, suficiencia y eficacia constantes.

d) El proceso de administración, aprobación y aceptación reglamentaria del manual.

Documentos de referencia cruzada

Manual de la calidad, manual de ingeniería, etc.

2. Requisitos reglamentarios de SMS

Objetivo

Abordar los reglamentos de SMS y el material guía actuales para obtener una referencia necesaria y toma de conciencia de todos los interesados.

Criterios

a) Explicar en detalle los reglamentos/normas actuales de SMS. Incluir el marco de tiempo del cumplimiento y las referencias del material de asesoramiento, según corresponda.

b) Donde corresponda, elaborar o explicar la importancia y las implicaciones de los reglamentos para la organización.

c) Establecer una correlación con otros requisitos o normas relacionados con la seguridad operacional, donde corresponda.

Documentos de referencia cruzada

Referencias de reglamentos/requisitos de SMS, referencias de documentos de guía de SMS, etc.

3. Alcance e integración del sistema de gestión de la seguridad operacional

Objetivo

Describir el alcance y extensión de las operaciones e instalaciones relacionadas con la aviación de la organización, dentro de las cuales se aplicará el SMS. También se debe abordar el alcance de los procesos, los equipos y las operaciones consideradas idóneas para el programa de identificación de peligros y mitigación de riesgos (HIRM) de la organización.

Criterios

a) Explicar la naturaleza del negocio de aviación de la organización y su posición o función dentro de la industria como un todo.

b) Identificar las áreas, los departamentos, los talleres y las instalaciones principales de la organización, dentro de las cuales se aplicará el SMS.

c) Identificar los procesos, las operaciones y los equipos principales que se consideran idóneos para el programa HIRM de la organización, especialmente aquellos que son pertinentes para la seguridad operacional de la aviación. Si el alcance de los procesos, las operaciones y los equipos idóneos de HIRM es demasiado detallado o extenso, se puede controlar de acuerdo con un documento complementario, según corresponda.

d) Donde se espera que el SMS se opere o administre en un grupo de organizaciones o contratistas interconectados, defina y documente dicha integración y las responsabilidades asociadas, según corresponda.

e) Donde hayan otros sistemas de control/gestión relacionados dentro de la organización, como QMS, OSHE y SeMS, identifique su integración pertinente (donde corresponda) dentro del SMS de la aviación.

Documentos de referencia cruzada

Manual de la calidad, manual de ingeniería, etc.

4. Política de seguridad operacional

Objetivo

Describir las intenciones de la organización, sus principios de gestión y su compromiso con la mejora de la seguridad operacional de la aviación, en términos del proveedor de productos o servicios. Una política de seguridad operacional debe ser una descripción corta, parecida a una declaración de la misión.

Criterios

a) La política de seguridad operacional debe ser adecuada para la envergadura y complejidad de la organización.

b) La política de seguridad operacional señala las intenciones de la organización, sus principios de gestión y el compromiso con la mejora continua en la seguridad operacional de la aviación.

c) El ejecutivo responsable aprueba y firma la política de seguridad operacional.

d) El ejecutivo responsable y el resto de los gerentes promueven la política de seguridad operacional.

e) La política de seguridad operacional se revisa periódicamente.

f) El personal en todos los niveles participa en el establecimiento y mantenimiento del sistema de gestión de la seguridad operacional.

g) La política de seguridad operacional se comunica a todos los empleados con la intención de crear conciencia de sus obligaciones de seguridad operacional individuales.

Documentos de referencia cruzada

Política de seguridad operacional de OSHE, etc.

5. Objetivos de seguridad operacional

Objetivo

Describir los objetivos de seguridad operacional de la organización. Los objetivos de seguridad operacional deben ser una declaración corta que describa a grandes rasgos lo que espera lograr la organización.

Criterios

a) Se hayan establecido los objetivos de seguridad operacional.

b) Los objetivos de seguridad operacional se expresan como una declaración de nivel superior que describe el compromiso de la organización para lograr la seguridad operacional.

c) Existe un proceso formal para desarrollar un conjunto coherente de objetivos de seguridad operacional.

d) Los objetivos de seguridad operacional se difunden y distribuyen.

e) Se han asignado recursos para lograr los objetivos.

f) Los objetivos de seguridad operacional se vinculan con los indicadores de seguridad operacional para facilitar el control y la medición, como corresponda.

Documentos de referencia cruzada

Documento de indicadores de rendimiento en materia de seguridad operacional, etc.

6. Funciones y responsabilidades

Objetivo

Describir las autoridades y responsabilidades de la seguridad operacional para el personal que participa en el SMS.

Criterios

a) El ejecutivo responsable se encarga de garantizar que el sistema de gestión de la seguridad operacional se implemente correctamente y se desempeñe según los requisitos en todas las áreas de la organización.

b) Se asignó un gerente (oficina) de seguridad operacional correspondiente, un comité de seguridad operacional o grupos de acción de seguridad operacional, según corresponda.

c) Las autoridades y responsabilidades de seguridad operacional del personal en todos los niveles de la organización están definidos y documentados.

d) Todo el personal comprende sus autoridades y responsabilidades en relación con los procesos, las decisiones y las medidas de la gestión de seguridad operacional.

e) Se dispone de un diagrama de responsabilidades institucionales del SMS.

Documentos de referencia cruzada

Manual de exposición de la empresa, manual de SOP, manual de administración, etc.

7. Notificación de seguridad operacional

Objetivo

Un sistema de notificación debe incluir medidas reactivas (informes de accidentes/incidentes, etc.) y proactivas/predictivas (informes de peligros). Describir los sistemas de notificación respectivos. Entre los factores que se deben considerar se incluyen: el formato del informe, la confidencialidad, los destinatarios, los procedimientos de investigación/evaluación, las medidas correctivas/preventivas y la divulgación del informe.

Criterios

a) La organización tiene un procedimiento que proporciona la captura de sucesos internos, como accidentes, incidentes y otros sucesos pertinentes para el SMS.

b) Se debe hacer una distinción entre los informes obligatorios (accidentes, incidentes graves, defectos importantes, etc.) que se deben notificar a la CAA y otros informes de sucesos de rutina, que permanecen dentro de la organización.

c) También existe un sistema de notificación de peligros/sucesos voluntaria y confidencial, que incorpora la protección de identidad/datos adecuada, según corresponda.

d) Los procesos de notificación respectivos son simples, accesibles y proporcionales a la envergadura de la organización.

e) Los informes de alto impacto y las recomendaciones asociadas se abordan y revisan según el nivel de gestión correspondiente.

f) Los informes se recopilan en una base de datos adecuada para facilitar el análisis necesario.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

8. Identificación de peligros y evaluación de riesgos

Objetivo

Describir el sistema de identificación de peligros y cómo se recopilan tales datos. Describir el proceso para la categorización de peligros/riesgos y su posterior priorización para una evaluación de seguridad operacional documentada. Describir cómo se lleva a cabo el proceso de evaluación de seguridad operacional y cómo se implementan planes de acción preventiva.

Criterios

a) Los peligros identificados se evalúan, priorizan y procesan para la evaluación de riesgos, según corresponda.

b) Existe un proceso estructurado para la evaluación de riesgos que implica la evaluación de gravedad, probabilidad, tolerabilidad y controles preventivos.

c) Los procedimientos de identificación de peligros y evaluación de riesgos se centran en la seguridad operacional de la aviación, así como también, en su contexto fundamental.

d) El proceso de evaluación de riesgos usa hojas de cálculo, formularios o software correspondientes a la complejidad de la organización y las operaciones involucradas.

e) El nivel de gestión correspondiente aprueba las evaluaciones de seguridad operacional completadas.

f) Existe un proceso para evaluar la eficacia de las medidas correctivas, preventivas y de recuperación que se han desarrollado.

g) Existe un proceso para la revisión periódica de las evaluaciones de seguridad operacional completadas y la documentación de sus resultados.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

9. Control y medición del rendimiento en materia de seguridad operacional

Objetivo

Describir el componente de control y medición del rendimiento en materia de seguridad operacional del SMS. Esto incluye los indicadores de rendimiento en materia de seguridad operacional (SPI) del SMS de la organización.

Criterios

a) El proceso formal para desarrollar y mantener un conjunto de indicadores de rendimiento en materia de seguridad operacional y sus objetivos eficaces asociados.

b) Correlación establecida entre los SPI y los objetivos de seguridad operacional de la organización, donde corresponda, y el proceso de aceptación reglamentaria de los SPI, donde sea necesario.

c) El proceso de control del rendimiento de estos SPI, incluido el procedimiento de medidas correctivas, cada vez que se activen tendencias inaceptables o anormales.

d) Cualquier otro criterio o proceso de control y medición del rendimiento en materia de seguridad operacional o de SMS complementario.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

10. Investigaciones relacionadas con la seguridad operacional y las medidas correctivas

Objetivo

Describir cómo se investigan y procesan los accidentes/incidentes/sucesos dentro de la organización, incluida la correlación con el sistema de identificación de peligros y gestión de riesgos del SMS de la organización.

Criterios

a) Procedimientos para garantizar que se investiguen de forma interna los accidentes e incidentes notificados.

b) Divulgación interna de los informes de investigación completados al igual que a la CAA, según corresponda.

c) Un proceso para garantizar que se lleven a cabo las medidas correctivas tomadas o recomendadas y para evaluar sus resultados/eficacia.

d) Procedimiento sobre la consulta y las medidas disciplinarias asociadas con los resultados del informe de investigación.

e) Condiciones definidas claramente según las cuales se podrían considerar medidas disciplinarias punitivas (por ejemplo, actividad ilegal, imprudencia, negligencia grave o conducta impropia deliberada).

f) Un proceso para garantizar que las investigaciones incluyan la identificación de averías activas, así como también, factores y peligros que contribuyen.

g) El procedimiento y el formato de la investigación proporcionan hallazgos sobre factores o peligros contribuyentes que se procesarán para la medida de seguimiento con el sistema de identificación de peligros y gestión de riesgos de la organización, donde corresponda.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

11. Capacitación y comunicación de seguridad operacional

Objetivo

Describir el tipo de SMS y otra capacitación relacionada con la seguridad operacional que reciba el personal y el proceso para garantizar la eficacia de la capacitación. Describir cómo se documentan tales procedimientos de capacitación. Describir los procesos/canales de comunicación de seguridad operacional dentro de la organización.

Criterios

a) Se documenta el programa de capacitación, la idoneidad y los requisitos.

b) Existe un proceso de validación que mide la eficacia de la capacitación.

c) La capacitación incluye capacitación inicial, recurrente y de actualización, donde corresponda.

d) La capacitación de SMS de la organización es parte del programa de capacitación general de la organización.

e) Se incorpora la toma de conciencia de SMS en el programa de empleo o adoctrinamiento.

f) Los procesos/canales de comunicación de la seguridad operacional dentro de la organización.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

12. Mejora continua y auditoría de SMS

Objetivo

Describir el proceso para la revisión y mejora continuas del SMS.

Criterios

a) El proceso para una auditoría/revisión internas regulares del SMS de la organización para garantizar su continua sustentabilidad, suficiencia y eficacia.

b) Describir cualquier otro programa que contribuya con la mejora continua del SMS de la organización y el rendimiento en materia de seguridad operacional, por ejemplo, MEDA, estudios de seguridad operacional, sistemas ISO.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

13. Gestión de los registros de SMS

Objetivo

Describir el método de almacenamiento de todos los registros y documentos relacionados con SMS.

Criterios

a) La organización tiene registros de SMS o un sistema de archivo que garantiza la conservación de todos los registros generados en conjunto con la implementación y operación del SMS.

b) Los registros que deben guardarse incluyen informes de peligros, informes de evaluación de riesgos, notas de grupos de acción de seguridad operacional/reuniones de seguridad operacional, diagramas de indicadores de rendimiento en materia de seguridad operacional, informes de auditoría del SMS y registros de la capacitación de SMS.

c) Los registros deben permitir que se rastreen todos los elementos del SMS y que estén accesibles para la administración de rutina del SMS, así como también, para propósitos de auditorías internas y externas.

Documentos de referencia cruzada

- - - - - - - - - - - - - -

14. Gestión de cambio

Objetivo

Describir el proceso de la organización para gestionar los cambios que pueden tener un impacto en los riesgos de la seguridad operacional y cómo tales procesos se integran con el SMS.

Criterios

a) Procedimientos para garantizar que los cambios institucionales y operacionales sustanciales consideran cualquier impacto que puedan tener en los riesgos existentes de la seguridad operacional.

b) Procedimientos para garantizar que se lleva a cabo una evaluación de seguridad operacional correspondiente antes de la introducción de nuevos equipos o procesos que tengan implicaciones de riesgos de seguridad operacional.

c) Procedimientos para la revisión de evaluaciones de seguridad operacional existentes cada vez que se apliquen cambios al proceso o equipo asociado.

Documentos de referencia cruzada

SOP de la empresa relacionado con la gestión de cambio, etc.

15. Plan de respuesta ante emergencias/contingencia

Objetivo

Describir las intenciones de la organización acerca de situaciones de emergencia y sus controles de recuperación correspondientes, además de su compromiso para abordar dichas situaciones. Describir las funciones y responsabilidades del personal clave. El plan de respuesta ante emergencias puede ser un documento separado o puede ser parte del manual de SMS.

Criterios (como corresponda para la organización)

a) La organización tiene un plan de emergencia que describe las funciones y responsabilidades en caso de un incidente, una crisis o un accidente importante.

b) Existe un proceso de notificación que incluye una lista de llamadas de emergencia y un proceso de movilización interno.

c) La organización tiene disposiciones con otras agencias para recibir ayuda y la disposición de servicios de emergencia, según corresponda.

d) La organización tiene procedimientos para las operaciones del modo de emergencia, donde corresponda.

e) Existe un procedimiento para vigilar el bienestar de todas las personas afectadas y para notificar al familiar más cercano.

f) La organización ha establecido procedimientos para tratar con los medios de comunicación y temas relacionados con el seguro.

g) Existen responsabilidades de investigación de accidentes definidas dentro de la organización.

h) El requisito para preservar la evidencia, asegurar el área afectada y la notificación obligatoria/gubernamental está claramente declarada.

i) Existe una capacitación de preparación y respuesta ante emergencias para el personal afectado.

j) La organización desarrolló un plan de evacuación en caso de una aeronave o un equipo averiado con el asesoramiento de propietarios de aeronaves/equipos, explotadores de aeródromo u otras agencias, según corresponda.

k) Existe un procedimiento para registrar las actividades durante una respuesta ante emergencias.

Documentos de referencia cruzada

Manual de ERP, etc.

Apéndice 5 del Capítulo 5

SISTEMAS DE NOTIFICACIÓN VOLUNTARIA Y CONFIDENCIAL

[Véase 5.3.42 a 5.3.52; 5.3.66 a 5.3.73; 5.5.4, Elemento 2.1 a)]

Nota.— La siguiente guía se basa en el ejemplo de un explotador aéreo integrado y la organización de mantenimiento. Para otros tipos de organizaciones de proveedores de servicios, este material guía podría personalizarse, si fuera necesario.

El sistema de notificación voluntaria y confidencial de una organización debe, como mínimo, definir:

a) el objetivo del sistema de notificación;

Ejemplo:

El objetivo clave del sistema de notificación voluntaria y confidencial de [Nombre de la organización] es mejorar la seguridad operacional de nuestras actividades de aviación de la empresa mediante la recopilación de informes sobre deficiencias reales y posibles de la seguridad operacional que, de lo contrario, no se informarían mediante otros canales. Tales informes pueden implicar sucesos, peligros o amenazas pertinentes para la seguridad operacional de nuestras actividades de aviación. Este sistema no elimina la necesidad de la notificación formal de accidentes e incidentes, de acuerdo con los SOP de nuestra empresa, ni tampoco, el envío de los informes obligatorios de sucesos a las autoridades reglamentarias pertinentes.

El [Nombre del sistema] es un sistema de notificación de sucesos y peligros voluntario, no punitivo y confidencial que administra [Nombre del departamento/oficina]. Proporciona un canal para la notificación voluntaria de sucesos y peligros de aviación pertinentes para las actividades de seguridad operacional de nuestra organización, mientras protege la identidad del notificados.

Nota.— Al establecer dicho sistema, la organización tendrá que decidir si integra o segrega su sistema de notificación de seguridad, salud y ambiente en el trabajo (OSHE) del sistema de notificación de seguridad operacional de la aviación. Esto puede depender de las expectativas o los requisitos de las autoridades de OSHE y aviación respectivas. Donde exista un sistema de notificación de OSHE separado en la empresa, se debe destacar en conformidad en este párrafo para guiar al notificador, según sea necesario.

b) el alcance de los sectores/áreas de aviación que aborda el sistema;

Ejemplo:

El [Nombre del sistema] aborda áreas como:

a) operaciones de vuelo;

b) mantenimiento de la aeronave en el hangar;

c) mantenimiento de componentes en el taller;

d) gestión de la flota técnica;

e) gestión técnica del inventario;

f) planificación de ingeniería;

g) servicios técnicos;

h) registros técnicos;

i) mantenimiento de línea;

j) etc.

c) quien pueda hacer un informe voluntario;

Ejemplo:

Si pertenece a cualquiera de estas áreas o departamentos operacionales, puede contribuir con la mejora de la seguridad operacional de la aviación mediante [Nombre del sistema] al notificar los sucesos, los peligros o las amenazas pertinentes para las actividades de aviación de nuestra organización:

a) miembros de la tripulación de vuelo y de la cabina;

b) controladores de tránsito aéreo;

c) ingenieros, técnicos o mecánicos de aeronaves con licencia;

d) empleados de organizaciones de mantenimiento, diseño y fabricación;

e) explotadores de servicios de escala del aeropuerto;

f) empleados del aeródromo;

g) personal de aviación general;

h) etc.

d) cuando se debe hacer dicho informe;

Ejemplo:

Debe hacer un informe cuando:

a) desee que otros aprendan y se beneficien del incidente o peligro, pero está preocupado de proteger su identidad;

b) no existe otro procedimiento o canal de notificación adecuado; y

c) ha probado con otro procedimiento o canal de notificación sin que el problema se haya abordado.

e) cómo se procesan los informes;

Ejemplo:

El [Nombre del sistema] presta particular atención a la necesidad de proteger la identidad del notificador cuando se procesan todos los informes. El gerente leerá y validará cada informe. El gerente puede comunicarse con el notificador para asegurarse de que comprenda la naturaleza y las circunstancias del suceso/peligro informado o para obtener información y clarificación adicional necesarias.

Cuando el gerente esté satisfecho con que la información obtenida es completa y coherente, omitirá la identidad de quien entrega la información e ingresará los datos en la base de datos del [Nombre del sistema]. En caso que se deba buscar aportes de cualquier tercero, solo se usarán datos no identificados.

El formulario del [Nombre del sistema], con la fecha de retorno anotada, será devuelto finalmente al notificador. El gerente intentará completar el procesamiento dentro de diez (10) días hábiles si no se necesita información adicional. En los casos donde el gerente debe conversar con el notificador o consultar a un tercero, se necesitará más tiempo.

Si el gerente no está en su oficina por un tiempo prolongado, el gerente suplente procesará el informe. Los notificadores pueden estar tranquilos de que el gerente o el gerente suplente leerá y seguirá cada informe de [Nombre del sistema].

Distribución de información de seguridad operacional dentro de la empresa y la comunidad de la aviación

Se pueden compartir informes y extractos no identificados pertinentes dentro de la empresa, así como también, con accionistas de aviación externa, según se considere adecuado. Esto permitirá que todo el personal y los departamentos interesados dentro de la empresa, además de los accionistas de aviación externos, revisen sus propias operaciones y respalden la mejora de la seguridad operacional de la aviación como un todo.

Si el contenido de un informe de [Nombre del sistema] sugiere una situación o condición que represente una amenaza inmediata o urgente para la seguridad operacional de la aviación, el informe se tratará con prioridad y se derivará, luego de eliminar la identidad del notificador, a las organizaciones o autoridades pertinentes lo antes posible, para permitirles tomar las medidas de seguridad operacional necesarias.

f) comunicación con el gerente de [Nombre del sistema];

Ejemplo:

Si lo desea, puede llamar al gerente de [Nombre del sistema] para consultar sobre [Nombre del sistema] o para solicitar un análisis preliminar con el gerente de [Nombre del sistema] antes de hacer un informe. Puede comunicarse con el gerente y el gerente suplente durante horas de oficina de lunes a viernes en los siguientes números de teléfono:

Administrador del [Nombre del sistema]	Administrador suplente
El Sr. ABC	El Sr. XYZ
Tel.:	Tel.:

Apéndice 6 del Capítulo 5

INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DEL SMS

1. Las Tablas 5-A6-1 a 5-A6-4 (ejemplos de indicadores de seguridad operacional) proporcionan ejemplos ilustrativos de los indicadores de rendimiento en materia de seguridad operacional (SPI) colectivos del Estado y sus criterios de configuración de alertas y objetivos correspondientes. Los SPI del SMS se reflejan en el lado derecho de las tablas. Los criterios del nivel de alerta y objetivos correspondientes para cada indicador se deben explicar como se muestra. Los indicadores de rendimiento en materia de seguridad operacional del SSP a la izquierda de las tablas aparecen para indicar la correlación necesaria entre los indicadores de seguridad operacional de SMS y SSP. Los proveedores de productos y servicios deben desarrollar los SPI del SMS con el asesoramiento de sus organizaciones reglamentarias estatales respectivas. Sus SPI propuestos deberán ser coherentes con los indicadores de seguridad operacional de SSP del Estado; por lo tanto, se debe obtener un acuerdo/aceptación necesario.

2. La Tabla 5-A6-5 (ejemplo de un diagrama del indicador de rendimiento en materia de seguridad operacional del SMS) es un ejemplo de como luce un diagrama del indicador de rendimiento en materia de seguridad operacional del SMS de alto impacto. En este caso, es la tasa de incidentes que pueden notificarse/obligatorios del explotador de una línea aérea. El diagrama de la izquierda es el rendimiento del año anterior, mientras que el diagrama de la derecha representa las actualizaciones de datos constantes del año actual. La configuración del nivel de alerta se basa en criterios de desviación estándar de la métrica de seguridad operacional básica. La fórmula de la hoja de cálculo Excel es “=STDEVP”. Para propósitos del cálculo de desviación estándar manual, la fórmula es:

$$\sigma = \sqrt{\frac{\Sigma\,(x - \mu)^2}{N}}$$

donde “X” es el valor de cada punto de datos; “N” es el número de puntos de datos y “μ” es el valor promedio de todos los puntos de datos.

3. La configuración de objetivos es una mejora porcentual deseada (en este caso el 5%) en el promedio del punto de datos del año anterior. Este diagrama se genera con la hoja de datos de la Tabla 5-A6-6.

4. La hoja de datos en la Tabla 5-A6-6 se usa para generar el diagrama del indicador de rendimiento en materia de seguridad operacional que aparece en la Tabla 5-A6-5. Lo mismo puede usarse para generar cualquier otro indicador de rendimiento en materia de seguridad operacional con la entrada de datos adecuada y la enmienda del descriptor del indicador de rendimiento en materia de seguridad operacional.

5. La Tabla 5-A6-7 (ejemplo del resumen de rendimiento de un SMS) proporciona un resumen de todos los indicadores de seguridad operacional del SMS de los explotadores, con sus resultados del nivel de alertas y objetivos respectivos anotados. Tal resumen podrá compilarse al final de cada período de control para proporcionar una descripción general del rendimiento del SMS. Si se desea una medición del resumen del rendimiento más cuantitativa, se pueden asignar puntos adecuados para cada resultado Sí/No para cada resultado de objetivos y alertas. Ejemplo:

Indicadores de alto impacto:

Nivel de alerta no violado	[Sí (4), No (0)]
Objetivo alcanzado	[Sí (3), No (0)]

Indicadores de bajo impacto:

Nivel de alerta no violado	[Sí (2), No (0)]
Objetivo alcanzado	[Sí (1), No (0)]

Gracias a esto se puede obtener una puntuación (o porcentaje) de resumen para indicar el rendimiento en materia de seguridad operacional general del SMS al final de cualquier período de control determinado.

Tabla 5-A6-1. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores aéreos

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores aéreos (solo explotadores aéreos del Estado)											
Tasa de accidentes/ incidentes graves mensual/ trimestral del explotador aéreo colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador aéreo colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa de incidentes graves mensual de la flota individual del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes mensual de la flota combinada del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
Tasa de incidentes de IFSD trimestral del motor del explotador aéreo colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la inspección de la estación de línea del explotador aéreo colectivo de CAA (hallazgos por inspección)	Consideración	Consideración	Tasa de incidentes graves mensual de la flota combinada del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador (hallazgos por auditoría)	Consideración	Consideración
			% de LEI promedio anual de la inspección de vigilancia de la plataforma del explotador aéreo extranjero de CAA (para cada explotador extranjero)	Consideración	Consideración	Tasa de incidentes de IFSD del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros voluntario del explotador (por ejemplo, cada 1 000 FH)	Consideración	Consideración
			Tasa del informe de incidentes de DGR del explotador colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa del informe de incidentes de DGR del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
etc.											

Tabla 5-A6-2. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores del aeródromo

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores de aeródromos											
Tasa de incidentes graves/ accidentes en tierra mensual/ trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador del aeródromo colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa de incidentes graves/accidentes en tierra trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador del aeródromo (hallazgos por auditoría)	Consideración	Consideración
Tasa de incidentes en la excursión en pista mensual/trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa de incidentes en la excursión en pista trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros de objetos extraños/suciedad trimestral del explotador del aeródromo (por ejemplo, cada 10 000 movimientos en tierra)	Consideración	Consideración
Tasa de incidentes en la incursión en pista mensual/trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa de incidentes en la incursión en pista trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros voluntario del explotador (por personal de operaciones por trimestre)	Consideración	Consideración

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
									Tasa trimestral del informe de incidentes de daños por objetos extraños en la aeronave del explotador del aeródromo — Implica daños a la aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
etc.											

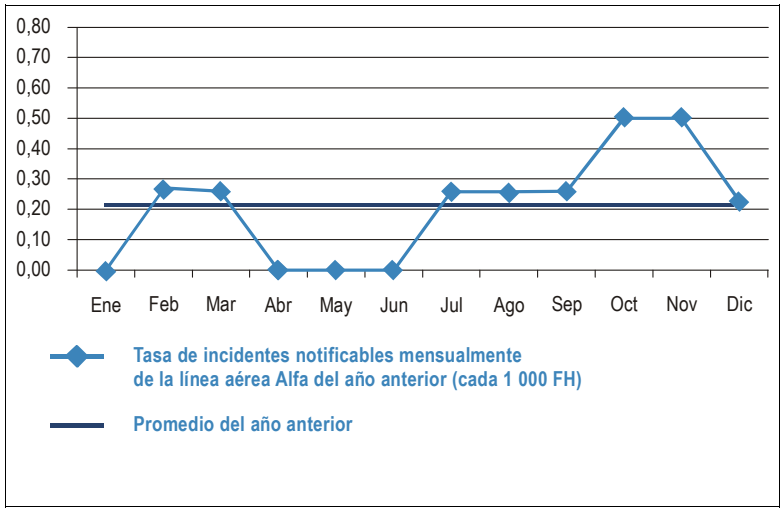
Tabla 5-A6-3. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores de ATS

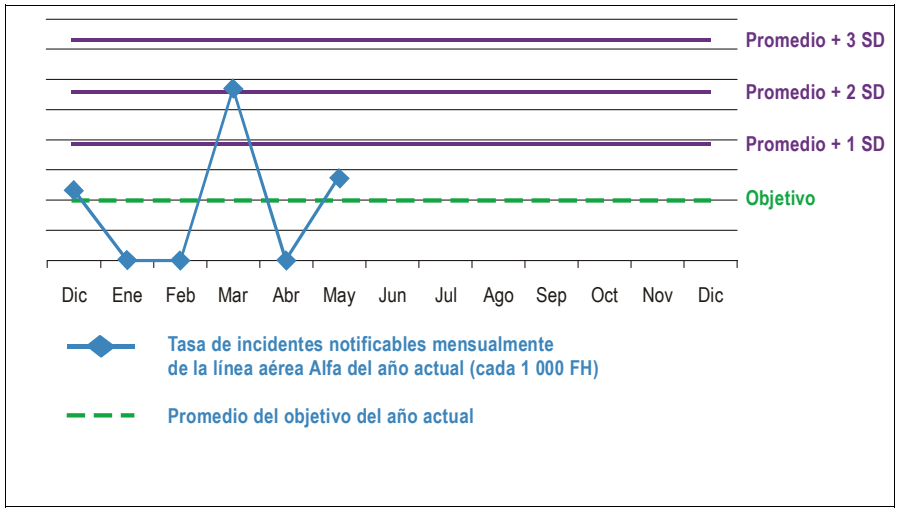
Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores de ATS											
Tasa de incidentes graves (espacio aéreo) de FIR trimestral de ATS colectivos de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes trimestral del RA de los TCAS de la FIR de ATS colectivos de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes graves de FIR trimestral del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimien-tos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes trimestral del RA de los TCAS de la FIR del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
			Tasa de incidentes trimestral (LOS) de salidas de nivel de suelo de FIR de ATS colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes de cuasicolisión trimestral/anual del explotador de ATS (por ejemplo, cada 100 000 movi-mientos en vuelo)	Suponiendo que el promedio anual histórico es 3, la tasa de alerta posible podría ser 5.	Suponiendo que el promedio anual histórico es 3, la tasa de objetivo posible podría ser 2.	Tasa de incidentes trimestral (LOS) de salidas de nivel de suelo de FIR del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
			Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador de ATS colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración				Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador de ATS (hallazgos por auditoría)	Consideración	Consideración
etc.											

Tabla 5-A6-4. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para organizaciones de mantenimiento, producción y diseño (DOA/POA/MRO)

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
DOA/POA/MRO											
Informes obligatorios de defectos (MDR) trimestrales de la MRO colectiva de CAA recibidos	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia de MRO/POA/DOA colectivas de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa trimestral de MRO/POA de reclamos de la garantía técnica de los componentes	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna de MRO/POA/DOA (hallazgos por auditoría)	Consideración	Consideración
Tasa trimestral de POA/DOA colectiva de CAA de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración				Tasa trimestral de POA/DOA de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración	Tasa de averías/rechazos trimestral de la inspección final/ pruebas de MRO/POA/DOA (debido a problemas de calidad interna)	Consideración	Consideración
						Tasa trimestral de MRO/POA de los informes obliga-torios/importantes de defectos de componentes emitidos (debido a problemas de calidad interna)	Consideración	Consideración	Tasa de informes de peligros voluntarios de MRO/POA/DOA (por personal de operaciones por trimestre)	Consideración	Consideración
etc.											

Tabla 5-A6-5. Ejemplo de un diagrama del indicador de rendimiento en materia de seguridad operacional del SMS (con la configuración del nivel de alerta y objetivo)





a) Configuración de nivel de alerta:

El nivel de alerta de un nuevo período de control (año actual) se basa en lal performance del período anterior (año anterior), es decir, su promedio de datos y desviación estándar. Las tres líneas de alerta son el promedio + 1 SD, promedio + 2 SD y promedio + 3 SD.

b) Activador del nivel de alerta:

Se indica una alerta (tendencia anormal/inaceptable) si cualquiera de las siguientes condiciones se cumple en el período de control actual (año actual):

— cualquier punto único está sobre la línea 3 SD
— 2 puntos consecutivos están sobre la línea 2 SD
— 3 puntos consecutivos están sobre la línea 1 SD.

Cuando se activa una alerta (posible situación de alto riesgo o fuera de control), se espera una medida de seguimiento correspondiente, como un análisis posterior para determinar la fuente y causa de origen de la tasa de incidente anormal y cualquier medida necesaria para abordar la tendencia inaceptable.

c) Configuración del nivel de objetivo (mejora planificada):

La configuración del nivel de objetivo puede estar menos estructurada que la configuración del nivel de alerta, por ejemplo, tenga como objetivo la nueva tasa promedio del período de control (año actual) para que indique ser un 5% inferior (mejor) que el valor promedio del período anterior.

d) Logro del objetivo:

Al final del año actual, si la tasa promedio del año actual es inferior en al menos un 5% o más que la tasa promedio del año anterior, el objetivo establecido de 5% de mejora se considera como logrado.

e) Niveles de alerta y objetivo — Período de validez:

Los niveles de alerta y objetivo deben revisarse/restablecerse para cada nuevo período de control, según la tasa promedio y SD del período anterior equivalente, según corresponda.

Tabla 5-A6-6. Hoja de datos de muestra usada para generar un diagrama de alto impacto del indicador de seguridad operacional del SMS (con criterios de la configuración de alerta y objetivo)

Año anterior				
Mes	*FH totales de la línea aérea Alfa*	*Cantidad de incidentes de notificación obligatoria*	*Tasa de incidentes**	*Promedio*
Enero	3 992	—	0,00	0,21
Febrero	3 727	1,00	0,27	0,21
Marzo	3 900	1,00	0,26	0,21
Abril	3 870	—	0,00	0,21
Mayo	3 976	—	0,00	0,21
Junio	3 809	—	0,00	0,21
Julio	3 870	1,00	0,26	0,21
Agosto	3 904	1,00	0,26	0,21
Septiembre	3.864	1,00	0,26	0,21
Octubre	3 973	2,00	0,50	0,21
Noviembre	3 955	2,00	0,51	0,21
Diciembre	4 369	1,00	0,23	0,21
		Promedio	0,21	
		SD	0,18	

Año actual							
Mes	*FH totales de la línea aérea Alfa*	*Cantidad de inci-.dentes de notificación obligatoria*	*Tasa de incidentes**	*Promedio del año anterior + 1 SD*	*Promedio del año anterior + 2 SD*	*Promedio del año anterior + 3 SD*	*Promedio del objetivo del año actual*
Diciembre	4 369	1,00	0,23	0,39	0,56	0,73	0,21
Enero	4 090	0,00	0,00	0,39	0,56	0,73	0,20
Febrero	3 316	0,00	0,00	0,39	0,56	0,73	0,20
Marzo	3 482	2,00	0,57	0,39	0,56	0,73	0,20
Abril	3 549	0,00	0,00	0,39	0,56	0,73	0,20
Mayo	3 633	1,00	0,28	0,39	0,56	0,73	0,20
Junio				0,39	0,56	0,73	0,20
Julio				0,39	0,56	0,73	0,20
Agosto				0,39	0,56	0,73	0,20
Septiembre				0,39	0,56	0,73	0,20
Octubre				0,39	0,56	0,73	0,20
Noviembre				0,39	0,56	0,73	0,20
Diciembre				0,39	0,56	0,73	0,20
		Promedio					
		SD					

Promedio + 1 SD	Promedio + 2 SD	Promedio + 3 SD
0,39	0,56	0,73

El objetivo del año actual indica una tasa de mejora promedio del 5% sobre la tasa promedio del año anterior, la que es:	0,20

Los criterios de configuración del nivel de alerta del año actual se basan en el año anterior (Promedio + 1/2/3 SD).

* Cálculo de la tasa (cada 1 000 FH).

Tabla 5-A6-7. Ejemplo de la medición de rendimiento en materia de seguridad operacional del SMS de la línea aérea Alfa (digamos, para el año 2010)

Indicador de rendimiento en materia de seguridad operacional de alto impacto					
	Descripción del SPI	*Criterios del nivel de alerta del SPI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios del nivel de objetivos del SPI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Tasa de incidentes graves mensual de la flota A320 de la línea aérea Alfa (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No
2	Tasa de incidentes de IFSD de la flota A320 de la línea aérea Alfa (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	Sí	3% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
3	etc.				

Indicadores de seguridad operacional de bajo impacto					
	Descripción del SPI	*Criterios del nivel de alerta del SPI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios del nivel de objetivos del SPI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Tasa de incidentes mensual de la flota combinada del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No
2	Tasa de % o hallazgos de LEI anual de la auditoría de QMS interna del explotador (hallazgos por auditoría)	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
3	Tasa del informe de peligros voluntario del explotador (por ejemplo, cada 1 000 FH)	TBD		TBD	
4	Tasa del informe de incidentes de DGR del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	No	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
5	etc.				

Nota 1.— Otros indicadores del proceso. Además de los indicadores de seguridad operacional del nivel de SMS mencionado anteriormente, puede que haya otros indicadores del nivel de sistema dentro de cada área operacional de una organización. Entre los ejemplos se incluyen indicadores de control específicos del proceso o del sistema en ingeniería, operaciones, QMS, etc., o indicadores asociados con programas basados en rendimiento, como la gestión de riesgos por fatiga o la gestión de combustible. Tales indicadores específicos del proceso o del sistema deben administrarse correctamente como parte del sistema o proceso de interés. Pueden verse como indicadores de nivel específicos del sistema o proceso, lo que complementa los indicadores de rendimiento en materia de seguridad operacional de mayor nivel. Deben abordarse dentro de los manuales/SOP del sistema o proceso respectivos, según corresponda. Sin embargo, los criterios para configurar los niveles de alertas u objetivos para tales indicadores deben, de preferencia, alinearse con aquellos de los indicadores de rendimiento en materia de seguridad operacional del nivel de SMS, donde corresponda.

Nota 2.— Selección de indicadores y configuración. Una organización debe seleccionar la combinación (o paquete) de indicadores de seguridad operacional de alto y bajo impacto, de acuerdo con el alcance del sistema de la organización. Para aquellos indicadores donde los criterios sugeridos de la configuración del nivel de alerta u objetivo no sean aplicables, la organización puede considerar un criterio alternativo, según corresponda. La guía general es configurar las alertas y los objetivos que consideran el rendimiento reciente histórico o actual.

Apéndice 7 del Capítulo 5

LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHAS Y PLAN DE IMPLEMENTACIÓN DEL SMS

1. LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHAS INICIAL (TABLA 5-A7-1)

1.1 La lista de verificación del análisis de brechas inicial en la Tabla 5-A7-1 puede usarse como una plantilla para realizar el primer paso de un análisis de brechas del SMS. Este formato con sus respuestas generales "Sí/No/Parcial" proporcionará una indicación inicial del amplio alcance de las brechas y, por lo tanto, la carga de trabajo general que puede esperarse. El cuestionario puede ajustarse para adaptarse a las necesidades de la organización y a la naturaleza del producto o servicio suministrado. Esta información inicial debe ser útil para que la administración superior anticipe la escala del esfuerzo de implementación del SMS y, por lo tanto, los recursos que se proporcionarán. Esta lista de verificación inicial necesitaría de seguimiento con un plan de implementación adecuado, según las Tablas 5-A7-2 y 5-A7-3.

1.2. Una respuesta "Sí" indica que la organización satisface o supera las expectativas de la pregunta en cuestión. Una respuesta "No" indica una brecha importante en el sistema existente, en relación con la expectativa de la pregunta. Una respuesta "Parcial" indica que se requiere una posterior mejora o trabajo de desarrollo para un proceso existente a fin de satisfacer las expectativas de la pregunta.

Nota.— El SSP hace referencia en corchetes [ ] al material guía en este manual, en relación con la pregunta del análisis de brechas.

Tabla 5-A7-1. Lista de verificación del análisis de brechas

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
Componente 1 — POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL			
Elemento 1.1 — Compromiso y responsabilidad de la gestión			
1.1-1	¿Está implementada una política de seguridad operacional? [5.3.7 a 5.3.15; 5.5.3]	☐ Sí ☐ No ☐ Parcial	
1.1-2	¿Refleja la política de seguridad operacional el compromiso de la administración superior acerca de la gestión de la seguridad operacional? [5.3.7 a 5.3.15]	☐ Sí ☐ No ☐ Parcial	
1.1-3	¿Es adecuada la política de seguridad operacional según la envergadura, naturaleza y complejidad de la organización? [5.3.7 a 5.3.15]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
1.1-4	¿Es pertinente la política de seguridad operacional para la seguridad operacional de la aviación? [5.3.7 a 5.3.15]	☐ Sí ☐ No ☐ Parcial	
1.1-5	¿Ha firmado el ejecutivo responsable la política de seguridad operacional? [5.3.7 a 5.3.15; 5.5.3]	☐ Sí ☐ No ☐ Parcial	
1.1-6	¿Se comunica la política de seguridad operacional, con un respaldo visible, en toda la [Organización]? [5.5.3]	☐ Sí ☐ No ☐ Parcial	
1.1-7	¿Se revisa periódicamente la política de seguridad operacional para garantizar que siga siendo pertinente y adecuada para la [Organización]? [5.5.3]	☐ Sí ☐ No ☐ Parcial	
Elemento 1.2 — Responsabilidades de la seguridad operacional			
1.2-1	¿Ha identificado [Organización] a un ejecutivo responsable que, sin importar otras funciones, tenga la máxima responsabilidad, en nombre de [Organización], de la implementación y mantenimiento del SMS? [5.3.16 a 5.3.26; 5.5.2]	☐ Sí ☐ No ☐ Parcial	
1.2-2	¿Tiene el ejecutivo responsable total control de los recursos financieros y humanos necesarios para las operaciones autorizadas que se realizarán según el certificado de operaciones? [5.3.16 a 5.3.26]	☐ Sí ☐ No ☐ Parcial	
1.2-3	¿Tiene el ejecutivo responsable la autoridad final sobre todas las actividades de aviación de su organización? [5.3.16 a 5.3.26]	☐ Sí ☐ No ☐ Parcial	
1.2-4	¿Ha identificado y documentado [Organización] las responsabilidades de seguridad operacional de la gestión, así como también, del personal de operaciones, en relación con el SMS? [5.3.16 a 5.3.26]	☐ Sí ☐ No ☐ Parcial	
1.2-5	¿Existe un comité de seguridad operacional o consejo de revisión para el propósito de revisión del SMS y el rendimiento en materia de seguridad operacional? [5.3.27 a 5.3.33; Apéndice 4]	☐ Sí ☐ No ☐ Parcial	
1.2-6	¿Lidera al comité de seguridad operacional un ejecutivo responsable o un delegado asignado correctamente, confirmado debidamente en el manual del SMS? [5.3.27 a 5.3.33; Apéndice 4]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
1.2-7	¿Incluye el comité de seguridad operacional a líderes de departamento u operacionales pertinentes, según corresponda? [5.3.27 a 5.3.33; Apéndice 4]	☐ Sí ☐ No ☐ Parcial	
1.2-8	¿Existen grupos de acción de seguridad operacional que trabajan junto con el comité de seguridad operacional (en particular para las organizaciones grandes/complejas)? [5.3.27 a 5.3.33; Apéndice 4]	☐ Sí ☐ No ☐ Parcial	
Elemento 1.3 — Nombramiento del personal de seguridad operacional clave			
1.3-1	¿Ha asignado [Organización] a una persona calificada para gestionar y vigilar la operación diaria del SMS? [5.3.27 a 5.3.33; 5.5.2; Apéndice 2]	☐ Sí ☐ No ☐ Parcial	
1.3-2	¿Tiene la persona calificada acceso o notificación directa al ejecutivo responsable, acerca de la implementación y operación del SMS? [5.3.27 a 5.3.33; 5.5.2; Apéndice 2, 6.1]	☐ Sí ☐ No ☐ Parcial	
1.3-3	¿Tiene el gerente responsable de administrar el SMS otra responsabilidad más que pueda entrar en conflicto o perjudicar su papel como gerente de SMS? [Apéndice 2, 6.4]	☐ Sí ☐ No ☐ Parcial	
1.3-4	¿Es el puesto de gerente de SMS un puesto administrativo superior que no es inferior jerárquicamente o subordinado a otros puestos operacionales o de producción? [Apéndice 2, 6.4]	☐ Sí ☐ No ☐ Parcial	
Elemento 1.4 — Coordinación de la planificación de respuesta ante emergencias			
1.4-1	¿Tiene [Organización] un plan de respuesta ante emergencias/contingencia adecuado para la envergadura, naturaleza y complejidad de la organización? [Apéndice 3]	☐ Sí ☐ No ☐ Parcial	
1.4-2	¿Aborda el plan de emergencia/contingencia todos los escenarios de emergencia/crisis posibles o probables, en relación con los suministros de productos o servicios de aviación de la organización? [Apéndice 3, 4 f)]	☐ Sí ☐ No ☐ Parcial	
1.4-3	¿Incluye el ERP procedimientos para la producción, la entrega y el respaldo seguros y continuos de los productos o servicios de la aviación durante tales emergencias o contingencias? [Apéndice 3, 4 e)]	☐ Sí ☐ No ☐ Parcial	
1.4-4	¿Existe un plan y registro para los ensayos o ejercicios en relación con el ERP? [Apéndice 3, 5 c)]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
1.4-5	¿Aborda el ERP la coordinación necesaria de sus procedimientos de respuesta ante emergencias/contingencia con los procedimientos de contingencia de emergencia/respuesta de otras organizaciones, donde corresponda? [Apéndice 3, 4 d)]	☐ Sí ☐ No ☐ Parcial	
1.4-6	¿Tiene [Organización] un proceso para distribuir y comunicar el ERP a todo el personal pertinente, incluidas las organizaciones externas pertinentes? [Apéndice 3, 5 d)]	☐ Sí ☐ No ☐ Parcial	
1.4-7	¿Existe un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continuas? [Apéndice 3, 5 f)]	☐ Sí ☐ No ☐ Parcial	
Elemento 1.5 — Documentación de SMS			
1.5-1	¿Existe un resumen de SMS de nivel superior o documento de exposición que esté aprobado por el gerente responsable y aceptado por la CAA? [5.3.36 a 5.3.38]	☐ Sí ☐ No ☐ Parcial	
1.5-2	¿Aborda la documentación del SMS el SMS de la organización y sus componentes y elementos asociados? [5.3.36 a 5.3.38; 5.4.1; Apéndice 4]	☐ Sí ☐ No ☐ Parcial	
1.5-3	¿Está el marco de trabajo de SMS de [Organización] en alineación con el marco de trabajo del SMS reglamentario? [5.3.36 a 5.3.38; 5.4.1; Apéndice 4]	☐ Sí ☐ No ☐ Parcial	
1.5-4	¿Mantiene [Organización] un registro de documentación de respaldo pertinente para la implementación y operación del SMS? [5.3.36 a 5.3.38; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
1.5-5	¿Tiene [Organización] un plan de implementación de SMS para establecer su proceso de implementación de SMS, incluidas las tareas específicas y sus hitos de implementación pertinentes? [5.4.4]	☐ Sí ☐ No ☐ Parcial	
1.5-6	¿Aborda el plan de implementación de SMS la coordinación entre el SMS del proveedor de servicios y el SMS de las organizaciones externas, donde corresponde? [5.4.4]	☐ Sí ☐ No ☐ Parcial	
1.5-7	¿Respalda el ejecutivo responsable el plan de implementación de SMS? [5.4.4; 5.5.2]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
Componente 2 — GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL			
Elemento 2.1 — Identificación de peligros			
2.1-1	¿Existe un proceso para la notificación de peligros/amenazas voluntaria de todos los empleados? [5.3.42 a 5.3.52; 5.5.4]	☐ Sí ☐ No ☐ Parcial	
2.1-2	¿Es simple la notificación de peligros/amenazas voluntaria, está disponible a todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios? [5.3.42 a 5.3.52]	☐ Sí ☐ No ☐ Parcial	
2.1-3	¿Incluye el SDCPS de [Organización] procedimientos para la notificación de incidentes/accidentes mediante personal operacional o producción? [5.3.42 a 5.3.52; 5.5.4; Capítulo 4, Apéndice 3]	☐ Sí ☐ No ☐ Parcial	
2.1-4	¿Es simple la notificación de incidentes/accidentes, es accesible para todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios? [5.3.42 a 5.3.52; 5.5.4]	☐ Sí ☐ No ☐ Parcial	
2.1-5	¿Tiene [Organización] procedimientos para la investigación de todos los incidentes/accidentes notificados? [5.3.42 a 5.3.52; 5.5.4]	☐ Sí ☐ No ☐ Parcial	
2.1-6	¿Existen procedimientos para garantizar que los peligros/amenazas identificados o descubiertos durante los procesos de investigación de incidentes/accidentes se explican correctamente y se integran en la recopilación de peligros y el procedimiento de mitigación de riesgos de la organización? [2.13.9; 5.3.50 f); 5.5.5]	☐ Sí ☐ No ☐ Parcial	
2.1-7	¿Existen procedimientos para revisar peligros/amenazas de informes industriales pertinentes para medidas de seguimiento o la evaluación de riesgos, donde corresponda? [5.3.5.1]	☐ Sí ☐ No ☐ Parcial	
Elemento 2.2 — Evaluación y mitigación de riesgos de seguridad operacional			
2.2-1	¿Existe un procedimiento de identificación de peligros y mitigación de riesgos (HIRM) documentado que implique el uso de herramientas de análisis de riesgos objetivas? [2.13; 2.14; 5.3.53 a 5.3.61]	☐ Sí ☐ No ☐ Parcial	
2.2-2	¿Aprobaron los gerentes de departamento o un nivel superior los informes de evaluación de riesgos, donde corresponda? [2.15.5; 5.3.53 a 5.3.61]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
2.2-3	¿Existe un procedimiento para la revisión periódica de los registros de mitigación de riesgos existentes? [5.5.4]	☐ Sí ☐ No ☐ Parcial	
2.2-4	¿Existe un procedimiento para explicar las medidas de mitigación cada vez que se identifican niveles de riesgos inaceptables? [5.5.4]	☐ Sí ☐ No ☐ Parcial	
2.2-5	¿Existe un procedimiento para priorizar los peligros identificados para las medidas de mitigación de riesgos? [5.5.4]	☐ Sí ☐ No ☐ Parcial	
2.2-6	¿Existe un programa para la revisión sistemática y progresiva de todas las operaciones, los procesos, las instalaciones y los equipos relacionados con la seguridad operacional de la aviación sujetos al proceso de HIRM, como lo identificó la organización? [5.5.4]	☐ Sí ☐ No ☐ Parcial	
Componente 3 — ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL			
Elemento 3.1 — Control y medición del rendimiento en materia de seguridad operacional			
3.1-1	¿Existen indicadores de rendimiento en materia de seguridad operacional identificados para medir y controlar el rendimiento en materia de seguridad operacional de las actividades de aviación de la organización? [5.3.66 a 5.3.73; 5.4.5; 5.5.4; 5.5.5; Apéndice 6]	☐ Sí ☐ No ☐ Parcial	
3.1-2	¿Son pertinentes los indicadores de rendimiento en materia de seguridad operacional para la política de seguridad operacional de la organización, así como también, los objetivos/metas de seguridad operacional de alto nivel? [5.3.66 a 5.3.73; 5.4.5; Apéndice 6]	☐ Sí ☐ No ☐ Parcial	
3.1-3	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional una configuración de alerta/objetivo para definir regiones de rendimiento inaceptables y metas de mejora planificadas? [5.3.66 a 5.3.73; 5.4.5; 5.5.4; 5.5.5; Apéndice 6]	☐ Sí ☐ No ☐ Parcial	
3.1-4	¿Se basa la configuración de niveles de alerta o los criterios fuera de control en principios de métricas de seguridad operacional objetivos? [5.3.66 a 5.3.73; 5.4.5; Apéndice 6]	☐ Sí ☐ No ☐ Parcial	
3.1-5	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional un control cuantitativo de resultados de seguridad operacional de alto impacto (por ejemplos, tasas de incidentes de accidentes e incidentes graves), así como también, eventos de bajo impacto (por ejemplo, tasa de no cumplimiento, desviaciones)? [5.3.66 a 5.3.73; 5.4.5; 5.5.4; 5.5.5; Apéndice 6]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
3.1-6	¿Están los indicadores de rendimiento en materia de seguridad operacional y su configuración de rendimiento asociada desarrollados en función del acuerdo de la autoridad de aviación civil y sujetos a este? [5.3.66 a 5.3.73; 5.4.5.2; 5.5.4; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
3.1-7	¿Existe un procedimiento para una medida correctiva o de seguimiento que puede tomarse cuando no se logran los objetivos o se violan los niveles de alerta? [5.4.5; Apéndice 6, Tabla 5-A6-5 b)]	☐ Sí ☐ No ☐ Parcial	
3.1-8	¿Se revisan periódicamente los indicadores de rendimiento en materia de seguridad operacional? [5.4.5; Apéndice 6]	☐ Sí ☐ No ☐ Parcial	
Elemento 3.2 — La gestión de cambio			
3.2-1	¿Existe un procedimiento para la revisión de instalaciones y equipos existentes relacionados con la seguridad operacional de la aviación (incluidos los registros de HIRM) cada vez que haya cambios pertinentes a aquellas instalaciones y equipos? [5.3.74 a 5.3.77; 5.5.4]	☐ Sí ☐ No ☐ Parcial	
3.2-2	¿Existe un procedimiento para revisar las operaciones y los procesos existentes relacionados con la seguridad operacional de la aviación pertinentes (como cualquier registro de HIRM) cada vez que haya cambios a aquellas operaciones o procesos? [5.3.74 a 5.3.77; 5.5.4]	☐ Sí ☐ No ☐ Parcial	
3.2-3	¿Existe un procedimiento para revisar las nuevas operaciones y los procesos relacionados con la seguridad operacional de la aviación en busca de peligros/riesgos antes de implementarlos? [5.5.4]	☐ Sí ☐ No ☐ Parcial	
3.2-4	¿Existe un procedimiento para revisar las instalaciones, los equipos, las operaciones o los procesos existentes pertinentes (incluidos los registros de HIRM) cada vez que existan cambios pertinentes que sean externos a la organización, como normas reglamentarias/industriales, mejores prácticas o tecnología? [5.5.4]	☐ Sí ☐ No ☐ Parcial	
Elemento 3.3 — Mejora continua del SMS			
3.3-1	¿Existe un procedimiento para la evaluación/auditoría interna periódica del SMS? [5.3.78 a 5.3.82; 5.5.4; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
3.3-2	¿Existe un plan actual de la auditoría/evaluación de SMS interna? [5.3.78 a 5.3.82; 5.5.4; 5.5.5]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
3.3-3	¿Incluye la auditoría de SMS la toma de muestras de las evaluaciones existentes completadas/de riesgos de seguridad operacional? [5.5.5]	☐ Sí ☐ No ☐ Parcial	
3.3-4	¿Incluye el plan de auditoría del SMS la toma de muestras de los indicadores de rendimiento en materia de seguridad operacional para conocer la actualidad de los datos y el rendimiento de su configuración de objetivos/alertas? [5.4.5; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
3.3-5	¿Aborda el plan de auditoría de SMS la interfaz de SMS con los subcontratistas o clientes, donde corresponda? [5.4.1; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
3.3-6	¿Existe un proceso para que los informes de auditoría/evaluación de SMS puedan enviarse o destacarse para la atención del gerente responsable, cuando sea necesario? [5.3.80; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
Componente 4 — PROMOCIÓN DE LA SEGURIDAD OPERACIONAL			
Elemento 4.1 — Capacitación y educación			
4.1-1	¿Existe un programa para proporcionar la capacitación/familiarización de SMS al personal que participa en la implementación u operación del SMS? [5.3.86 a 5.3.91; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
4.1-2	¿Ha tomado el ejecutivo responsable un curso de familiarización, sesión informativa o capacitación de SMS adecuado? [5.3.86 a 5.3.91; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
4.1-3	¿Se brinda al personal que participa en la evaluación de riesgos capacitación o familiarización adecuadas de la gestión de riesgos? [5.3.86 a 5.3.91; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
4.1-4	¿Existe evidencia de esfuerzos de educación o toma de conciencia del SMS a nivel de la organización? [5.3.86 a 5.3.91; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
Elemento 4.2 — Comunicación de la seguridad operacional			
4.2-1	¿Participa [Organización] en la distribución de información de seguridad operacional a proveedores de productos y servicios u organizaciones industriales externos pertinentes, incluidas las organizaciones reglamentarias de aviación pertinentes? [5.3.92; 5.3.93; 5.5.5]	☐ Sí ☐ No ☐ Parcial	

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
4.2-2	¿Existe evidencia de una publicación, un circular o un canal de seguridad operacional (SMS) para comunicar la seguridad operacional y asuntos de SMS a los empleados? [5.3.92; 5.3.93; 5.5.5]	☐ Sí ☐ No ☐ Parcial	
4.2-3	¿Hay un manual de SMS de [Organización] y material guía relacionado accesible o distribuido a todo el personal pertinente? [5.3.92; 5.3.93; 5.5.5]	☐ Sí ☐ No ☐ Parcial	

2. ANÁLISIS DE BRECHAS DE SMS DETALLADO Y TAREAS DE IMPLEMENTACIÓN (TABLA 5-A7-2)

La lista de verificación del análisis de brechas inicial en la Tabla 5-A7-1 debe seguirse mediante el "plan de identificación del análisis de brechas y tarea de implementación del SMS" descrito en la Tabla 5-A7-2. Una vez completada, la Tabla 5-A7-2 debe proporcionar un análisis de seguimiento sobre los detalles de las brechas y ayudar a traducir esto en tareas y subtareas necesarias reales en el contexto específico de los procesos y procedimientos de la organización. Entonces, cada tarea se asignará en conformidad a las personas adecuadas o grupos de acción. Es importante que en la Tabla 5-A7-2 se proporcione la correlación del desarrollo del elemento/tarea individuales con sus apoderados descriptivos en el documento del SMS para activar la actualización progresiva del borrador de documento de SMS a medida que se implementa o mejora cada elemento. (Las críticas iniciales del elemento en los documentos del SMS tienden a ser anticipativas en lugar de ser declarativas).

3. PROGRAMA DE IMPLEMENTACIÓN DE MEDIDAS/TAREAS (TABLA 5-A7-3)

La Tabla 5-A7-3 mostrará los hitos (fechas de inicio y fin) programados para cada tarea/medida. Para un enfoque de implementación en etapas, estas tareas/acciones se deberán organizar de acuerdo con la asignación de la etapa de sus elementos relacionados. Véase la Sección 5.5 de este capítulo para la priorización en etapas de los elementos del SMS, como corresponda. La Tabla 5-A7-3 puede ser una consolidación por separado de todas las acciones/tareas pendientes o, si se prefiere, ser una continuación de la Tabla 5-A7-2 en la forma de una hoja de cálculo. Donde se anticipa que la cantidad real de tareas/medidas y sus hitos son lo suficientemente voluminosos y complejos como para requerir el uso de un software de gestión de proyectos para administrarlas, se puede hacer al usar un software como MS Project/diagrama Gantt, como corresponda. La Tabla 5-A7-4 es una ilustración de un diagrama Gantt.

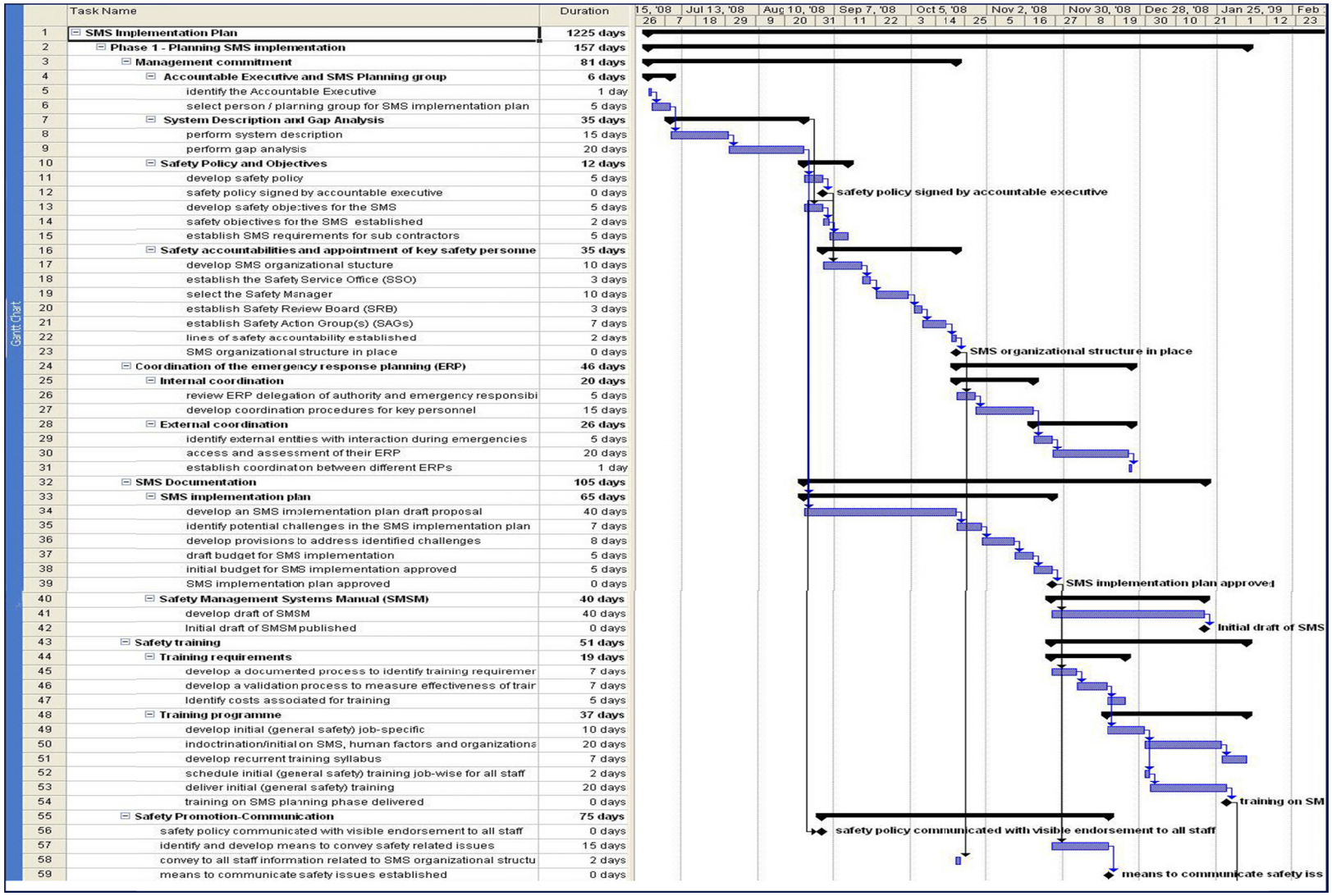
Tabla 5-A7-2. Ejemplo de un plan de identificación de análisis de brechas y tareas de implementación del SMS

Ref. de GAQ	*Pregunta del análisis de brechas*	*Respuesta (Sí/No/Parcial)*	*Descripción de la brecha*	*Medida/tarea necesaria para llenar la brecha*	*Grupo/persona de tarea asignada*	*Referencia del documento de SMS*	*Estado de la medida/tarea (abierta/WIP/cerrada)*
1.1-1	¿Está implementada una política de seguridad operacional?	Parcial	La política de seguridad operacional existente aborda solo OSHE.	a) mejorar la política de seguridad operacional existente para incluir objetivos y políticas de SMS de la aviación o desarrollar una política de seguridad operacional de aviación por separado; b) solicitar que el ejecutivo responsable apruebe y firme la política de seguridad operacional.	Tarea Grupo 1	Capítulo 1, Sección 1.3.	Abierto
etc.							

Tabla 5-A7-3. Ejemplo de un programa de implementación de SMS

Medida/tarea necesaria para llenar la brecha	*Ref. del documento de SMS*	*Grupo de tarea/ persona asignada*	*Estado de la medida /tarea*	*Programa/cronología*												
				1Q 10	*2Q 10*	*3Q 10*	*4Q 10*	*1Q 11*	*2Q 11*	*3Q 11*	*4Q 11*	*1Q 12*	*2Q 12*	*3Q 12*	*4Q 12*	*etc.*
1.1-1 a) Mejorar la política de seguridad operacional existente para incluir objetivos y políticas de SMS de la aviación o desarrollar una política de seguridad operacional de aviación por separado.	Capítulo 1, Sección 1.3.	Grupo de tareas 1	Abierto													
1.1-1 b) Requerir que el ejecutivo responsable apruebe y firme la política de seguridad operacional.																
etc.																

Tabla 5-A7-4. Programa de implementación de SMS de muestra (diagrama Gantt)



Adjunto

TEXTOS DE ORIENTACIÓN CONEXOS DE LA OACI

MANUALES

Manual sobre sistemas avanzados de guía y control de movimientos en la superficie (A-SMGCS)(Doc 9830)

Manual de servicios de aeropuertos (Doc 9137)
Parte 1 — *Salvamento y extinción de incendios*
Parte 5 — *Traslado de las aeronaves inutilizadas*
Parte 7 — *Planificación de emergencia en los aeropuertos*

Manual de aeronavegabilidad (Doc 9760)

Plan mundial de navegación aérea (Doc 9750)

Concepto operacional de gestión del tránsito aéreo mundial (Doc 9854)

Directrices sobre factores humanos para los sistemas de gestión del tránsito aéreo (ATM) (Doc 9758)

Directrices sobre factores humanos en el mantenimiento de aeronaves (Doc 9824)

Directrices sobre factores humanos en las auditorías de la seguridad operacional (Doc 9806)

Manual de instrucción sobre factores humanos (Doc 9683)

Auditoría de la seguridad de las operaciones de línea aérea (LOSA) (Doc 9803)

Manual sobre la interceptación de aeronaves civiles (Doc 9433)

Manual sobre las medidas de seguridad relativas a las actividades militares potencialmente peligrosas para las operaciones de aeronaves civiles (Doc 9554)

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 de operaciones de deshielo/antihielo de la aeronave inmovilizada en tierra (Doc 9640)

Manual de operaciones todo tiempo (Doc 9365)

Manual de medicina aeronáutica civil (Doc 8984)

*Manual de procedimientos para la inspección, certificación y supervisión permanente de las operaciones (*Doc 8335)

Manual de radiotelefonía (Doc 9432)

Manual de sistemas de guía y control del movimiento en la superficie (SMGCS) (Doc 9476)

Manual sobre requisitos del sistema de gestión del tránsito aéreo (Doc 9882)

Manual sobre la metodología de planificación del espacio aéreo para determinar las mínimas de separación (Doc 9689)

Manual de certificación de aeródromos (Doc 9774)

Manual sobre la actuación mundial del sistema de navegación aérea (Doc 9883)

Manual sobre una separación vertical mínima de 300 m (1 000 ft) entre FL 290 y FL 410 inclusive (Doc 9574)

Manual sobre organizaciones regionales de investigación de accidentes e incidentes (Doc 9946)

Manual sobre performance de comunicación requerida (RCP) (Doc 9869)

Manual sobre operaciones simultáneas en pistas de vuelo por instrumentos paralelas o casi paralelas (SOIR) (Doc 9643)

Manual sobre la prevención de incursiones en la pista (Doc 9870)

Manual del sistema de gestión de la calidad para el suministro de servicios meteorológicos para la navegación aérea internacional (Doc 9873)

Estudio de la seguridad de las operaciones normales (NOSS) (Doc 9910)

Manual sobre la navegación basada en la performance (PBN) (Doc 9613)

Manual de vigilancia de la seguridad operacional (Doc 9734)

Manual sobre la observación continua del Programa universal de auditoría de la vigilancia de la seguridad operacional (Doc 9735)

CIRCULARES

Marco unificado para modelos de riesgo de colisión en apoyo del Manual sobre la metodología de planificación del espacio aéreo para determinar las mínimas de separación (Doc 9689) (Cir 319)

Evaluación de la vigilancia ADS-B y la vigilancia por multilateración en apoyo de los servicios de tránsito aéreo y las directrices de implantación (Cir 326)

Orientación sobre asistencia a las víctimas de accidentes de aviación y sus familiares (Cir 285)

Riesgos en los lugares de accidentes de aviación (Cir 315)

Compendio sobre factores humanos núm. 15 — Factores humanos y seguridad operacional en la cabina (Cir 300)

Compendio sobre factores humanos núm. 16 — Los factores transculturales en la seguridad aeronáutica (Cir 302)

Manejo de amenazas y errores (TEM) en el control de tránsito aéreo (Cir 314)

Operación de nuevos aeroplanos de mayor tamaño en los aeródromos existentes (Cir 305)

Guía de instrucción para investigadores de accidentes de aviación (Cir 298)

— FIN —

ISBN 978-92-9249-315-8