GUÍA PARA DESARROLLAR UN MANUAL SMS PARA LOS PROVEEDORES DE SERVICIOS DE NAVEGACIÓN AÉREA

SRVSOP

Un manual SMS es parte fundamental de la documentación SMS que debe tener disponible cualquier proveedor de servicios.

El propósito de este documento es proporcionar una guía para apoyar especialmente a los Proveedores de Servicios de Navegación Aérea (ANSP) en la implantación de un Manual del Sistema de Gestión de la Seguridad Operacional (SMS).

Esta guía tiene en cuenta los conceptos del SMS y el desarrollo de políticas de gestión y procesos para implementar y mantener un SMS efectivo.

Primera Edición
Diciembre 2019
Enmienda 2

INDICE

ENMIENDAS

Registro de Enmiendas			
Enmienda N°	**Fecha de aplicación**	**Fecha de anotación**	**Anotado por:**
1ra. Edición	18/12/2018	18/12/2018	Comité Técnico
Enmienda 1	12/04/2019	12/04/2019	Comité Técnico
Enmienda 2	29/11/2019	01/12/2019	Comité Técnico

GLOSARIO

ABREVIATURAS Y ACRÓNIMOS

ADREP	Notificación de datos sobre accidentes/incidentes (OACI)
ALoSP	Nivel aceptable del rendimiento en materia de seguridad operacional
ANSP	Proveedor de Servicios de navegación aérea
ASB	Boletín de servicio de alerta
ATC	Control de tránsito aéreo
ATM	Gestión del tránsito aéreo
ATS	Servicios de tránsito aéreo
ATSP	Proveedor de servicios de tránsito Aéreo
AAC	Autoridad de aviación civil
CNS	Comunicaciones, navegación y vigilancia
EMC	Centro de gestión de emergencia
EMS	Sistema de gestión ambiental
ERP	Plan de respuesta ante emergencias
SARPS	Normas y métodos recomendados (OACI)
SDCPS	Sistema de recopilación y procesamiento de datos sobre seguridad operacional
SMM	Manual de 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
SPT	Meta de rendimiento en materia de seguridad operacional
USOAP	Programa universal de auditoría de la vigilancia de la seguridad operacional

DEFINICIONES

Accidente. *Todo suceso relacionado con la utilización de una aeronave, que, en el caso de una aeronave tripulada, ocurre entre el momento en que una persona entra a bordo de la aeronave, con la intención de realizar un vuelo, y el momento en que todas las personas han desembarcado, o en el caso de una aeronave no tripulada, que ocurre entre el momento en que la aeronave está lista para desplazarse con el propósito de realizar un vuelo y el momento en que se detiene, al finalizar el vuelo, y se apaga su sistema de propulsión principal, durante el cual:*

a) cualquier persona sufre lesiones mortales o graves a consecuencia de:

— hallarse en la aeronave, o
— por contacto directo con cualquier parte de la aeronave, incluso las partes que se hayan desprendido de la aeronave, o
— por exposición directa al chorro de un reactor,

excepto cuando las lesiones obedezcan a causas naturales, se las haya causado una persona a sí misma o hayan sido causadas por otras personas o se trate de lesiones sufridas por pasajeros clandestinos escondidos fuera de las áreas destinadas normalmente a los pasajeros y la tripulación; o

b) la aeronave sufre daños o roturas estructurales que:

— afectan adversamente su resistencia estructural, su performance o sus características de vuelo; y
— que normalmente exigen una reparación importante o el recambio del componente afectado,

excepto por falla o daños del motor, cuando el daño se limita a un solo motor (incluido su capó o sus accesorios); hélices, extremos de ala, antenas, sondas, álabes, neumáticos, frenos, ruedas, carenas, paneles, puertas de tren de aterrizaje, parabrisas, revestimiento de la aeronave (como pequeñas abolladuras o perforaciones), o por daños menores a palas del rotor principal, palas del rotor compensador, tren de aterrizaje y a los que resulten de granizo o choques con aves (incluyendo perforaciones en el radomo); o

c) la aeronave desaparece o es totalmente inaccesible.

Nota 1. — Para uniformidad estadística únicamente, toda lesión que ocasione la muerte dentro de los 30 días contados a partir de la fecha en que ocurrió el accidente, está clasificada por la OACI como lesión mortal.
Nota 2. — Una aeronave se considera desaparecida cuando se da por terminada la búsqueda oficial y no se han localizado los restos.
Nota 3. — El tipo de sistema de aeronave no tripulada que se investigará se trata en 5.1 del Anexo 13.
Nota 4. — En el Adjunto E del Anexo 13 figura orientación para determinar los daños de aeronave.

Análisis de la seguridad operacional. *El análisis de la seguridad operacional es el proceso de aplicar técnicas estadísticas o analíticas de otro tipo para verificar, examinar, describir, transformar, condensar, evaluar y visualizar los datos y la información sobre seguridad operacional a efectos de descubrir información útil, sugerir conclusiones y apoyar la toma de decisiones basada en datos.*

Datos sobre seguridad operacional. *Conjunto de hechos definidos o conjunto de valores de seguridad operacional recopilados de diversas fuentes de aviación, que se utiliza para mantener o mejorar la seguridad operacional.*

Nota.— Dichos datos sobre seguridad operacional se recopilan a través de actividades preventivas o reactivas relacionadas con la seguridad operacional, incluyendo, entre otros, lo siguiente:

a) investigaciones de accidentes o incidentes;
b) notificaciones de seguridad operacional;
c) notificaciones sobre el mantenimiento de la aeronavegabilidad;
d) supervisión de la eficiencia operacional;
e) inspecciones, auditorías, constataciones; o
f) estudios y exámenes de seguridad operacional.

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

Director Ejecutivo. *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.*

Estudios de seguridad operacional. *Estudios de carácter cultural para proporcionar información útil respecto de la participación del personal en el SMS. También puede servir de indicador de la cultura de seguridad operacional de la organización.*

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.*

Incidente. *Todo suceso relacionado con la utilización de una aeronave, que no llegue a ser un accidente, que afecte o pueda afectar la seguridad de las operaciones.*

Nota. — Entre los tipos de incidentes que son de interés para los estudios relacionados con la seguridad operacional figuran los incidentes enumerados en el Anexo 13, Adjunto C.

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

Información sobre seguridad operacional. *Datos sobre seguridad operacional procesados, organizados o analizados en un determinado contexto a fin de que sean de utilidad para fines de gestión de la seguridad operacional.*

Meta de rendimiento en materia de seguridad operacional (SPT). *La meta proyectada o prevista del Estado o proveedor de servicios que se desea conseguir, en cuanto a un indicador de rendimiento en materia de seguridad operacional, en un período de tiempo determinado que coincide con los objetivos de seguridad operacional.*

Mitigación de riesgos. *Proceso de incorporación de defensas 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.*

Peligro*. Condición u objeto que entraña la posibilidad de causar un incidente o accidente de aviación o contribuir al mismo.*

Ocurrencia. *Un suceso de seguridad operacional.*

Programa estatal de seguridad operacional (SSP). *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.*

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

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

Suceso de seguridad operacional. *Es un término usado para abarcar todos los eventos que tienen o podrían tener importancia en el contexto de seguridad operacional, que van desde accidentes y accidentes graves, incidentes o eventos que deben notificarse, a casos de menor gravedad que, en la opinión de quien reporta el suceso, podría tener importancia para la seguridad operacional.*

Supervisión de la seguridad operacional. *Función desempeñada por los Estados para garantizar que las personas y las organizaciones que llevan a cabo una actividad aeronáutica cumplan las leyes y reglamentos nacionales relacionados con la seguridad operacional.*

Vigilancia. *Actividades estatales mediante las cuales el Estado verifica, de manera preventiva, con inspecciones y auditorías, que los titulares de licencias, certificados, autorizaciones o aprobaciones en el ámbito de la aviación sigan cumpliendo los requisitos y la función establecidos, al nivel de competencia y seguridad operacional que el Estado requiere.*

INTRODUCCIÓN

La implantación de un SMS tiene como objetivo proporcionar a los proveedores de servicios un enfoque sistemático para la gestión de la seguridad operacional. Este enfoque está diseñado para mejorar continuamente el rendimiento en seguridad operacional a través de: la identificación de peligros, la recopilación y análisis de datos e información de seguridad operacional y la evaluación continua de riesgos de seguridad operacional. El SMS busca, a través de un enfoque proactivo, mitigar los riesgos de seguridad operacional antes de que los mismos deriven en incidentes y/o accidentes de aviación.

Como todo sistema de gestión, el SMS establece metas, planificación y medición del rendimiento. Un sistema de gestión de seguridad operacional eficiente es el mejor soporte estructural de una organización y va más allá del cumplimiento de las normas prescriptivas. Esta gestión apunta a un enfoque sistemático donde los riesgos de seguridad potenciales se identifican y se gestionan para lograr un nivel aceptable de riesgo.

Es necesario enfatizar que el compromiso y liderazgo en la gestión de seguridad operacional es clave para la implementación de un SMS efectivo y se afirma a través de una política de seguridad operacional y el establecimiento de objetivos.

Ese compromiso con la seguridad operacional se demuestra a través de la toma de decisiones de gestión y asignación de recursos. Estas acciones y decisiones siempre deben ser coherentes con la política de seguridad operacional y los objetivos para fomentar una cultura de seguridad positiva.

Por su significancia, la seguridad operacional es una responsabilidad ineludible y necesariamente compartida a través de toda la organización y la participación de todo el personal en los procesos de seguridad operacional es clave para el éxito.

La aspiración es que el SMS sea un enfoque proactivo e integrado para la gestión de seguridad y para ello, se necesita establecer las necesarias estructuras de organización y definir las responsabilidades, las políticas, los procesos y los procedimientos.

Para ayudar a esa integración, se debe desarrollar y fomentar una cultura organizacional que refleje la política de seguridad operacional y los objetivos de cada organización. El SMS no es un sistema modelo que se ajusta perfectamente igual a todo tipo de organizaciones. Las organizaciones deben adaptar sus SMS para adecuarse al tamaño, naturaleza y complejidad de sus operaciones y/o productos, así como a los peligros y riesgos inherentes a sus actividades.

En el corazón del SMS está el proceso formal de la gestión del riesgo que identifica peligros, evalúa y mitiga el riesgo. Es importante reconocer que incluso con medidas

mitigatorias u controles implantados, seguirá existiendo un riesgo residual y solamente un SMS eficiente y eficaz permitirá a las organizaciones a gestionar este riesgo residual.

También se deben tener en cuenta los riesgos generados por las actividades contratadas a terceros. En esos casos, la cultura SMS puede tener que extenderse más allá de la propia organización en el análisis de riesgos. Por lo tanto, cuando la organización tiene un acuerdo formal con otra organización deberá incluir disposiciones para la gestión de la seguridad operacional. Esto también debe incluir el reporte de procedimientos de seguridad operacional relacionados con el objeto del contrato.

Finalmente, no se puede obviar la importancia que significa la capacitación del personal para ser eficiente y eficaz en el cumplimiento de las obligaciones de la vigilancia de la seguridad operacional y para poder identificar y analizar los peligros y evaluar y controlar los riesgos a la seguridad operacional.

Este Manual se fundamenta en el marco para la implantación y el mantenimiento de un SMS. El mismo consta de cuatro componentes y doce elementos que constituyen los requisitos mínimos para la implantación de un SMS:

1. Política y objetivos de seguridad operacional
   - Compromiso de la dirección
   - Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional
   - Designación del personal clave de seguridad operacional
   - Coordinación de la planificación de respuestas ante emergencias
   - Documentación SMS
2. Gestión de riesgos de seguridad operacional
   - Identificación de peligros
   - Evaluación y mitigación de riesgos de seguridad operacional
3. Aseguramiento de la seguridad operacional
   - Observación y medición del rendimiento en materia de seguridad operacional
   - Gestión del cambio
   - Mejora continua del SMS
4. Promoción de la seguridad operacional
   - Instrucción y educación
   - Comunicación de la seguridad operacional

PROPÓSITO

Un Manual SMS es parte fundamental de la documentación SMS que debe tener disponible cualquier organización prestadora de servicios a la navegación aérea y está basada en el Anexo 19 de la OACI Gestión de la Seguridad Operacional y en el Doc 9859 de la OACI Manual de Gestión de la Seguridad Operacional (SMM).

El propósito de este documento es proporcionar una guía para apoyar a los Proveedores de Servicios de Navegación Aérea (ANSP) en el desarrollo de un Manual para la gestión de la seguridad operacional (SMS) en sus organizaciones. Esta guía se enfoca en los conceptos del SMS y el desarrollo de políticas de gestión y procesos para implementar y mantener un SMS eficiente y eficaz.

APLICACIÓN

Esta guía no pretende ser exhaustiva, pero puede ser utilizada como base para el desarrollo del Manual SMS en cualquiera de las organizaciones proveedoras de servicios de navegación aérea adaptándola a sus características particulares y al tamaño de su organización.

1. DOCUMENTACIÓN DEL SMS

1.1 Entre la documentación SMS que debe tener una organización se debe incluir un Manual SMS de alto nivel, que describa las políticas SMS, los procesos y los procedimientos del proveedor de servicios para facilitar la administración interna de la organización, comunicación y mantenimiento de los SMS.

1.2 Este Manual apunta a ayudar al personal a entender de qué manera se llevarán a cabo las funciones SMS de la organización y cómo se cumplirá con la política de seguridad operacional y los objetivos.

1.3 La documentación debe incluir una descripción del sistema indicando los límites de los SMS. También debe ayudar a aclarar la relación entre las diferentes políticas, procesos, procedimientos y prácticas y definir cómo éstos se vinculan a los objetivos y la política de seguridad operacional del proveedor de servicios. La documentación debe ser adaptada y escrita para la dirección de las actividades de

gestión de la seguridad operacional que tienen que ser fácilmente entendidas por todo el personal de la organización.

1.4 El Manual SMS sirve también como una herramienta principal de comunicación de seguridad entre el proveedor y otros actores claves en la seguridad (por ej.: la AAC con el propósito de aceptación en términos reglamentarios, la evaluación y el seguimiento posterior de los SMS).

1.5 El Manual SMS puede ser un documento independiente o puede integrarse con otros documentos organizacionales (o documentación) del proveedor de servicios. En el caso de que la información de los procesos de la organización SMS ya se encuentre detallada en documentos existentes la referencia cruzada apropiada para tales documentos es suficiente.

1.6 Es recomendable que el Manual SMS haga referencia a la documentación sobre la preparación, recopilación y mantenimiento de registros operacionales que acreditan la implantación y operación efectiva del SMS.

1.7 Los registros operacionales son el resultado de los procesos SMS y de procedimientos tales como las actividades de aseguramiento de la seguridad operacional y la Gestión de Seguridad del Riesgo (SRM). Estos registros operacionales SMS deben ser almacenados y mantenidos conforme a los períodos de retención establecidos. Los registros operacionales típicos del SMS deben incluir:

a) registros de peligros e informes de seguridad sobre peligros;
b) indicadores de rendimiento de seguridad (SPIs) y cuadros de análisis de riesgo relacionados;
c) registros de valoraciones de seguridad del riesgo finalizadas;
d) revisión interna SMS o registros de auditorías;
e) registros de auditorías internas;
f) registros de los registros de capacitación en seguridad/SMS;
g) actas de las reuniones del comité de seguridad/SMS;
h) plan de Implantación SMS (durante la implantación inicial); y
i) análisis del faltante (“gap analysis”) para apoyar el plan de implantación;
j) informes de accidentes/ incidentes de aviación.

1.8 Este Manual, así como cualquier documento existente SMS debe mantenerse al día. Como parte del proceso de actualización, debe tenerse presente que antes de realizar modificaciones significativas en el Manual SMS, es necesario un acuerdo con la AAC ya que este es un manual de control.

2. ¿QUÉ DEBE INCLUIR EL MANUAL SMS?

2.1 El Manual SMS debe incluir una descripción detallada de los servicios prestados por el proveedor, las políticas, procesos y procedimientos incluyendo:

a) la política y los objetivos de seguridad operacional;
b) las referencias a cualquier requerimiento SMS regulatorio aplicable;
c) una descripción del sistema;
d) la obligación de rendición de cuentas y personal clave de seguridad operacional;
e) la planificación para la coordinación de las respuestas a las emergencias (si es aplicable);
f) los procesos y procedimientos para la identificación de peligros y para la evaluación y mitigación de riesgos de seguridad operacional;
g) los procesos y procedimientos del sistema de reporte de seguridad operacional voluntario y mandatorio;
h) los procedimientos para las investigaciones de seguridad operacional;
i) los procedimientos para el establecimiento y monitoreo de los indicadores de rendimiento del sistema;
j) los procesos, procedimientos y comunicación para capacitación en SMS;
k) los procesos y procedimientos de comunicación de seguridad operacional;
l) los procedimientos de auditoria interna;
m) los procedimientos de gestión del cambio; y
n) los procedimientos para la gestión de la documentación SMS.

2.2 El proveedor de servicios preparará, recopilará y mantendrá registros operacionales de SMS como parte de su documentación SMS.

3. REFERENCIAS A LA NORMATIVA SMS APLICABLE

3.1 En esta parte del Manual se describirán las referencias normativas internacionales, la legislación básica nacional y reglamentos, circulares, guías de orientación nacionales, y todo documento que refiera a la aplicación e implantación de los sistemas de gestión para la seguridad operacional (SMS) del proveedor de servicios.

4. POLÍTICA DE LA SEGURIDAD OPERACIONAL Y OBJETIVOS

4.1 La política de seguridad operacional y objetivos es el primer componente de un Sistema de Gestión de la Seguridad (SMS). Los cinco elementos que lo integran son:

a) compromiso de la dirección;
b) obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional;
c) designación del personal clave de seguridad operacional;
d) coordinación de la planificación de respuestas ante emergencias; y
e) documentación SMS.

4.1.1 Compromiso de la dirección

4.1.1.1 El proveedor de servicios tiene que definir cuál será su política de seguridad operacional de conformidad con los requisitos nacionales e internacionales vigentes.

4.1.1.2 Esta política de seguridad operacional debe reflejar un compromiso organizacional en el cual también se deberá incluir el fomento de una cultura positiva de seguridad operacional y también debe declararse cuales son los recursos necesarios que se destinarán para su puesta en práctica.

4.1.1.3 Como parte del compromiso se deberá establecer un procedimiento explicando los procesos a seguir para presentar los informes en materia de seguridad.

4.1.1.4 Asimismo, se deberá indicar claramente qué tipos de comportamientos son inaceptables en lo que respecta a las actividades que realiza el proveedor de servicios y también deberá incluir las circunstancias en las que no se podrán aplicar medidas disciplinarias apuntando a una cultura justa y de protección de los empleados.

4.1.15 En el caso de proveedores de servicio de navegación aérea que estén dentro del marco de la administración pública del Estado se puede hacer referencia a Leyes y Decretos de carácter laboral u otros documentos que establecen las normas de conducta, ética y cumplimiento administrativo para funcionarios de la administración.

4.1.1.6 La declaración de la política y el compromiso asumido debe estar escrita y firmada por el directivo responsable de la organización. Se comunicará con apoyo ostensible y será difundida a toda la organización.

4.1.1.7 Esta declaración de la política y los compromisos asumidos se examinarán periódicamente para asegurarse de que la misma siga siendo pertinente y apropiada y debe reflejarse íntegramente en esta parte del Manual SMS.

4.1.2 Obligación de rendición de cuentas y responsabilidades

Director Ejecutivo

4.1.2.2 El Director Ejecutivo del proveedor de servicios debe ser nombrado e identificado en el Manual SMS. Es la persona que tiene autoridad definitiva sobre la operación segura de la organización. Establece y promueve la política y objetivos de seguridad operacional y debe inculcar la seguridad operacional como un valor organizacional de base.

4.1.2.3 El Director ejecutivo independientemente de otras funciones que realice, tiene la obligación de rendir cuentas en nombre de la organización con respecto de la implantación y el mantenimiento de un SMS eficaz y esto debe estar establecido en la descripción de sus deberes y responsabilidades.

***Nota 1**: A los efectos de este Manual, el concepto de "obligación de rendición de cuentas" se refiere a una "obligación" que no puede delegarse, y "responsabilidades" se refiere a las funciones y actividades que pueden delegarse.*

4.1.2.3 Es absolutamente imprescindible que el Director Ejecutivo tenga la autoridad en materia de seguridad operacional, para tomar decisiones en nombre de la organización, tenga el control de los recursos tanto financieros como humanos, sea responsable de las acciones apropiadas que se tomen para abordar temas de seguridad operacional y los riesgos de seguridad operacional, y sea responsable para responder a accidentes e incidentes.

***Nota 2:** No es una tarea fácil para el proveedor de servicios identificar a la persona más adecuada para ser el Director Ejecutivo, especialmente en grandes organizaciones complejas con varias entidades y varios certificados, autorizaciones o aprobaciones. Es importante que la persona seleccionada se encuentre organizacionalmente al más alto nivel de la organización, garantizando así que se toman las correctas decisiones estratégicas en materia de seguridad operacional.*

4.1.2.4 El Director Ejecutivo define las responsabilidades específicas de seguridad operacional de todos los miembros de la gestión y su papel en relación con el servicio SMS deberá reflejar cómo ellos pueden contribuir a una cultura de seguridad positiva. Las responsabilidades de seguridad operacional, las obligaciones de rendición de cuentas y las autoridades deben ser documentadas y comunicadas a toda la organización. Las responsabilidades de seguridad de los gerentes deben incluir la asignación de los recursos humanos, técnicos o financieros necesarios para el rendimiento eficaz y eficiente del servicio SMS.

4.1.2.5 Cuando se aplica un SMS a varios y distintos certificados, autorizaciones o aprobaciones que son parte de la misma entidad jurídica, debe haber un solo director ejecutivo. Cuando esto no sea posible, los diferentes ejecutivos responsables deben ser

identificados para cada certificado de la organización, autorización o aprobación y las líneas claras responsabilidad y coordinación deben estar claramente definidas.

4.1.2.6 Una forma efectiva en la que el Director Ejecutivo puede estar visiblemente involucrado, es en el liderazgo de reuniones ejecutivas periódicas de seguridad operacional. Participar activamente en estas reuniones permite que el Director Ejecutivo:

a) revise los objetivos de seguridad operacional;

b) supervise los rendimientos de seguridad operacional y los logros en los objetivos de seguridad operacional establecidos;

c) tome decisiones de seguridad operacional a tiempo;

d) asigne los recursos apropiados;

e) pedir cuentas a los respectivos jefes por sus responsabilidades por seguridad operacional, rendimiento y fechas de implantación; y

f) ser visualizado por todo el personal como un ejecutivo a cargo y comprometido con la seguridad operacional.

4.1.2.7 El Director Ejecutivo no está generalmente implicado en las actividades diarias de la organización o los problemas que a diario se enfrentan en el trabajo y por lo tanto se debe asegurar que existe una estructura organizacional adecuada para administrar y operar el SMS. La responsabilidad de la gestión de la seguridad operacional a menudo se delega en el equipo de alta gerencia y otro personal clave de seguridad operacional.

4.1.2.8 Aunque puede delegarse la responsabilidad de la operación diaria del servicio SMS, el Director Ejecutivo no puede delegar la rendición de cuentas para el SMS ni puede delegar las decisiones sobre los riesgos de seguridad operacional. Por ejemplo, no se puede delegar la rendición de cuentas de seguridad operacional siguientes:

a) garantizar que las políticas de la seguridad operacional sean apropiadas y eficientemente comunicadas;

b) garantizar recursos necesarios (financieros, personal, capacitación, compras); y

c) garantizar los límites de riesgo de seguridad operacional aceptables y los recursos para los controles necesarios.

4.1.2.9 El Director Ejecutivo debe ser responsable de:

a) proveer suficiente financiamiento y recursos humanos para la apropiada implantación de un eficiente y eficaz SMS;

b) promover una cultura de seguridad operacional positiva;

c) establecer y promover una política de seguridad operacional;

d) establecer los objetivos de seguridad operacional de la organización;

e) garantizar que el SMS es apropiadamente implantado y está de acuerdo con los requerimientos y necesidades; y

f) supervisar la mejora continua del SMS.

4.1.2.10 La responsabilidad del Director Ejecutivo también incluye la toma de decisión final en:

a) resolución sobre asuntos de seguridad operacional; y

b) operaciones bajo certificado, autorización o aprobación de la organización, incluyendo la cancelación de operaciones o actividades.

4.1.2.11 Un asunto importante que debe definirse es la autoridad para tomar decisiones respecto a la tolerabilidad del riesgo de seguridad operacional. Esto incluye el que puedan tomar decisiones sobre la aceptabilidad de los riesgos, así como la autoridad a aceptar que el cambio puede ser implantado. La autoridad puede asignarse a un individuo, una posición de administración o un Comité.

4.1.2.12 La autoridad para tomar decisiones de tolerancia de riesgo de seguridad debe ser acorde con la toma de decisiones generales del Director Ejecutivo que tiene la autoridad para asignar los recursos. Un gerente de nivel inferior (o grupo de gestión) puede ser autorizado a tomar decisiones de tolerancia hasta un cierto nivel, pero cuando los niveles de riesgo considerados exceden la autoridad del gerente del nivel inferior los mismos deben ser comunicados para consideración a un nivel superior de gestión con mayor autoridad. Estos diferentes niveles de toma de decisión deben establecerse claramente.

4.1.2.13 La obligación de rendir cuentas y las responsabilidades de todo el personal (administración y personal) en tareas relacionadas con la seguridad operacional tanto en la entrega de productos seguros como en la realización de las operaciones propias de la organización deben estar claramente establecidas. Las responsabilidades de seguridad operacional deben centrarse en la contribución del funcionario para el buen rendimiento de la seguridad operacional de la organización (los resultados de la organización en materia de seguridad operacional).

4.1.2.14 Todas las obligaciones, responsabilidades y autoridad deben ser definidas en la documentación SMS del proveedor de servicios y comunicadas a toda la organización. Las obligaciones y responsabilidades de seguridad de cada gerente son componentes integrales de la descripción de su trabajo. Asimismo, deben ser establecidas las diferentes funciones de los diferentes gerentes de línea y el gerente de seguridad.

4.1.2.15 El proveedor de servicios debe procurar evitar conflictos de intereses entre las responsabilidades de seguridad de los miembros del personal y otras responsabilidades de su organización. Deben asignarse las obligaciones de rendir

cuentas SMS y responsabilidades, de forma de reducir al mínimo cualquier superposición o vacíos.

4.1.3 Rendición de cuentas y responsabilidades en relación a organizaciones externas.

4.1.3.1 Un proveedor de servicios es responsable de la seguridad operacional con respecto a su posible impacto desde organismos externos donde se encuentra una interfaz SMS. El proveedor de servicios puede tener que rendir cuentas sobre el funcionamiento de la seguridad operacional de los productos o servicios proporcionados por organizaciones externas, en apoyo a sus actividades, incluso si las organizaciones externas no cuentan con un SMS.

4.1.3.2 Tomando en cuenta lo anterior, es esencial para el SMS del proveedor del servicio establecer una interfaz con los sistemas de seguridad operacional de las organizaciones externas que contribuyen con productos o servicios a sus actividades. De ahí la importancia que tiene que la organización proveedora de servicios efectúe una descripción del sistema lo más detallada posible.

5. DESCRIPCIÓN DEL SISTEMA

5.1 Cuando se considera una descripción del sistema, es importante entender que un "sistema" es un conjunto de cosas trabajando juntas como partes de una red de interconexión. En un SMS, es cualquiera de los productos de la organización, personas, procesos, procedimientos, instalaciones, servicios y otros aspectos (incluyendo factores externos), que están relacionadas con y pueden afectar a las actividades de seguridad operacional de la organización.

5.2 Una descripción del sistema ayuda a identificar los procesos de la organización, así como las interfases necesarias que se deben analizar para definir el alcance del SMS.

5.3 En el desarrollo de esta descripción del sistema se pueden identificar subsistemas. Estos sistemas y subsistemas tienen muchas interacciones que componen fuentes de riesgos y contribuyen a la gestión de los riesgos de seguridad operacional.

5.4 Algunas de las interfases internas pueden parecer, a primera vista, que no están muy relacionadas con la seguridad operacional, al menos directamente, sin embargo algunas decisiones de áreas como la de marketing, finanzas, jurídica o de recursos humanos, por nombrar algunas, pueden impactar internamente la seguridad operacional sobre inversiones, recursos humanos o con acuerdos o contratos con otras

organizaciones que no necesariamente aplican procesos de seguridad operacional en sus actividades, procesos o en sus productos.

5.5 Debajo en la **Figura 1** se visualiza un ejemplo de cómo un proveedor de servicios ATS podría mapear las distintas organizaciones con las cuales interactúa e identificar cualquier interfaz SMS. El objetivo de este mapeo es producir una lista completa de todas las interfases.

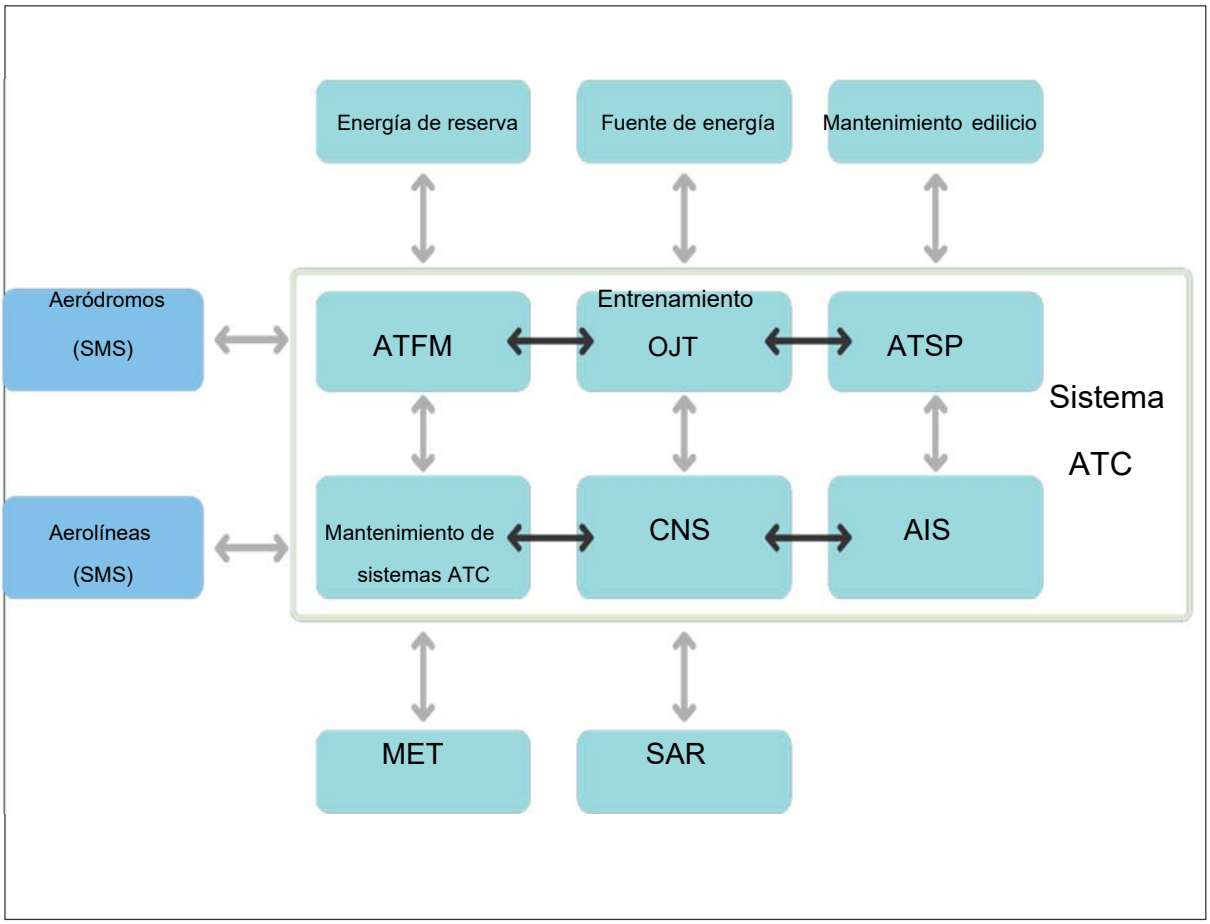

Figura 1: Ejemplo de las interfases SMS del Proveedor de Servicios de Tránsito Aéreo

5.6 La razón fundamental de este ejercicio es que puede que existan interfases SMS de las cuales una organización no sea totalmente consciente. También pueden existir interfases con las cuales no hay acuerdos formales, por ejemplo, una empresa responsable de la fuente de alimentación o una empresa de mantenimiento edilicio.

5.7 Una vez que se han identificado las interfases SMS, el proveedor del servicio debe considerar su importancia relativa. Esto permite al proveedor de servicios dar prioridad a la gestión de las interfases más importantes y sus potenciales riesgos de seguridad. Es apropiado considerar:

a) **Qué** se provee;

b) **Por qué** es necesario;

c) **Tiene un SMS** u otro Sistema de gestión implantado la organización proveedora?; y

d) **La interfase** contempla la compartición de datos de seguridad operacional/ información.

5.8 El proveedor del servicio al analizar las interfases con las otras organizaciones o sistemas, debe identificar cualquier peligro relacionado con las mismas y llevar la gestión para la identificación de peligros y evaluación de riesgo de la seguridad operacional.

5.9 Una descripción del sistema puede incluir una lista con viñetas con referencias a las políticas y procedimientos. Una representación gráfica como un diagrama de flujo de proceso u organigrama anotado, puede ser suficiente para algunas organizaciones. Puede incluso que algunas organizaciones tengan ya establecido un formato utilizable para este tipo de descripción.

5.10 Es necesario detallar las estructuras organizativas, los procesos y los acuerdos que sean importantes para las funciones de gestión de seguridad operacional. Puede ser que, al describir el sistema, la organización identifique la necesidad de desarrollar políticas, procesos y/o procedimientos para establecer requisitos adicionales para mejorar la gestión de la seguridad operacional.

5.11 Asimismo, cuando una organización elige hacer un cambio significativo o sustancial en los procesos identificados en la descripción del sistema, los cambios pueden potencialmente afectar a su línea de base de evaluación de riesgos de seguridad operacional. Por lo tanto, la descripción del sistema también debe ser revisada como parte de la gestión cuando se desarrollan procesos de cambio.

5.12 Todos los problemas de seguridad o los riesgos de seguridad relacionados con las interfases deben ser documentados y accesibles a cada organización para ser compartidos y revisados. Esto posibilita el intercambio de lecciones aprendidas y la compartición de datos de seguridad operacional que serán valiosos para ambas organizaciones.

5.13 La descripción de su organización y las funciones prestadas para cumplir con los compromisos organizacionales con la seguridad operacional, el proveedor de servicios puede también identificar más fácilmente los puntos de la estructura organizativa donde el personal asignado cumple funciones claves para alcanzar los objetivos de seguridad operacional establecidos.

6. PERSONAL CLAVE DE SEGURIDAD OPERACIONAL

6.1 La asignación de personal competente para desempeñarse como Gerente de seguridad operacional es esencial para un SMS efectivamente implementado y en funcionamiento. El Gerente de seguridad operacional puede ser identificado por diversos títulos dependiendo de la normativa en cada Estado. A los efectos de este manual, el término genérico "Gerente de seguridad operacional" se utiliza y se refiere a la función, no necesariamente al título de un individuo.

6.2 La persona encargada de la función de Gerente de seguridad operacional es responsable ante el Director Ejecutivo por el rendimiento de los SMS y por la prestación de servicios de seguridad operacional a los otros departamentos de la organización.

6.3 El Gerente de seguridad operacional le informa al Director Ejecutivo y a los demás Gerentes de línea en temas de gestión de seguridad operacional y es responsable de coordinar y comunicar problemas de seguridad operacional dentro de la organización, así como con miembros externos de la comunidad de la aviación. Sus funciones incluyen, pero no se limitan a:

a) administrar el plan de implementación de SMS en nombre del Director ejecutivo responsable (tras la implementación inicial);
b) realizar/facilitar la identificación de peligros y el análisis de riesgos de seguridad operacional;
c) efectuar un seguimiento de la implantación de las medidas correctivas o mitigatorias y evaluar sus resultados;
d) proporcionar informes periódicos sobre el rendimiento de seguridad de la organización;
e) mantener la documentación y registros SMS actualizados;
f) planificar y facilitar la capacitación en seguridad operacional del personal;
g) proporcionar asesoramiento independiente en materia de seguridad;
h) controlar problemas de seguridad en la industria de la aviación y su impacto en las operaciones de la organización con respecto a la entrega sus de productos y servicios; y
i) coordinar y comunicar en nombre del Director ejecutivo con la Autoridad de Aviación Civil (AAC) y otras autoridades del Estado sobre asuntos de seguridad operacional según sea necesario o requerido.

6.4 En la mayoría de las organizaciones, una persona es nombrada como Gerente de seguridad operacional. Dependiendo del tamaño, naturaleza y complejidad de la organización, el rol del Gerente de seguridad operacional puede ser una función exclusiva o se puede combinar con otras funciones. En alguna organización esta función es asignada a un grupo de personas.

6.5 El Proveedor de servicios debe asegurarse de que la opción elegida no resulte enmarcada en algún conflicto de intereses. Siempre que sea posible, el Gerente de seguridad operacional no debe participar directamente en la entrega de un producto o servicio, pero debe tener un conocimiento del trabajo realizado en estas actividades. La designación del Gerente de seguridad operacional debe considerar también los posibles conflictos de interés con otras tareas y funciones. Tales conflictos de interés podrían incluir:

a) competencia por financiamiento (ej. Gerente Financiero actuando como Gerente de seguridad Operacional);
b) conflictos en las prioridades por recursos; y
c) cuando el Gerente de seguridad operacional evalúa la efectividad SMS de las actividades operacionales en las que él mismo está envuelto por su otra actividad.

6.6 En el caso que la función se asigna a un grupo de personas, (por ejemplo, cuando los proveedores de servicios extienden sus SMS a través de múltiples actividades) una de las personas debe designarse como Gerente de Seguridad Operacional líder para mantener una línea de información directa e inequívoca con el Director Ejecutivo.

6.7 Las competencias para un Gerente Operacional deberían incluir, pero no estar limitadas a lo siguiente:

a) experiencia en gestión de Seguridad operacional o Calidad;
b) experiencia operacional con respecto al producto o servicio ofrecido por la organización;
c) formación técnica para entender los sistemas que soportan las operaciones, el producto o servicio prestado;
d) habilidades interpersonales;
e) habilidades analíticas para la solución de problemas;
f) habilidades en gestión de proyectos;
g) habilidad para comunicarse adecuadamente en forma oral y/o escrita; y
h) comprensión y conocimiento de los factores humanos.

6.8 Puede que por su tamaño o complejidad la organización requiera personal adicional para apoyar al Gerente de Seguridad sobre todo para las tareas de una pronta recolección de datos, análisis o la rápida y apropiada distribución dentro de la

organización de la información de seguridad operacional relacionadas con la valoración del riesgo y su control que deben ser hechos.

6.9 Los proveedores de servicios deben establecer comités de seguridad operacional de alto nivel que apoyan las funciones SMS en toda la organización. Esto debe incluir la determinación de quién debe participar en el Comité de seguridad operacional y la frecuencia de sus reuniones. Estos Comités pueden ayudar a facilitar:

a) la efectividad del SMS;
b) una respuesta a tiempo en la implantación de acciones para controlar el riesgo operacional;
c) el funcionamiento y rendimiento de la seguridad operacional en relación con la política de seguridad y objetivos de la organización;
d) la eficacia general de las estrategias de mitigación de riesgo de seguridad operacional;
e) efectividad de los procesos de gestión de la seguridad operacional de la organización que apoyan:
    1. la prioridad organizacional declarada de gestión de la seguridad operacional; y
    2. la promoción y fomento de la seguridad operacional a través de toda la organización.

6.10 Una vez que una dirección estratégica ha sido desarrollada por el Comité de seguridad operacional de más alto nivel, la aplicación de las estrategias de seguridad operacional seleccionadas debe ser coordinada en toda la organización. Grupos especiales de seguridad operacional se pueden crear para ayudar a implantar estas estrategias:

a) realizando el control del rendimiento de la seguridad operacional dentro de sus áreas funcionales de la organización y asegurar que las actividades apropiadas de SRM se llevan a cabo;
b) revisando los datos de seguridad operacional disponibles e identificando la implantación de estrategias de control de riesgos de seguridad operacional y asegurando se proporcione retroalimentación al empleado;
c) evaluando el impacto en la seguridad operacional relacionados con la introducción de cambios organizativos o de nuevas tecnologías;
d) coordinando la implementación de las acciones relacionadas con controles de riesgo de seguridad operacional y asegurar que se adopten medidas rápidamente; y
e) revisando la eficacia de los controles específicos de riesgo de seguridad operacional.

7. PLAN PARA LA COORDINACIÓN DE LAS EMERGENCIAS

7.1 Por definición, una emergencia es una situación repentina, imprevista o un evento que requieren una acción inmediata. La coordinación de planificación de respuesta a emergencias se refiere a la planificación de actividades que se desarrollan dentro de un período limitado de tiempo durante una situación de emergencia operacional no planificado.

7.2 La coordinación de planificación de respuesta de emergencia se aplica sólo a aquellos proveedores de servicio que deben establecer y mantener un ERP ("Emergency Response Plan").

7.3 El proveedor de servicios a quien se le exige que establezca y mantenga un ERP para accidentes e incidentes en operaciones de aeronaves y otras emergencias de aviación deberá garantizar que el plan de respuesta ante emergencias se coordine en forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que deba interactuar al suministrar sus servicios o productos.

7.4 Un plan de respuesta de emergencia (ERP) es un componente integral del proceso SRM de un proveedor de servicio para atender emergencias relacionadas con la aviación, las crisis o eventos. Donde existe la posibilidad de operaciones de la aviación de un proveedor de servicios o actividades sean comprometidas por situaciones de emergencia como una emergencia de salud pública/pandemia, estos escenarios deben también abordarse en su ERP según corresponda.

7.5 El ERP debe abordar emergencias previsibles identificadas a través de los SMS e incluyen acciones atenuantes, procesos y controles para administrar con eficacia las emergencias relacionadas con la aviación.

7.6 El objetivo del ERP es garantizar la continuación segura de las operaciones y asegurar el retorno a la normalidad de las operaciones tan pronto como sea posible. El proceso incluye:

a) una transición ordenada y eficiente de la actividad normal de las operaciones a una actividad operacional de emergencia;
b) la asignación de responsabilidades en emergencia y delegación de autoridad;
c) asegurarse que el personal clave para las acciones contenidas en el plan posea las autorizaciones correspondientes;
d) garantizar la coordinación que sea necesaria con otras organizaciones;
e) asegurar la continuación segura de las operaciones o el retorno a la normalidad operacional lo antes posible.

Nota 3: *Debido a que la mayoría de las situaciones de emergencia requiere una acción coordinada entre las diferentes organizaciones, posiblemente con otros proveedores de servicios*

y con otras organizaciones externas tales como los servicios de emergencias no relacionadas con la aviación el ERP debe ser fácilmente accesible al personal clave apropiado, así como a las organizaciones externas.

8. GESTIÓN DE RIESGOS DE LA SEGURIDAD OPERACIONAL

8.1 Los proveedores de servicios deben garantizar que están administrando sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional (SRM), que incluye la identificación de peligros, y la evaluación y mitigación de riesgos de seguridad operacional.

8.2 El proceso SRM se basa en una identificación sistemática de los peligros que existen en el contexto de un proveedor de servicios en la entrega de sus productos o servicios. Los riesgos pueden ser el resultado de los sistemas que son deficientes en su diseño, función técnica, interfaz humano o interacciones con otros sistemas y procesos.

8.3 También puede existir una falta de sistemas o procesos existentes para adaptarse a los cambios en el entorno operativo del proveedor de servicios. Se debe realizar un análisis cuidadoso de estos factores para identificar cualquier riesgo potencial en cualquier punto de la operación o ciclo de vida de la actividad.

8.4 La comprensión del Sistema y su entorno operacional es clave para lograr un alto nivel de rendimiento en seguridad operacional. Los peligros se pueden identificar tanto por fuentes internas como externas.

8.5 Procesos y procedimientos para la identificación de peligros

8.5.1. La identificación de peligros es el primer paso en el proceso de la gestión de riesgos de la seguridad operacional (SRM). En el Apéndice 2 del Anexo 19 de la OACI se indica en 2.1.1 que "*el proveedor de servicios definirá y mantendrá un proceso para identificar los peligros asociados a sus productos o servicios de aviación*" y en 2.1.2 que "*la identificación de los peligros se basará en una combinación de métodos reactivos y preventivos".*

8.5.2 Como se puede apreciar, aunque la norma requiere que un proceso se ponga en marcha para identificar los peligros, no especifica lo que debería ser un proceso. Por lo tanto, los proveedores de servicios deben diseñar su propia metodología para la identificación de los peligros. Las dos metodologías utilizadas más importantes son la metodología reactiva y la proactiva.

8.5.3 Este proceso formal debe considerar los equipos, instalaciones y sistemas. Cualquier riesgo relacionado con la seguridad operacional que se pueda identificar y

controlar será un aporte muy beneficioso para la seguridad operacional. También es importante considerar los peligros que puedan existir como resultado de las interfases SMS con organizaciones externas.

Nota 4: *Una guía más detallada sobre la identificación de peligros y los procedimientos para la valoración del riesgo operacional se puede consultar en el Capítulo 2 del Doc 9859 de la OACI en su Cuarta edición.*

8.5.4 El proveedor debe individualizar las diversas fuentes para identificación de peligros tanto internas como externas que nutren los datos del análisis y establecer los procedimientos para su identificación. Debajo en la **Figura 2** se pueden visualizar los componentes generales del proceso en un proveedor de servicios para la identificación de peligros y la gestión de riesgos asociados a la seguridad operacional.

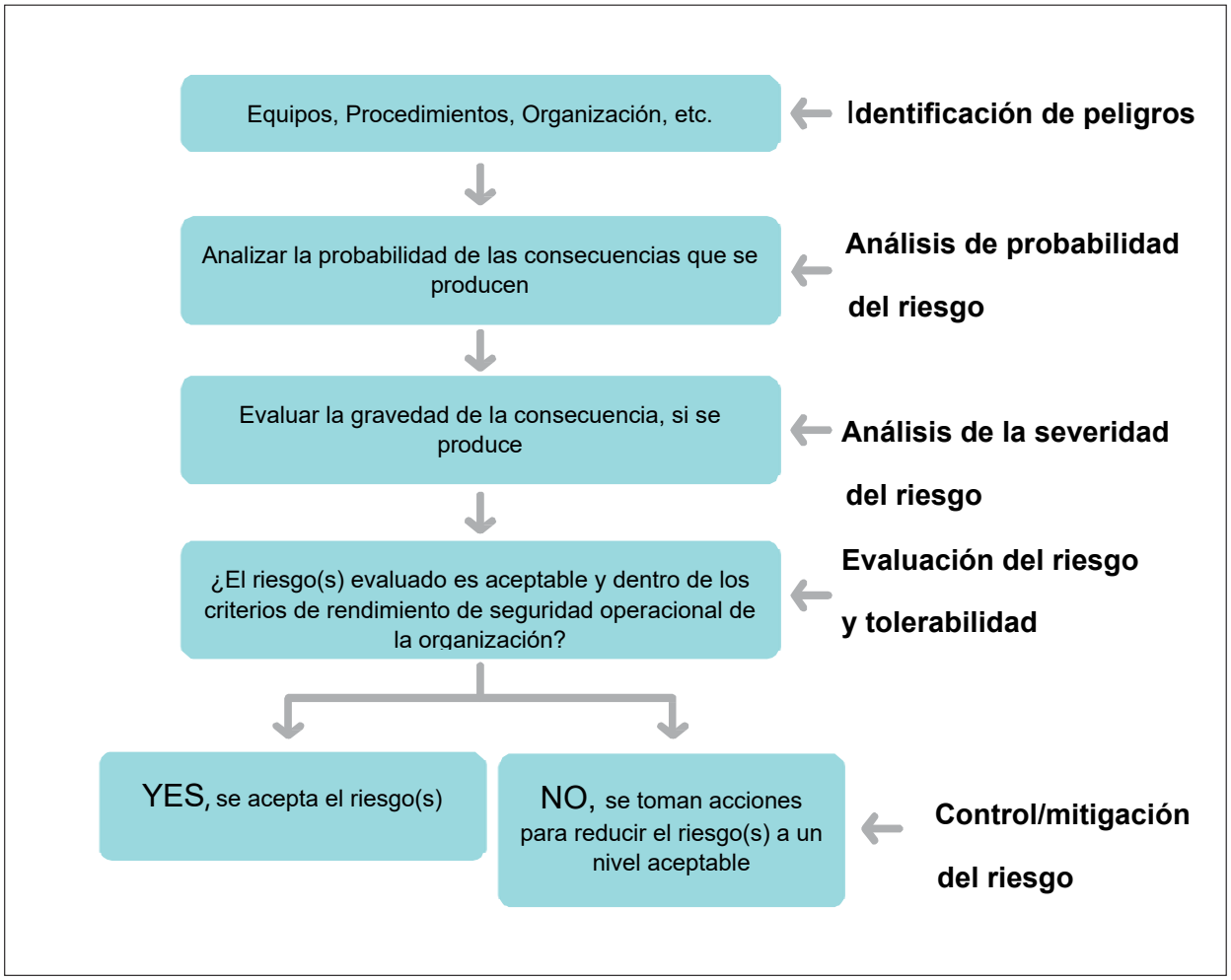

Figura 2: Proceso de gestión de riesgos e identificación de peligros

8.5.5 Las fuentes internas de identificación de peligros pueden incluir, entre otras, el monitoreo normal de las operaciones, las grabaciones de sistemas de monitoreo automatizado como el FDM, análisis de vuelo (FDA), notificaciones voluntarias y

obligatorias sobre peligros o asuntos que pueden afectar o afectan la seguridad operacional, informes de inspecciones o auditorías internas, retroalimentación del entrenamiento inter-activo y reportes de incidentes.

8.5.6 Algunos ejemplos de fuentes externas para la identificación de peligros pueden incluir los reportes de accidentes incluso de otros Estados, auditorías multinacionales del SRVSOP o del USOAP e informes de Asociaciones de la Industria entre otras.

8.6 Sistema de reporte de la seguridad operacional

8.6.1 Una fuente muy importante para la identificación de peligros a la seguridad operacional del sistema lo constituye el sistema de notificación de seguridad operacional voluntaria de información que proporciona un canal importante de información para posibles problemas de seguridad operacional como peligros, cuasi accidentes o errores.

8.6.2 El proveedor debe brindar una protección adecuada para animar a las personas a informar lo que observan o experimentan sobre posibles problemas de seguridad operacional. Se debe indicar claramente que la información divulgada se utilizará únicamente para apoyar la mejora de la seguridad operacional. El objetivo es promover una cultura justa de información eficaz y la identificación proactiva de posibles deficiencias de seguridad operacional.

8.6.3 Los sistemas de notificación voluntaria deben ser confidenciales. La custodia de la información debe limitarse a unos pocos individuos, típicamente restringidos al Gerente de seguridad operacional y el personal involucrado en la investigación de seguridad operacional. El mantenimiento de la confidencialidad estimula la cultura de la notificación, sin temor a represalias o vergüenza.

8.6.4 Para ser eficaces, los sistemas de notificación de seguridad operacional deben ser accesibles a todo el personal sea utilizando un formulario en papel, un formulario basado en la web u otro que se utilice por la administración. Tener múltiples métodos de entrada disponibles maximiza la probabilidad de que el personal pueda notificar voluntariamente si se ha concientizado adecuadamente el beneficio que estos reportes pueden aportar.

8.6.5 Cualquier persona que realiza una notificación sobre seguridad operacional debe recibir la retroalimentación respectiva sobre qué decisiones o acciones se tomaron. Esta retroalimentación sirve para demostrar que dichos informes se consideran seriamente y ayuda a promover una cultura de seguridad operacional positiva y animar a futuros informes.

8.6.6 Es importante que se documenten los peligros identificados. Una vez que se identifican los peligros, sus consecuencias (es decir, cualquier evento específico o resultado) deben ser determinadas.

8.7 Investigación de Peligros

8.7.1 La identificación de peligros debe ser continua y parte de las actividades regulares del proveedor de servicio. Algunas condiciones pueden merecer una investigación más detallada. Estas pueden incluir:

a) instancias donde la organización experimenta un aumento inexplicado de eventos relacionados con la seguridad operacional o de no-cumplimiento; o
b) cambios significativos en la organización o sus actividades.

8.8 Proceso de investigación

8.8.1 La Gestión de la seguridad operacional eficiente y eficaz depende de calidad de las investigaciones para analizar los eventos, los riesgos de seguridad operacional y conclusiones y recomendaciones para mejorar la seguridad de las operaciones.

8.8.2 Mientras que la investigación de accidentes e incidentes graves en el Anexo 13 son responsabilidad del estado, las investigaciones de seguridad operacional del proveedor de servicio se llevan a cabo por los proveedores de servicios como parte de sus SMS para apoyar la identificación de riesgos y procesos de evaluación y mitigación del riesgo. Hay muchos sucesos de seguridad operacional que caen fuera del Anexo 13 que pueden proporcionar una valiosa fuente de identificación de los peligros o identificar debilidades en los controles de riesgo. Estos problemas pueden ser descubiertos y mitigados por una investigación de seguridad operacional gestionada por el proveedor de servicios.

8.8.3 El objetivo principal de la investigación de seguridad operacional del proveedor de servicio es entender lo que sucedió y cómo evitar que situaciones similares ocurran en el futuro para eliminar o mitigar las deficiencias de seguridad operacional. Esto se logra a través del examen cuidadoso y metódico del evento y aplicando las lecciones aprendidas para reducir la probabilidad y/o la consecuencia de las repeticiones futuras. Estas investigaciones de seguridad operacional del proveedor son una parte integral de SMS de los servicios.

8.8.4 Los beneficios de llevar a cabo una investigación de seguridad incluyen:

a) comprender mejor los acontecimientos que condujeron al suceso;
b) identificar los factores humanos, técnicos y organizacionales contribuyentes;
c) identificar peligros y realizar evaluaciones de riesgo;
d) hacer recomendaciones para reducir o eliminar riesgos inaceptables; y
e) identificar lecciones aprendidas que deben ser compartidas con los miembros apropiados de la comunidad de la aviación.

8.8.5 Una investigación de seguridad operacional del proveedor de servicio es iniciada generalmente por una notificación (informe) a través del sistema de notificación de la seguridad operacional.

8.8.6 No todos los eventos o peligros pueden o deben ser investigados; la decisión de llevar a cabo una investigación y su profundidad dependerá de las consecuencias reales o potenciales de riesgo del peligro o del evento. Un escrutinio preliminar de los eventos y peligros considerados es necesario para determinar el alto o menor riesgo potencial. La prioridad la debe tener el alto riesgo potencial. Para investigar ayuda tener estructurado y definido un enfoque para la toma de decisiones. Qué investigar y cuál será el alcance de la investigación.

8.8.7 Este enfoque estructurado puede considerar:

a) la severidad o gravedad potencial de los resultados;
b) requisitos reglamentarios o de organización para llevar a cabo una investigación;
c) se puede mejorar la seguridad operacional;
d) oportunidad para que se puedan tomar medidas de seguridad operacional;
e) riesgos asociados si no se efectúa la investigación;
f) contribución a los programas de seguridad operacional específicos;
g) identificar tendencias;
h) beneficios para el entrenamiento; y
i) disponibilidad de recursos.

8.8.8 Para comenzar una investigación primero conviene designar a un investigador o un equipo de investigación con las habilidades necesarias y conocimientos. Los recursos financieros necesarios deben ponderarse en esta decisión. El tamaño del equipo y el perfil de conocimientos de sus miembros dependen de la naturaleza y severidad del suceso investigado. El equipo de investigación puede requerir la ayuda de otros especialistas adicionales. A menudo, se asigna a una sola persona para llevar a cabo una investigación interna, con el apoyo de las operaciones y expertos de la oficina de seguridad operacional.

8.8.9 Es recomendable que los investigadores de seguridad operacional que analizarán el suceso en un servicio o área no sean de la misma área organizacionalmente hablando. Se obtienen mejores resultados si el investigador(es) está bien informado(s) (entrenado) y capacitado(s) (experiencia) en investigaciones de seguridad operacional del proveedor de servicio. El investigador o investigadores deberían elegirse en base a sus conocimientos, habilidades y carácter, que deben incluir: integridad, objetividad, pensamiento lógico, pragmatismo y pensamiento lateral.

8.8.10 La investigación debe identificar lo que sucedió y por qué sucedió y esto puede requerir aplicar un análisis de la causa raíz como parte de la investigación.

Idealmente, las personas involucradas en el evento deben ser entrevistadas tan pronto como sea posible después del evento. La investigación debe incluir:

a) establecer un cronograma (líneas de tiempo) de eventos clave, incluyendo las acciones de las personas involucradas;
b) revisión de las políticas y procedimientos relacionados con las actividades;
c) revisión de toda decisión tomada en relación con el evento;
d) identificación de los controles de riesgo que eran aplicados y que debería haber prevenido la ocurrencia del evento; y
e) revisión de datos de seguridad operacional para cualquier evento anterior o similar.

8.8.11 Una investigación de seguridad operacional debe centrarse en los peligros identificados y los riesgos de seguridad y oportunidades de mejora, no en la culpa o el castigo. La manera en la que la investigación es conducida, y más importante aún, en cómo se redacta el informe, influirá probablemente en la seguridad operacional, la futura cultura organizacional de la seguridad operacional, y la efectividad de las iniciativas de seguridad operacional del futuro.

9.8.12 La investigación debe concluir con resultados claramente definidos y las recomendaciones que eliminan o mitigan las deficiencias de seguridad operacional.

8.9 Valoración y mitigación del riesgo operacional (SRM)

8.9.1 El proveedor de servicios debe desarrollar un modelo de evaluación de riesgos de seguridad y procedimientos que permitirán un enfoque coherente y sistemático para la evaluación de riesgos de seguridad. Esto debe incluir un método que le ayudará a determinar qué riesgos son aceptables o inaceptables y priorizar acciones.

8.9.2 Las herramientas SRM utilizadas pueden necesitar ser revisadas y modificadas para requisitos particulares periódicamente para asegurar que son adecuadas para el entorno operativo de los servicios.

8.9.3 Con el tiempo se pueden gestionar enfoques más sofisticados que reflejen mejor las necesidades de su operación a medida que la aplicación de su SMS gana experiencia y madurez. El proveedor de servicios y la AAC deben acordar una metodología.

8.9.4 El proceso de evaluación de riesgos de seguridad debe utilizar todos los datos y la información de seguridad operacional que está disponible. Una vez que se han evaluado los riesgos de seguridad, el proveedor de servicios participará en un proceso de toma de decisiones basada en datos para determinar qué controles de riesgos de seguridad son necesarios.

8.9.5 Las evaluaciones de riesgos de seguridad operacional a veces tienen que usar información cualitativa (juicio experto) en lugar de datos cuantitativos debido a falta

de datos. La utilización de la matriz de riesgos de seguridad operacional permite al usuario expresar el riesgo de seguridad asociado con los riesgos identificados en un formato cuantitativo. Esto permite la comparación de la magnitud directa entre los riesgos de seguridad identificados. Un criterio de evaluación de riesgo de seguridad cualitativa como "probable" o "improbable" se puede asignar a cada riesgo de seguridad identificado donde la información cuantitativa no está disponible.

8.9.6 Para los proveedores de servicio que tienen operaciones en varias ubicaciones con entornos operativos específicos, puede ser más eficaz establecer comités locales de seguridad para llevar a cabo las evaluaciones de riesgos de seguridad e identificación de control de riesgos de seguridad. De ahí la importancia de adecuar el sistema al tamaño y complejidad de cada organización.

8.9.7 Los proveedores de servicios deben asignar prioridades a sus evaluaciones de riesgo y tomar decisiones sobre qué controles de riesgo adoptar. Para asignar esas prioridades, el proveedor del servicio debe considerar:

a) evaluar y controlar el riesgo más alto de seguridad operacional;

b) asignar recursos a los más altos riesgos de seguridad operacional;
c) mantener la mejora y la eficiencia de la seguridad operacional;
d) alcanzar los objetivos de seguridad operacional establecidos y acordados y los objetivos de rendimiento de seguridad operacional (SPTs); y
e) satisfacer los requisitos de las regulaciones del estado en materia de control de riesgos de seguridad operacional.

8.9.8 Después de que se han evaluado los riesgos de seguridad, se pueden implementar controles de riesgo apropiados de seguridad operacional. Es importante involucrar a los "usuarios finales" y expertos en la determinación estos controles. Asegurando que participan los expertos correctos se optimiza la puesta en práctica de las mitigaciones elegidas para el control de riesgos de la seguridad operacional.

8.9.9 La determinación de las consecuencias no intencionadas, particularmente la introducción de nuevos riesgos, debe hacerse antes de la implementación de los controles de riesgo de seguridad.

8.9.10 Una vez que el control de riesgos de seguridad operacional ha sido acordado y puesto en ejecución, las condiciones de seguridad operacional deben ser vigiladas para asegurar la efectividad del control de riesgo de seguridad operacional. Esto es necesario para verificar la integridad, eficiencia y eficacia de los nuevos controles de riesgos de seguridad operacional bajo las condiciones operativas.

8.9.11 Los resultados del proceso SRM deben documentarse. Esto debe incluir los riesgos y sus consecuencias, la evaluación de riesgos de seguridad operacional y cualquier acción de control de riesgo de seguridad operacional implantada. Estos resultados pueden ser contenidos en un registro accesible que permita su seguimiento y supervisión.

8.9.12 Esta documentación SRM se convierte en una fuente organizacional histórica de conocimiento de seguridad operacional que puede usarse como referencia en la toma de decisiones y para el intercambio de información sobre seguridad operacional.

8.9.13 Asimismo, esta documentación es un material importante para los análisis de tendencia, entrenamiento y comunicación además de constituir una valiosa información para la auditoría interna al evaluar si los controles de riesgo de la seguridad operacional y las acciones implantadas han sido efectivos.

9. ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

9.1 El aseguramiento de la seguridad operacional se basa en procesos y actividades realizadas para determinar si el SMS está operando según las expectativas y los requisitos. Esto implica el seguimiento continuo de sus procesos, así como su entorno operativo para detectar cambios o desviaciones que puedan presentar riesgos de seguridad operacional emergentes o la degradación de los controles de riesgos de seguridad operacional existentes. Dichos cambios o desviaciones pueden abordarse a través del proceso SRM.

9.2 Las actividades de aseguramiento de la seguridad operacional deben incluir el desarrollo y la implementación de las medidas adoptadas en respuesta a problemas identificados, teniendo un impacto potencial de la seguridad. Estas acciones mejoran continuamente el rendimiento de SMS de los servicios.

9.3 La evaluación de la eficacia de los controles de riesgo de seguridad operacional es importante, ya que su aplicación no siempre alcanza el resultado esperado. Esto sirve para determinar si el control de riesgo seleccionado fue el correcto y si no ha dado el resultado previsto abrir paso a la aplicación de una estrategia diferente de control de riesgos de seguridad operacional.

9.4 Para verificar el funcionamiento de la seguridad operacional y validar la efectividad de los controles de riesgo de seguridad operacional se requiere el uso de una combinación de auditorías internas y el establecimiento y seguimiento de indicadores de rendimiento de seguridad operacional (SPIs).

9.5 Auditorías internas

9.5.1 Las auditorías internas son más efectivas cuando son conducidas por personas o departamentos independientes de las funciones o procesos que se auditan. Estas auditorías internas deben proporcionar al Director Ejecutivo y al Gerente de Seguridad Operacional con una retroalimentación sobre:

a) cumplimiento con las regulaciones;
b) cumplimiento con las políticas, procesos y procedimientos;
c) la efectividad de los controles de riesgo de la seguridad operacional;
d) la efectividad de las acciones correctivas; y
e) la efectividad del SMS.

9.5.2 Algunas organizaciones no pueden garantizar independencia apropiada de una auditoría interna, en estos casos, el proveedor del servicio debe considerar participación de auditores externos o auditores de otra organización.

9.5.3 La planificación de las auditorías internas debe tener en cuenta la importancia de la seguridad de los procesos, los resultados de anteriores auditorías y evaluaciones (de todas las fuentes) y los controles de riesgo de seguridad operacional implementado. La auditoría interna debe identificar el incumplimiento de regulaciones y políticas, procesos y procedimientos. También debe identificar deficiencias del sistema, falta de efectividad de los controles de riesgo de seguridad operacional y oportunidades de mejora.

9.5.4 Tanto la evaluación de cumplimiento y la eficacia son esenciales para lograr el funcionamiento de la seguridad operacional. En la auditoría se pueden formular un conjunto de preguntas para evaluar el cumplimiento y efectividad de cada proceso o procedimiento:

a) Para determinar el cumplimiento:

1. ¿El procedimiento o proceso requerido existe?
2. ¿El proceso o procedimiento está documentado (entradas, actividades, interfaces y salidas definidas)?
3. ¿El proceso o procedimiento reúne los requisitos (criterios)?
4. ¿Está el proceso o procedimiento siendo utilizado?
5. ¿Está todo el personal involucrado siguiendo el proceso o el procedimiento en forma consistente?
6. ¿Están siendo producidas salidas definidas?
7. ¿Han sido documentados e implantados los cambios en los procesos y los procedimientos?

b) Para evaluar la efectividad

1. ¿Entiende el usuario el proceso o el procedimiento?

2. ¿El propósito perseguido por el proceso o el procedimiento se está alcanzando consistentemente?
3. ¿Los resultados de los procesos y los procedimientos son los que el cliente espera?
4. ¿Los procesos o procedimientos son revisados regularmente?
5. ¿Se realiza una evaluación de seguridad operacional cuando hay cambios en los procesos y procedimientos?
6. ¿Las mejoras en los procesos y los procedimientos han resultado en los beneficios esperados?

9.5.5 Adicionalmente, las auditorías internas deben vigilar el progreso de cierre en los incumplimientos del proveedor de servicios que se hayan identificado previamente. Estos deben haber sido abordados a través de un análisis causa raíz y el desarrollo e implantación de planes de acciones correctivas y preventivas. Los resultados de los análisis de las causas o de los factores contribuyentes para cualquier incumplimiento deben alimentar los procesos SRM del Proveedor de Servicios.

9.5.6 Los resultados del proceso de auditoría interna constituyen una de las varias entradas a las funciones de aseguramiento de la seguridad operacional y SRM. Las auditorías internas informan al proveedor de servicios del nivel de cumplimiento de las normas dentro de la organización, si el grado de los controles de riesgos de seguridad operacional es efectivo y donde se requiere una acción correctiva o preventiva.

9.5.7 La vigilancia del rendimiento de la seguridad operacional se lleva a cabo a través de la recolección de datos e información de seguridad operacional de variadas fuentes generalmente disponibles en la organización. La disponibilidad de datos para apoyar la toma de decisiones sustentada en datos e información es uno de los aspectos más importantes de los SMS.

9.5.8 La vigilancia del rendimiento de la seguridad operacional y su medición debe ser dirigida observando algunos principios básicos El rendimiento de la seguridad operacional alcanzado es un indicio de comportamiento organizacional y es también una medida de la eficacia de los SMS. Esto requiere que la organización defina:

a) objetivos de seguridad operacional, que se deben establecer primero para reflejar los logros estratégicos o los resultados deseados relacionados con preocupaciones de seguridad específicas del contexto operacional de la organización;

b) Indicadores de rendimiento de seguridad operacional (SPIs), que son parámetros tácticos relacionadas con los objetivos de seguridad y, por lo tanto, son la referencia para la recolección de datos; y

c) objetivos de rendimiento de seguridad operacional (SPTs), que también son parámetros tácticos utilizados para supervisar el progreso hacia el logro de los objetivos de seguridad.

9.5.9 Para el establecimiento de los objetivos de seguridad operacional debe tenerse en cuenta lo siguiente:

a) Definir qué es lo que la organización espera alcanzar.
b) Debe ser una declaración de un resultado deseado.
c) Los objetivos de seguridad operacional deben ser declaraciones cortas y de alto nivel sobre las prioridades de seguridad operacional y deben reflejar la política de seguridad operacional de la organización.
d) Los objetivos de seguridad operacional deben abordar los riesgos más significativos de la organización.

9.6 Indicadores de rendimiento de seguridad operacional (SPIs)

9.6.1 Al establecer los SPIs los proveedores de servicio deben considerar:

a) Medir las cosas correctas: Determinar los mejores SPIs que mostrarán que la organización está en camino para alcanzar sus objetivos de seguridad operacional. También se debe considerar cuáles son los mayores problemas de seguridad operacional y los riesgos que enfrenta la organización e identificar los SPI que mostrarán que se realiza un control efectivo de estos.

b) Disponibilidad de datos: ¿Hay datos disponibles que se alinean con lo que la organización desea medir? Si no hay, puede ser necesario establecer fuentes de recolección de datos adicionales. Para las organizaciones pequeñas con una cantidad limitada de datos, la puesta en común de los conjuntos de datos también puede ayudar a identificar las tendencias. Esto se puede apoyar por asociaciones de la industria que pueden recopilar datos de seguridad de múltiples organizaciones.

c) Fiabilidad de los datos: los datos pueden ser poco fiables debido a su subjetividad o porque está incompleto.

d) SPIs comunes de la industria: puede ser útil acordar SPIs comunes con organizaciones similares para que puedan hacer comparaciones entre organizaciones. Las asociaciones de industria o regulador pueden activarlos.

9.6.2 Los SPIs puede requerir el monitoreo de los datos de diversas fuentes tales como:

a) Sucesos y/o eventos de seguridad operacional;
b) Informes de seguridad operacional;

c) Estudios de seguridad operacional;
d) Revisiones de seguridad operacional incluyendo análisis de tendencias;
e) Auditorías;
f) Encuestas;
g) Investigaciones internas de seguridad operacional.

Nota 5: *Un suceso de seguridad operacional es el término usado para abarcar todos los eventos que tienen o podrían tener importancia en el contexto de seguridad operacional, que van desde accidentes y accidentes graves, incidentes o eventos que deben notificarse, a casos de menor gravedad que, en la opinión de quien reporta el suceso, podría tener importancia para la seguridad operacional.*

9.6.3 Una vez que se han establecido los SPIs, el proveedor del servicio puede considerar si es apropiado identificar SPTs; niveles de alerta.

Nota 6: *A pesar que el Anexo 19 no exige un nivel o criterio de valor establecido ("safety trigger") para un determinado indicador de rendimiento de seguridad que sirve para iniciar una acción necesaria, (por ejemplo, una evaluación, ajuste o acción correctiva), este criterio de valor ("safety trigger") es usado por algunas organizaciones que se respaldan en datos históricos de seguridad operacional suficientes o relevantes.*

9.6.4 Para que los SPTs puedan servir para mejorar el rendimiento de la seguridad operacional no se puede perder de vista el objetivo principal de mejorar el funcionamiento de la seguridad operacional. Suele suceder que en algunas ocasiones la extrema focalización la meta de rendimiento a ser alcanzada hace dejar de lado lo principal. En tales casos puede ser más apropiado supervisar el SPI en base a tendencias.

9.6.5 El desarrollo de la SPI debe vincularse a los objetivos de seguridad operacional y se basa en el análisis de datos que está disponible u obtenible. El proceso de seguimiento y medición implica el uso de indicadores de rendimiento de seguridad seleccionado, SPTs correspondientes e iniciadores.

9.6.6 La organización debe supervisar el rendimiento establecido SPIs y SPTs para identificar cambios anormales en el funcionamiento de la seguridad operacional. Pero debe quedar claro que los SPTs deben ser realistas, dentro de un contexto específico y realizable al considerar los recursos disponibles para la organización y el sector de servicio considerado.

9.6.7 Sobre todo, la vigilancia de la seguridad operacional y la medición proporciona un medio para verificar la eficacia de los controles de riesgo de seguridad operacional. Además, proporcionan una medida de la integridad y eficacia de actividades y procesos SMS.

Nota 7: *Para obtener más información sobre la gestión de rendimiento de la seguridad operacional, consulte la Cuarta Edición del Doc 9859 Capítulo 4 de la OACI.*

9.7 La gestión del cambio

9.7.1 El proveedor de servicios definirá y mantendrá un proceso para identificar los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus productos o servicios de aviación, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios.

9.7.2 Los proveedores de servicio están sujetos a continuos cambios debido a un número de factores que pueden incluir una contracción o expansión de su organización, mejoras introducidas tanto en sistemas internos como en procesos y procedimientos que sustentan la seguridad operacional de sus productos o servicios, los cambios en el entorno operacional, cambios en la interfaz con organizaciones externas y cambios regulatorios, económicos y en riesgos emergentes.

9.7.3 Estos cambios pueden afectar la efectividad de los controles de riesgos de seguridad operacional existentes. Además, nuevos peligros y riesgos relacionados con la seguridad operacional pueden ser inadvertidamente introducidos en una operación cuando se produce el cambio. Los peligros que introduce el cambio deben ser identificados y los riesgos de seguridad operacionales relacionados con esos peligros deben ser evaluados y controlados en la forma que la organización ha definido para la identificación de peligros y/o procedimientos SRM.

9.7.4 Los procesos de la organización para la gestión del cambio debe tener en cuenta las siguientes consideraciones:

a) Cuán crítico es el impacto del cambio en las actividades de su organización, y el impacto en otras organizaciones del sistema aeronáutico en su conjunto.

b) Es importante que expertos clave de la comunidad aeronáutica estén involucrados en las actividades de gestión del cambio desde un primer momento. Esto puede incluir a individuos de organizaciones externas.

c) Disponibilidad de información y datos de rendimiento de la seguridad operacional. Es necesario conocer qué datos e información está disponible y si se puede utilizar como información sobre la situación y maximizar el análisis previo al cambio planificado.

9.7.5 Pequeños cambios sumados en el tiempo, a menudo pasan desapercibidos, pero su efecto acumulativo puede tener un impacto considerable. Los cambios, sean grandes o pequeños pueden afectar la descripción del sistema de la organización. Por lo tanto, la descripción del sistema debe ser revisada regularmente para determinar su vigencia, dado que la mayoría de los proveedores de servicios experimentan cambios en forma regular, o incluso permanente.

9.7.6 El proveedor del servicio debe definir qué activa el proceso de cambio formal. Cambios que pueden desencadenar la gestión del cambio formal incluyen:

a) introducción de nueva tecnología o equipo;
b) cambios en el entorno operacional;
c) cambios en personal clave;
d) cambios significativos en los niveles de personal;
e) cambios en los requisitos normativos de seguridad operacional;
f) significativa reestructuración de la organización; y
g) cambios físicos (nuevas instalaciones, cambios de diseño de aeródromo etc.).

9.7.8 El proveedor del servicio debe considerar también el impacto del cambio en el personal. Esto podría afectar la manera que el cambio es aceptado por los afectados. El compromiso y comunicación temprana mejorará la aceptación y su implantación, aunque puede ser necesario que determinado personal actúe como agentes facilitadores del cambio.

9.7.9 El proceso de gestión del cambio deben considerar lo siguiente:

a) comprender y definir el cambio. Esto debe incluir una descripción del cambio y por qué se está implementando;

b) comprender y definir quién y qué afectará; estos pueden ser individuos dentro de la organización, otros departamentos o personas externas o de organizaciones. Los equipos, sistemas y procesos también pueden ser afectados. Puede ser necesaria una revisión de la descripción del sistema y las interfases de las organizaciones. Esta es una oportunidad para determinar quién debe participar en el cambio. Los cambios pueden afectar los controles de riesgo establecidos, y por lo tanto, el cambio podría aumentar los riesgos en áreas que no son inmediatamente evidentes;

c) identificar los peligros relacionados con el cambio y llevar a cabo una evaluación de riesgo de seguridad; esto debe identificar cualquier peligro directamente relacionado con el cambio, pero nuevamente también debe revisarse el impacto en los riesgos y controles de riesgo de seguridad que pueden ser afectados por el cambio. Este paso debe utilizar procesos SRM de la organización existente;

d) desarrollar un plan de acción; esto debe definir lo que debe hacerse, por quién y cuándo. Debe haber un plan claro que describe cómo se implementará el cambio y quién será responsable de las acciones y la secuenciación y la programación de cada tarea;

e) el ejecutivo responsable de liderar la implantación del cambio debe firmar el cambio; para confirmar que el cambio no afecta la seguridad operacional; y

f) plan de aseguramiento; se trata de determinar qué medidas de seguimiento son necesarias. Considerar cómo será comunicado el cambio y si son necesarias

otras actividades adicionales (por ejemplo, auditorías) durante o después del cambio. Cualquier suposición realizada debe ser probada.

9.8 Mejora continua del SMS

9.8.1 La organización debe buscar continuamente mejorar su rendimiento en la seguridad operacional. La mejora continua debe ser alcanzada a través de:

a) evaluación proactiva del día a día las operaciones, instalaciones, equipos, documentación y procedimientos a través de auditorías de seguridad operacional y encuestas;

b) evaluación del rendimiento individual para verificar el cumplimiento de sus responsabilidades de seguridad operacional;

c) evaluaciones reactivas para comprobar la eficacia del sistema de control y mitigación de riesgo, por ejemplo: incidentes, accidentes e investigaciones;

d) seguimiento de los cambios organizativos para asegurar que son eficaces; y

e) revisión periódica del funcionamiento de la seguridad y planes de acción de seguridad de la organización.

10. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

10.1 Instrucción y educación

10.1.1 El proveedor de servicios creará y mantendrá un programa de instrucción en seguridad operacional que garantice que el personal cuente con la instrucción y las competencias necesarias para cumplir sus funciones en el marco del SMS. El alcance del programa de instrucción en seguridad operacional será apropiado para el tipo de participación que cada persona tenga en el SMS y deberá actualizarse periódicamente.

10.1.2 El Gerente de seguridad operacional es el responsable de asegurar que existe un programa de formación de seguridad adecuada implantado. El programa de capacitación debe incluir requerimientos de entrenamiento inicial y recurrente para mantener las competencias. Entrenamiento inicial de seguridad debe considerar, como mínimo, lo siguiente:

a) las políticas de seguridad organizacional y los objetivos de seguridad operacional;
b) roles organizacionales y responsabilidades relacionadas con la seguridad operacional;
c) principios básicos SRM;
d) sistemas de notificación de seguridad operacional;
e) procesos y procedimientos SMS de la organización; y

f) factores humanos.

10.1.3 El entrenamiento recurrente de seguridad operacional debe enfocarse en los cambios en las políticas, procesos y procedimientos SMS y debería resaltar cualquier problema específico de seguridad operacional que sea relevante para la organización o lecciones aprendidas.

10.1.4 El programa de capacitación se debe adaptar a las necesidades del rol que desempeña el individuo dentro de los SMS. Por ejemplo, el nivel y profundidad de formación para directivos en los comités de seguridad operacional de la organización será más extensos que para el personal directamente involucrado con la entrega de productos o servicios de la organización. El personal no directamente involucrado en las operaciones puede requerir sólo un resumen de alto nivel de SMS de la organización.

10.1.5 Debe existir formación específica de seguridad para el Director Ejecutivo, los Gerentes de Seguridad y demás directivos que incluya los siguientes temas:

a) formación específica en concientizar nuevos ejecutivos responsables y titulares de puestos que deben rendir cuentas y responsabilidades SMS;
b) importancia del cumplimiento de los requisitos de seguridad operacional a nivel nacional y organizacional;
c) compromiso de gestión;
d) asignación de recursos;
e) promoción de la política de seguridad operacional y los SMS;
f) promoción de una cultura de seguridad operacional positiva;
g) comunicación interdepartamental de seguridad operacional efectivas;
h) objetivo de seguridad operacional, SPTs y niveles de alerta; y
i) política disciplinaria.

10.2 Comunicación de la seguridad operacional

10.2.1 El proveedor de servicios creará y mantendrá un medio oficial de comunicación en relación con la seguridad operacional orientada a:

a) *garantizar que el personal es plenamente consciente del SMS;* esta es una buena forma de promover la política y los objetivos de seguridad operacional de la organización.

b) *transmitir información crítica para la seguridad operacional;* la información crítica para la seguridad operacional es información específica relacionada con problemas y riesgos de seguridad operacional que podrían exponer a la organización a ese tipo de riesgo. Podría tratarse de información recopilada de fuentes internas o externas como enseñanzas obtenidas o relacionadas con controles de riesgos de seguridad operacional. El proveedor de servicios

determina el tipo de información que se considera crítica para la seguridad operacional, así como la oportunidad de comunicarla.

c) *crear conciencia sobre nuevos controles de riesgos de seguridad operacional y medidas correctivas;* los riesgos de seguridad operacional que enfrenta el proveedor de servicios cambiarán con el tiempo, y si se trata de un nuevo riesgo de seguridad operacional que ha sido identificado o de cambios en los controles de riesgos de seguridad operacional dichos cambios deberán comunicarse al personal apropiado.

d) *proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados;* cuando se actualizan los procedimientos de seguridad operacional es importante que las personas apropiadas tengan conocimientos de dichos cambios.

e) *promover una cultura de seguridad operacional positiva y alentar al personal a identificar y notificar peligros;* la comunicación de seguridad operacional es en ambos sentidos. Es importante que todo el personal comunique los problemas de seguridad operacional a la organización a través del sistema de notificaciones de seguridad operacional.

f) *proporcionar comentarios e información;* proporcionar comentarios al personal que presenta notificaciones de seguridad operacional respecto de las medidas que se han adoptado para abordar las preocupaciones identificadas.

10.2.2 Elegir el tipo adecuado de medio de comunicación es lo primero que debemos atender y para ello debemos tener claro qué se desea alcanzar, cuál es el efecto que se busca después de comunicar. ¿Mayor conocimiento, mejor entendimiento más motivación o participación, o se desea llevar adelante algún tipo de acción o cambio del comportamiento o de la cultura organizacional?

10.2.3 Los medios de información y de comunicación pueden incluir: boletines informativos, boletines de seguridad y avisos; presentaciones; sitios web y correos electrónicos; reuniones informales de trabajo entre el personal y el Gerente de seguridad operacional u otros directivos y responder a dudas e inquietudes que puedan formular los participantes.
