CIRCULAR DE ASESORAMIENTO

REGISTRO DE APROBACIÓN

Circular de Asesoramiento número: **CA: 24.145-001**

ASUNTO: IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA **SEGURIDAD** OPERACIONAL (SMS) EN UNA ORGANIZACIÓN DE MANTENIMIENTO RAC-24.145

Revisión: 2
Fecha: 14 de julio de 2020

Responsable (autor):
Ing. Jorge Luis Diaz Reyes

Ing. Jorge Luis Diaz Reyes
Inspector Aeronavegabilidad
DIA/IACC

Aprobación Preliminar:

Subdirector DIA

Ing. Antonio Lahera Sam
Subdirector de Ingeniería y Aeronavegabilidad
IACC

Instituto de Aeronáutica Civil de Cuba
Cuño
Dirección de ingeniera y Aeronavegabilidad
MITRANS

Aprobación Director

Ing. José López Vázquez
Director de Ingeniería y Aeronavegabilidad IACC

CIRCULAR DE ASESORAMIENTO

CA-24.145-001
FECHA: 14/07/2020
REVISION: 02
EMITIDA POR: DIA/IACC

TEMA: IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN UNA ORGANIZACIÓN DE MANTENIMIENTO RAC-24.145.

La presente circular de asesoramiento sobre implementación de un Sistema de Gestión de la Seguridad Operacional (SMS) en una organización de mantenimiento RAC-24.145, se corresponde con la similar emitida por el Sistema Regional de Vigilancia SVRSOP y sirve de guía y orientación a las organizaciones de mantenimiento para instrumentar este sistema en correspondencia con los requisitos de las Regulaciones Aeronáuticas Cubanas RAC-24.145 y RAC-19.

DOCUMENTOS DE REFERENCIA:

- Circular de Asesoramiento CA-AIR-145-002, revisión 3 del 26.09.2018 emitida por el SVRSOP.
- Regulación Aeronáutica Cubana RAC-24.145, Capitulo C "Sistema de Gestión de Seguridad Operacional"
- RAC-19 "Gestión de la Seguridad Operacional", Anexo 2 "Marco para un Sistema de la Seguridad Operacional".

DEFINICIÓN DE TÉRMINOS Y ABREVIATURAS:

AOC : Certificado de explotador aéreo
MAC : Métodos aceptables de cumplimiento
MEI : Material explicativo e informativo
RAC : Regulaciones Aeronáuticas Cubanas.
OMA : Organización de Mantenimiento Aprobada.
DIA/IACC: Dirección de Ingeniería y Aeronavegabilidad/ Instituto de Aeronáutica Civil de Cuba.
AAC : Autoridad de la Aeronáutica Civil

AUTORIDAD:

En la RAC-24.145 ”Organizaciones de Mantenimiento Aprobadas¨ vigente, en su Capítulo C ¨Sistema de Gestión de Seguridad Operacional¨, requisito 145.200, inciso (a) establece: Una OMA RAC 24.145 establecerá, implementará y mantendrá un Sistema de Gestión de Seguridad Operacional (SMS) que se ajuste a la dimensión y complejidad de la organización, el cual sea aceptado por la DIA/IACC.

Así mismo, en la RAC-19 en su Capítulo III “Responsabilidades Estatales en Materia de Gestión de la Seguridad Operacional”, Sección Primera “Programa de Seguridad Operacional del Estado (SSP)”, Articulo 3 menciona los prestadores que deben implementar un SMS aceptable para el IACC, entre los que se encuentran las Organizaciones de Mantenimiento Aprobadas (OMA) RAC-24.145 (inciso c). En la misma RAC y Capitulo, en su Artículo 5, inciso a, indica que este SMS se establecerá de conformidad con los elementos de marco que figuran en el Anexo 2 “Marco para un Sistema de la Seguridad Operacional”, de esta RAC-19.

INDICE DE CONTENIDOS:

Sección A – Propósito

La presente circular de asesoramiento (CA) proporciona orientación para las organizaciones de mantenimiento RAC 24. 145 sobre la implementación de un marco del sistema de gestión de la seguridad operacional (SMS) en conformidad con las Regulaciones Aeronáuticas Cubanas RAC-24.145 y RAC-19.

Esta CA sirve de guía a las organizaciones de mantenimiento aprobadas (OMA), para el cumplimiento de los requisitos establecidos en la Sección 145.225 "Implementación del sistema de gestión de la seguridad operacional (SMS)", así como del capítulo C "Sistema de Gestión de Seguridad Operacional", de la RAC-24.145.

La RAC-24.145 especifica el marco para la implementación y mantenimiento de un SMS. Independientemente del tamaño y la

complejidad de la organización de mantenimiento, se aplican todos los elementos del marco de SMS. La implementación debe adaptarse a la organización y sus actividades. Asimismo, esta CA constituye una guía para la implementación del SMS en una organización de mantenimiento, establece textos de orientación que contienen un ordenamiento propuesto y las acciones mínimas para cumplir con los requisitos de las siguientes secciones de la RAC-24.145:

- 145.205 - Política y Objetivos de Seguridad Operacional;
- 145.210 - Gestión del Riesgo de Seguridad Operacional;
- 145.215 - Aseguramiento de la Seguridad Operacional y
- 145.220 - Promoción de la Seguridad Operacional.

Sección B – Alcance

El alcance está orientado a los siguientes aspectos:

a) Proporcionar una guía para las organizaciones que solicitan una aprobación como organización de mantenimiento o para la modificación de una aprobación existente [145.100 (b)].

b) Proporcionar una guía a las organizaciones de mantenimiento aprobadas según la RAC-24.145, para la correcta interpretación del requisito RAC 145.225

c) Proporcionar lineamientos de como cumplir de una manera aceptable con los requisitos antes listados y verificar la implementación de los requisitos del Capítulo C de la RAC-24.145 en la OMA, en los plazos máximos que establezca la DIA/ IACC.

d) La presente CA es un método aceptable de cumplimiento del requisito 145.225 "Implementación del Sistema de Gestión de Seguridad Operacional (SMS)", pero no es el único método.

Sección C – Introducción.

a) El propósito de un SMS es proporcionar a las organizaciones de mantenimiento un enfoque sistemático para gestionar la seguridad operacional. Es Diseñado para mejorar continuamente el desempeño de seguridad operacional a través de: la identificación de peligros, la recolección y el análisis de datos e información de seguridad operacional, y la evaluación continua de los riesgos de seguridad operacional. El SMS

busca proactivamente mitigar los riesgos de seguridad operacional antes de que resulten en accidentes e incidentes de aviación. Permite a los proveedores de servicios efectivamente administrar sus actividades, el rendimiento de la seguridad operacional y los recursos, al tiempo que obtiene una mayor comprensión de su contribución a Seguridad operacional de la aviación. Un SMS eficaz demuestra a los Estados la capacidad del proveedor de servicios para gestionar los riesgos de seguridad operacional y proporciona una gestión eficaz de la seguridad operacional a nivel estatal.

b) La RAC-24.145 en lo relativo al SMS establece requisitos basados en rendimiento ya que se enfoca en resultados en lugar de concentrarse únicamente en como cumplir estos requisitos. La implementación del SMS es un requisito de certificación para las organizaciones de mantenimiento que soliciten aprobación como OMA RAC-24.145, y este sistema debe implementarse en las OMAs que realicen mantenimiento en aeronaves y componentes de aeronaves, especialmente cuando prestan servicios a los explotadores de servicios aéreos.

c) La implementación de un SMS es un proceso que busca incorporar las exigencias de un Sistema de Gestión de la Seguridad Operacional (SMS). Este sistema podrá tener una mayor o menor dificultad en su diseño y funcionamiento, dependiendo de la dimensión y complejidad de la organización de mantenimiento. Sin embargo, el proceso de implementación será igual en su contenido y deberán encuadrarse en los tiempos que la DIA IACC establezca. Por casos muy especiales y justificados, la DIA IACC podrá autorizar una extensión de este plazo, bajo un estricto control de cumplimiento de las extensiones autorizadas.

d) Para una organización ya certificada este proceso requerirá de una planificación y un control detallado en su desarrollo, con el objetivo de cumplir las metas de implementación del SMS y simultáneamente no afectar las capacidades de mantenimiento y producción que posee la OMA.

e) La primera publicación del Doc. 9859, la Organización de Aviación Civil Internacional (OACI) recomendó un enfoque en etapas, por lo tanto, la implementación de un SMS maduro es un proceso que toma varios años. Esto permitirá que el SMS sea mucho más sólido a medida que se completa cada etapa de implementación. Es importante completar los procesos de gestión de seguridad operacional fundamentales antes de pasar a etapas sucesivas que impliquen procesos de mayor complejidad.

f) En la publicación del Doc. 9859 Tercera edición del año 2013, se propusieron cuatro (4) etapas de implementación del SMS. Cada etapa se asoció con varios elementos (o subelementos) según el marco de trabajo. Sin embargo, las cuatro (4) etapas recomendadas no están diseñadas para ser absolutas. Por lo tanto, los proveedores de servicio y los Estados podían elegir hacer ajustes de acuerdo a la realidad del Estado y a la dimensión y complejidad de las operaciones o circunstancias.

g) Basado en esta recomendación, se desarrollaron reglamentos y circulares de asesoramiento en donde se establecían cuatro (4) etapas (fases) con sus respectivos elementos, que fueron aplicados en los últimos años por las organizaciones de mantenimiento (Ver Tabla 1), en donde se resumían las cuatro (4) etapas (fases) de implementación del SMS y sus elementos correspondientes.

h) Las cuatro (4) etapas (fases) que se establecieron, recomendaban un tiempo total de cinco (5) años para la implementación. Sin embargo, el plazo de los cinco (5) años que se recomendó se inició en el año 2006 con la publicación del Doc. 9859 Primera edición y no comenzó en el año 2013 con la publicación del Doc. 9859 Tercera edición.

i) En el año 2013 se publicó la Primera edición del Anexo 19 sobre la gestión de la seguridad operacional, el cual en su Capítulo 4 estableció los requisitos aplicables al SMS y en su Apéndice 2 prescribió el marco de trabajo para el SMS, considerando los 4 componentes y 12 elementos que fueron tratados en los documentos previamente publicados por la OACI.

j) Posteriormente en el año 2016, la OACI publicó la Segunda edición del Anexo 19 en donde se ratifica lo concerniente a los requisitos aplicables al SMS tanto en el Capítulo 4 como en el Apéndice 3 de dicho Anexo.

k) Es importante mencionar que el Anexo 19 establece que la orientación para la implementación de un SMS en un proveedor de servicios se debe referir al Manual de gestión de seguridad operacional (SMS) Doc. 9859, por lo tanto, para la implementación del SMS en cualquier organización de mantenimiento se utilizará dicho documento para los procesos que se tengan que desarrollar.

l) El Doc. 9859 Cuarta edición del año 2018, en su Capítulo 9 ha desarrollado las guías relacionadas a los Sistemas de gestión

de seguridad operacional (SMS) aplicables a los proveedores de servicio, dentro de los cuales se encuentran las organizaciones de mantenimiento. Sin embargo, en este documento ya no se establecen las etapas (fases) que se trataron en las ediciones previas del Documento 9859. Esto, es debido a que la OACI ha considerado que desde el tiempo que se emitieron las publicaciones de orientación, las organizaciones de mantenimiento, han debido implementar la gestión de la seguridad operacional.

m) El SMS exige de un cambio en la cultura de seguridad operacional de la organización, lo cual requiere de preparación, capacitación y el entendimiento del personal sobre el sistema de gestión de seguridad operacional en general y de su participación en particular, ya que ésta será una importante herramienta de información y de compromiso que el sistema necesita para lograr sus objetivos.

n) También, necesita incorporar nuevos elementos/procesos y revisar otros existentes, (por ejemplo: organización, auditorias de calidad, prevención e investigación de accidentes) para optimizar la recolección de datos, que permita la obtención de información fidedigna para una mejor clasificación y gestión de los peligros que afectan a las actividades de la OMA, permitiendo un uso más efectivo y eficiente de los recursos disponibles, para incrementar los niveles de seguridad operacional.

o) La suma de estos objetivos debe asegurar que la organización de mantenimiento ha logrado en ese plazo, modificar su sistema de funcionamiento inicial, sin afectar la seguridad operacional en el proceso, generando una nueva capacidad de detección, análisis y gestión de los riesgos que afectan su actividad de mantenimiento, un aumento en los niveles de seguridad operacional, una integración en este tema con los explotadores de servicios aéreos con los que se relaciona, un mayor compromiso de la alta dirección y de su personal con este tema y una potencial disminución de costos, derivados de la disminución de la probabilidad de ocurrencia de incidentes o accidentes, de una optimización de los recursos que la organización invierte en su funcionamiento y de una mayor eficiencia en su accionar.

p) Por lo tanto, el proceso de implementación debe responder a una metodología secuencial donde es necesario llevar un control estricto y detallado de la ejecución del plan de

implementación desarrollado por la organización de mantenimiento y aceptado por la DIA IACC, ya que cualquier demora afectará directamente el logro de los objetivos parciales y finales del proceso.

q) Para efectos de que se mantenga un orden en la implementación del SMS y considerando que ya existían organizaciones certificadas antes de la publicación del Anexo 19 de la OACI y que aún no han completado la implementación del SMS se hace necesario que las OMAs establezcan sus faltantes (brechas) y en coordinación con la DIA / IACC presenten un plan de implementación de acuerdo a la dimensión y complejidad de la organización de mantenimiento, el cual debe cumplirse en el tiempo acordado con la DIA / IACC y éste será vigilado a fin de asegurar su cumplimiento en cada fecha acordada (Ver **Apéndice 1**).

r) Para las organizaciones certificadas antes de la publicación del Anexo 19 de la OACI y que aún no han completado la implementación del SMS, estas organizaciones deberán demostrar como mínimo que han completado la implementación de todos los elementos que se establecieron en las tres primeras etapas (fases) más los elementos de la Cuarta etapa recomendados en la Tercera edición del Doc. 9859, relacionados con:

1. integrar los procedimientos de identificación de peligros y gestión de los riesgos con el SMS
2. establecer programas de auditorías del SMS o integrarlos en los programas de auditoría internos y externos existentes y
3. establecer otros programas de revisión/estudio del SMS operacional, donde corresponda.

s) La OMA certificada de acuerdo a lo mencionado en el ítem (r), efectuar una autoevaluación y determinar el estado de los elementos que aún no se han implementado (determinar el avance de cada elemento faltante en porcentaje) y coordinar con la DIA IACC a fin de presentar el plan de implementación, el cual no deberá exceder de dieciocho (18) meses.

t) El plan de implementación debe tener metas de cumplimiento (hitos) que serán verificados por el inspector designado a la OMA, quien se asegurará de que las metas se estén cumpliendo.

u) Para las organizaciones de mantenimiento nuevas, los elementos de los componentes del SMS que deberán

ser desarrollados antes de obtener la aprobación se encuentran establecidos en la CA-24.145-002, en el MAC del requisito 145.100 (b).

Sección D – Proceso implementación.

a) Los primeros objetivos y tareas del proceso de implementación del SMS en la organización de mantenimiento nacen de la necesidad de establecer cuál es la condición en que se encuentra la organización, en relación al desarrollo de los requisitos de aceptación del SMS que deben ser implementados, de acuerdo con los requisitos reglamentarios de la RAC-24.145 aplicables.

b) Para permitir a la organización de mantenimiento y a la DIA IACC verificar el avance de los diferentes elementos que soportan la implementación del SMS, y por la conveniencia de establecer un orden y control, se continuarán utilizando únicamente los elementos y la secuencia de desarrollo de las cuatro (4) etapas (fases) de implementación propuestas en la Tercera edición del Doc. 9859, excepto los plazos propuestos.

c) Inicialmente la OMA junto con los miembros del equipo de implementación del SMS, deberán establecer el alcance de su SMS, en base a un análisis de su accionar, procesos de mantenimiento, política y objetivos del SMS, y fundamentalmente establecer las interfaces del sistema con otras organizaciones o contratistas.

Con el alcance, será posible establecer las brechas existentes entre los requisitos del SMS y las capacidades, procesos y procedimientos que posee la OMA, a fin de determinar la magnitud del trabajo a realizar, la envergadura y los costos del proceso de implementación del SMS a realizar, y la manera como este trabajo será efectuado en un plazo definido (plan de implementación).

d) Definido esto, también será necesario establecer en que tiempo se establecerán e implementaran los elementos del marco de trabajo del SMS (los tiempos variarán de acuerdo a la dimensión y complejidad de la organización de mantenimiento), cuáles serán los medios humanos y materiales que se asignarán y la estructura funcional que se ocupará para efectuar esta actividad, en forma simultánea al funcionamiento normal de la OMA, según sea aplicable.

e) Conjuntamente y por su importancia, se debe iniciar la instrucción y la comunicación del SMS en la OMA para la preparación y concientización del personal en este nuevo sistema de gestión de los riesgos en la organización y sobre la importancia de su participación en estos procesos. Estas actividades son parte del proceso de implementación y en el caso de la capacitación se irán incorporando paulatinamente los nuevos requisitos y procedimientos al programa de capacitación que la OMA tenía implementado al certificarse. Al iniciar la implementación del SMS el convencimiento de la alta dirección sobre la importancia de este sistema y su involucramiento en este proceso serán fundamentales para su éxito.

f) Este hito se completará cuando estén definidas y solucionadas estas interrogantes y se encuentre coordinado con la DIA / IACC los plazos de cumplimiento y las metas a lograr en cada una de las actividades de implementación del SMS (plan de implementación).

g) En el siguiente paso, la organización que ya definió como efectuará la implementación de su SMS, establecerá la política y los objetivos que orientarán el desarrollo de la documentación y procedimientos, asimismo definirá las responsabilidades internas que deberán ser asumidas en todos los niveles de la organización como consecuencia de incorporar este nuevo sistema. Esto último requiere ser difundido por el gerente responsable, dado su importancia y trascendencia y por la necesidad de hacer comprender que la implementación del SMS es responsabilidad de toda la organización.

h) Una vez que la organización ha definido la política, objetivos y las responsabilidades internas, se dará inicio a la confección del manual del SMS (MSMS) y de los primeros documentos orientados al funcionamiento interno de la OMA. Asimismo, se designará a la junta de revisión de seguridad operacional (SRB) y al grupo de acción de seguridad operacional (SAG), cuando sea aplicable. Durante esta fase y de ser necesario, la organización de mantenimiento también desarrollará el plan de respuesta ante emergencias para accidentes e incidentes en coordinación con los explotadores de aeronaves y otras emergencias de aviación, según sea aplicable. Este plan deberá estar coordinado de forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que la organización deba interactuar al suministrar sus servicios o productos.

i) El siguiente paso se corresponde con establecer los elementos que tiene como objetivo establecer procesos de gestión de riesgos del marco de trabajo del SMS. Con el establecimiento de estos elementos la OMA estará lista para recopilar datos de seguridad operacional y realizar análisis basados en la información obtenida mediante diversos sistemas de notificación.

j) Se deben implementar los procedimientos e indicadores con que deberá trabajar la nueva oficina o departamento creado bajo la dirección de un responsable de SMS, nominado por el gerente responsable, que está participando en la implementación. Con estas herramientas y el desarrollo de la documentación en ejecución es posible empezar a recibir y procesar en la oficina o departamento de seguridad operacional la información de SMS de la OMA.

k) También, para las organizaciones de mantenimiento ya certificadas, es el momento de incorporar al sistema toda aquella información que la OMA posee de los accidentes e incidentes en los que ha estado involucrado previamente, con sus correspondiente evaluaciones y acciones correctivas, las acciones de prevención desarrolladas y las auditorias de calidad internas y externas que la OMA realiza como parte de los requisitos de calidad que debe cumplir desde su certificación. Esta información permitirá el desarrollo de indicadores de alta gravedad/baja probabilidad y alta probabilidad/baja gravedad, y empezar a completar las bases de información o de datos de seguridad de la OMA. La DIA / IACC deberá aceptar los indicadores presentados por la OMA, desarrollados en base a la experiencia y sustentados en datos de seguridad operacional.

l) Los elementos de la implementación y funcionamiento maduro del SMS se corresponden a la consolidación del sistema y a la incorporación plena de esta nueva organización interna de SMS (sección o departamento) en la OMA; a la consolidación de una nueva cultura de trabajo con responsabilidades, procedimientos y manuales complementarios en la organización; indicadores que permitan orientar su desempeño con una optimización de los recursos asignados y una mejora potencial en la seguridad operacional en el producto o servicio que entrega, en su imagen corporativa, en su relación con sus operadores, y subcontratistas; y finalmente en el compromiso de su personal con la OMA y su sistema de seguridad operacional.

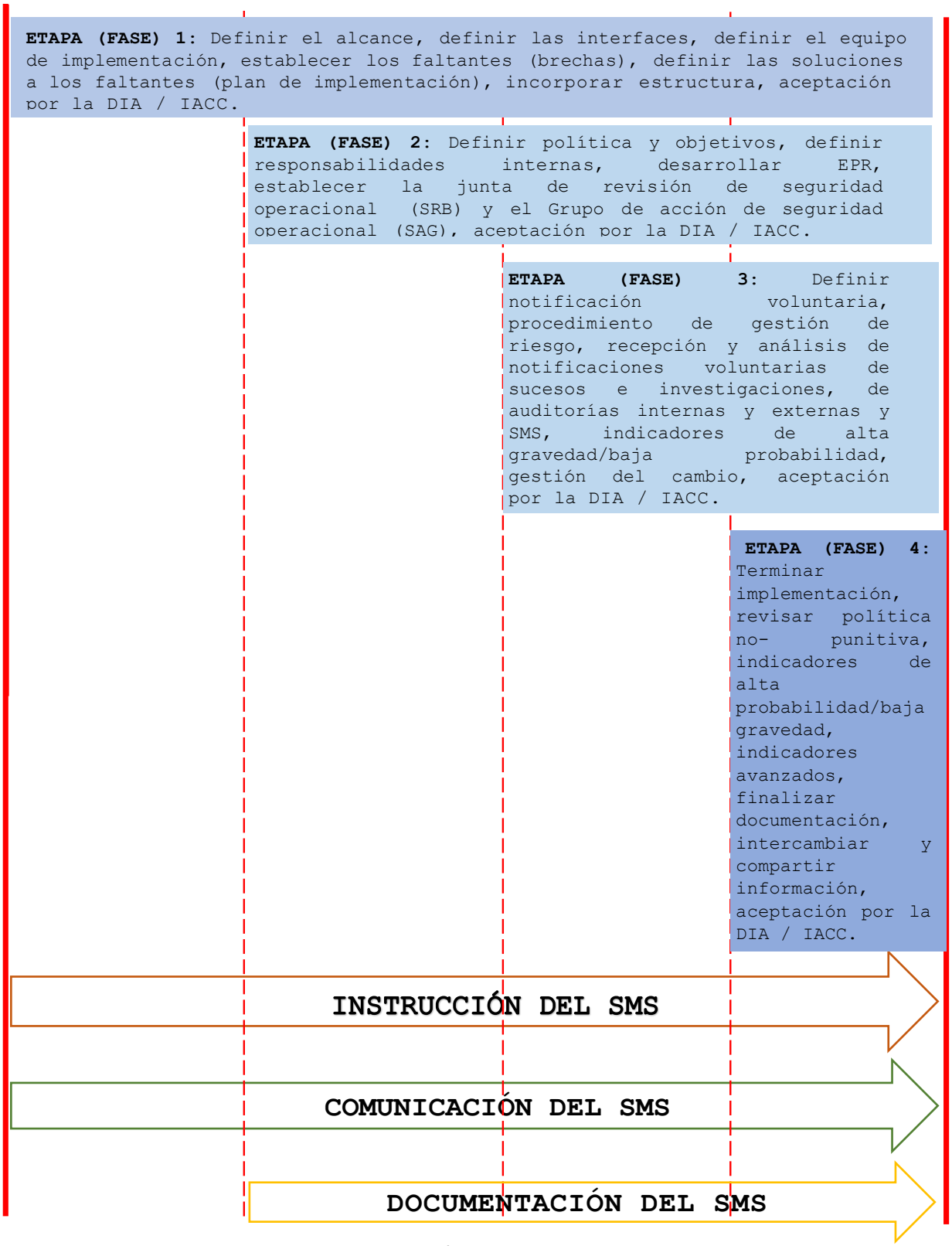
m) Para las OMA ya certificadas, todo el desarrollo efectuado deberá mostrar sus resultados, así como su efectividad y eficiencia. Será la demostración de si la OMA efectuó en buena forma la incorporación del SMS a sus actividades normales, luego de su certificación inicial previa.

n) También, se debe asegurar que los procesos de capacitación normales de la OMA incorporen en forma permanente estos nuevos temas de SMS y se mantenga la motivación, compromiso y participación del personal en el sistema, mediante una buena difusión de los logros alcanzados, el compromiso permanente de la alta dirección y la retroalimentación de los análisis de causa raíz realizados a la información de peligros por ellos informados, junto a las acciones tomadas para solucionarlos, en los casos que lo amerite.

o) Una vez completado el plan de implementación aceptado por la DIA / IACC se culminará el proceso de aceptación, al demostrar a la DIA / IACC que se ha completado en forma efectiva y eficiente la implementación del SMS, de acuerdo a la dimensión y complejidad de la OMA.

En la siguiente figura (**Figura 1**) se representan las cuatro etapas de implementación del sistema SMS en una organización de mantenimiento.

Figura 1. Implementación del SMS.



Sección E – Marco de trabajo del SMS

a) Independiente del tamaño y la complejidad de la organización de mantenimiento, todos los elementos del marco de trabajo del SMS son aplicables. La implementación debe adaptarse a la organización y sus actividades.

b) El Marco de trabajo se compone de cuatro (4) componentes y doce (12) elementos:

COMPONENTE	ELEMENTO
1.Política y objetivos de seguridad operacional	1.1. Compromiso de la Dirección
	1.2. Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional
	1.3. Designación del personal clave de seguridad operacional
	1.4. Coordinación de la planificación de respuestas ante emergencias
	1.5. Documentación SMS
2.Gestión de riesgos de seguridad operacional	2.1 Identificación de peligros
	2.2 Evaluación y mitigación de riesgos de seguridad operacional
3.Aseguramiento de la seguridad operacional	3.1 Observación y medición del rendimiento en materia de seguridad
	3.2 Gestión del cambio
	3.3 Mejora continua del SMS
4.Promoción de la seguridad operacional	4.1 Instrucción y educación
	4.2 Comunicación de la seguridad operacional

1. COMPONENTE 1: POLITICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

a) El primer componente del marco del SMS se centra en la creación de un entorno de gestión de la seguridad operacional efectivo. Se basa en una política y objetivos de seguridad operacional que establecen el compromiso de la alta dirección con la seguridad operacional, sus objetivos y la estructura organizacional de apoyo.

b) El compromiso de la gerencia y el liderazgo en seguridad operacional es clave para la implementación de un SMS eficaz y se afirma a través de la política de seguridad operacional y el establecimiento de objetivos de seguridad operacional. El compromiso de la gerencia con la seguridad operacional se demuestra a través de la toma de decisiones gerenciales y la asignación de recursos; estas decisiones y acciones siempre deben ser coherentes con la política y los objetivos de seguridad operacional para cultivar una cultura de seguridad operacional positiva.

c) La política de seguridad operacional deberá ser desarrollada y respaldada por la alta gerencia, y debe ser firmada por el gerente responsable. El personal de seguridad clave y, cuando corresponda, los órganos de representación del personal (foros de empleados, sindicatos) deberían ser consultados en el desarrollo de la política y los objetivos de seguridad operacional para promover un sentido de responsabilidad compartida.

1.1. Compromiso y responsabilidad de la gerencia

1.1.1 Política de seguridad operacional

1.1.1.1 La política de seguridad operacional deberá ser endosada (firmada) visiblemente por el gerente responsable de la organización de mantenimiento. El "endoso visible" se refiere a hacer que la política de seguridad operacional sea visible para el resto de la organización de mantenimiento. Esto puede hacerse a través de cualquier medio de comunicación (página intranet de la organización, avisos, documentos de acceso a todo el personal de la organización, entre otros) y mediante la alineación de las actividades con la política de seguridad operacional.

1.1.1.2 Es responsabilidad de la gerencia comunicar la política de seguridad operacional en toda la organización para

garantizar que todo el personal comprenda y trabaje de acuerdo con la política de seguridad operacional establecida.

1.1.1.3 Para reflejar el compromiso de la organización con la seguridad operacional, la política debe incluir un compromiso para:

a) mejorar continuamente el nivel de rendimiento de seguridad operacional;

b) promover y mantener una cultura de seguridad operacional positiva dentro de la organización;

c) cumplir con todos los requisitos reglamentarios aplicables;

d) proporcionar los recursos necesarios para entregar un producto o servicio seguro;

e) garantizar que la seguridad sea una responsabilidad primaria de todos los gerentes; y

f) garantizar que se entienda, implemente y mantenga en todos los niveles.

1.1.1.4 La política de seguridad operacional también deberá hacer referencia al sistema de notificaciones de seguridad operacional para alentar la comunicación de problemas de seguridad operacional e informar al personal sobre la política disciplinaria no punitiva aplicada en caso de eventos o problemas de seguridad operacional que se informan.

1.1.1.5 La política disciplinaria se usa para determinar si se ha producido un error o se ha cometido una infracción, de modo que la organización pueda establecer si se debe tomar alguna medida disciplinaria. Para asegurar el trato justo de las personas involucradas, es esencial que los responsables de tomar esa determinación cuenten con conocimientos técnicos necesarios para que el contexto del evento pueda ser considerado en su totalidad.

1.1.1.6 Una política sobre la protección de los datos y la información de seguridad operacional, así como de quienes hacen las notificaciones, puede tener un efecto positivo en la cultura de notificar. La organización de mantenimiento debe desidentificar a las personas que notifican algún problema de seguridad operacional de forma voluntaria para permitir que se lleven a cabo análisis de seguridad operacional significativos sin tener que implicar al personal. Debido a que las ocurrencias principales pueden invocar procesos y procedimientos fuera del SMS de la organización de

mantenimiento, la autoridad estatal pertinente puede no permitir la pronta identificación de las notificaciones en todas las circunstancias. No obstante, una política que permita la desidentificación adecuada de las notificaciones puede mejorar la calidad de los datos recopilados.

1.1.2 Objetivos de seguridad operacional

1.1.2.1 Teniendo en cuenta su política de seguridad operacional, la organización de mantenimiento también deberá establecer objetivos de seguridad operacional para definir lo que pretende lograr con respecto a los resultados de seguridad operacional. Los objetivos de seguridad operacional deberán ser declaraciones breves y de alto nivel de las prioridades de seguridad operacional de la organización y deben abordar sus riesgos de seguridad operacional más significativos. Los objetivos de seguridad operacional pueden incluirse en la política de seguridad operacional (o documentarse por separado) y requieren el establecimiento de objetivos de seguridad que definan lo que la organización pretende lograr en términos de gestión de seguridad operacional. Los indicadores de rendimiento de seguridad operacional (SPI) y las metas de rendimiento de seguridad operacional (SPT) son necesarios para monitorear el logro de estos objetivos de seguridad operacional y se detallan en el Componente 3 del marco de trabajo del SMS.

1.1.2.2 La política y los objetivos de seguridad operacional deben revisarse periódicamente para garantizar que permanezcan actualizados. Por ejemplo, un cambio en el gerente responsable requeriría su revisión.

1.2. Responsabilidad y rendición de cuentas de seguridad operacional

1.2.1 El gerente responsable de la organización de mantenimiento es la persona que tiene la máxima autoridad sobre la operación segura de la OMA. El gerente responsable es quien establece y promueve la política y los objetivos de seguridad operacional que inculcan la seguridad operacional como un valor central de la organización. El gerente responsable debe:

- tener la autoridad para tomar decisiones en nombre de la organización;
- tener el control de los recursos, tanto financieros como humanos; y

- ser responsable de garantizar que se tomen las medidas adecuadas para abordar los problemas y los riesgos de seguridad operacional, y responder a los accidentes e incidentes.

1.2.2 Puede haber desafíos para que la organización de mantenimiento identifique a la persona para ocupar el cargo de gerente responsable, especialmente en grandes organizaciones de mantenimiento (complejas) con múltiples certificaciones y aprobaciones. Es importante que la persona seleccionada esté ubicada organizacionalmente en el nivel más alto de la organización, asegurando así que se tomen las decisiones estratégicas correctas de seguridad operacional.

1.2.3 Se requiere que la organización de mantenimiento identifique al gerente responsable, colocando la responsabilidad del rendimiento de seguridad operacional general a un nivel en la organización con la autoridad para tomar medidas para garantizar que el SMS sea efectivo. Deben definirse las responsabilidades específicas de seguridad operacional de todos los miembros de la gerencia y su rol en relación con el SMS debe reflejar cómo pueden contribuir a una cultura de seguridad operacional positiva. Las responsabilidades de seguridad operacional, los deberes y las autoridades deben documentarse y comunicarse en toda la organización. Las responsabilidades de seguridad operacional de los gerentes deben incluir la asignación de los recursos humanos, técnicos, financieros u otros necesarios para el desempeño efectivo y eficiente del SMS.

Nota. – El término "rendición de cuentas" se refiere a obligaciones que no pueden ser delegadas. El término "responsabilidades" se refiere a las funciones y actividades que pueden delegarse.

1.2.4 En el caso donde un SMS se aplica a varias aprobaciones diferentes, que son todas, parte de la misma entidad legal, podría haber un solo ejecutivo o gerente responsable. Donde esto no sea posible, se deben identificar individualmente a los ejecutivos o gerentes responsables para la aprobación de cada organización y se deben definir líneas claras de responsabilidad; también es importante identificar cómo se coordinarán sus rendiciones de cuentas de seguridad operacional.

1.2.5 Una de las maneras más efectivas en que el gerente responsable puede involucrarse visiblemente, es liderando reuniones de seguridad operacional ejecutivas regulares. Como

son los máximos responsables de la seguridad operacional de la organización, participar activamente en estas reuniones permite al gerente responsable:

a) revisar los objetivos de seguridad operacional;

b) monitorear el rendimiento de seguridad operacional y el logro de los objetivos de seguridad operacional;

c) tomar decisiones de seguridad operacional oportunas;

d) asignar recursos apropiados;

e) mantener la rendición de cuentas de los gerentes para las responsabilidades, rendimiento y los plazos de implementación de seguridad operacional; y

f) ser visto por todo el personal como un gerente responsable que está interesado y a cargo de la seguridad operacional.

1.2.6 El gerente responsable no suele participar en las actividades cotidianas de la organización de mantenimiento ni en los problemas que se presentan en el lugar de trabajo. Él debe garantizar que exista una estructura organizacional adecuada para gestionar y operar el SMS. La responsabilidad de la gestión de seguridad operacional es a menudo delegada en el equipo de alta gerencia y otro personal clave de seguridad operacional. Aunque se puede delegar la responsabilidad de la operación diaria del SMS, el gerente responsable no puede delegar la responsabilidad de rendir cuenta del sistema ni se pueden delegar decisiones sobre riesgos de seguridad operacional. Por ejemplo, las siguientes responsabilidades de rendición de cuentas de seguridad no se pueden delegar:

a) garantizar que las políticas de seguridad operacional sean apropiadas y se comuniquen;

b) garantizar la asignación necesaria de los recursos (financiación, personal, capacitación, adquisición); y

c) establecimiento de los límites de riesgo de seguridad operacional aceptables y asignación de controles necesarios.

1.2.7 Es apropiado que el gerente responsable tenga las siguientes responsabilidades de rendición de cuenta de seguridad operacional:

a) proporcionar suficientes recursos financieros y humanos para la implementación adecuada de un SMS efectivo;

b) promover una cultura de seguridad operacional positiva;

c) establecer y promover la política de seguridad operacional;

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

e) asegurar que el SMS se implemente de manera adecuada y que cumpla con los requisitos; y

f) ver a la mejora continua del SMS.

1.2.8 La autoridad del gerente responsable incluye tener la autoridad final, pero no se limitan a:

a) para la resolución de todos los problemas de seguridad operacional; y

b) sobre las operaciones bajo el certificado/aprobación de la organización de mantenimiento, incluida la autoridad para detener la operación o actividad.

1.2.9 Deberá definirse la autoridad para tomar decisiones con respecto a la tolerabilidad del riesgo de seguridad operacional. Esto incluye quién puede tomar decisiones sobre la aceptabilidad de los riesgos, así como la autoridad para acordar que se puede implementar un cambio. La autoridad puede asignarse a un individuo, un puesto de gestión o un comité.

1.2.10 La autoridad para tomar decisiones de tolerabilidad de los riesgos de seguridad deberá ser proporcional a la autoridad general de toma de decisiones y asignación de recursos del gerente. Un gerente de nivel inferior (o grupo de gestión) puede estar autorizado para tomar decisiones de tolerabilidad hasta cierto nivel. Los niveles de riesgo que exceden la autoridad del gerente deben ser escalados para su consideración a un nivel de gestión más alto con mayor autoridad.

1.2.11 Todo lo mencionado debe ser considerado en el manual de SMS en las funciones y responsabilidades del gerente responsable.

Rendición de cuentas y responsabilidades

1.2.12 La rendición de cuentas y responsabilidades de todo el personal, personal de gestión y personal operativo, involucradas en tareas relacionadas con la seguridad operacional que apoyan la entrega de productos y operaciones seguras deben estar claramente definidas. Las responsabilidades de seguridad operacional deben centrarse en

la contribución del miembro del personal al desempeño de seguridad operacional de la organización (los resultados de seguridad de la organización de mantenimiento). La gestión de la seguridad operacional es una función fundamental; como tal, cada gerente tiene un grado de participación en la operación del SMS.

1.2.13 Todas las responsabilidades de rendición de cuenta, responsabilidades y autoridades definidas deben indicarse en la documentación de SMS de la organización de mantenimiento y deben comunicarse a toda la organización. Las responsabilidades de rendición de cuenta y responsabilidades de seguridad operacional de cada gerente son componentes integrales de sus descripciones de trabajo. Esto también debería capturar las diferentes funciones de gestión de la seguridad entre los gerentes de línea y el gerente de seguridad operacional (ver 1.3 para más detalles).

1.2.14 Las líneas de responsabilidad de rendición de cuenta de seguridad operacional en toda la organización y cómo se definen dependerán del tipo y la complejidad de la organización y de sus métodos de comunicación preferidos. Por lo general, las responsabilidades de rendición de cuenta y responsabilidades de seguridad operacional se reflejarán en los organigramas, los documentos que definen las responsabilidades del departamento y las descripciones de funciones o roles de trabajo del personal.

1.2.15 La organización de mantenimiento debe tratar de evitar conflictos de intereses entre las responsabilidades de seguridad operacional de los miembros del personal y sus otras responsabilidades organizativas. Deben asignar sus responsabilidades de rendición de cuenta y responsabilidades de SMS, de manera que minimice cualquier superposición y / o brecha.

Rendición de cuentas y responsabilidades con respecto a las organizaciones externas

1.2.16 La organización de mantenimiento es responsable del rendimiento de seguridad operacional de las organizaciones externas donde hay una interfaz de SMS. La organización de mantenimiento puede ser responsable de la rendición de cuentas de seguridad operacional de los productos o servicios proporcionados por organizaciones externas que respaldan sus actividades, incluso si las organizaciones externas no están

obligadas a tener un SMS. Es esencial que los SMS de la organización de mantenimiento interactúen con los sistemas de seguridad operacional de cualquier organización externa que contribuya a la entrega segura de sus productos o servicios.

1.3. Nombramiento del personal clave de seguridad operacional

1.3.1 El nombramiento de una persona o personas competentes para cumplir el rol de Responsable de seguridad operacional es esencial para un SMS efectivamente implementado y en funcionamiento. El Responsable de seguridad operacional puede ser identificado por diferentes títulos. Para los propósitos de esta circular de asesoramiento, se usa el término genérico "gerente de seguridad operacional" y se refiere a la función, no necesariamente al individuo. La persona que lleva a cabo la función de gerente de seguridad operacional es responsable ante el gerente responsable por el rendimiento del SMS y por la entrega de servicios de seguridad operacional a los otros departamentos de la organización.

1.3.2 El gerente de seguridad operacional asesora al gerente responsable y a los gerentes de línea en asuntos de gestión de seguridad operacional, y es responsable de coordinar y comunicar los asuntos de seguridad operacional dentro de la organización, así como con los miembros externos de la comunidad aeronáutica. Las funciones del gerente de seguridad operacional incluyen, pero no están limitadas a:

a) administrar el plan de implementación de SMS en nombre del gerente responsable (en la implementación inicial);

b) realizar / facilitar la identificación de peligros y el análisis de riesgos de seguridad operacional;

c) monitorear acciones correctivas y evaluar sus resultados;

d) proporcionar informes periódicos sobre el rendimiento de seguridad operacional de la organización;

e) mantener documentación y registros de SMS;

f) planificar y facilitar la instrucción de seguridad operacional del personal;

g) proporcionar asesoramiento independiente sobre problemas de seguridad operacional;

h) las preocupaciones de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones de la organización de mantenimiento dirigidas a la entrega de

productos y servicios; y

i) coordinar y comunicar (en nombre del gerente responsable) con la AAC del Estado y otras autoridades estatales, según sea necesario, acerca de problemas relacionados con la seguridad operacional.

Nota: Todas estas funciones deberán establecerse en el manual de SMS.

1.3.3 En la mayoría de las organizaciones, se designa a un individuo como el gerente de seguridad operacional. Dependiendo del tamaño, naturaleza y complejidad de la organización, la función del gerente de seguridad operacional puede ser una función exclusiva o puede combinarse con otras funciones. Además, algunas organizaciones de mantenimiento pueden necesitar asignar el rol a un grupo de personas. La organización de mantenimiento debe asegurarse de que la opción elegida no genere ningún conflicto de intereses. Siempre que sea posible, el gerente de seguridad operacional no deberá involucrarse directamente en la entrega del producto o servicio, pero deberá tener un conocimiento práctico de estos. El nombramiento también debe considerar posibles conflictos de interés con otras tareas y funciones. Tales conflictos de interés podrían incluir:

a) competencia por la financiación (por ejemplo, el gerente financiero es el gerente de seguridad operacional);

b) prioridades conflictivas para los recursos; y

c) cuando el gerente de seguridad operacional tiene una función operativa y su capacidad para evaluar la efectividad de SMS de las actividades operacionales en las que está involucrado.

1.3.4 En los casos donde la función se asigna a un grupo de personas (por ejemplo, cuando las organizaciones de mantenimiento extienden sus SMS a través de múltiples actividades) una de las personas debe ser designada como gerente de seguridad operacional "principal" para mantener una línea directa e inequívoca con el gerente responsable.

1.3.5 Las competencias para un gerente de seguridad operacional deben incluir, entre otras, las siguientes:

a) experiencia en gestión de seguridad operacional / calidad;

b) experiencia operativa relacionada con el producto o servicio provisto por la organización de mantenimiento;

c) antecedentes técnicos para comprender los sistemas que

respaldan las operaciones o producto / servicio provisto;

d) habilidades interpersonales;

e) habilidades analíticas y de resolución de problemas;

f) habilidades de gestión de proyectos;

g) habilidades de comunicación oral y escrita; y

h) una comprensión de los factores humanos.

Nota: Si la organización de mantenimiento lo considera necesario, los requisitos de competencia los puede desarrollar en el manual de SMS.

1.3.6 Dependiendo del tamaño, naturaleza y complejidad de la organización, el personal adicional puede apoyar al gerente de seguridad operacional. El gerente de seguridad operacional y el personal de apoyo son responsables de garantizar la recopilación y el análisis oportunos de los datos de seguridad operacional y la distribución apropiada dentro de la organización de mantenimiento de la información de seguridad operacional relacionada, de manera que se puedan tomar decisiones y controles de riesgos de seguridad operacional, según sea necesario.

1.3.7 La organización de mantenimiento deberá establecer comités de seguridad operacional adecuados para apoyar las funciones de SMS en toda la organización. Esto debería incluir determinar quién debería participar en el comité de seguridad operacional y la frecuencia de las reuniones.

1.4. Coordinación del plan de respuesta ante emergencia (ERP)

1.4.1. Por definición, una emergencia es una situación repentina y no planificada o un evento que requiere una acción inmediata. La coordinación de la planificación de respuesta ante emergencias se refiere a la planificación de actividades que tienen lugar dentro de un período de tiempo limitado durante una situación de emergencia operacional de aviación no planificada. Un plan de respuesta ante emergencia (ERP) es un componente integral del proceso de gestión de riesgos de seguridad operacional (SRM) de una organización de mantenimiento para abordar emergencias, crisis o eventos relacionados en donde la organización tenga que participar.

Cuando existe la posibilidad de que las operaciones o actividades de aviación de un explotador aéreo, al cual la organización de mantenimiento le brinda sus servicios, se vean

comprometidas por emergencias como una emergencia de salud pública / pandemia, estos escenarios también deben abordarse en el ERP, según corresponda. El ERP debe abordar las emergencias previsibles identificadas a través del SMS e incluir acciones, procesos y controles atenuantes para gestionar de manera efectiva las emergencias relacionadas con la aviación.

1.4.2. El objetivo general del ERP es la continuación segura de las operaciones y el retorno a las operaciones normales tan pronto como sea posible. Esto debería garantizar una transición ordenada y eficiente de las operaciones normales a las de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de autoridad. Incluye el período de tiempo requerido para restablecer las operaciones "normales" después de la emergencia. El ERP identifica las acciones que deberá realizar el personal responsable durante una emergencia. La mayoría de las emergencias requerirán una acción coordinada entre diferentes organizaciones, posiblemente con otros proveedores de servicios y con otras organizaciones externas, como los servicios de emergencia no relacionados con la aviación. El ERP deberá ser fácilmente accesible para el personal clave apropiado, así como para las organizaciones externas coordinadoras.

1.4.3. La coordinación de la planificación de respuesta ante emergencias se aplica solo a los proveedores de servicios requeridos a establecer y mantener un ERP como es el caso de los aeropuertos y explotadores aéreos. Sin embargo, las organizaciones de mantenimiento que brindan soporte de mantenimiento a los explotadores aéreos o que tienen sus instalaciones dentro de un aeropuerto, se encargarán de brindar su apoyo en los planes de respuestas ante emergencias de dichos proveedores de servicio. Para ello, se deberán establecer los procedimientos en donde se detallen funciones y responsabilidades que deberán cumplirse en caso de un accidente o incidente grave en el cual se solicite su colaboración.

1.4.4. Una organización de mantenimiento que realiza trabajos de mantenimiento a componentes de aeronaves no es necesario que tenga un plan de respuesta ante emergencias.

1.4.5. En el **Apéndice 4**, se presenta el contenido de un plan de respuesta ante emergencias (ERP).

1.3.8 El comité de seguridad operacional de alto nivel, a veces referido como junta de revisión de seguridad operacional (SRB, por sus siglas en ingles), incluye al gerente responsable y los

gerentes, con el gerente de seguridad operacional participante en carácter de asesor. El SRB es estratégico y se ocupa de cuestiones de alto nivel relacionadas con las políticas, la asignación de recursos y el monitoreo del rendimiento organizacional. La SRB monitorea:

a) La efectividad del SMS;

b) respuesta oportuna de las acciones de control de riesgos de seguridad operacional necesarias;

c) el rendimiento de seguridad operacional contra la política y los objetivos de seguridad operacional de la organización;

d) la efectividad general de las estrategias de mitigación de riesgos de seguridad operacional;

e) la eficacia de los procesos de gestión de la seguridad operacional de la organización de mantenimiento que apoyan:

1) la prioridad organizativa declarada de la gestión de la seguridad y,

2) promoción de la seguridad en toda la organización.

Nota: Este SRB debe ser establecido en organizaciones de mantenimiento de grandes organizaciones de mantenimiento y podría establecerse también en organizaciones de mantenimiento medianas. Para determinar si una organización es pequeña, mediana o grande de acuerdo a su dimensión y la complejidad se debe recurrir a la CA-24-145-002.

1.3.9 Una vez que el comité de seguridad operacional de más alto nivel haya desarrollado una dirección estratégica, la implementación de las estrategias de seguridad operacional debería coordinarse en toda la organización. Esto se puede lograr creando un grupo de acción de seguridad operacional (SAG, por sus siglas en inglés) que esté más centrado en las operaciones. Los SAG normalmente están compuestos por gerentes y personal de primera línea y están presididos por un gerente designado. Los SAG son entidades tácticas que se ocupan de cuestiones de implementación específicas según la dirección del SRB. El SAG:

a) monitorea el rendimiento de la seguridad operacional dentro de las áreas funcionales de la organización y asegura que se lleven a cabo las actividades adecuadas de la gestión de riesgos de seguridad operacional (SRM);

b) revisa los datos de seguridad operacional disponibles e identifica la implementación de las estrategias apropiadas de control de riesgos de seguridad operacional y asegura que se brinde retroalimentación a los empleados;

c) evalúa el impacto de seguridad operacional relacionado con la introducción de cambios operacionales o nuevas tecnologías;

d) coordina la implementación de cualquier acción relacionada con los controles de riesgos de seguridad operacional y asegura que las acciones se tomen con prontitud; y

e) revisa la efectividad de los controles de riesgo de seguridad operacional.

Nota: Este SAG debe ser establecido en grandes organizaciones de mantenimiento y podría establecerse también en organizaciones de mantenimiento medianas. Para determinar si una organización es pequeña, mediana o grande de acuerdo a su dimensión y la complejidad se debe recurrir a la CA-24-145-002.

1.5. Documentación del SMS

1.5.1 El manual de SMS también sirve como una herramienta de comunicación de seguridad operacional primaria entre la organización de mantenimiento y las partes interesadas clave en seguridad operacional (por ejemplo, la DIA IACC con el propósito de la aceptación reglamentaria, la evaluación y el seguimiento posterior del SMS). El manual de SMS puede ser un documento independiente, o puede estar integrado con otros documentos organizacionales (o documentación) mantenidos por la organización de mantenimiento. Cuando ya se abordan los detalles de los procesos de SMS de la organización en los documentos existentes, basta con referencias cruzadas apropiadas a dichos documentos. Este manual o documento de SMS deberá mantenerse actualizado. Como manual controlado, se requiere de la aceptación de la DIA / IACC antes de realizar modificaciones significativas.

1.5.2 El manual de SMS debe incluir una descripción detallada de las políticas, procesos y procedimientos del proveedor del servicio, que incluyen:

a) política y objetivos de seguridad de seguridad operacional;

b) referencia a cualquier requisito de SMS reglamentario aplicable;

c) descripción del sistema;

d) rendición de cuentas de seguridad operacional y personal de clave de seguridad operacional;

e) procesos y procedimientos del sistema de notificación de seguridad operacional voluntaria y obligatoria;

f) procesos y procedimientos de identificación de peligros y evaluación de riesgos de seguridad operacional;

g) procedimientos de investigación de seguridad operacional;

h) procedimientos para establecer y monitorear indicadores de rendimiento de seguridad operacional;

i) procesos y procedimientos de instrucción y comunicación de SMS;

j) procesos y procedimientos de comunicación de seguridad operacional;

k) procedimientos de auditoría interna;

l) procedimientos de gestión del cambio;

m) procedimientos de gestión de documentación de SMS y,

n) cuando corresponda, coordinación de la planificación de respuesta ante emergencias.

1.5.3 En el **Apéndice 4** se presenta una guía para el desarrollo de un Manual de SMS.

1.5.4 La documentación de SMS también incluye la compilación y el mantenimiento de los registros operativos que corroboran la existencia y el funcionamiento continuo del SMS. Los registros operativos son los resultados de los procesos y procedimientos de SMS, como la gestión de riesgos de seguridad operacional (SRM) y las actividades de seguridad operacional. Los registros operacionales de SMS deben almacenarse y mantenerse de acuerdo con los períodos de retención existentes. Los registros operativos típicos de SMS deberían incluir:

a) registro de peligros y notificaciones de peligros / seguridad operacional;

b) SPI y gráficos relacionados;

c) registro de evaluaciones de riesgos de seguridad operacional completados;

d) revisión interna del SMS o registros de auditoría;

e) registros de auditoría interna;

f) registros de SMS / registros de instrucción de seguridad operacional;

g) minutas de reuniones del comité de seguridad operacional SMS;

h) plan de implementación de SMS (durante la implementación

inicial) y,

i) análisis de brechas para apoyar el plan de implementación.

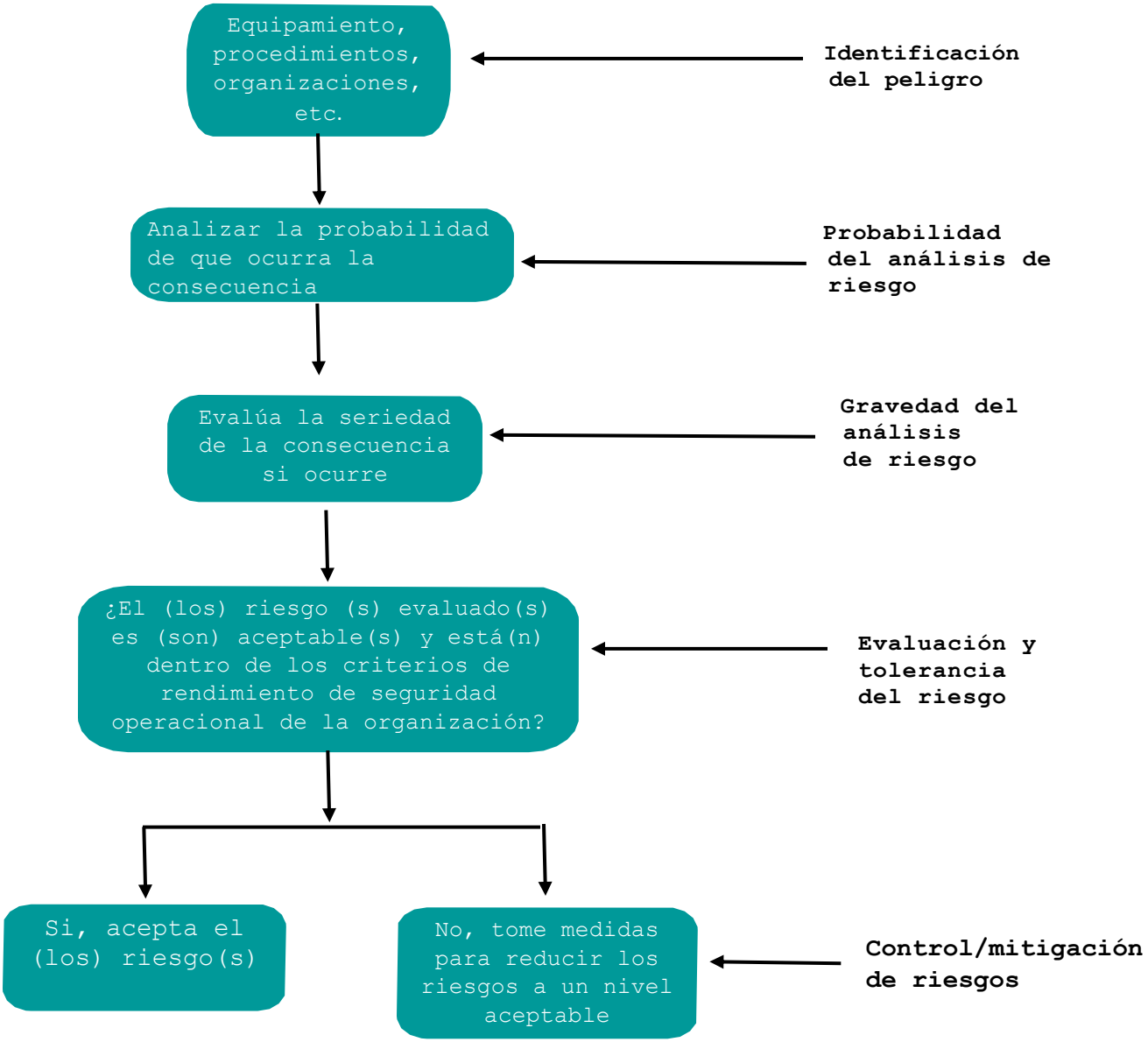
2. COMPONENTE 2: GESTIÓN DEL RIESGO DE LA SEGURIDAD OPERACIONAL

a) Las organizaciones de mantenimiento deberán asegurarse de que están administrando sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional (SRM por sus siglas en ingles), que incluye la identificación de peligros, la evaluación de riesgos de seguridad y la mitigación de riesgos de seguridad operacional.

b) El proceso de SRM identifica sistemáticamente los peligros que existen en el contexto de la entrega de sus productos o servicios. Los peligros pueden ser el resultado de sistemas que son deficientes en su diseño, función técnica, interfaz humana o interacciones con otros procesos y sistemas. También pueden ser el resultado de una falla de los procesos o sistemas existentes para adaptarse a los cambios en el entorno operativo dela organización de mantenimiento. El análisis cuidadoso de estos factores a menudo puede identificar peligros potenciales en cualquier punto de la operación o ciclo de vida de la actividad.

c) Comprender el sistema y su entorno operativo es esencial para lograr un alto rendimiento de seguridad operacional. Tener una descripción detallada del sistema que defina el sistema y sus interfaces ayudará. Los peligros pueden identificarse a lo largo del ciclo de vida operacional desde fuentes internas y externas. Las evaluaciones de riesgos de seguridad operacional y las medidas de mitigación de riesgos de seguridad operacional deberán revisarse continuamente para garantizar que sigan siendo efectivas.

Figura 2. El proceso de gestión de riesgos de la seguridad operacional



2.1. Identificación del peligro

2.1.1 La identificación del peligro es el primer paso en el proceso de SRM. La organización de mantenimiento deberá desarrollar y mantener un proceso formal para identificar los peligros que podrían afectar la seguridad operacional en todas las áreas de operación y actividades. Esto incluye equipos, instalaciones y sistemas. Cualquier peligro relacionado con la seguridad operacional de la organización de mantenimiento identificado y controlado es beneficioso para la seguridad operacional de la operación. También es importante considerar los peligros que pueden existir como resultado de las interfaces de SMS con organizaciones externas.

Fuentes para la identificación de peligros

2.1.2 Hay una variedad de fuentes para la identificación de peligros, internas o externas a la organización. Algunas fuentes internas incluyen:

- Monitoreo normal de la operación; se utilizan técnicas de observación para monitorear las operaciones y actividades diarias.

- Sistemas de notificación de seguridad operacional voluntarios y obligatorios; esto proporciona a todos, incluido el personal de organizaciones externas, la oportunidad de notificar los peligros y otros problemas de seguridad operacional a la organización.

- Auditorías; estas pueden usarse para identificar peligros en la tarea o proceso que se audita. Estos también deberían coordinarse con los cambios organizacionales para identificar los peligros relacionados con la implementación del cambio.

- Retroalimentación de la instrucción; la instrucción que es interactiva (bidireccional) puede facilitar la identificación de nuevos peligros por parte de los participantes.

- Investigaciones de seguridad operacional de la organización de mantenimiento; peligros identificados en la investigación de seguridad operacional interna e

informes de seguimiento de accidentes / incidentes.

2.1.3 Los ejemplos de fuentes externas para identificación de peligros incluyen:

- Informes de accidentes e incidentes de aviación; al revisar los informes de accidentes o incidentes, esto puede estar relacionado con accidentes o incidentes en el mismo Estado o con un tipo de aeronave, región o entorno operativo similar.

- Sistemas estatales de notificación obligatorios y voluntarios de seguridad operacional; algunos Estados proporcionan resúmenes de las notificaciones de seguridad operacional recibidos de los proveedores de servicios.

- Auditorías de supervisión estatal y auditorías de terceros; las auditorías externas a veces pueden identificar peligros. Estos pueden estar documentados como un peligro no identificado o capturados de forma menos obvia dentro de un hallazgo de auditoría.

- Asociaciones comerciales y sistemas de intercambio de información; muchas asociaciones comerciales y grupos industriales pueden compartir datos de seguridad operacional que pueden incluir peligros identificados.

Sistema de notificación de seguridad operacional

2.1.4 Una de las principales fuentes para identificar peligros es el sistema de notificaciones de seguridad operacional, especialmente el sistema voluntario de notificación de seguridad operacional. Mientras que el sistema obligatorio se utiliza normalmente para los incidentes que se han producido, el sistema voluntario proporciona un canal de notificación adicional para potenciales problemas de seguridad operacional tales como peligros, cuasi-accidentes o errores. Pueden proporcionar información valiosa a la organización de mantenimiento sobre eventos de bajo impacto.

2.1.5 Es importante que las organizaciones de mantenimiento brinden las protecciones adecuadas para alentar a las personas a notificar lo que ven o experimentan. Por ejemplo,

la acción obligante de cumplimiento reglamentario puede no aplicarse a las notificaciones de errores o, en algunas circunstancias, a la ruptura de reglas. Debería indicarse claramente que la información presentada se utilizará únicamente para respaldar la mejora de la seguridad operacional. La intención es promover una cultura de notificación efectiva y la identificación proactiva de potenciales deficiencias de seguridad operacional.

2.1.6 Los sistemas de notificación voluntarios de seguridad operacional deberán ser confidenciales, lo que requiere que toda la información de identificación del notificador sea conocida solo por el custodio para permitir el seguimiento de las acciones. El rol del custodio debe mantenerse en unos pocos individuos, por lo general restringido al gerente de seguridad operacional y al personal involucrado en la investigación de seguridad operacional. Mantener la confidencialidad ayudará a facilitar la divulgación de los peligros que conducen al error humano, sin temor a represalias o vergüenza. Las notificaciones voluntarias de seguridad operacional se pueden desidentificar y archivar una vez que se toman las medidas de seguimiento necesarias. Las notificaciones desidentificadas pueden respaldar futuros análisis de tendencias para rastrear la efectividad de la mitigación de riesgos e identificar los peligros emergentes.

2.1.7 Se alienta al personal en todos los niveles y en todas las disciplinas a identificar y notificar los peligros y otros problemas de seguridad operacional a través de sus sistemas de notificación de seguridad operacional. Para ser eficaz, los sistemas de notificación de seguridad operacional deberán ser de fácil acceso para todo el personal. Dependiendo de la situación, se puede usar un formulario en papel, de la web o de escritorio. Tener múltiples métodos de entrada disponibles maximiza la probabilidad de participación del personal. Todos deben conocer los beneficios de las notificaciones de seguridad operacional y lo que debe informarse.

2.1.8 Cualquiera que envíe una notificación de seguridad operacional debería recibir comentarios sobre qué decisiones o acciones se han tomado. La alineación de los requisitos del sistema de notificación, las herramientas y los métodos de análisis puede facilitar el intercambio de información de seguridad operacional, así como la comparación de ciertos

indicadores de rendimiento seguridad operacional. La retroalimentación a los notificadores en los esquemas de notificación voluntario también sirve para demostrar que tales informes se consideran seriamente. Esto ayuda a promover una cultura de seguridad operacional positiva y estimula las notificaciones futuras.

2.1.9 Es posible que sea necesario filtrar las notificaciones de entrada cuando hay una gran cantidad de notificaciones de seguridad operacional. Esto puede implicar una evaluación inicial de riesgos de seguridad operacional para determinar si es necesaria una mayor investigación y qué nivel de investigación se requiere.

2.1.10 Las notificaciones de seguridad operacional a menudo se filtran mediante el uso de una taxonomía o un sistema de clasificación. El filtrado de información mediante una taxonomía puede facilitar la identificación de problemas y tendencias comunes. La organización de mantenimiento deberá desarrollar taxonomías que cubran su (s) tipo (s) de operación. La desventaja de usar una taxonomía es que a veces el peligro identificado no se ajusta claramente en ninguna de las categorías definidas. El desafío entonces es usar taxonomías con el grado apropiado de detalle; lo suficientemente específico como para que los peligros sean fáciles de asignar, pero lo suficientemente genéricos como para que los peligros sean valiosos para el análisis. Algunos Estados y asociaciones internacionales han desarrollado taxonomías que puede ser usada.

2.1.11 Otros métodos de identificación de peligros incluyen talleres o reuniones en las que los expertos en la materia realizan escenarios detallados de análisis. Estas sesiones se benefician de las contribuciones de un rango de personal operativo y técnico experimentado. Las reuniones existentes del comité de seguridad (SRB, SAG, etc.) podrían usarse para tales actividades; el mismo grupo también se puede usar para evaluar los riesgos de seguridad asociados.

2.1.12 Los peligros identificados y sus consecuencias potenciales deberán documentarse. Esto se usará para los procesos de evaluación de riesgos de seguridad operacional.

2.1.13 El proceso de identificación de peligros considera todos los peligros posibles que puedan existir dentro del

alcance de las actividades de aviación de la organización de mantenimiento, incluidas las interfaces con otros sistemas, tanto dentro como fuera de la organización. Una vez identificados los peligros, se deben determinar sus consecuencias (es decir, cualquier evento o resultado específico).

Investigación de peligros

2.1.14 La identificación de peligro debe ser continua y parte de las actividades en proceso de la organización de mantenimiento. Algunas condiciones pueden merecer una investigación más detallada. Estas pueden incluir:

a) instancias donde la organización experimenta un aumento inexplicable de eventos relacionados con la seguridad operacional o incumplimiento normativo; o

b) cambios significativos en la organización o sus actividades.

Investigación de seguridad operacional en la organización de mantenimiento

2.1.15 La gestión eficaz de la seguridad operacional depende de las investigaciones de calidad para analizar los sucesos y peligros de seguridad operacional, y notificar los resultados y las recomendaciones para mejorar la seguridad operacional en el entorno operativo.

2.1.16 Existe una clara distinción entre las investigaciones de accidentes e incidentes según el Anexo 13 y las investigaciones de seguridad operacional de las organizaciones de mantenimiento. La investigación de accidentes e incidentes graves conforme al Anexo 13 es responsabilidad del Estado, tal como se define en el Anexo 13. Este tipo de información es esencial para difundir las lecciones aprendidas de accidentes e incidentes. Las investigaciones de seguridad operacional de las organizaciones de mantenimiento son realizadas como parte de su SMS para respaldar los procesos de identificación de peligros y evaluación de riesgos. Existen muchos casos de seguridad operacional que quedan fuera del Anexo 13 que podrían proporcionar una fuente valiosa de identificación de peligros o identificar debilidades en los controles de

riesgos. Estos problemas pueden ser revelados y solucionados por una investigación de seguridad liderada por la organización de mantenimiento.

2.1.17 El objetivo principal de la investigación de seguridad operacional de la organización de mantenimiento es comprender qué sucedió y cómo evitar situaciones similares en el futuro al eliminar o mitigar las deficiencias de seguridad operacional. Esto se logra a través de un examen cuidadoso y metódico del evento y la aplicación de las lecciones aprendidas para reducir la probabilidad y / o consecuencia de recurrencias futuras. Las investigaciones de seguridad operacional de la organización de mantenimiento son una parte integral de los SMS de la organización.

2.1.18 Las investigaciones de las organizaciones de mantenimiento sobre sucesos y peligros de seguridad operacional son una actividad esencial del proceso general de gestión de riesgos. Los beneficios de llevar a cabo una investigación de seguridad operacional incluyen:

a) obtener una mejor comprensión de los eventos que condujeron al suceso;

b) identificar los factores contribuyentes humanos, técnicos y organizacionales;

c) identificar peligros y realizar evaluaciones de riesgos;

d) hacer recomendaciones para reducir o eliminar los riesgos inaceptables; y

e) identificar las lecciones aprendidas que deben ser compartidas con los miembros apropiados de la comunidad aeronáutica.

Desencadenantes de la investigación

2.1.19 Una investigación de seguridad operacional de la organización de mantenimiento generalmente se desencadena por una notificación (informe) enviado a través del sistema de notificaciones de seguridad operacional. La Figura 3 describe el proceso de decisión de la investigación de seguridad operacional y la distinción entre cuándo debe realizar una investigación de seguridad operacional, la

organización de mantenimiento, y cuándo se debe iniciar una investigación conforme a las disposiciones del Anexo 13.

2.1.20 No todos los sucesos o peligros pueden o deberían ser investigados, la decisión de llevar a cabo una investigación y su profundidad deben depender de las consecuencias reales o potenciales del suceso o el peligro. Los sucesos y peligros considerados de alto riesgo son más propensos a ser investigados y deben ser investigados con mayor profundidad que aquellos con menor riesgo potencial. Las organizaciones de mantenimiento deberán usar un enfoque estructurado de toma de decisiones con puntos desencadenantes definidos. Estos guiarán las decisiones de investigación de seguridad operacional: qué investigar y el alcance de la investigación. Esto podría incluir:

a) la gravedad o gravedad potencial del resultado;

b) requisitos reglamentarios u organizativos para llevar a cabo una investigación;

c) valor de seguridad operacional que se obtendrá;

d) oportunidad para tomar medidas de seguridad operacional;

e) riesgos asociados con ninguna investigación;

f) contribución a programas de seguridad operacional específicos;

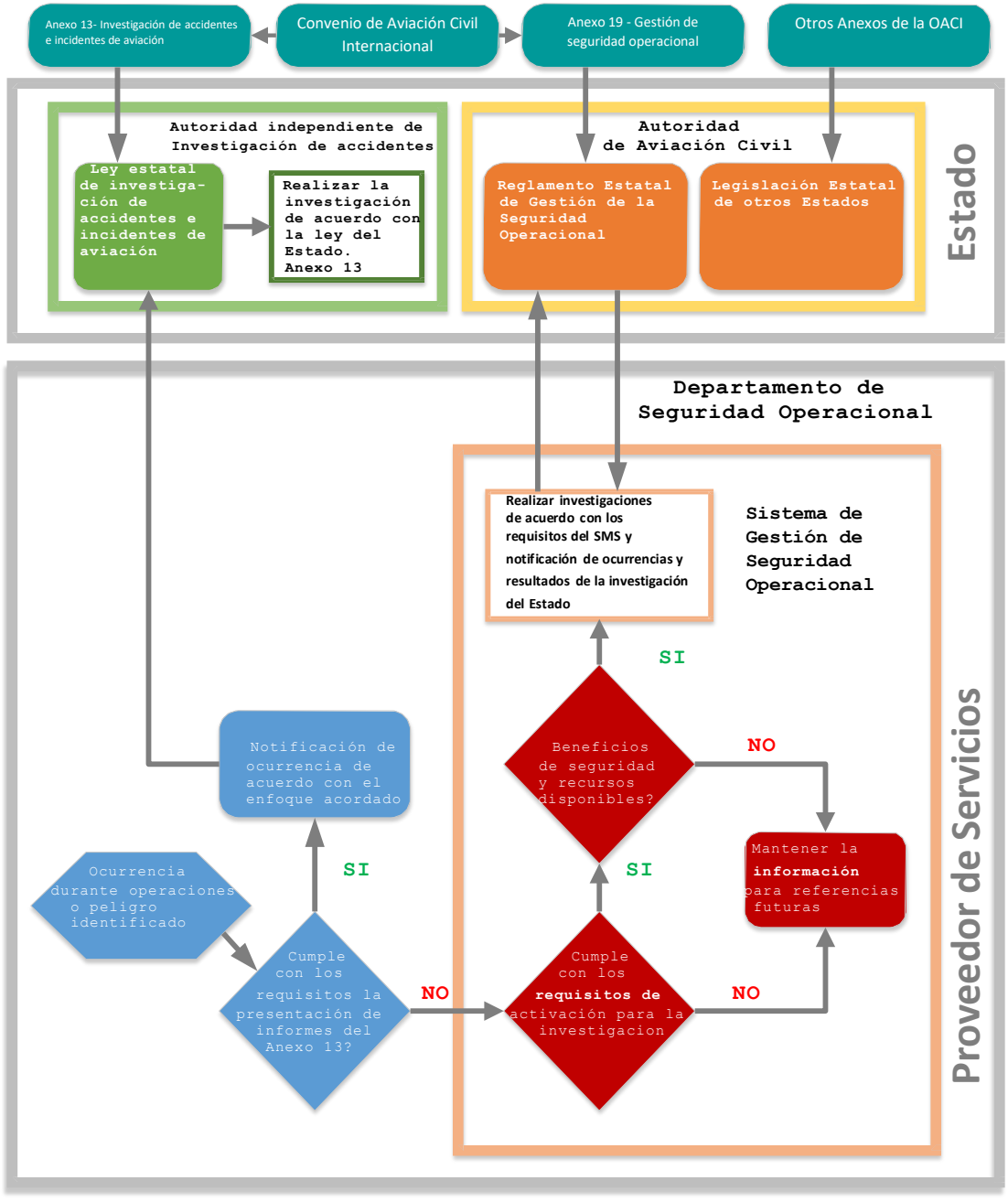
g) tendencias identificadas;

h) beneficio a la instrucción; y

i) disponibilidad de los recursos.

Figura 3. Proceso de decisión de investigación de seguridad operacional

Figura 3. Proceso de decisión de investigación de seguridad operacional



Asignando un investigador

2.1.21 Si una investigación está por comenzar, la primera acción será designar un investigador o un equipo de investigación con las habilidades y experiencia necesarias, cuando los recursos estén disponibles. El tamaño del equipo y el perfil de expertos de sus miembros dependen de la naturaleza y la gravedad del suceso que se investiga. El equipo de investigación puede requerir la asistencia de otros especialistas. A menudo, se asigna a una sola persona para llevar a cabo una investigación interna, con el apoyo de expertos de operaciones y de la oficina de seguridad operacional.

2.1.22 Los investigadores de seguridad operacional de la organización de mantenimiento son idealmente independientes organizacionalmente del área asociada con el suceso o el peligro identificado. Se obtendrán mejores resultados si el (los) investigador (es) son conocedores (capacitados) y expertos (con experiencia) en las investigaciones de seguridad operacional de la organización. Los investigadores idealmente serían elegidos para el papel debido a su conocimiento, habilidades y rasgos de carácter, que deberían incluir: integridad, objetividad, pensamiento lógico, pragmatismos y pensamiento lateral.

El proceso de investigación

2.1.23 La investigación debe identificar qué sucedió y por qué sucedió, y esto puede requerir que se aplique un análisis de causa raíz como parte de la investigación. Idealmente, las personas involucradas en el evento deberían ser entrevistadas tan pronto como sea posible después del evento. La investigación debe incluir:

a) establecer cronologías de eventos clave y las acciones de las personas involucradas;

b) revisión de cualquier política y procedimiento relacionado con las actividades;

c) revisión de cualquier decisión tomada relacionada con el evento;

d) identificación de cualquier control de riesgo existente

que debería haber evitado que ocurriera el evento; y

e) revisión de los datos de seguridad operacional para cualquier evento previo o similar.

2.1.24 La investigación de seguridad operacional deberá enfocarse en los peligros y los riesgos de seguridad operacional identificados y las oportunidades de mejora, no en culpas o castigos. La forma en que se lleva a cabo la investigación y, lo más importante, cómo se redacta el informe, influirá en el posible impacto de la seguridad operacional, la cultura de seguridad operacional futura de la organización y la eficacia de las futuras iniciativas de seguridad operacional.

2.1.25 La investigación deberá concluir con hallazgos claramente definidos y recomendaciones que eliminen o mitiguen las deficiencias de seguridad operacional.

2.2 Evaluación y mitigación del riesgo de seguridad operacional

2.2.1 La organización de mantenimiento debe desarrollar un modelo y procedimientos de evaluación de riesgos de seguridad operacional que permitan un enfoque sistemático y consistente para la evaluación de los riesgos de seguridad operacional. Esto debería incluir un método que ayudará a determinar qué riesgos de seguridad operacional son aceptables o inaceptables y a priorizar acciones.

2.2.2 Es posible que las herramientas de la SRM utilizadas necesiten ser revisadas y personalizadas periódicamente para garantizar que sean adecuadas para el entorno operativo de la organización de mantenimiento. La organización puede encontrar enfoques más sofisticados que reflejen mejor las necesidades de su operación a medida que el SMS madura. La organización de mantenimiento y la DIA / IACC deberían acordar una metodología.

2.2.3 Se encuentran disponibles enfoques más sofisticados para la clasificación de riesgos de seguridad operacional. Estos pueden ser más adecuados si la organización de mantenimiento tiene experiencia con la gestión de seguridad operacional o si opera en un entorno de alto riesgo.

2.2.4 El proceso de evaluación de riesgos de seguridad operacional deberá usar cualquier dato e información de seguridad operacional disponible. Una vez que se han evaluado los riesgos de seguridad operacional, la organización de mantenimiento participará en un proceso de toma de decisiones basado en datos para determinar qué controles de riesgos de seguridad operacional son necesarios.

2.2.5 Las evaluaciones de riesgos de seguridad operacional a veces tienen que usar información cualitativa (juicio de experto) en lugar de datos cuantitativos debido a la falta de disponibilidad de datos. El uso de la matriz de riesgos de seguridad operacional permite al usuario expresar el (los) riesgo (s) de seguridad operacional asociados con el peligro identificado en un formato cuantitativo. Esto permite una comparación de magnitud directa entre los riesgos de seguridad operacional identificados. Se puede asignar un criterio cualitativo de evaluación de riesgos de seguridad operacional tal como "probable que ocurra" o "improbable" a cada riesgo identificado de seguridad operacional cuando los datos cuantitativos no estén disponibles.

2.2.6 Para las organizaciones de mantenimiento que tienen ubicaciones adicionales con entornos operativos específicos, puede ser más efectivo establecer comités locales de seguridad operacional para realizar evaluaciones de riesgos de seguridad operacional e identificar el control de riesgos de seguridad operacional. El asesoramiento a menudo se solicita a un especialista en el área operativa (interna o externa a la organización de mantenimiento). Las decisiones finales o la aceptación del control pueden ser requeridas por las autoridades superiores para que se proporcionen los recursos apropiados.

2.2.7 Es una decisión propia la organización de mantenimiento como prioriza sus evaluaciones de riesgos de seguridad operacional y adopta controles de riesgos de seguridad operacional. Como guía, la organización de mantenimiento deberá declarar en el proceso de priorización, como:

a) evalúa y controla el mayor riesgo de seguridad operacional;

b) asigna recursos a los más altos riesgos de seguridad operacional;

c) mantiene o mejora efectivamente la seguridad operacional;

d) logra los objetivos de seguridad operacional establecidos y acordados y los SPT; y

e) cumple con los requisitos de los reglamentos del Estado con respecto al control de los riesgos de seguridad operacional.

2.2.8 Después de que se hayan evaluado los riesgos de seguridad operacional, se pueden implementar los controles de riesgo apropiados. Es importante involucrar a los "usuarios finales" y a los expertos en la materia para determinar los controles de riesgo de seguridad operacional apropiados. Garantizar la participación de las personas correctas maximizará la practicidad de las mitigaciones riesgo de seguridad operacional elegidas. Una determinación de cualquier consecuencia imprevista, particularmente la introducción de nuevos peligros, deberá hacerse antes de la implementación de cualquier control de riesgos de seguridad operacional.

2.2.9 Una vez que se haya acordado e implementado el control de riesgos de seguridad operacional, se debe monitorear el rendimiento de seguridad operacional para asegurar la efectividad del control de riesgos de seguridad operacional. Esto es necesario para verificar la integridad, eficiencia y eficacia de los nuevos controles de riesgo de seguridad operacionales en condiciones operacionales.

2.2.10 Los resultados de la SRM deben documentarse. Esto deberá incluir el peligro y cualquiera consecuencia, la evaluación de riesgos de seguridad operacional y cualquier acción de control de riesgos de seguridad operacional que se tome. Estos a menudo se capturan en un registro para que puedan ser rastreados y monitoreados. Esta documentación de la SRM se convierte en una fuente histórica de conocimiento de seguridad organizacional que puede usarse como referencia al tomar decisiones de seguridad operacional y para el intercambio de información de seguridad operacional. Este

conocimiento de seguridad operacional proporciona material para análisis de tendencias de seguridad operacional, e instrucción y comunicación de seguridad operacional. También es útil para las auditorías internas para evaluar si los controles riesgos de seguridad operacional y acciones han sido implementadas y son efectivos.

3. COMPONENTE 3: ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

a) Se requiere que las organizaciones de mantenimiento desarrollen y mantengan los medios para verificar el rendimiento de seguridad operacional de la organización y validar la efectividad de los controles de riesgos de seguridad operacional. El componente de aseguramiento de la seguridad operacional del SMS de la organización proporciona estas capacidades.

b) El aseguramiento de la seguridad operacional consiste en procesos y actividades llevadas a cabo para determinar si el SMS está funcionando de acuerdo con las expectativas y los requisitos. Esto implica monitorear continuamente sus procesos, así como su entorno operativo, para detectar cambios o desviaciones que pueden introducir riesgos de seguridad operacional emergentes o la degradación de los controles de riesgos de seguridad operacional existentes. Dichos cambios o desviaciones pueden abordarse mediante el proceso de la SRM.

c) Las actividades de aseguramiento de la seguridad operacional deben incluir el desarrollo y la implementación de acciones tomadas en respuesta a cualquier problema identificado que tenga un impacto potencial en la seguridad operacional. Estas acciones mejoran continuamente el rendimiento del SMS de la organización de mantenimiento.

3.1 Monitoreo y medición del rendimiento de seguridad operacional.

3.1.1 Para verificar el rendimiento de seguridad operacional y validar la efectividad de los controles de riesgos de seguridad operacional, se requiere el uso de una combinación de auditorías internas y el establecimiento y monitoreo de los SPI. Evaluar la efectividad de los controles de riesgos de seguridad operacional es importante ya que su aplicación no siempre logra los resultados

previstos. Esto ayudará a identificar si se seleccionó el control de riesgos de seguridad operacional correcto y puede dar como resultado la aplicación de una estrategia de control de riesgos de seguridad operacional diferente.

Auditoria interna

3.1.2 Se realizan auditorías internas para evaluar la efectividad del SMS e identificar áreas para una mejora potencial. La mayoría de las reglamentaciones de seguridad operacional de la aviación son controles de riesgos de seguridad operacional genéricos que han sido establecidos por el Estado. Asegurar el cumplimiento de las reglamentaciones a través de la auditoría interna es un aspecto principal del aseguramiento de la seguridad operacional.

3.1.3 También es necesario garantizar que todos los controles de riesgos de seguridad operacional se implementen y monitoreen efectivamente. Las causas y los factores que contribuyen deberán ser investigados y analizados donde se identifican las no conformidades y otros problemas. El foco principal de la auditoría interna está en las políticas, procesos y procedimientos que proporcionan los controles de riesgo de seguridad operacional.

3.1.4 Las auditorías internas son más efectivas cuando las realizan personas o departamentos independientes de las funciones que se auditan. Dichas auditorías deberán proporcionar al gerente responsable y a la alta gerencia retroalimentación sobre el estado de:

a) cumplimiento con los reglamentos;

b) cumplimiento de políticas, procesos y procedimientos;

c) la efectividad de los controles de riesgo de seguridad operacional;

d) la efectividad de las acciones correctivas y,

e) la efectividad del SMS.

3.1.5 Algunas organizaciones de mantenimiento no pueden garantizar la independencia apropiada de una auditoría

interna, en tales casos, la organización de mantenimiento debe considerar contratar auditores externos (por ejemplo, auditores independientes o auditores de otra organización).

3.1.6 La planificación de las auditorías internas deberá tener en cuenta la criticidad de la seguridad operacional de los procesos, los resultados de auditorías y evaluaciones previas (de todas las fuentes) y los controles de riesgos de seguridad operacional implementados. Las auditorías internas deben identificar el incumplimiento con los reglamentos y políticas, procesos y procedimientos. También deberán identificar las deficiencias del sistema, la falta de efectividad de los controles de riesgos de seguridad operacional y las oportunidades de mejora.

3.1.7 La Evaluación del cumplimiento y la efectividad son esenciales para lograr el rendimiento de seguridad operacional. El proceso de auditoría interna se puede usar para determinar tanto el cumplimiento como la efectividad. Se pueden formular las siguientes preguntas para evaluar el cumplimiento y la eficacia de cada proceso o procedimiento:

a) Determinación del cumplimiento

1) ¿Existe el proceso o procedimiento requerido?

2) ¿Está documentado el proceso o procedimiento (están definidas las entradas, actividades, interfaces y resultados)?

3) ¿El proceso o procedimiento cumple con los requisitos (criterios)?

4) ¿Se está utilizando el proceso o el procedimiento?

5) ¿Todo el personal afectado sigue el proceso o procedimiento de manera consistente?

6) ¿Se están produciendo los resultados definidos?

7) ¿Se ha documentado e implementado un cambio en un proceso o procedimiento?

b) Evaluación de la efectividad

1) ¿Los usuarios entienden el proceso o procedimiento?
2) ¿Se está logrando el propósito del proceso o procedimiento de manera consistente?
3) ¿Son los resultados del proceso o procedimiento lo que el "cliente" solicitó?
4) ¿El proceso o procedimiento se revisa regularmente?
5) ¿Se realiza una evaluación de riesgos de seguridad operacional cuando hay cambios en el proceso o procedimiento?
6) ¿Las mejoras al proceso o al procedimiento dieron como resultado los beneficios esperados?

3.1.8 Además, en las auditorías internas deberán monitorearse el progreso en el cierre de incumplimientos previamente identificados. Esto debería haberse abordado mediante el análisis de la causa raíz y el desarrollo y la implementación de planes de acción correctivos y preventivos. Los resultados del análisis de la (s) causa (s) y los factores que contribuyen a cualquier incumplimiento deberán alimentar los procesos de SRM del proveedor del servicio.

3.1.9 Los resultados del proceso de auditoría interna se convierten en una de las varias entradas del SRM y las funciones de aseguramiento de la seguridad operacional. Las auditorías internas informan a la gerencia de la organización de mantenimiento del nivel de cumplimiento de la organización, el grado en que los controles de riesgo de seguridad operacional son efectivos y donde se requieren acciones correctivas o preventivas.

3.1.10 Las AAC pueden proporcionar retroalimentación adicional sobre el estado del cumplimiento con las reglamentaciones y la efectividad del SMS y de las asociaciones de la industria u otras terceras partes seleccionadas por la organización de mantenimiento para auditar su organización y procesos. Los resultados de dichas auditorías de segunda y tercera parte son entradas para la función de aseguramiento de seguridad operacional, proporcionando al proveedor del servicio indicaciones sobre la efectividad de sus procesos de auditoría interna y oportunidades para mejorar sus SMS.

Monitoreo del rendimiento de la seguridad operacional

3.1.11 La supervisión del rendimiento de seguridad operacional se lleva a cabo a través de la recopilación de datos e información de seguridad operacional de una variedad de fuentes normalmente disponibles para una organización de mantenimiento. La disponibilidad de datos para apoyar la toma de decisiones informadas es uno de los aspectos más importantes del SMS. El uso de estos datos para el monitoreo y la medición del rendimiento de seguridad operacional son actividades esenciales que generan la información necesaria para la toma de decisiones de riesgos de seguridad operacional.

3.1.12 El monitoreo y medición del rendimiento de seguridad operacional deberá realizarse siguiendo algunos principios básicos. El rendimiento de seguridad operacional logrado es una indicación del comportamiento organizacional y también es una medida de la efectividad del SMS. Esto requiere que la organización de mantenimiento defina:

a) objetivos de seguridad operacional, que deberían establecerse primero para reflejar los logros estratégicos o los resultados deseados relacionados con problemas de seguridad operacional específicos del contexto operacional de la organización;

b) SPI, que son parámetros tácticos relacionados con los objetivos de seguridad operacional y, por lo tanto, son la referencia para la recopilación de datos; y

c) SPT, que también son parámetros tácticos utilizados para monitorear el progreso hacia el logro de los objetivos de seguridad operacional.

3.1.13 Se logrará una imagen más completa y realista del rendimiento de seguridad operacional de la organización de mantenimiento si los SPI abarcan un amplio espectro de indicadores. Esto debería incluir:

a) eventos de baja probabilidad / alta gravedad (por ejemplo, accidentes e incidentes graves);

b) eventos de alta probabilidad / baja gravedad (por ejemplo, eventos operativos sin incidentes, informes de

no conformidad, desviaciones, etc.) y,

c) rendimiento del proceso (por ejemplo, instrucción, mejoras del sistema y procesamiento de notificaciones).

3.1.14 Los SPI se utilizan para medir el rendimiento de seguridad operacional de la organización de mantenimiento y el rendimiento de sus SMS. Los SPI se basan en el monitoreo de datos e información de diversas fuentes, incluido el sistema de notificación de seguridad operacional. Deberán ser específicos para la organización de mantenimiento individual y estar vinculados a los objetivos de seguridad operacional ya establecidos.

3.1.15 Al establecer los SPI, la organización de mantenimiento debe considerar:

a) Medición de las cosas correctas: determinar los mejores SPI que mostrarán que la organización está en vía de lograr sus objetivos de seguridad operacional. También considerar cuáles son los mayores problemas y riesgos de seguridad operacional que enfrenta la organización, e identificar los SPI que mostrarán un control efectivo de estos.

b) Disponibilidad de datos: ¿Hay datos disponibles que se alineen con lo que la organización quiere medir? Si no es así, puede ser necesario establecer fuentes adicionales de recopilación de datos. Para organizaciones pequeñas con cantidades limitadas de datos, la agrupación de conjuntos de datos también puede ayudar a identificar tendencias. Esto puede ser respaldado por asociaciones industriales que pueden recopilar datos de seguridad de múltiples organizaciones.

c) Confiabilidad de los datos: Los datos pueden no ser confiables debido a su subjetividad o porque están incompletos.

d) SPI comunes de la industria: puede ser útil acordar SPI comunes con organizaciones similares para que se puedan hacer comparaciones entre organizaciones. El regulador o las asociaciones de la industria pueden permitir esto.

3.1.16 Una vez que se han establecido los SPI, la

organización de mantenimiento deberá considerar si es apropiado identificar los SPT y los niveles de alerta. Los SPT son útiles para impulsar mejoras de seguridad operacional, pero, implementados de forma deficiente, se sabe que conducen a conductas indeseables, es decir, individuos y departamentos que se centran demasiado en alcanzar la meta y quizás pierden de vista la meta que se pretendía lograr, en lugar de una mejora en el rendimiento de la seguridad organizacional. En tales casos, puede ser más apropiado monitorear los SPI en busca de tendencias.

3.1.17 En el Apéndice 5 se ha desarrollado la información correspondiente a los indicadores (SPI) y metas (SPT) de rendimiento de seguridad operacional.

3.1.18 Las siguientes actividades pueden proporcionar fuentes para monitorear y medir el rendimiento de seguridad operacional:

a) Los estudios de seguridad operacional son análisis para obtener una comprensión más profunda de los problemas de seguridad operacional o comprender mejor una tendencia en el desempeño de seguridad operacional.

b) El análisis de datos de seguridad operacional utiliza los datos de notificaciones de seguridad operacional para descubrir problemas o tendencias comunes que podrían justificar una investigación adicional.

c) Las encuestas de seguridad operacional examinan los procedimientos o procesos relacionados con una operación específica. Las encuestas de seguridad operacional pueden incluir el uso de listas de verificación, cuestionarios y entrevistas informales confidenciales. Las encuestas de seguridad generalmente brindan información cualitativa. Esto puede requerir validación a través de la recolección de datos para determinar si se requiere acción correctiva. No obstante, las encuestas pueden proporcionar una fuente de notificación de seguridad operacional barata y valiosa.

d) Las auditorías de seguridad operacional se centran en evaluar la integridad de los SMS y los sistemas de soporte de la organización de mantenimiento. Las auditorías de seguridad operacional también se pueden

usar para evaluar la efectividad de los controles de riesgo de seguridad operacional instalados o para monitorear el cumplimiento con la reglamentación de seguridad operacional. Garantizar la independencia y la objetividad es un desafío para las auditorías de seguridad operacional. La independencia y la objetividad se pueden lograr mediante la participación de entidades externas o auditorías internas con protecciones establecidas: políticas, procedimientos, roles, protocolos de comunicación.

e) Los hallazgos y recomendaciones de las investigaciones de seguridad operacional pueden proporcionar información de seguridad operacional útil que se puede analizar en comparación con otros datos de seguridad recopilados.

f) Sistemas de recolección de datos operacionales como el FDA, monitoreo de la condición de los motores, la información del radar puede proporcionar datos útiles sobre eventos y rendimiento operacional.

3.1.19 El desarrollo de SPI debe vincularse con los objetivos de seguridad operacional y basarse en el análisis de los datos disponibles o que se pueden obtener. El proceso de monitoreo y medición implica el uso de indicadores de rendimiento de seguridad operacional seleccionados, los SPT correspondientes y las alertas de seguridad operacional.

3.1.20 La organización deberá monitorear el rendimiento de SPI y SPT establecidos para identificar cambios anormales en el rendimiento de seguridad operacional. Los SPT deberán ser realistas, específicos del contexto y alcanzables al considerar los recursos disponibles para la organización y el sector de aviación asociado.

3.1.21 Principalmente, el monitoreo y medición del rendimiento de seguridad operacional proporciona un medio para verificar la efectividad de los controles de riesgos de seguridad operacional. Además, proporcionan una medida de la integridad y efectividad de los procesos y actividades del SMS.

3.1.22 El Estado puede tener procesos específicos para la aceptación de SPI y SPT que necesitarán seguirse. Por lo tanto, durante el desarrollo de SPI y SPT, la organización

de mantenimiento deberá consultar con la DIA/IACC o cualquier información relacionada que el Estado haya publicado.

3.2 La gestión del cambio.

3.2.1 Las organizaciones de mantenimiento experimentan cambios debido a una serie de factores que incluyen, pero no limitados a:

a) expansión organizacional o contracción;

b) mejoras comerciales que impactan la seguridad operacional; esto puede dar como resultado cambios en los sistemas internos, procesos o procedimientos que respaldan la entrega segura de los productos y servicios;

c) cambios en el entorno operativo de la organización;

d) cambios en las interfaces de SMS con organizaciones externas; y

e) cambios regulatorios externos, cambios económicos y riesgos emergentes.

3.2.2 El cambio puede afectar la efectividad de los controles de riesgo de seguridad operacional existentes. Además, los nuevos peligros y los riesgos de seguridad operacional relacionados podrían introducirse inadvertidamente en una operación cuando se produce un cambio. Los peligros deberán identificarse y los riesgos de seguridad operacional relacionados deben evaluarse y controlarse como se define en los procedimientos de identificación de peligros o SRM de la organización.

3.2.3 La gestión del cambio del proceso de la organización de mantenimiento deberá tener en cuenta las siguientes consideraciones:

a) Criticidad. ¿Cuán crítico es el cambio? la organización de mantenimiento deberá considerar el impacto en las actividades de su organización y el impacto en otras organizaciones y el sistema de aviación.

b) Disponibilidad de expertos en la materia. Es importante

que los miembros clave de la comunidad aeronáutica participen en las actividades de gestión del cambio. Esto puede incluir individuos de organizaciones externas.

c) Disponibilidad de datos e información sobre el rendimiento de seguridad operacional.
¿Qué datos e información están disponibles que se pueden usar para proporcionar información sobre la situación y permitir el análisis del cambio?

3.2.4 Pequeños cambios incrementales a menudo pasan desapercibidos, pero el efecto acumulativo puede ser considerable. Los cambios, grandes y pequeños, pueden afectar la descripción del sistema de la organización y pueden llevar a la necesidad de su revisión. Por lo tanto, la descripción del sistema debe revisarse regularmente para determinar su validez continua, dado que la mayoría de las organizaciones de mantenimiento experimentan cambios regulares, o incluso continuos.

3.2.5 La organización de mantenimiento debe definir el desencadenante para el proceso de cambio formal. Los cambios que probablemente desencadenarán la gestión formal del cambio incluyen:

a) Introducción de tecnología o equipamiento nuevos;

b) Cambios en el entorno operacional;

c) Cambios en el personal clave;

d) Cambios significativos en los niveles del personal;

e) Cambio en los requisitos reglamentarios de seguridad operacional;

f) Reestructuración significativa de la organización; y

g) Cambios físicos (instalación o base nueva, cambios en el diseño del aeródromo, entre otros)

3.2.6 La organización de mantenimiento deberá considerar también el impacto del cambio en el personal. Esto puede afectar como el cambio es aceptado por quienes son

afectados. La comunicación y el compromiso anticipado normalmente mejorarán la forma en que se percibe e implementa el cambio.

3.2.7 El proceso de gestión del cambio debe incluir las siguientes actividades:

a) comprender y definir el cambio, esto deberá incluir una descripción del cambio y por qué está siendo implementado;

b) comprender y definir quién y qué será afectado, esto puede ser personas dentro de la organización, otros departamentos o personas u organizaciones externas. El equipamiento, los sistemas y los procesos también pueden verse afectados. Puede ser necesaria una revisión de la descripción del sistema y las interfaces de la organización. Esta es una oportunidad para determinar quién deberá estar involucrado en el cambio. Los cambios pueden afectar los controles de riesgo ya existentes para mitigar otros riesgos y, por lo tanto, el cambio podría aumentar los riesgos en áreas que no son inmediatamente obvias;

c) identificar los peligros relacionados con el cambio y llevar a cabo una evaluación de riesgos de seguridad operacional, esto deberá identificar cualquier peligro directamente relacionado con el cambio. También se debe revisar el impacto en los peligros existentes y los controles de riesgos de seguridad operacional que pueden verse afectados por el cambio. Este paso deberá usar los procesos de la SRM de la organización existente;

d) desarrollar un plan de acción, esto deberá definir lo que se debe hacer, quién lo hará y cuándo. Deberá haber un plan claro que describa cómo se implementará el cambio y quién será responsable de qué acciones, y la secuencia y programación de cada tarea;

e) firmar el cambio, esto es para confirmar que el cambio es seguro de implementar. El individuo con la responsabilidad y autoridad general para implementar el cambio debe firmar el plan de cambio; y

f) plan de aseguramiento, esto es para determinar qué acción

de seguimiento se necesita. Considerar cómo se comunicará el cambio y si se necesitan actividades adicionales (como auditorías) durante o después del cambio. Cualquier suposición hecha necesita ser probada.

3.3. Mejora continua del SMS

3.3.1 La organización de mantenimiento supervisa y evalúa sus procesos de SMS para mantener o mejorar continuamente la efectividad general del SMS. El mantenimiento y la mejora continua de la efectividad del SMS de la organización de mantenimiento se respaldan en actividades de aseguramiento de la seguridad operacional que incluyen la verificación y el seguimiento de las acciones y los procesos de auditoría interna. Se deberá reconocer que mantener y mejorar continuamente el SMS es una actividad permanente ya que la organización y el entorno operativo cambiarán constantemente.

3.3.2 Las auditorías internas implican la evaluación de las actividades de la organización de mantenimiento que pueden proporcionar información útil para los procesos de toma de decisiones de la organización. La función de auditoría interna incluye la evaluación de todas las funciones de gestión de la seguridad operacional en toda la organización.

3.3.3 La efectividad del SMS no debe basarse únicamente en los SPIs; la organización de mantenimiento deberá tratar de implementar una variedad de métodos para determinar su efectividad, medir los resultados, así como también los resultados de los procesos, y evaluar la información recopilada a través de estas actividades. Dichos métodos pueden incluir:

a) Auditorías, esto incluye auditorías internas y auditorías llevadas a cabo por otras organizaciones.

b) Evaluaciones, incluye evaluaciones de cultura de seguridad operacional y efectividad del SMS.

c) Monitoreo de ocurrencias, monitoree la recurrencia de eventos de seguridad operacional incluyendo accidentes e incidentes, así como también errores y situaciones de incumplimiento de reglas.

d) Encuestas de seguridad operacional, incluidas las encuestas culturales que proporcionan una retroalimentación útil sobre el compromiso del personal con el SMS. También puede proporcionar un indicador de la cultura de seguridad de la organización.

e) Revisiones de gestión, examinar si la organización de mantenimiento está logrando los objetivos de seguridad operacional y es una oportunidad para examinar toda la información disponible sobre el rendimiento de seguridad operacional para identificar tendencias generales. Es importante que la alta gerencia revise la efectividad del SMS. Esto se puede llevar a cabo como una de las funciones del comité de seguridad operacional de más alto nivel.

f) Evaluación de SPIs y SPTs, posiblemente como parte de la revisión de la gestión, como se consideran las tendencias y, cuando los datos apropiados están disponibles, se pueden comparar con otras organizaciones de mantenimiento o datos estatales o globales.

g) Abordar las lecciones aprendidas, desde los sistemas de notificación de seguridad operacional y las investigaciones de seguridad operacional de la organización de mantenimiento. Estas deberán conducir a la implementación de mejoras de seguridad operacional.

3.3.4 En resumen, el monitoreo del rendimiento de seguridad operacional y los procesos de auditoría interna contribuyen a la capacidad de la organización de mantenimiento para mejorar continuamente su rendimiento de seguridad operacional. El monitoreo continuo del SMS, sus controles de riesgos de seguridad operacional relacionados y los sistemas de soporte aseguran a la organización de mantenimiento y al Estado que los procesos de gestión de seguridad operacional están logrando sus objetivos de rendimiento de seguridad operacional deseados.

4. COMPONENTE 4: PROMOCIÓN DE LA SEGURIDAD OPERACIONAL.

a) La promoción de la seguridad operacional fomenta una cultura de seguridad positiva y ayuda a alcanzar los objetivos de seguridad operacional de la organización de mantenimiento, a través de la combinación de competencia

técnica que se mejora continuamente a través de instrucción y educación, comunicación efectiva y compartición de información. La alta gerencia proporciona el liderazgo para promover la cultura de seguridad en toda la organización.

b) La gestión eficaz de la seguridad operacional no puede lograrse únicamente por mandato o la estricta adherencia a las políticas y procedimientos. La promoción de la seguridad operacional afecta ambos; el comportamiento individual y organizacional, y complementa las políticas, procedimientos y procesos de la organización, proporcionando un sistema de valores que respalda los esfuerzos de seguridad operacional.

c) la organización de mantenimiento debe establecer e implementar procesos y procedimientos que faciliten la comunicación bidireccional efectiva en todos los niveles de la organización. Esto debería incluir una clara dirección estratégica desde la parte superior de la organización y permitiendo una comunicación "ascendente" que fomente una retroalimentación abierta y constructiva desde todo el personal.

4.1 Instrucción y educación

4.1.1 La organización de mantenimiento debe desarrollar y mantener un programa de instrucción de seguridad operacional que garantiza que el personal está capacitado y competente para realizar sus deberes relacionados con el SMS. De la misma manera, se requiere que el alcance del programa de instrucción de seguridad operacional sea apropiado al involucramiento individual en el SMS. El gerente de seguridad operacional es responsable de garantizar que exista un programa de instrucción de seguridad operacional adecuado. Esto incluye proporcionar la información de seguridad operacional apropiada relevante a los problemas de seguridad operacional específicos conocidos de la organización. El personal capacitado y competente para realizar sus tareas de SMS, independientemente de su nivel en la organización, es una indicación del compromiso de la gerencia con un SMS efectivo. El programa de instrucción debe incluir requisitos de instrucción inicial y continua para mantener las competencias. La instrucción inicial de seguridad operacional debe considerar, como mínimo, lo

siguiente:

a) políticas y objetivos de seguridad operacional organizacional;

b) roles organizacionales y responsabilidades relacionadas con la seguridad operacional;

c) principios básicos de la SRM;

d) sistemas de notificación de seguridad operacional;

e) los procesos y procedimientos de SMS de la organización; y

f) factores humanos.

4.1.2 La instrucción de seguridad operacional continua debe centrarse en los cambios a las políticas, procesos y procedimientos de SMS, y debe resaltar cualquier problema de seguridad operacional específico relevante para la organización o las lecciones aprendidas.

4.1.3 El programa de instrucción deberá adaptarse a las necesidades del rol del individuo dentro del SMS. Por ejemplo, el nivel y la profundidad de la instrucción de los gerentes que participan en los comités de seguridad operacional de la organización serán más extensos que los del personal directamente involucrado en la entrega de los productos o servicios de la organización. Si bien el personal que no participa directamente en las operaciones puede requerir solo una descripción general de alto nivel del SMS de la organización.

Análisis de necesidades de instrucción

4.1.4 Para la mayoría de las organizaciones de mantenimiento, es necesario un análisis formal de las necesidades de capacitación (TNA) para garantizar que haya una comprensión clara de la operación, las obligaciones de seguridad operacional del personal y la instrucción disponible. Una TNA típica normalmente comenzará realizando un análisis de audiencia, que generalmente incluye los siguientes pasos:

a) Todo el personal de la organización de mantenimiento se verá afectados por la implementación del SMS, pero no de la misma manera o en la misma medida. Identifique cada agrupación de personal y de qué manera interactuarán con los procesos de gestión de la seguridad operacional, las entradas y salidas, en particular las obligaciones de seguridad operacional. Esta información deberá estar disponible desde las descripciones de los puestos / rol. Normalmente, comenzarán a surgir agrupaciones de individuos que tengan necesidades de aprendizaje similares. La organización de mantenimiento debe considerar si es valioso extender el análisis al personal de las organizaciones de interfaz externas;

b) Identificar el conocimiento y competencias necesarias para realizar cada tarea de seguridad operacional y que cada agrupación de personal requiera.

c) Llevar a cabo un análisis para identificar la brecha entre las habilidades actuales de seguridad operacional y el conocimiento en toda la fuerza de trabajo y aquellos necesarios para llevar a cabo con eficacia las tareas de seguridad operacional asignadas.

d) Identificar el enfoque de desarrollo de habilidades y conocimiento más apropiado para cada grupo con el objetivo de desarrollar un programa de instrucción apropiado a la participación de cada individuo o grupo en la gestión de seguridad operacional. El programa de instrucción también deberá considerar las necesidades continuas de conocimiento y competencia de seguridad operacional del personal, esta necesidad generalmente se satisfará a través de un programa de instrucción continua.

4.1.5 También es importante identificar el método apropiado para la impartir la instrucción. El objetivo principal es que, al finalizar la instrucción, el personal sea competente para realizar sus tareas de SMS. Los instructores competentes suelen ser la consideración más importante, su compromiso, sus habilidades de enseñanza y su experticia en gestión de seguridad operacional tendrán un impacto significativo en la efectividad de la instrucción impartida. El programa de instrucción en seguridad operacional también deberá especificar las responsabilidades para el desarrollo

del contenido y la programación de la instrucción, así como los registros de los archivos de instrucción y competencia.

4.1.6 La organización debe determinar quién deberá recibir instrucción y a qué profundidad y esto dependerá de su participación en el SMS. La mayoría de las personas que trabajan en la organización de mantenimiento tienen alguna relación directa o indirecta con la seguridad operacional de la aviación y, por lo tanto, tienen algunos deberes de SMS. Esto se aplica al personal directamente involucrado en la entrega de los productos y servicios y al personal involucrado en los comités de seguridad operacional de la organización. Además, algunos miembros del personal administrativo y de apoyo aún tienen algunas responsabilidades limitadas de SMS, ya que su trabajo puede tener un impacto indirecto en la seguridad operacional de la aviación y aún necesitaría algo de instrucción de SMS.
4.1.7 La organización de mantenimiento deberá identificar las responsabilidades de SMS del personal y esto se deberá usar para determinar el alcance del programa de instrucción de seguridad operacional y garantizar que cada individuo reciba instrucción alineada con su participación en el SMS. El programa de instrucción en seguridad operacional deberá especificar el contenido de la instrucción en seguridad operacional para el personal de apoyo, el personal operativo, los gerentes y supervisores, los gerentes principales y el gerente responsable.

4.1.8 Deberá haber instrucción de seguridad operacional específica para el gerente responsable y los altos directivos que incluya los siguientes temas:

a) instrucción específica de sensibilización para los nuevos gerentes responsables y los titulares de puestos en sus responsabilidades de rendición de cuentas y responsabilidades de SMS;

b) importancia del cumplimiento de los requisitos de seguridad nacional y organizacional;

c) compromiso de gestión;

d) asignación de recursos;

e) promoción de la política de seguridad operacional y el

SMS;

f) promoción de una cultura de seguridad operacional positiva;

g) comunicación efectiva de seguridad operacional interdepartamental;

h) objetivo de seguridad operacional, SPT y niveles de alerta; y
i) política disciplinaria.

4.1.9 El objetivo principal del programa de instrucción en seguridad operacional es garantizar que el personal, en todos los niveles de la organización, mantenga su competencia para cumplir con sus funciones de seguridad; por lo tanto, las competencias del personal deberían revisarse regularmente.

4.2 Comunicación de seguridad operacional

4.2.1 La organización de mantenimiento deberá comunicar los objetivos y procedimientos de SMS de la organización a todo el personal apropiado. Deberá haber una estrategia de comunicación que permita que la comunicación de seguridad operacional se brinde por el método más apropiado en función de la función del individuo y la necesidad de recibir información relacionada con la seguridad operacional. Esto puede hacerse a través de una hoja informativa de seguridad operacional, avisos, boletines, sesiones informativas o cursos de instrucción. El gerente de seguridad operacional también deberá asegurarse de que las lecciones aprendidas de las investigaciones y los historiales o experiencias, tanto internamente como desde otras organizaciones, se distribuyan ampliamente. Por lo tanto, la comunicación de seguridad operacional tiene como objetivo:

a) asegurar que el personal tenga pleno conocimiento 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 de seguridad operacional es información específica relacionada con

problemas de seguridad operacional y riesgos de seguridad operacional que podrían exponer a la organización a riesgos de seguridad operacional. Esto podría ser a partir de la información de seguridad operacional recopilada de fuentes internas o externas, como las lecciones aprendidas o relacionadas con los controles de riesgos de seguridad operacional. La organización de mantenimiento determina qué información se considera de seguridad operacional crítica y la oportunidad de su comunicación.

c) crear conciencia sobre nuevos controles de riesgos de seguridad operacional y acciones correctivas, los riesgos de seguridad operacional que enfrenta la organización de mantenimiento cambiará con el tiempo y si se trata de un nuevo riesgo de seguridad operacional identificado o cambios en los controles de riesgos de seguridad operacional, estos 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 adecuadas conozcan estos cambios.

e) promover una cultura de seguridad operacional positiva y alentar al personal a identificar y notificar los peligros; la comunicación de seguridad operacional es bidireccional. 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 retroalimentación al personal que presente notificaciones de seguridad operacional sobre qué acciones se han tomado para abordar cualquier problema identificado.

4.2.2 Las organizaciones de mantenimiento deberán considerar si alguna de la información de seguridad operacional enumerada anteriormente necesita ser comunicada a organizaciones externas.

4.2.3 Las organizaciones de mantenimiento deben evaluar la

efectividad de sus comunicaciones de seguridad operacional al verificar que el personal haya recibido y entendido cualquier información crítica de seguridad operacional que haya sido distribuida. Esto se puede hacer como parte de las actividades de auditoría interna o cuando se evalúa la efectividad del SMS.

4.2.4 Las actividades de promoción de la seguridad operacional deberían llevarse a cabo durante todo el ciclo de vida del SMS, no solo al principio.

5. Planificación de la implementación

5.1. Descripción del sistema

5.1.1 Una descripción del sistema ayuda a identificar los procesos de la organización, incluyendo cualquier interfaz para definir el alcance del SMS. Esto proporciona una oportunidad para identificar cualquier brecha relacionada con los componentes y elementos de SMS de la organización de mantenimiento y puede servir como punto de partida para identificar los peligros operacionales y de la organización. Una descripción del sistema sirve para identificar las características del producto, el servicio o las actividades para que la SRM y la garantía de seguridad puedan ser efectivos.

5.1.2 La mayoría de las organizaciones de mantenimiento se componen de una red compleja de interfaces e interacciones que involucran diferentes departamentos internos, así como diferentes organizaciones externas que contribuyen a la operación segura de la organización. El uso de una descripción del sistema permite a la organización tener una imagen más clara de sus muchas interacciones e interfaces. Esto permitirá una mejor gestión de los riesgos y los controles de riesgos de seguridad operacional si se describen y ayuda a comprender el impacto de los cambios en los procesos y procedimientos de SMS.

5.1.3 Cuando se considera una descripción del sistema, es importante comprender que un "sistema" es un conjunto de cosas que funcionan juntas como partes de una red de

interconexión. En un SMS, se trata de cualquiera de los productos, personas, procesos, instalaciones, servicios y otros aspectos de una organización, incluidos los factores externos, que están relacionados y pueden afectar las actividades de seguridad operacional de la aviación de la organización. A menudo, un "sistema" es un sistema de sistemas, que también se puede ver como un sistema con subsistemas. Estos sistemas y sus interacciones entre ellos constituyen las fuentes de los peligros y contribuyen al control de los riesgos de seguridad operacional. Los sistemas importantes incluyen tanto aquellos que podrían tener un impacto directo en la seguridad de la aviación como aquellos que afectan la habilidad o capacidad de una organización para realizar una gestión de seguridad operacional efectiva.

5.1.4 Se deberá incluir una descripción general del sistema y las interfaces de SMS en la documentación de SMS. Una descripción del sistema puede incluir una lista con viñetas con referencias a políticas y procedimientos. Una representación gráfica, como un diagrama de flujo del proceso o un organigrama, puede ser suficiente para algunas organizaciones. Una organización de mantenimiento debe usar un método y formato que funcione para esa organización.

5.1.5 Debido a que cada organización es única, no existe un método "único para todos" para la implementación de SMS. Se espera que cada organización implemente un SMS que funcione para su situación única. Cada organización deberá definir por sí misma cómo pretende cumplir los requisitos fundamentales. Para lograr esto, es importante que cada organización prepare una descripción del sistema que identifique sus estructuras organizacionales, procesos y acuerdos comerciales que considere importantes para las funciones de gestión de seguridad operacional. Con base en la descripción del sistema, la organización deberá identificar o desarrollar políticas, procesos y procedimientos que establezcan sus propios requisitos de gestión de seguridad operacional.

5.1.6 Cuando una organización elige realizar un cambio significativo o sustancial en los procesos identificados en la descripción del sistema, los cambios deberán ser visto como potencialmente afectan la línea base de evaluación de riesgo de seguridad operacional de referencia. Por lo tanto,

la descripción del sistema deberá revisarse como parte de la gestión de los procesos de cambio.

5.2. Gestión de interfaz

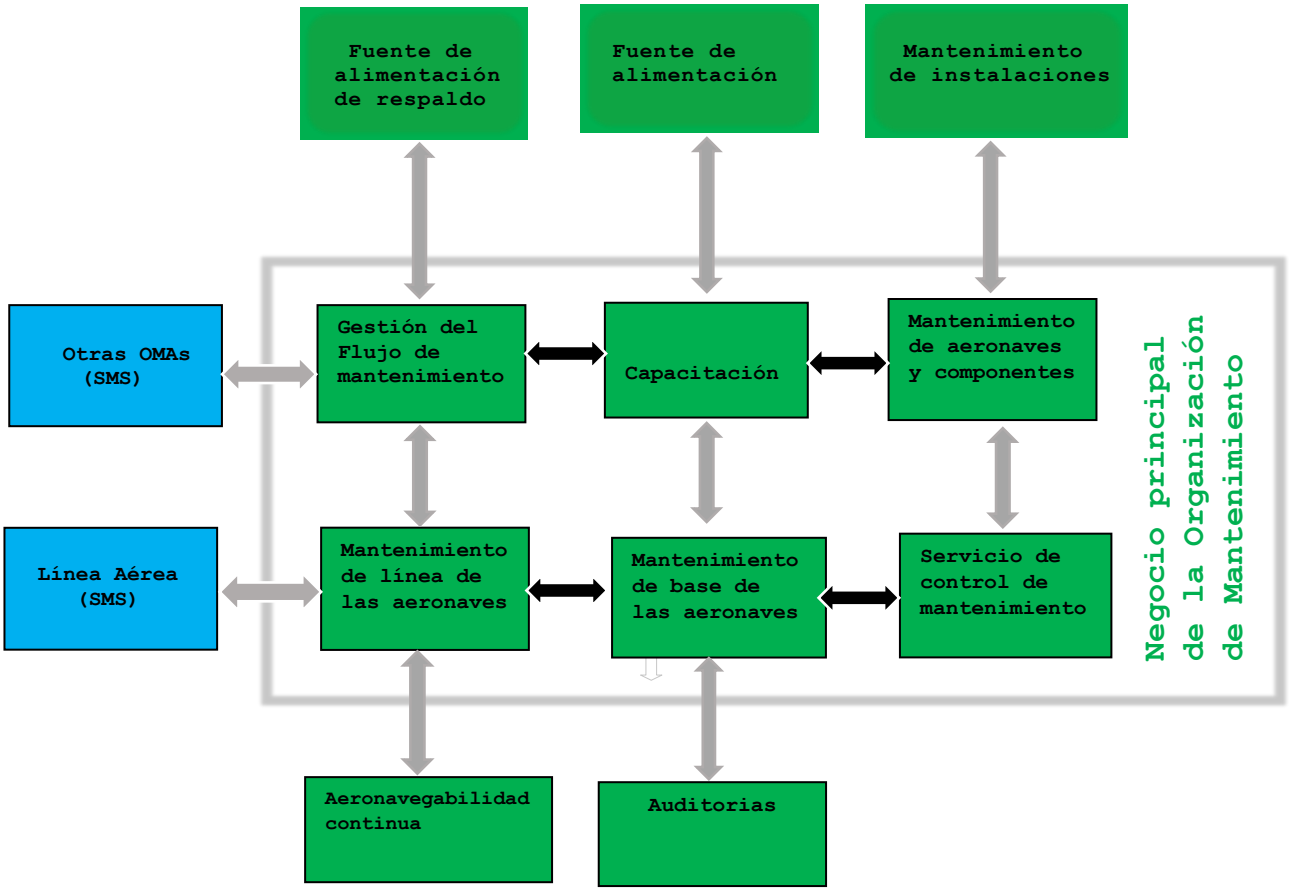
Los riesgos de seguridad operacional que enfrentan las organizaciones de mantenimiento se ven afectadas por las interfaces. Las interfaces pueden ser internas (por ejemplo, entre departamentos) o externas (por ejemplo, otras organizaciones de mantenimiento, funciones de mantenimiento o servicios contratados). Al identificar y gestionar estas interfaces, el proveedor del servicio tendrá más control sobre los riesgos de seguridad operacional relacionados con las interfaces. Estas interfaces deberán definirse dentro de la descripción del sistema.

5.3 Identificación de las interfaces de SMS

5.3.1 Inicialmente, las organizaciones de mantenimiento deberían concentrarse en las interfaces en relación con sus actividades comerciales. La identificación de estas interfaces deberá detallarse en la descripción del sistema que establece el alcance del SMS y debe incluir interfaces internas y externas.

5.3.2 La Figura 4 es un ejemplo de cómo una organización de mantenimiento podría mapear las diferentes organizaciones con las que interactúa para identificar cualquier interfaz de SMS. El objetivo de esta revisión es producir una lista completa de todas las interfaces. El motivo de este ejercicio es que puede haber interfaces de SMS de las que una organización no está necesariamente al tanto. Puede haber interfaces donde no hay un acuerdo formal. En este caso, la fuente de alimentación o el mantenimiento del edificio son buenos ejemplos.

Figura 4. Ejemplo de las interfaces del SMS de la OMA



5.3.3 Algunas de las interfaces internas pueden estar relacionadas con áreas comerciales que no están directamente relacionadas con la seguridad operacional, como marketing, finanzas, recursos legales y humanos. Estas áreas pueden tener un impacto sobre la seguridad operacional a través de sus decisiones que impactan en los recursos internos y la inversión, así como en los acuerdos y contratos con organizaciones externas, y pueden no necesariamente tener en cuenta la seguridad operacional.

5.3.4 Una vez que se han identificado las interfaces del SMS, la organización de mantenimiento deberá considerar su criticidad relativa. Esto permite a la organización priorizar la gestión de las interfaces más críticas y sus posibles riesgos de seguridad operacional. Las cosas a considerar son:

a) qué se está proporcionando;

b) por qué es necesario;

c) si las organizaciones involucradas tienen un SMS u otro sistema de gestión en funcionamiento; y

d) si la interfaz implica el intercambio de datos / información de seguridad.

Evaluar el impacto de seguridad operacional de las interfaces

5.3.5 La organización de mantenimiento deberá entonces identificar cualquier peligro relacionado con las interfaces y llevar a cabo una evaluación de riesgos de seguridad operacional utilizando sus procesos existentes de identificación de peligros y evaluación de riesgos de seguridad operacional.

5.3.6 Con base en los riesgos de seguridad operacional identificados, la organización de mantenimiento puede considerar trabajar con la otra organización para determinar y definir una estrategia de control de riesgos de seguridad operacional apropiada. Al involucrar a la otra organización, esta puede contribuir a identificar peligros, evaluar el riesgo de seguridad operacional y determinar el control de riesgos de seguridad operacional apropiado. Este esfuerzo de colaboración es necesario porque la percepción de los riesgos de seguridad operacional puede no ser la misma para cada organización. El control de riesgos podría ser llevado a cabo por la organización de mantenimiento o la organización externa.

5.3.7 También es importante reconocer que cada organización involucrada tiene la responsabilidad de identificar y gestionar los peligros que afectan a su propia organización. Esto puede significar que la naturaleza crítica de la interfaz es diferente para cada organización, ya que pueden aplicar diferentes clasificaciones de riesgos de seguridad operacional y tener diferentes prioridades de riesgo de seguridad operacional (en términos de rendimiento de seguridad operacional, recursos, tiempo, etc.).

Gestionar y monitorear las interfaces

5.3.8 La organización de mantenimiento es responsable de gestionar y monitorear las interfaces para garantizar que provea productos y servicios seguros. Esto garantizara que las interfaces son gestionadas eficazmente y se mantienen actualizadas y relevantes. Los Acuerdos formales son una manera efectiva de cumplir esto, ya que la interface y las responsabilidades asociadas pueden estar claramente definidas. Cualquier cambio en las interfaces y los impactos asociados deberán comunicarse a las organizaciones relevantes.

5.3.9 Los desafíos asociados con la capacidad de la organización de mantenimiento para gestionar los riesgos de seguridad operacional de la interfaz incluyen:

a) los controles de riesgo de seguridad operacional de una organización no son compatibles con la otra organización;

b) disposición de ambas organizaciones para aceptar cambios en sus propios procesos y procedimientos;

c) disponibilidad insuficiente de recursos o experticia técnica para gestionar y monitorear la interfaz; y

d) número y ubicación de las interfaces.

5.3.10 Es importante reconocer la necesidad de coordinación entre las organizaciones involucradas en la interfaz. La coordinación efectiva deberá incluir:

a) aclaración de los roles y responsabilidades de cada organización;

b) acuerdo de decisiones sobre las acciones a tomar (por ejemplo, acciones de control de riesgos de seguridad operacional y escalas de tiempo);

c) identificación de qué información de seguridad necesita ser compartida y comunicada;

d) cómo y cuándo debería tener lugar la coordinación (grupos de trabajo, reuniones regulares, reuniones ad-hoc o dedicadas); y

e) acordar soluciones que beneficien a ambas organizaciones pero que no perjudiquen la efectividad del SMS.

5.3.11 Todos los problemas o riesgos de seguridad operacional relacionados con las interfaces deben documentarse y ponerse a disposición de cada organización para su compartición y revisión. Esto permitirá compartir las lecciones aprendidas y mancomunar los datos de seguridad operacional que serán valiosos para ambas organizaciones. Los beneficios de seguridad operacional se pueden lograr a través de una mejora de la seguridad operacional alcanzada por cada organización como resultado de la propiedad compartida de los riesgos y la responsabilidad de la seguridad operacional.

5.4. Escalabilidad del SMS

5.4.1 El SMS de la organización de mantenimiento, incluidas las políticas, procesos y procedimientos, deben reflejar el tamaño y la complejidad de la organización y sus actividades. Deberá considerar:

a) la estructura organizacional y la disponibilidad de recursos;

b) tamaño y complejidad de la organización (incluidos múltiples sitios y bases); y

c) complejidad de las actividades y las interfaces con organizaciones externas.

5.4.2 La organización de mantenimiento deberá realizar un análisis de sus actividades para determinar el nivel correcto de recursos para gestionar el SMS. Esto debería incluir la determinación de la estructura organizacional necesaria para gestionar el SMS. Esto podría incluir consideraciones sobre quién será responsable de gestionar y mantener el SMS, qué comités de seguridad se necesitan, si es que se necesita alguno, y la necesidad de especialistas de seguridad operacional específicos.

Consideraciones de riesgo de seguridad operacional

5.4.3 Independientemente del tamaño de la organización de mantenimiento, la escalabilidad también debe ser una función inherente del riesgo de seguridad operacional de las actividades de la organización de mantenimiento. Incluso las organizaciones pequeñas pueden participar en actividades que pueden implicar riesgos significativos para la seguridad operacional de la aviación. Por lo tanto, la capacidad de gestión de seguridad operacional debe ser proporcional con el riesgo de seguridad operacional gestionado.

Datos de información de seguridad operacional y su análisis

5.4.4 Para organizaciones de mantenimiento pequeñas, el bajo volumen de datos puede significar que es más difícil identificar tendencias o cambios en el rendimiento de seguridad operacional. Esto puede requerir reuniones para plantear y discutir problemas de seguridad operacional con los expertos adecuados. Esto puede ser más cualitativo que cuantitativo, pero ayudará a identificar los peligros y riesgos de la organización de mantenimiento. Puede ser útil colaborar con otras organizaciones de mantenimiento o asociaciones de la industria, ya que estos pueden tener datos que la organización de mantenimiento no tiene. Por ejemplo, las organizaciones de mantenimiento más pequeñas pueden intercambiar con organizaciones / operaciones similares para compartir información de riesgos de seguridad operacional e identificar tendencias de rendimiento de seguridad operacional. Las organizaciones de mantenimiento deberán analizar y procesar adecuadamente sus datos internos, a pesar de que pueden ser limitados.

5.4.5 Para las organizaciones de mantenimiento con muchas interacciones e interfaces, necesitarán considerar cómo reúnen datos e información de seguridad operacional de múltiples organizaciones. Esto puede dar lugar a que se recopilen grandes volúmenes de datos que se cotejarán y analizarán más adelante. Estas organizaciones de mantenimiento deberán utilizar un método apropiado para gestionar dichos datos. También se debe considerar la calidad de los datos recopilados y el uso de taxonomías para ayudar con el análisis de los datos.

5.5. Integración de sistemas de gestión

5.5.1 La gestión de la seguridad operacional deberá ser considerada como parte de un sistema de gestión (y no aisladamente). Por lo tanto, una organización de mantenimiento puede implementar un sistema de gestión integrado que incluya el SMS. Un sistema de gestión integrado puede ser utilizado para capturar múltiples certificados, autorizaciones o aprobaciones o para abarcar otros sistemas de gestión empresarial, tales como los sistemas de gestión de calidad, seguridad, gestión de la salud ocupacional y el medio ambiente. Esto se hace para eliminar la duplicación y explotar las sinergias mediante la gestión de los riesgos a través de múltiples actividades. Por ejemplo, cuando una organización de mantenimiento tiene múltiples aprobaciones, puede escoger por implementar un sistema de gestión único para cubrir todas sus actividades. La organización de mantenimiento deberá decidir cuáles son los mejores medios para integrar o segregar sus SMS para ajustarlos a sus necesidades de negocio u organizacionales.

5.5.2 Un sistema típico de gestión integrado puede incluir:

a) sistema de gestión de la calidad (QMS);

b) sistema de gestión de la seguridad operacional (SMS);

c) sistema de gestión de la seguridad de la aviación (SeMS);

d) sistema de gestión ambiental (EMS);

e) sistema de gestión de la seguridad operacional y salud ocupacional (OHSMS);

f) sistema de gestión financiera (FMS);

g) sistema de gestión de la documentación (DMS) y,

h) sistema de gestión del riesgo de la fatiga (FRMS)

5.5.3 Una organización de mantenimiento podría escoger integrar estos sistemas de gestión basados en sus necesidades únicas. Los procesos de gestión de riesgos y los procesos de auditoría interna son características esenciales de la mayoría de estos sistemas de gestión. Deberá reconocerse que los riesgos y controles de riesgo

desarrollados en cualquiera de estos sistemas podrían tener un impacto en otros sistemas. Además, pueden existir otros sistemas operativos asociados a las actividades empresariales que también pueden integrarse, como la gestión de proveedores, la gestión de instalaciones, entre otros.

5.5.4 Una organización de mantenimiento podría también considerar la aplicación del SMS a otras áreas que no tienen un requisito reglamentario actual para un SMS. Alternativamente, puede haber situaciones en las que se prefiera un SMS individual para cada tipo de actividad de aviación. Los proveedores de servicios deberán determinar los medios más adecuados para integrar o segregar sus sistemas de gestión de acuerdo con su modelo de negocio, el entorno operativo, los requisitos reglamentarios, estatutarios y de las partes interesadas. Sea cual sea la opción tomada, deberá garantizar que reúna los requisitos de SMS.

Beneficios y desafíos de la integración de sistemas de gestión

5.5.5 La integración de las diferentes áreas bajo un sistema de gestión único mejorará la eficiencia mediante:

a) reducción de la duplicación y superposición de procesos y recursos.

b) reducción de las responsabilidades y relaciones potencialmente conflictivas.

c) consideración de los impactos más amplios de los riesgos y las oportunidades en todas las actividades; y

d) permitir un seguimiento y una gestión eficaces del desempeño en todas las actividades

5.5.6 Los posibles desafíos de la integración del sistema de gestión incluyen:

a) los sistemas existentes pueden tener diferentes gerentes funcionales quienes se resisten a la integración, esto podría generar conflictos;

b) podría haber resistencia al cambio para el personal

afectado por la integración, ya que esto requerirá una mayor cooperación y coordinación;

c) impacto en la cultura general de seguridad operacional dentro de la organización ya que puede haber diferentes culturas con respecto a cada sistema que crea conflictos;

d) las reglamentaciones pueden impedir tal integración o los diferentes reguladores y organismos de normalización pueden tener expectativas divergentes sobre cómo se deben cumplir sus requisitos; y

e) la integración de diferentes sistemas de gestión (como QMS y SMS) puede crear trabajo adicional para poder demostrar que se cumplen los requisitos de cada sistema de gestión.

5.5.7 Para maximizar los beneficios de la integración y abordar los desafíos relacionados, el compromiso y liderazgo de la alta dirección es esencial para gestionar el cambio de manera efectiva. Es importante identificar a la persona que tiene la responsabilidad general del sistema de gestión integrado.

5.6. Integración de SMS y QMS

5.6.1 Las organizaciones de mantenimiento tienen tanto sistema de gestión de la seguridad operacional (SMS) y sistema de gestión de calidad (QMS). Algunas veces se integran en un único sistema de gestión. El QMS generalmente se define como la estructura organizacional y las responsabilidades de rendición de cuentas asociadas, recursos, procesos y procedimientos necesarios para establecer y promover un sistema de aseguramiento y mejora continua de la calidad al entregar un producto o servicio.

5.6.2 Ambos sistemas son complementarios, el SMS se centra en la gestión de los riesgos y el rendimiento de la seguridad operacional mientras que el QMS se centra en el cumplimiento de los reglamentos y requisitos prescriptivos para cumplir con las expectativas del cliente y las obligaciones contractuales. Los objetivos de un SMS son identificar los peligros, evaluar el riesgo asociado de seguridad operacional asociado e implementar controles efectivos de riesgos de seguridad operacional. En contraste,

el QMS se enfoca en la entrega consistente de productos y servicios que cumplen con las especificaciones aplicables. No obstante, ambos, el SMS como el QMS:

a) deberán ser planificados y gestionados;

b) involucran todas las funciones organizacionales relacionadas con la entrega de productos y servicios de aviación;

c) identifican procesos y procedimientos ineficaces;

d) se esfuerzan por mejorar continuamente; y

e) tienen el mismo objetivo de proporcionar productos y servicios seguros y confiables a los clientes.

5.6.3 El SMS se centra en:

a) identificación de los peligros relacionados con la seguridad operacional que enfrenta la organización;

b) evaluación del riesgo de seguridad operacional asociado;

c) implementación de controles de riesgo efectivos para mitigar los riesgos de seguridad operacional;

d) medición del rendimiento de seguridad operacional; y

e) mantener una asignación de recursos apropiada para cumplir con los requisitos de rendimiento de seguridad operacional.

5.6.4 El QMS se centra en:

a) cumplimiento de los reglamentos y requisitos;

b) consistencia en la entrega de productos y servicios;

c) cumplimiento con los estándares de rendimiento especificados;

d) entrega de productos y servicios que sean "aptos para el propósito" y libres de defectos o errores.

5.6.5 El monitoreo del cumplimiento de los reglamentos es necesario para asegurar que los controles de riesgo de seguridad operacional, aplicados en forma de reglamentos, sean efectivamente implementados y monitoreados por la organización de mantenimiento. Las causas y factores contribuyentes de cualquier incumplimiento, deberán también ser analizados y abordados.

5.6.6 Dado los aspectos complementarios de SMS y QMS, es posible integrar ambos sistemas sin comprometer cada función. Esto se puede resumir de la siguiente manera:

a) un SMS está soportado por procesos del QMS tales como auditoría, inspección, investigación, análisis de causa raíz, diseño de procesos, análisis estadístico de tendencias y medidas preventivas;

b) un QMS puede identificar problemas de seguridad operacional o debilidad en los controles de riesgos de seguridad operacional;

c) un QMS puede prever problemas de seguridad operacional que existen a pesar de que la organización cumple con los estándares y especificaciones;

d) los principios, políticas y prácticas de calidad deben estar alineados con los objetivos de la gestión de la seguridad operacional; y

e) las actividades del QMS deben considerar peligros identificados y controles de riesgos de seguridad operacional para la planificación y realización de auditorías internas.

5.6.7 En conclusión, en un sistema de gestión integrado con metas unificadas y toma de decisiones teniendo en cuenta los impactos más amplios en todas las actividades, los procesos de gestión de la calidad y gestión de la seguridad operacional serán altamente complementarios y apoyarán el logro de las metas generales de seguridad operacional.

5.7. Análisis de brechas (GAP) e implementación del SMS

5.7.1 Antes de implementar un SMS, la organización de mantenimiento deberá llevar a cabo un análisis de brechas. Esto compara los procesos y procedimientos existentes de

gestión de seguridad operacional del proveedor de servicios con los requisitos de SMS determinados por el Estado. Las organizaciones de mantenimiento ya pueden tener algunas de las funciones de SMS en funcionamiento. El desarrollo de un SMS deberá basarse en las políticas y procesos organizativos existentes. El análisis de brechas identifica las brechas que deberán ser abordadas a través de un plan de implementación de SMS, que define las acciones necesarias para implementar un SMS totalmente funcional y efectivo (Ver Apéndice 2).

5.7.2 El plan de implementación de SMS debe proporcionar una imagen clara de los recursos, tareas y procesos necesarios para implementar el SMS. El calendario y la secuencia del plan de implementación pueden depender de una variedad de factores que serán específicos de cada organización, tales como:

a) requisitos reglamentarios, de clientes y estatuarios;

b) detentar de múltiples certificados (posiblemente con diferentes fechas de implementación reglamentarias);

c) la extensión en que el SMS puede construirse sobre estructuras y procesos existentes;

d) la disponibilidad de recursos y presupuestos;

e) interdependencias entre las diferentes etapas (se debe implementar un sistema de notificaciones antes de establecer un sistema de análisis de datos); y

f) la cultura de seguridad operacional existente.

5.7.3 El plan de implementación del SMS deberá ser desarrollado en consulta con el gerente responsable y otros altos directivos, y se deberá incluir a quien será responsable de las acciones y los plazos. El plan deberá abordar la coordinación con organizaciones externas o contratistas, donde sea aplicable.

5.7.4 El plan de implementación de SMS puede documentarse en diferentes formas, que pueden variar desde una simple hoja de cálculo hasta un software especializado de gestión de proyectos. El plan deberá ser monitoreado regularmente y

actualizado según sea necesario. También deberá aclarar cuándo un elemento específico puede considerarse implementado con éxito (Ver Apéndice 2).

5.7.5 Tanto el Estado como las organizaciones de mantenimiento deberán reconocer que lograr un SMS efectivo puede llevar varios años. Las organizaciones de mantenimiento deberán referirse a su Estado ya que puede haber requisitos para un enfoque por fases para la implementación del SMS

Apéndice 1

ANÁLISIS DE BRECHAS

LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHA INICIAL

1. La lista de verificación será el primer paso de un análisis de brechas del SMS. Sus respuestas generales "Sí/No/Parcial" indicará el alcance de las brechas y permitirá dimensionar la carga de trabajo y el costo que puede ser requerido para cumplir con el requisito reglamentario en la organización de mantenimiento.

2. El cuestionario puede ser adaptado a las necesidades de la organización de mantenimiento y a la naturaleza del mantenimiento realizado. Esta información inicial debe ser útil para que la alta gerencia anticipe, programe y asigne el esfuerzo de implementación requerido por el SMS y, por lo tanto, los recursos que necesitará proporcionar.

3. Una respuesta "Sí" indica que la organización satisface o supera las expectativas del requisito señalado en la pregunta, no siendo necesaria una acción en particular. Una respuesta "No" indica una brecha importante existente en la OMA, en relación con el cumplimiento del requisito indicado en la pregunta, siendo necesario asignar medios e implementar. Una respuesta "Parcial" indica que se requiere una adecuación de lo existente o un trabajo de desarrollo para adecuar el proceso o procedimiento existente a los requisitos de SMS. En el espacio *condición de implementación* se deberá señalar la condición que posee el requisito para ser implementado y aspectos generales de lo requerido para realizarlo.

Componente 1 – POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

a) Elemento 1.1 — Compromiso y responsabilidad de la gestión

1.2.1. ¿Está implementada una política de seguridad operacional?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.2. ¿Refleja la política de seguridad operacional el compromiso de la administración superior acerca de la gestión de la seguridad operacional?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.3. ¿Es adecuada la política de seguridad operacional según la dimensión, naturaleza y complejidad de la organización?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.4. ¿Es pertinente la política de seguridad operacional para la seguridad operacional de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.5. ¿Ha firmado el gerente responsable la política de seguridad operacional?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.6. ¿Se comunica, en toda la OMA, la política de seguridad operacional, con un respaldo visible del gerente responsable?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.7. ¿Se revisa periódicamente la política de seguridad operacional para garantizar que siga siendo pertinente y adecuada para la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

b) Elemento 1.2 — Responsabilidades de la seguridad operacional

1.2.1. ¿Ha identificado la OMA a un gerente responsable que, sin importar otras funciones, tenga la máxima responsabilidad, en nombre de ésta, de la implementación y mantenimiento del SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.2. ¿Tiene el gerente responsable total control de los recursos financieros y humanos necesarios para los trabajos de mantenimiento autorizados, que se realizarán según el certificado de OMA y su lista de capacidad?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.3. ¿Tiene el gerente responsable la autoridad final sobre todas las actividades de mantenimiento de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.4. ¿Ha identificado y documentado la OMA las responsabilidades de seguridad operacional de la gestión, así como también de los gerentes responsables y del personal de mantenimiento, en relación con el SMS?
☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.5. ¿Existe una junta de revisión de seguridad operacional (SRB) para el propósito de revisión del SMS y el rendimiento en materia de seguridad operacional?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.6. ¿Lidera la junta de seguridad operacional el gerente responsable o un delegado asignado correctamente, confirmado debidamente en el manual del SMS o en la documentación de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.7. ¿Incluye la junta de seguridad operacional a los responsables de departamento o jefes de sección pertinentes, según corresponda?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.2.8. ¿Existen grupos de acción de seguridad operacional

(GAP) que trabajan junto con el comité de seguridad operacional (en particular para las organizaciones grandes/complejas)?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

c) Elemento 1.3 — Nombramiento del personal de seguridad operacional clave.

1.3.1. ¿Ha asignado la OMA a una persona calificada (responsable de SMS) para gestionar y vigilar la operación diaria del SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.3.2. ¿Tiene la persona calificada (responsable de SMS) acceso o notificación directa al Gerente Responsable, acerca de la implementación y operación del SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.3.3. ¿Tiene el responsable de administrar el SMS otras responsabilidades que puedan entrar en conflicto o perjudicar su papel como responsable de SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.3.4. ¿Es el puesto de responsable de SMS un puesto alta gerencia, que no es inferior jerárquicamente o subordinado a otros puestos de cargos de gestión de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

d) Elemento 1.4 — Coordinación de la planificación de respuesta ante emergencias.

1.4.1. ¿Tiene la OMA por ubicación física (aeródromos), tipo de habilitaciones (aeronaves o motores), y/o requisitos de explotadores de servicios aéreos, la necesidad de tener un plan de respuesta ante emergencias (ERP)?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.2. ¿Tiene la OMA un plan de respuesta ante emergencias (ERP) adecuado para la dimensión, naturaleza y complejidad de la organización?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.3. ¿Aborda el plan de emergencia/contingencia todos los escenarios de emergencia/crisis posibles o probables, en relación con los suministros de componentes de aeronaves o servicios de mantenimiento de la organización?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.4. ¿Incluye el ERP procedimientos para la producción, la entrega y el respaldo seguros y continuos de los servicios de mantenimiento durante tales emergencias o contingencias?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.5. ¿Existe un plan y registro para los ensayos o ejercicios de entrenamiento, relacionados con el ERP?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.6. ¿Aborda el ERP la coordinación necesaria de su ERP, con los procedimientos de contingencia de emergencia/respuesta de otras organizaciones, si corresponde?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.7. ¿Tiene la OMA un proceso para distribuir y comunicar el ERP a todo el personal pertinente, incluidas las organizaciones externas, si corresponde?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.4.8. ¿Existe un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continua?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

e) 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 DIA / IACC?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.5.2. ¿Aborda la documentación del SMS, el SMS de la OMA, sus componentes y elementos asociados?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.5.3. ¿Está el marco de trabajo de SMS de la OMA alineado con el marco de trabajo del SMS reglamentario?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.5.4. ¿Mantiene la OMA un registro de documentación de respaldo pertinente para la implementación y operación del SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.5.5. ¿Tiene la OMA un plan de implementación de SMS para establecer su proceso de implementación de SMS, incluidas las tareas específicas y los hitos de implementación pertinentes?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.5.6. ¿Aborda el plan de implementación de SMS la coordinación entre el SMS de la OMA y el SMS de los explotadores aéreos, otras OMA, subcontratistas u otras organizaciones externas, cuando corresponda?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

1.5.7. ¿Respalda el gerente responsable el plan de implementación de SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

Componente 2 – GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

a) Elemento 2.1 – identificación de peligros

2.1.1. ¿Existe un proceso para la notificación de peligros / amenazas voluntario de todo el personal de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.1.2. ¿Es simple el proceso de notificación de peligros / amenazas voluntario, está disponible a todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.1.3. ¿Incluye el sistema de procesamiento y recolección y recolección de datos de seguridad operacional (SDCPS) de OMA procedimientos para la notificación de incidentes/accidentes mediante personal de mantenimiento?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.1.4. ¿Es simple la notificación de incidentes / accidentes, accesible para todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la dimensión de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.1.5. ¿Tiene la OMA procedimientos para la investigación de todos los incidentes/accidentes notificados?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.1.7. ¿Existen procedimientos para revisar peligros / amenazas de informes industriales pertinentes para medidas de seguimiento o la evaluación de riesgos, donde corresponda?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

b) 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 causa raíz y de riesgos objetivas?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.2.2. ¿Aprueban los gerentes de áreas o de un nivel superior los informes de evaluación de riesgos, cuando corresponda?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.2.3. ¿Existe un procedimiento para la revisión periódica de los registros de mitigación de riesgos existentes?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.2.4. ¿Existe un procedimiento para explicar las medidas de mitigación cada vez que se identifican niveles de riesgos inaceptables?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.2.5. ¿Existe un procedimiento para priorizar los peligros identificados para las medidas de mitigación de riesgos?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

2.2.6. ¿Existe un programa para la revisión sistemática y progresiva de todos los procedimientos, procesos, instalaciones y los equipos relacionados con la seguridad operacional de la OMA sujetos al proceso de HIRM, como lo identificó la organización?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

Componente 3 – ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

a) 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 mantenimiento de la organización?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.1.5. ¿Incluyen los indicadores de rendimiento en materia de seguridad operacional un control cuantitativo de resultados de seguridad operacional de alta gravedad / baja probabilidad (por ejemplos, tasas de accidentes e incidentes graves), así como también, eventos de baja gravedad / alta probabilidad (por ejemplo, tasa de no cumplimiento, desviaciones)?

☐ Si
☐ No
☐ Parcial
Condición de la 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 con la DIA / IACC y sujetos a éste?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.1.8. ¿Se revisan periódicamente los indicadores de rendimiento en materia de seguridad operacional?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

b) 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 OMA (incluidos los registros de HIRM) cada vez que haya cambios pertinentes a aquellas instalaciones y equipos?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.2.2. ¿Existe un procedimiento para revisar las operaciones y los procesos existentes relacionados con la seguridad operacional de la OMA pertinentes (como cualquier registro de HIRM) cada vez que haya cambios a aquellas operaciones o procesos?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.2.3. ¿Existe un procedimiento para revisar las nuevas operaciones y los procesos relacionados con la seguridad operacional de la OMA, en busca de peligros / riesgos, antes de implementarlos?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

c) Elemento 3.3 — Mejora continua del SMS.

3.3.1. ¿Existe un procedimiento para la evaluación/auditoría interna periódica del SMS?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.3.2. ¿Existe un plan actual de la auditoría/evaluación de SMS interna?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.3.3. ¿Incluye la auditoría de SMS la toma de muestras de las evaluaciones existentes completadas/de riesgos de seguridad operacional?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

3.3.5. ¿Aborda el plan de auditoría de SMS la interfaz de SMS con los subcontratistas o explotadores de servicios aéreos, según corresponda?
☐ Si
☐ No
☐ Parcial
Condición de la implementación:

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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

Componente 4 – PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

a) Elemento 4.1 — Instrucción 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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

4.1.2. ¿Ha tomado el gerente responsable un curso de familiarización, sesión informativa o instrucción de SMS adecuado?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

4.1.3. ¿Se brinda al personal que participa en la evaluación de riesgos instrucción o familiarización adecuadas de la gestión de riesgos?

☐ Si.
☐ No
☐ Parcial
Condición de la implementación:

4.1.4. ¿Existe evidencia de esfuerzos de educación o toma de conciencia del SMS a nivel de la organización?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

b) Elemento 4.2 – comunicación de la seguridad operacional

4.2.1. ¿Participa la OMA en la distribución de información de seguridad operacional a otras OMAs, subcontratistas u organizaciones operativas pertinentes, incluidas las AAC pertinentes?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

4.2.2. ¿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?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

4.2.3. ¿Hay un manual de SMS de la OMA y material guía relacionado que sea accesible o este distribuido a todo el personal de la OMA?

☐ Si
☐ No
☐ Parcial
Condición de la implementación:

Apéndice 2

PLAN DE IMPLEMENTACIÓN

a) DEFINICION DE TAREAS Y ASIGNACIÓN

1. La realización del análisis de brechas ha permitido determinar las brechas o faltantes que posee la OMA para implementar el SMS y/o aquellos proceso o procedimientos que requiere modificar.

2. Estas actividades que deben ser cumplidas en un plazo máximo de treinta y seis (36) meses o tres (3) años, de acuerdo a la regulación RAC-24.145, es necesario que se efectué un análisis detallado de cada una de las brechas determinadas y sean definidas todas las tareas y sub tareas que las OMA deberá realizar para su solución.

3. En este análisis será fundamental establecer el tipo de personal requerido para realizarlo. Una forma de efectuarlo es asignar cada tarea o sub tarea a grupos de trabajo u organizaciones internas de la OMA.

4. Basado en esta definición, la Tabla mostrada en la Figura 1, de este apéndice, permitirá inicialmente establecer todas las actividades que deberá realizar la OMA en el proceso de implementación y llevar posteriormente un control actualizado de su situación de cumplimiento (abierta / cerrada / parcial).

5. Esta tabla debe ser confeccionada siguiendo el orden y detalle del análisis de brechas realizado, incorporando todos los requisitos que deben ser cumplidos en el SMS; determinando y asignando las tareas o sub tareas necesarias de efectuar para cumplir con aquellos elementos en que se determinó una condición de cumplimiento parcial o no cumplido, en el análisis de brechas. Con esta acción estarán definidas en detalle cada una de las actividades a realizar, quien debe efectuarlas y se dispondrá de una herramienta básica para el control de su cumplimiento.

Figura 1 ASIGNACION DE TAREAS DE IMPLEMENTACIÓN DEL SMS.

Ref. de Brecha	Pregunta del análisis de brecha	Respuesta (Si / No /Parcial)	Descripción de la brecha	Medida / tarea necesaria para solucionar la brecha	Tarea asignada Grupo / individuo	Referencia del documento de SMS	Estado de la medida / tarea (abierta / proceso / cerrada)
1.1.1	¿esta implementada una política de seguridad operacional?	Parcial	La política de seguridad operacional existente aborda solo la política de calidad	a) Mejorar la política de seguridad operacional existente para incluir todos los objetivos de SMS o desarrollar una nueva política de seguridad operacional de la OMA para su SMS; b) Solicitar que el gerente responsable apruebe y firme la política de seguridad operacional.	Grupo 1	Capítulo 1, sección 1.3	Abierta
Etc.							

b) PROGRAMA DE IMPLEMENTACIÓN DEL SMS

1. Estas tareas de implementación del SMS definidas y ordenadas en la Tabla de la Figura 1 requerirán que sean organizadas por la OMA dentro del período de tiempo del que dispone (36 meses), por ser parte de los requisitos de certificación de la OMA (RAC-24.145.100).

2. Para cumplir con esto la OMA deberá efectuar una estimación del tiempo requerido para cumplir con cada una de las tareas y sub tareas requeridas y deberá determinar una secuencia de cumplimiento entre ellas que permitan: satisfacer los requisitos previos para el cumplimiento de la siguiente; la disponibilidad de medios humanos y materiales; la solución de errores y/o imprevistos; y el cumplimiento del plazo disponible.

3. Una forma de realizar y presentar el plan de implementación del SMS a la DIA / IACC para su aceptación, se muestra en la Figura 2, de este apéndice, donde en una hoja de cálculo se ha colocado a la izquierda las tareas o acciones pendientes a efectuar y a su derecha se señala el mes o meses en el cual será cumplida cada tarea, divido en cuatro (4) cuatrimestres cada año.

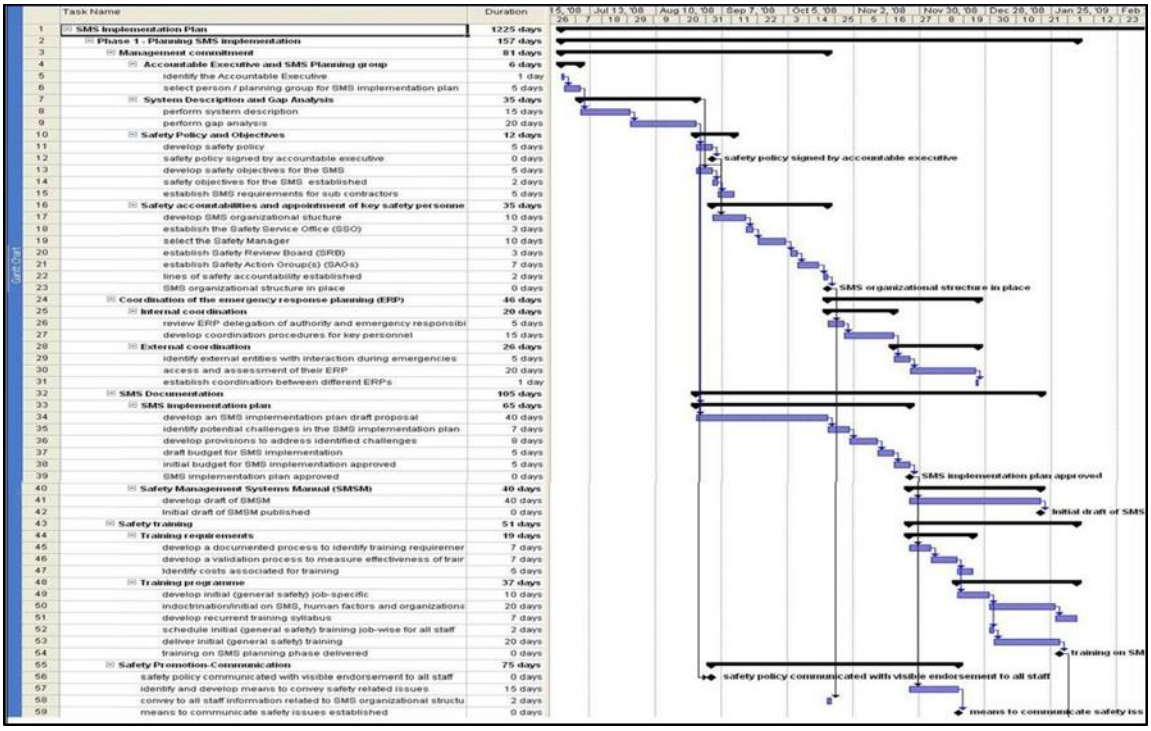
4. Para un enfoque de implementación en fases, estas tareas / acciones se deberán organizar de acuerdo con la asignación de los elementos de SMS, que deben ser cumplidos en cada fase. En cada una de las tareas o actividad se deberá indicar las secuencias de cumplimiento y los hitos de cumplimiento (fechas de inicio y fin).

Figura 2. PROGRAMA DE IMPLEMENTACIÓN DEL SMS.

Medida/tarea necesaria para llenar la brecha	*Ref. del documento de SMS*	*Grupo de tarea/ persona asignada*	*Estado de la medida /tarea*	*Programa/ meses del programa en semanas*												
				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 OMA o desarrollar una política de seguridad operacional de OMA nueva.	Capítulo 1, Sección 1.3.	Grupo de tareas 1	Abierto													
1.1-1 b) Requerir que el ejecutivo responsable apruebe y firme la nueva política de seguridad operacional.																
etc.																

5. Donde se anticipe que la cantidad de tareas o sub tareas a efectuar y sus requisitos son lo suficientemente voluminosos y complejos como para requerir el uso de un software de gestión de proyectos para administrarlas, se puede usar un software como MS Project/diagrama Gantt, o similar según sea conveniente a la OMA. La Figura 3, de este apéndice, muestra un diagrama Gantt.

Figura 3. ASIGNACIÓN DE TAREAS DE IMPLEMENTACION DEL SMS



6. Este Programa de implementación del SMS (Figura 2), unido al cuadro de asignación de tareas de implementación (Figura 1) y el análisis de brechas (Apéndice 1) permitirá cumplir con el requisito RAC-24.145.100 (a)(4) de certificación.

7. Para una organización de mantenimiento en el proceso de certificación como OMA RAC-24.145, o para una OMA previamente certificada antes de que el SMS sea aceptado por la DIA/IACC deberá establecer e implementar los elementos de acuerdo a las siguientes tablas:

Tabla 1. Implementación del SMS

Componentes y elementos del SMS			
1. **Elemento 1.1** del SMS (i): a) identificar al gerente responsable del SMS; b) establecer un equipo de implementación del SMS; c) definir el alcance e interfaces 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 instrucción 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 alta gravedad / baja probabilidad; c) desarrollar SPI de resultados de alta gravedad y baja probabilidad 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 dela calidad.	1. **Elemento 1.1** del SMS (iii): a) mejorar el procedimiento disciplinario / la política existente 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 alta probabilidad y baja gravedad; b) desarrollar SPI de resultado alta probabilidad y baja gravedad y una configuración de objetivos/alertas asociada. c) Desarrollar indicadores avanzados y una configuración de objetivos / alertas asociados. 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.

Tabla 2. Ítems de los elementos que desarrollará un solicitante antes de obtener su aprobación como OMA o la aceptación de la DIA / IACC, del SMS

Componentes y elementos del SMS (elementos por establecer)			
1. **Elemento 1.1** del SMS (i): a) identificar al gerente responsable del SMS; b) establecer un equipo de implementación del SMS; c) definir el alcance y las interfaces 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: d) 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 alta gravedad / baja probabilidad; c) desarrollar SPI de resultados de alta gravedad y baja probabilidad 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 dela calidad.	1. **Elemento 1.1** del SMS (iii): a) mejorar el procedimiento disciplinario / la política existente 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 alta probabilidad y baja gravedad; b) desarrollar SPI de resultado alta probabilidad y baja gravedad y una configuración de objetivos/alertas asociada. c) Desarrollar indicadores avanzados y una configuración de objetivos / alertas asociados. 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.

Tabla 3. Ítems de los elementos que desarrollará una OMA recién certificada hasta completar la implementación del SMS o la aceptación de la DIA/IACC, del SMS

Componentes y elementos del SMS (elementos por implementar)			
1. Elemento 1.1 del SMS (i): a) identificar al gerente responsable del SMS; b) establecer un equipo de implementación del SMS; c) definir el alcance y las interfaces 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 alta gravedad / baja probabilidad; **c) desarrollar SPI de resultados de alta gravedad y baja probabilidad 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 dela calidad.	1. **Elemento 1.1** del SMS (iii): a) mejorar el procedimiento disciplinario / la política existente 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 alta probabilidad y baja gravedad; b) desarrollar SPI de resultado alta probabilidad y baja gravedad y una configuración de objetivos / alertas asociada. c) Desarrollar indicadores avanzados y una configuración de objetivos / alertas asociados. 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.

Apéndice 3

PLAN DE RESPUESTA ANTE EMERGENCIAS

a) Un plan de respuesta ante emergencias (ERP) tiene por objetivo establecer por escrito lo que se debe hacer después de un accidente o un incidente de aviación y quién es responsable de cada acción.

b) Por lo tanto, cualquier organización de mantenimiento (OMA), que no tenga una participación en un accidente o incidente de aviación, no requiere contar con este documento, siendo esta determinación, la primera actividad que debe establecerse para su confección.

c) Una vez determinado que la OMA tendrá alguna participación en accidentes o incidentes de aviación, se estará en condiciones de iniciar su confección, como los ejemplos que se indican a continuación:

- Efectuar trabajos de mantenimiento de línea en aeronaves;
- Trabajar en aeródromos y ser requeridos para prestar apoyo a explotadores aéreos u otras OMAs ante incidentes o accidentes;
- Estar considerado para ayudar o asesorar técnicamente (información técnica o movimiento de aeronaves accidentadas), por un explotador aéreo o los sistemas del aeródromo ante una emergencia;
- Efectuar actividades de mantenimiento en aeronaves con sistemas en funcionamiento (pruebas de oxigeno o motores);
- Detección del incumplimiento de un requisito de aeronavegabilidad que pueda generar una condición de AOG en una aeronave que recibió mantenimiento.

d) Para el caso de OMAs que trabajan en componentes de aeronaves deberían considerarse además los siguientes ejemplos:

- Efectuar trabajos en hangares o bancos de prueba con sistemas funcionando;
- Los casos de donde se establezcan condiciones en las partes o ítems instalados en componentes de aeronaves,

que puedan generar con su mal funcionamiento condiciones operacionales que puedan generar accidentes o incidentes en las aeronaves donde se encuentren instaladas (motores, equipos de navegación, etc.), debiendo informar a los operadores que las recibieron;

- Detección de condiciones de pérdida de calibración o fallas en herramientas sometidas a calibración, que han sido usadas en proceso de mantenimiento o que estos errores puedan generar un accidente o incidente en la aeronave donde se encuentren instaladas (ej.: llaves de torque de componentes de motores, llaves de torque usadas en apreté de pernos de alas o componentes estructurales, instrumentos de calibración de equipamiento de navegación, etc.).

e) Definida la necesidad de confeccionar el ERP, la OMA deberá considerar como controlara en forma especial las primeras horas o días después de un evento de seguridad operacional importante, ya que afectarán directamente su eficacia y las consecuencias que de ella se deriven.

f) Esta respuesta satisfactoria ante una emergencia comienza con una planificación eficaz, donde el ERP deberá ser la base del proceso sistemático con que la OMA gestionará los asuntos de la organización durante las consecuencias de un evento no planificado importante, en el peor de los casos, un accidente o incidente importante.

g) En esta planificación se deberá garantizar y documentar claramente:

i. La delegación de la autoridad durante la emergencia;

ii. La asignación de responsabilidades de emergencia;

iii. La documentación de procedimientos y procesos a seguir en la emergencia;

iv. Una coordinación interna y externa de los esfuerzos, durante la emergencia;

v. La continuación segura de las actividades de mantenimiento básico, mientras se gestiona la crisis;

vi. La identificación de todos los posibles eventos /

escenarios de emergencia y sus medidas de mitigación correspondiente.

h) Para que su contenido pueda lograr ser eficaz para la OMA, su ERP debe:

i. Estar adecuado a su envergadura, naturaleza y complejidad;

ii. Ser revisado y actualizado cuando cambia los detalles, etc.;

iii. Tener detalles de contacto de referencia rápida de todo el personal involucrado;

iv. Incluir listas de verificación y procedimientos específicos para las situaciones de emergencia especificas consideradas;

v. Ser evaluados periódicamente, mediante ejercicios;

vi. Ser fácilmente accesible al personal involucrado y las otras organizaciones que participen en él, según corresponda.

i) Un ERP debe documentar y establecer las responsabilidades, las funciones y las medidas de las diversas agencias y el personal que participan abordando emergencias específicas.

j) Un EPR debe considerar lo siguiente:

i. **Políticas de los Estados.** El ERP debe proporcionar las leyes y reglamentos establecidos por los Estados para responder a emergencias, como para sus investigaciones posteriores, acuerdos con autoridades locales, políticas empresariales y prioridades.

ii. **Organización.** El ERP debe describir las estructuras de 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 funciones y responsabilidades del personal integrante de los equipos de respuesta;

3) establecer las líneas de notificación de la autoridad;

4) configurar un centro de control o gestión de la emergencia (EMC), si corresponde;

5) definir procedimientos para tramitar una gran cantidad de solicitudes de información, especialmente durante los primeros días después de un accidente importante;

6) designar quien será el responsable de la OMA para tratar con los medios;

7) definir qué recursos estarán disponibles para la emergencia;

8) designar quien representará a la OMA en cualquier investigación formal que lleven a cabo el IACC;

9) definir un plan de coordinación y llamado para el personal clave.

Se podría usar un diagrama institucional para mostrar las funciones institucionales y las relaciones de la comunicación.

iii. **Notificaciones**. Se 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 la necesidad de efectuar notificaciones de lo siguiente:

1) la gestión efectuada;

2) las autoridades del Estado a quien informar (búsqueda y salvamento, la autoridad reglamentaria, el consejo de investigación de accidentes, etc.);

3) los servicios de respuesta ante emergencias locales a quienes informar (autoridades del aeródromo, bomberos, policía, ambulancia, instituciones

médicas, etc.);

4) los familiares de las víctimas a informar (puede hacerlo la policía);

5) al personal de la empresa de lo ocurrido;

6) a los medios de comunicación, cuando se requiera o sea consultado y,

7) al área legal, contabilidad, aseguradores, según corresponda.

iv. **Respuesta inicial**. se puede considerar, si es conveniente para la situación, el envió al sitio del accidente o incidente a un equipo de repuesta inicial para aumentar los recursos disponibles y supervisar los intereses de la OMA. Los factores mínimos que deben considerarse en este equipo son:

1) ¿Quién lo liderará?

2) ¿Quién está incluido en él?

3) ¿Quién debe hablar en nombre de la OMA, en el sitio del accidente?

4) ¿Qué equipamiento especial, ropa, documentación, transporte, hospedaje se usará para este equipo?

v. **Ayuda adicional**. La OMA durante la preparación, el ejercicio y la actualización de su ERP debe considerar a sus profesionales con una mayor capacitación y experiencia en seguridad operacional, como un respaldo útil en la planificación y ejecución de tales tareas como:

1) abordar a los supervivientes o partes externas;

2) actuar como pasajeros o clientes en los ejercicios;

3) hablar con el familiar más cercano, las autoridades, etc.

vi. **Centro de gestión de emergencia (EMC).** Un EMC (normalmente en modo de espera) puede establecerse en la sede de la organización, si se requiere, luego de ser activado. Además, se puede establecer un puesto de mando (CP) cerca o en el sitio del accidente o incidente si este es fuera de la ubicación normal de la OMA. En caso de estar trabajando con un explotador aéreo, este EMC será de él y la OMA solo deberá considerar integrarse cuando sea requerido. 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) medios de comunicaciones (teléfonos, fax, Internet, etc.);

3) requisitos de documentación, mantenimiento de los registros durante la emergencia;

4) muebles y suministros de oficina y,

5) documentos de referencias (listas de verificación y procedimientos de respuesta ante emergencias, manuales de la empresa, planes de emergencia del aeródromo y listas telefónicas).

Una OMA pequeña puede contratar los servicios de un EMC para que resguarde los intereses del proveedor de servicios ante una crisis lejos de su ubicación.

vii. **Registros.** Además de la necesidad de la organización de mantener registros de los eventos y las actividades, la organización también necesitará proporcionar información a los equipos de investigación del IACC y del Estado. El ERP debe considerar disponer de los siguientes tipos de información que requieran los investigadores:

1) todos los registros pertinentes acerca del producto o servicio de mantenimiento relacionado con el incidente o accidente;

2) evidencias fotográficas o de otro tipo relativas al suceso;

3) notas de cualquier entrevista (o declaración) con alguien asociado con el evento;

4) listas de puntos de contacto y de cualquier personal de la OMA asociado con el suceso.

viii. **Sitio del accidente.** Para un accidente importante, los representantes de muchas jurisdicciones accederán al sitio, como son, por ejemplo, la policía; bomberos; médicos; autoridades del aeródromo; forenses (funcionarios encargados de examen médico); investigadores de accidentes de la Autoridad AIG; e incluso los medios de comunicación. La coordinación de las actividades de ellos es de responsabilidad de la autoridad de investigación o la policía del Estado, sin embargo, la OMA debe clarificar los siguientes aspectos para el sitio del accidente:

1) nominar a un representante superior de la OMA, 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 de la OMA, supervivientes;

3) las necesidades de los familiares de las víctimas de la OMA;

4) la seguridad de los restos de la aeronave, si le es requerida por el explotador aéreo solamente;

5) manipulación de los restos humanos y la propiedad personal de los fallecidos pertenecientes a la OMA;

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, si le es requerido por el explotador aéreo solamente; etc.

ix. **Medios de prensa**. La respuesta a los medios de comunicación puede afectar cuán bien y rápido se recupere la OMA del accidente o incidente, lo cual hace necesario se consideren claras instrucciones acerca de, por ejemplo:

1) qué información está protegida por la legislación o la investigación (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 gerente principal u otro gerente superior, gerente, propietario);

3) tener declaraciones preparadas para entregar una respuesta inmediata a las consultas de los medios de comunicación;

4) definición de qué información puede divulgarse (qué debe evitarse);

5) la sincronización y el contenido de la declaración inicial de la empresa;

6) actualizaciones regulares de la información a los medios de comunicación.

x. **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.

xi. **Ayuda para la familia**. El ERP debe considerar una guía sobre la forma como la OMA va a ayudar a las víctimas de los accidentes o incidentes o a las organizaciones del explotador aéreo, si corresponde. 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 de la OMA.

xii. **Revisión posterior al suceso**. Se deben incluir instrucciones que aseguren que, después de un incidente, accidente o 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.

xiii. **Listas de verificación**. el proceso de respuesta ante emergencias requiere del uso de las listas de verificación, que ayuden a los participantes, a evitar algún grado de desorientación en su accionar, en un accidente o incidente. Estas listas de verificación incluidas en el ERP de la OMA, deben regularmente:

1) ser revisadas y actualizadas (actualidad de las listas de llamada y los detalles de contacto) y,

2) ser evaluadas mediante ejercicios prácticos de entrenamiento.

xiv. **Capacitación y ejercicios**. Un ERP es un intento en papel, que con suerte y eficiencia nunca la OMA lo deberá probar bajo condiciones reales, por ello se requiere de entrenamiento para garantizar que su contenido tiene el respaldo operacional necesario. Esta condición hace necesario establecer ensayos de llamados y prácticas o ejercicios de emergencias para evaluar sus deficiencias y corregirlas antes que sea necesaria su implementación real.

Apéndice 4

MANUAL DE SEGURIDAD OPERACIONAL (MSMS)

1. **GENERALIDADES**

1.1. Este apéndice es una guía para que la OMA pueda reunir en un solo manual (o documento) de alto nivel sus procedimientos y definir el marco de trabajo de su SMS y sus elementos asociados. Puede ser un manual de SMS independiente (MSMS) o puede integrarse como una parte/capítulo de SMS consolidado dentro del manual de la organización de mantenimiento (MOM) de la OMA, manual aprobado correspondiente a los procedimientos de funcionamiento de la organización.

1.2. Al usar el formato sugerido y los elementos de contenido indicados en este apéndice y adaptarlos a su dimensión y complejidad, es una forma en que la organización puede desarrollar su propio manual de SMS de nivel superior. Los elementos del contenido de cada OMA dependerán del marco de trabajo de SMS específico y los elementos de la organización.

1.3. La descripción debajo de cada elemento deberá ser proporcional al alcance y la complejidad de los procesos de SMS de la OMA.

1.4. El MSMS servirá para comunicar el marco de trabajo de SMS a la organización de forma interna, así como también, con las organizaciones externas relacionadas. El manual debe someterse a la aceptación de la DIA / IACC como evidencia del cumplimiento del requisito de certificación de la OMA.

1.5. Debe existir una clara separación y distinción entre un manual de SMS y los registros y documentos de respaldo operacional. Esto 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**: numerado se incluye una descripción del "objetivo" de esa sección.

b) **Objetivo**: es lo que intenta lograr la organización al hacer lo que se describe en esa sección.

c) **Criterios**: definen el alcance de lo que se debe considerar al escribir esa sección.

d) **Documentos de referencia cruzada**: vinculan la información con otros manuales pertinentes o procedimientos de la organización, los que contienen detalles del elemento o proceso, según corresponda.

3. **CONTENIDO DEL MANUAL**

3.1. En el contenido del manual se incluyen las siguientes secciones:

a) Control de documentos;

b) Requisitos reglamentarios del SMS;

c) Alcance e integración del sistema de gestión de la seguridad operacional;

d) Política de seguridad operacional;

e) Objetivos de seguridad operacional;

f) Responsabilidades de la seguridad operacional y personal clave;

g) Notificación de seguridad operacional y medidas correctivas;

h) Identificación de peligros y evaluación de riesgos;

i) Control y medición del rendimiento en materia de seguridad operacional;

j) Investigaciones relacionadas con la seguridad operacional y medidas correctivas;

k) Instrucción y comunicación de seguridad operacional;

l) Mejora continua y auditoría de SMS;

m) Gestión de los registros de SMS;

n) Gestión del cambio y,

o) Plan de respuesta ante emergencias/contingencia.

3.2. Se señalará para cada sección del MSMS el tipo de información que puede incluirse, de acuerdo a lo indicado en el Párrafo 3.1.

a) **Control de documentos**: Busca establecer cómo el MSMS se mantendrá actualizado y cómo garantizará la OMA que el personal que participa en el SMS tenga la versión actualizada.

Requisitos:

i. Copia impresa o por medio electrónico controlado y con lista de distribución;

ii. Correlación entre el MSMS, el MOM, y otros manuales de la OMA como el manual de calidad o de ingeniería;

iii. Proceso de revisión periódica del MSMS y sus formularios/documentos relacionados para garantizar su sustentabilidad, suficiencia y eficacia constantes;

iv. proceso para la administración, aprobación y aceptación reglamentaria del MSMS.

b) **Requisitos reglamentarios de SMS**: indica los reglamentos de SMS y las guías actuales que pueden entregar una referencia y la toma de conciencia de todos los interesados.

Requisitos:

i. Detallar los reglamentos / normas aplicables actualmente en SMS. Indicar los meses de cumplimiento y las referencias de material explicativo existente para las OMA;

ii. Explicar según corresponda las implicaciones y su importancia de los reglamentos para la organización;

iii. Correlacionar el SMS con otros requisitos o normas aplicables (calidad u otras) según corresponda;

iv. Referenciar reglamentos/requisitos de SMS, documentos guía de SMS, u otros documentos de apoyo.

c) **Alcance e integración del sistema de gestión de la seguridad operacional:** Describir el alcance de las actividades de mantenimiento e instalaciones relacionadas con OMA, dentro de las cuales se aplicará el SMS. También se debe abordar el alcance de los procesos, los equipos y las actividades consideradas idóneas para el programa de identificación de peligros y mitigación de riesgos (HIRM).

Requisitos:

i. Explicar la naturaleza del mantenimiento de la organización y su posición función dentro de la industria aeronáutica en su conjunto un todo;

ii. Identificar las áreas, los departamentos, los talleres y las instalaciones de la organización, dentro de las cuales se aplicará el SMS;

iii. 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 las actividades de mantenimiento y apoyo operacional que realiza la organización. Si es demasiado extenso su alcance, es posible efectuar este control en un documento complementario;

iv. Definir y documentar la integración y las responsabilidades asociadas que se esperan que el SMS

de la OMA, opere o administre en un grupo de explotadores aéreos, OMAs o contratistas interconectados;

v. Si existen otros sistemas de control/gestión relacionados dentro de la organización, como QMS, identificar su integración, donde corresponda;

vi. referenciar los manuales de calidad e ingeniería, si corresponden.

d) **Política de seguridad operacional**: Debe ser una descripción corta, parecida a una declaración de la misión de la OMA, donde se señalen las intenciones, sus principios de gestión y su compromiso con la mejora de la seguridad operacional en su condición de proveedor de servicios de mantenimiento o de componentes de aeronaves.

Requisitos:

i. Debe ser adecuada para la envergadura y complejidad de la organización;

ii. Se debe indicar en la política las intenciones de la OMA, los principios de gestión y el compromiso con la mejora continua;

iii. El gerente responsable debe aprobar y firmarla;

iv. Quienes promoverán esta política serán el gerente responsable y el resto de los gerentes;

v. ser revisada periódicamente.

vi. Todo el personal participa en la implementación y el mantenimiento del sistema de gestión de la seguridad operacional (SMS);

vii. Esta política será comunicada a todos los empleados con la intención de crear conciencia de sus obligaciones individuales en seguridad operacional.

e) **Objetivos de seguridad operacional**: Deben ser una declaración corta que describa en líneas generales, lo que la OMA espera lograr con el SMS.

Requisitos:

i. Se hayan establecido los objetivos de seguridad operacional.

ii. Sean expresados como el compromiso del nivel superior, a su obtención, a través de una declaración firmada.

iii. Existe un proceso formal para desarrollar y asegurar la coherencia de los objetivos de la OMA.

iv. Serán difundidos y distribuidos.

v. Se han asignado recursos para lograrlos.

vi. Se han vinculado con los indicadores de seguridad operacional que facilitarán el control y la medición, como corresponda.

vii. Referenciar documentos de indicadores de rendimiento en materia de seguridad operacional.

f) **Funciones y responsabilidades:** Describir las autoridades y responsabilidades de la seguridad operacional para conocimiento del personal que participa en el SMS.

Requisitos:

i. Para el gerente responsable, garantizar que el sistema de gestión de la seguridad operacional se implemente correctamente y se desempeñe en todas las áreas de la organización, conforme a los requisitos reglamentarios;

ii. La asignación de un gerente (oficina) de seguridad operacional correspondiente, un comité de seguridad operacional o grupos de acción de seguridad operacional, según corresponda.

iii. La existencia de un diagrama de responsabilidades institucionales relativo al SMS.

iv. La definición documentada, para conocimiento del todo

el personal, de las autoridades y responsabilidades de seguridad operacional, en todos los niveles de la organización.

v. Todo el personal comprende sus autoridades y responsabilidades en relación con los procesos, las decisiones y las medidas de la gestión de seguridad operacional.

g) **Notificación de seguridad operacional**: Describir los sistemas de notificación existentes en la OMA, que debe incluir medidas reactivas (informes de accidentes/incidentes, etc.) y proactivas/predictivas (informes de peligros). Deben considerar incluir: el formato del informe, la confidencialidad, los destinatarios, los procedimientos de investigación/evaluación, las medidas correctivas/preventivas y la divulgación del informe.

Requisitos:

i. Un procedimiento que, para la captura de sucesos internos, como accidentes, incidentes y otros sucesos pertinentes para el SMS.

ii. Hace una diferencia entre los informes obligatorios (accidentes, incidentes graves, defectos importantes, etc.) que se deben notificar a la AAC y otros informes de sucesos de rutina, que permanecen dentro de la organización.

iii. existe un sistema de notificación voluntaria y confidencial de peligros / sucesos que considera una protección adecuada de identidad / datos, según corresponda.

iv. Los procesos de notificación son simples, accesibles y proporcionales a la envergadura de la OMA.

v. Los informes de alta gravedad / baja probabilidad y las recomendaciones asociadas se abordan y revisan según el nivel de gestión correspondiente.

vi. Los informes se recopilan en una base de datos adecuada para facilitar el análisis necesario.

h) **Identificación de peligros y evaluación de riesgos:** El sistema debe describir la forma de efectuar la identificación de peligros y cómo se recopilan tales datos; como es el proceso de categorización de peligros / riesgos y su posterior priorización para una evaluación de seguridad operacional documentada; cómo se lleva a cabo el proceso de evaluación de seguridad operacional y finalmente cómo se implementan los planes de acción preventiva.

Requisitos:

i. Los peligros identificados se evalúan, priorizan y procesan para la evaluación de riesgos, según corresponda.

ii. Existe un proceso estructurado para la evaluación de riesgos que implica la evaluación de gravedad, probabilidad, tolerabilidad y controles preventivos;

iii. Los procedimientos de identificación de peligros y evaluación de riesgos se centran en la seguridad operacional, así como también, en su contexto fundamental.

iv. El proceso de evaluación de riesgos, dependiendo de la complejidad de las actividades de mantenimiento que realiza la OMA y las operaciones involucradas en ella, usan las hojas de cálculo, formularios o el software apropiado.

v. El nivel de gestión correspondiente aprueba las evaluaciones de seguridad operacional completadas.

vi. Existe un proceso de evaluación de la eficacia de las acciones correctivas, preventivas y de recuperación que se han desarrollado para solucionar o disminuir las consecuencias de un peligro.

vii. Existe un proceso para la revisión periódica de las evaluaciones de seguridad operacional completadas y la documentación de sus resultados.

i) **Control y medición del rendimiento en materia de seguridad operacional:** Incluye una descripción de los

indicadores de control y rendimiento en materia de seguridad operacional (SPI) del SMS de la OMA.

Requisitos:

i. El proceso formal para desarrollar y mantener un conjunto de indicadores de rendimiento en materia de seguridad operacional y sus objetivos eficaces asociados.

ii. La correlación entre los SPI y los objetivos de seguridad operacional de la OMA, donde corresponda, y el proceso de aceptación de la DIA / IACC de los SPI, donde sea necesario.

iii. El proceso de control del rendimiento de estos SPI, incluido el procedimiento de medidas correctivas, cada vez que se activen tendencias inaceptables o anormales.

iv. Cualquier otro criterio o proceso de control y medición del rendimiento en materia de seguridad operacional o de SMS complementario.

j) **Investigaciones relacionadas con la seguridad operacional y las medidas correctivas:** cómo se procesan y se investigan los accidentes / incidentes / sucesos dentro de la OMA, incluida su correlación con el sistema de identificación de peligros y gestión de riesgos del SMS de la organización.

Requisitos:

i. Procedimientos que garantice que se investiguen de forma interna los accidentes e incidentes notificados.

ii. Divulgación interna de los resultados de los informes de investigación terminados, incluida a la DIA / IACC, según corresponda.

iii. Proceso para garantizar que se lleven a cabo las medidas correctivas definidas o recomendadas en la investigación y para posteriormente evaluar sus resultados / eficacia.

iv. Procedimiento sobre las medidas disciplinarias asociadas con los resultados del informe de investigación.

v. Definiciones claras de las condiciones bajo las cuales se podrían considerar medidas disciplinarias punitivas (por ejemplo, actividad ilegal, imprudencia, negligencia grave o conducta impropia deliberada).

vi. Proceso para garantizar que las investigaciones incluyan la identificación de averías activas, así como también, factores y peligros que contribuyen.

vii. Procedimiento y formato de la investigación que proporcionan hallazgos sobre factores o peligros contribuyentes que serán procesados para la medida de seguimiento con el sistema de identificación de peligros y gestión de riesgos de la organización, donde corresponda.

k) **Instrucción y comunicación de seguridad operacional**: Se debe considerar describir el tipo de SMS y otra instrucción relacionada con la seguridad operacional que recibe el personal; el proceso que permite garantizar la eficacia de ella, y cómo se documentan tales procedimientos de instrucción. También debe describir los procesos / canales de comunicación de seguridad operacional dentro de la OMA.

Requisitos:

i. Documentar el programa de instrucción, la idoneidad y los requisitos;

ii. El proceso de validación existente para medir la eficacia de esta instrucción.

iii. Que considere la instrucción inicial, continua y de actualización, donde corresponda.

iv. Que la instrucción de SMS, sea parte del programa de instrucción general de la OMA;

v. Sea incorporada la toma de conciencia del SMS en el

programa de inducción o adoctrinamiento de la OMA.

vi. Se señalen los procesos / canales de comunicación de la seguridad operacional dentro de la organización.

l) **Mejora continua y auditoría de SMS**: Describe el proceso para la revisión y mejora continuas del SMS.

Requisitos:

i. El proceso para una auditoría / revisión interna regulares del SMS de la organización para garantizar su continua sustentabilidad, suficiencia y eficacia.

ii. 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, calidad, estudios de seguridad operacional, sistemas ISO.

m) **Gestión de los registros de SMS**: Método de almacenamiento de los registros y documentos relacionados con SMS.

Requisitos:

i. Existen registros de SMS o un sistema de archivo que garantiza la conservación de todos los registros generados en conjunto, durante la implementación y la mantención del SMS.

ii. Los registros guardados 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.

iii. 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.

n) **Gestión del cambio:** Proceso de la OMA 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.

Requisitos:

i. Procedimientos para garantizar que los cambios organizacionales y de procedimientos sustanciales consideran cualquier impacto que puedan tener en los riesgos existentes de seguridad operacional.

ii. Procedimientos para garantizar que se lleva a cabo una evaluación de seguridad operacional correspondiente antes de la introducción de nuevos equipos o procesos de mantenimiento o de servicio que tengan implicaciones de riesgos de seguridad operacional.

iii. Procedimientos para la revisión de evaluaciones de seguridad operacional existentes cada vez que se apliquen cambios al proceso o equipo asociado.

o) **Plan de respuesta ante emergencias / contingencia:** Accionar de la OMA en situaciones de emergencia y sus controles de recuperación correspondientes, incluido su compromiso para abordar dichas situaciones. Describir las funciones y responsabilidades del personal clave. Este plan de respuesta ante emergencias puede ser un documento separado o puede ser parte del manual de SMS.

Requisitos:

i. el plan de emergencia describe las funciones y responsabilidades en caso de un incidente, una crisis o un accidente importante;

ii. existe un proceso de notificación con una lista de llamadas de emergencia y un proceso de movilización interno;

iii. la OMA posee procedimientos para las operaciones en condición de emergencia, donde corresponda;

iv. la organización tiene disposiciones con otras organizaciones para recibir ayuda y de servicios de emergencia, según sea aplicable;

v. considera un procedimiento para vigilar el bienestar de todas las personas afectadas y para notificar al familiar más cercano;

vi. se han establecido procedimientos para tratar con los medios de comunicación y temas relacionados con el seguro;

vii. las responsabilidades de investigación de accidentes o incidentes están definidas dentro de la OMA;

viii. el preservar la evidencia, asegurar el área afectada y la notificación obligatoria / gubernamental están definidas y declaradas;

ix. existe una capacitación al personal afectado sobre la preparación y respuesta ante emergencias;

x. se ha desarrollado 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;

xi. existe un procedimiento para registrar las actividades durante una respuesta ante emergencias.

Apéndice 5

INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DEL SMS (SPI)

1. Los ejemplos de indicadores de seguridad operacional, entrega en el lado izquierdo de la Figura 1, algunos indicadores de rendimiento en materia de seguridad operacional (SPI) colectivos del Estado y sus criterios de configuración de alertas y objetivos correspondientes, mientras que los SPI del SMS se reflejan en el lado derecho de esta misma Figura.

2. Los criterios del nivel de alerta y objetivos correspondientes para cada indicador se deben explicar de esta forma para señalar como los indicadores de rendimiento en materia de seguridad operacional del SSP, indicados a la izquierda de las tablas, muestran la correlación requerida con los indicadores de seguridad operacional del SMS (SSP vs SMS).

3. Por este motivo las OMA deben desarrollar los SPI del SMS con el asesoramiento de sus AAC 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 necesaria con su AAC respectiva.

Figura 1. Diagrama de indicador de rendimiento de seguridad operacional de una OMA

Ejemplos de indicadores de rendimiento de seguridad operacional (SSP) e Indicadores de rendimiento de seguridad operacional (SMS)

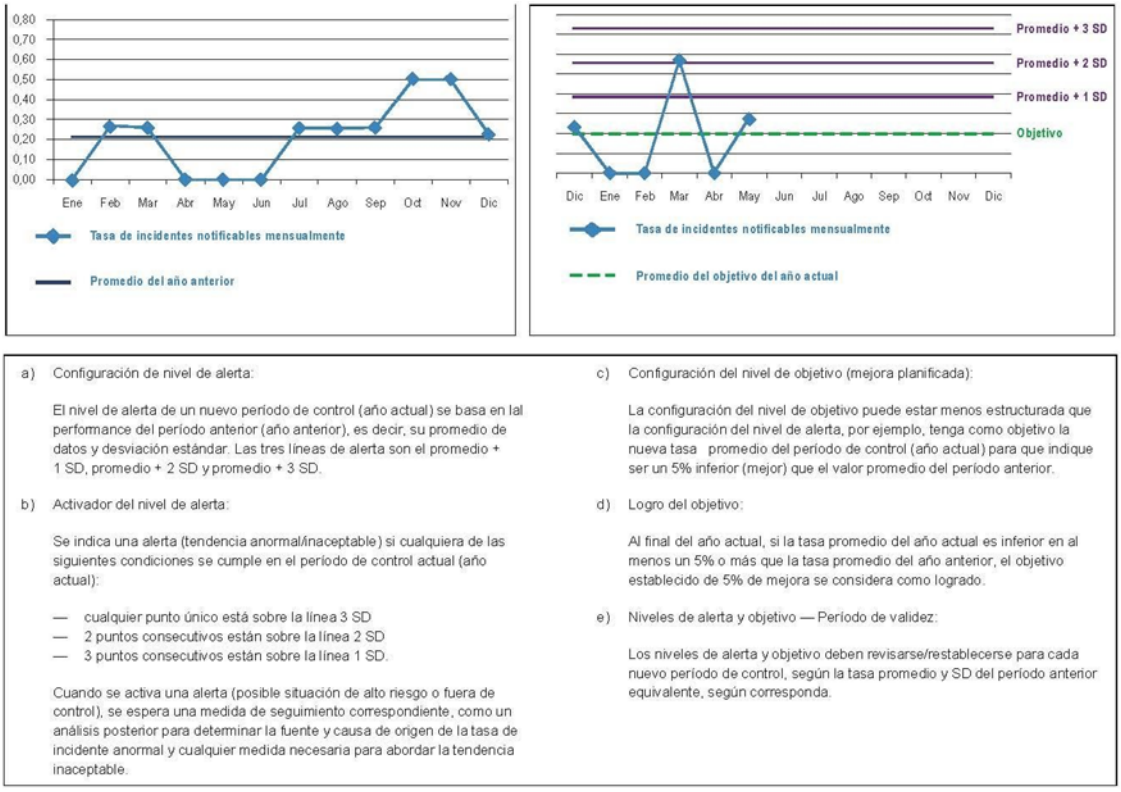
Indicadores de rendimiento en materia de seguridad operacional del SSP (Estado colectivo)						**Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)**					
Indicadores de alta gravedad / baja probabilidad (basados en sucesos/resultados)			**Indicadores de baja gravedad / alta probabilidad** (basados en eventos/actividad)			**Indicadores de alta gravedad / baja probabilidad** (basados en sucesos/resultados)			**Indicadores de baja gravedad / alta probabilidad** (basados en eventos/actividad)		
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**	**Indicador de rendimiento en materia de seguridad**	**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 (resta-blecimiento 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	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)	Consideration	Consideration
ETC											

4. La Figura 2, es un ejemplo del desarrollo de un diagrama del indicador de rendimiento en materia de seguridad operacional del SMS, donde muestra cómo luce un diagrama del indicador de rendimiento de alto impacto en materia de seguridad operacional.

5. En este caso, pueden representar la tasa de devoluciones de componentes por garantías a una OMA de componentes, en relación a la hora / hombre empleada en el programa anual de mantenimiento realizado, o la cantidad de constataciones establecidas en el programa de auditorías de SMS y calidad anual de la OMA o la cantidad de observaciones encontradas en las pruebas finales realizadas a las aeronaves después de efectuar su mantenimiento mayor, en relación a estas mismas

H/H de trabajo anual, etc., siendo evidenciadas con una notificación / obligatoria durante sus procesos de ejecución (control de H/H/; informe de auditorías e inspección final).

Figura 2. Diagrama de indicador de rendimiento en seguridad operacional de una OMA (con configuración de 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.

6. En el diagrama de la izquierda de esta Figura 2, se observa cual fue el rendimiento del año anterior, mientras que en el diagrama de la derecha se observan las variaciones que se están desarrollando en la actualidad, generándose un nuevo rendimiento que deberá ser evaluado en relación al anterior, para determinar su variación y el logro de los objetivos de mejora propuestos para el sistema.

7. Los tres niveles de alerta a utilizar en el proceso, estarán definidos por la variación promedio obtenida para el objetivo en evaluación durante el período anterior, al cual se le deberán sumar una, dos y tres veces respectivamente, la desviación estándar calculada estadísticamente.

8. Con estas referencias definidas, las cantidades determinadas en el año actual permitirán visualizar en el cuadro de la derecha las actualizaciones y su condición en relación a las desviaciones definidas respectos a las alertas, que permitirán tomar acciones de solución si se requieren. Cada uno de estos niveles de alerta estará relacionado con las variaciones estándar que se adhieran al promedio del período anterior.

9. La fórmula siguiente permitirá calcular la desviación estándar (σ), considerando que "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.

$$\sigma = \sqrt{\frac{\sum (x - \mu)2}{N}}$$

10. Con este método de visualización, alerta y control, es factible establecer los objetivos que se representan en un porcentaje (por ejemplo, un 5%) sobre el promedio del año anterior, generándose el diagrama de presentación a partir de una hoja de registros o datos similar a la mostrada en la Figura 3.

Figura 3. Diagrama de indicador de rendimiento en seguridad operacional de una OMA (con configuración de nivel de alerta y objetivo).

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	*H/H total de la OMA*	*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	

Promedio + 1 SD	Promedio + 2 SD	Promedio + 3 SD
0,39	0,56	0,73

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 H/H).

Año actual							
Mes	*H/H total de la OMA*	*Cantidad de incidentes 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					

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

11. Por lo tanto, y mediante la representación mostrada en la figura 4 es posible efectuar el resumen del rendimiento anual en materia de seguridad operacional, donde se comparan los niveles de objetivos buscados con la realidad de lo ocurrido para presentar visualmente el logro o no, de cada uno de los objetivos de alta gravedad / baja probabilidad, baja gravedad / alta probabilidad y avanzados.

Figura 4. Diagrama de indicador de rendimiento en seguridad operacional de una OMA (con configuración de nivel de alerta y objetivo).

Ejemplo de medición de rendimiento de seguridad operacional del SMS de una OMA (para el año 2018)

Indicador de rendimiento en materia de seguridad operacional de alta gravedad / baja probabilidad

Ítem	Descripción del SPI	Criterios del nivel de alerta del SPI (para 2018)	Nivel de alerta violado (Si / No)	Criterios del nivel de objetivos del SPI (para 2018)	Objetivo logrado (Si / No)
1	Tasa de incidentes graves mensual de la OMA J. BARRIOS Y ASOCIADOS, por cada 1 000 H / H	Promedio + 1 / 2 / 3 SD (establecidos anual o cada 2 años)	Si	5% de mejora de la tasa promedio de 2018 sobre la tasa promedio del 2017	No
2	Tasa de incidentes mensuales de la OMA J. BARRIOS Y ASOCIADOS, por cada 1 000 H / H	Promedio + 1 / 2 / 3 SD (establecidos anual o cada 2 años)	Si	3% de mejora de la tasa promedio de 2018 sobre la tasa promedio del 2018	Si
3	etc.				

Indicador de rendimiento en materia de seguridad operacional de baja gravedad / alta probabilidad

Ítem	Descripción del SPI	Criterios del nivel de alerta del SPI (para 2018)	Nivel de alerta violado (Si / No)	Criterios del nivel de objetivos del SPI (para 2018)	Objetivo logrado (Si / No)
1	Tasa de incidentes mensual de la flota combinada del explotador (cada 1 000 H / H	Promedio + 1 / 2 / 3 SD (establecidos anual o cada 2 años)	Si	5% de mejora de la tasa promedio de 2018 sobre la tasa promedio del 2017	No
2	Tasa de % o de hallazgos de la auditoria de QMS interna de la OMA (hallazgo por auditoría)	más del 25% del LEI promedio o cualquier hallazgo de nivel 1 o más de 5 hallazgos de nivel 2 por auditoría	Si	5% de mejora de la tasa promedio de 2018 sobre la tasa promedio del 2017	Si
3	Tasa de informes de peligros voluntarios de la OMA (cada 1 000 H / H)	TBD		TBD	
4	Tasa de notificación de incidentes de avión del explotador (por cada 1 000 H / H)	Promedio + 1 / 2 / 3 SD (establecidos anual o cada 2 años)	No	5% de mejora de la tasa promedio de 2018 sobre la tasa promedio del 2017	Si
5	etc.				

12. Finalmente, la OMA puede establecer un índice general de rendimiento del SMS, obtenido de la suma de todos los indicadores de rendimiento ponderados en un período de tiempo, lo que le permitirá evaluar si su organización en general ha avanzado en relación al período anterior.

13. Una forma de efectuarlo es asignar un valor a la condición particular de cumplimiento de cada indicador, efectuando la suma anual de resultado de su OMA. Así por ejemplo se puede utilizar lo siguiente:

	Indicador de alta gravedad / baja probabilidad	
	SI	**NO**
Nivel de alerta no violado	4	0
Objetivos alcanzados	3	0
	Indicador de baja gravedad / alta probabilidad	
Nivel de alerta no violado	2	0
Objetivos alcanzados	1	0

14. Los objetivos de rendimiento de seguridad operacional deben ser específicos y medibles a un nivel aceptable determinado por la OMA. Una meta de rendimiento de seguridad operacional comprende uno o más indicadores de rendimiento de seguridad, junto con los resultados deseados expresados en términos de esos indicadores.

15. Los objetivos de rendimiento de seguridad operacional se determinan durante la fase de planificación. Se establecen de manera que definen el logro del nivel aceptable de seguridad operacional para la organización. Una meta de rendimiento de seguridad operacional se puede expresar en términos absolutos o relativos. Un ejemplo de un objetivo absoluto podría ser: una devolución de un componente al cual se le brindo un servicio de mantenimiento por cada 1000 componentes trabajados. Un objetivo relativo podría ser una reducción del 5% en incidentes graves durante el próximo año. Un objetivo no tiene que ser un único valor; un rango de valores puede ser apropiado.

16. Una OMA deberá considerar estos factores al establecer sus objetivos de rendimiento de seguridad operacional:

- ✓ los objetivos deberán soportar el objetivo de seguridad primario y los ALosP de la AAC;
- ✓ la selección y priorización de objetivos deben basarse en el riesgo de la seguridad operacional;
- ✓ la fijación de objetivos deberá tomar en cuenta desarrollos nuevos o previstos, tanto internos como externos, que pueden afectar a la OMA, con el fin de medir la respuesta de la organización a esos cambios:
- ✓ los objetivos deberán ser realistas, y tener en cuenta el rendimiento anterior de la organización para determinar la magnitud de los cambios necesarios;
- ✓ la fijación de objetivos debe incluir la evaluación comparativa contra las organizaciones de buena performance (nacional e internacional);
- ✓ la terminación del objetivo período/fecha deberá tener en cuenta el riesgo para la seguridad operacional. Por ejemplo, las áreas críticas para la seguridad deben tener controles de progreso o hitos de desarrollo más frecuente;
- ✓ las OMAs deberán asegurarse de que ningún riesgo está por encima del máximo aceptable y se esfuerzan por conducir el riesgo 'tan bajo como sea razonablemente posible "

17. A continuación, se presentan una serie de ejemplos que pueden utilizarse para el desarrollo de sus propios indicadores de rendimiento de seguridad operacional, antes de utilizarlos es relevante determinar si el indicador es aplicable para su organización, teniendo en cuenta la madurez del SMS de la organización y las características que podría mejorar o que requieran mayor atención:

Tabla 4. INDICADORES DE CUESTIONES SISTEMICAS.

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
CONFORMIDAD	Monitoreo de auditorías/cumplimiento internas:todos los incumplimientos	Reducción del ____% de los incumplimientos analizados por su importancia para la seguridad operacional en comparación con los del año anterior.
CONFORMIDAD	Monitoreo de auditorías/cumplimiento incumplimientos importantes	Reducción del ___ % de incumplimientos significativos en comparación con el número total de internas: incumplimientos significativos del año anterior. Reducción del __% de incumplimientos repetidos dentro del ciclo de planificación de auditorías del año anterior.
CONFORMIDAD	Monitoreo de auditorías / cumplimiento internas: la capacidad de respuesta a las solicitudes de acción correctiva	Reducción en un _____ % del tiempo de espera promedio para completar las acciones correctivas por ciclo de planificación de supervisión – tendencia en comparación con las del año anterior
CONFORMIDAD	Monitoreo de auditorías/cumplimiento todos los incumplimientos	Reducción del _____% de los incumplimientos analizados por su importancia para la seguridad externas: operacional en comparación con los del año anterior.
CONFORMIDAD	Auditorías externas: incumplimientos importantes	Reducción del ____% de incumplimientos significativos en comparación con el número total de incumplimientos significativos del año anterior.
CONFORMIDAD	Auditorías externas: la capacidad de respuesta a las solicitudes de acción correctiva en	Reducción en un _____% del tiempo de espera promedio para completar las acciones correctivas por ciclo de planificación de supervisión - tendencia comparación con las del año anterior
CONFORMIDAD	Consistencia de los resultados entre auditorías internas y externas / control del cumplimiento	Reducción en un ___% de los incumplimientos significativos descubiertos solamente a través de las auditorías externas en comparación con las del año anterior.
EFECTIVIDAD DEL SMS	Gestión estratégica	Incremento en un ____% de la frecuencia con la que los planes oficiales de la organización y los documentos de estrategia son revisados con respecto a la seguridad operacional en relación al año anterior.
EFECTIVIDAD DEL SMS	Compromiso de la dirección	Número de reuniones de gestión dedicadas a la seguridad operacional al trimestre en relación al número total de reuniones planificadas a realizarse en dicho año.
EFECTIVIDAD DEL SMS	Tasa de rotación del personal clave de seguridad operacional	Duración del personal en el cargo, desde el momento es que asume el cargo hasta su retiro, en relación con los últimos dos años. Número de casos en los que se han analizado las razones de la salida del personal clave en relación a la salida de personal en los últimos dos años.
EFECTIVIDAD DEL SMS	Supervisión	Incremento en un ____% del número de casos en que los responsables de la supervisión expresaron seguimiento positivo sobre el comportamiento consciente en materia de seguridad operacional de su personal en comparación con el año anterior

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
EFECTIVIDAD DEL SMS	Notificación	Incremento en un ____% del número de notificaciones recibidas al año y la tendencia en comparación con la del año anterior. Incremento en ____% de las notificaciones a las que se proporcionó información al notificante dentro de los 10 días hábiles, en comparación con las del año anterior. Incremento en ____% de las notificaciones seguidas de una revisión independiente de la seguridad operacional, en comparación con las del año anterior.
EFECTIVIDAD DEL SMS	Identificación de los peligros	Reducción del _____% del número de escenarios de accidentes/incidentes graves analizados para apoyar la Gestión de Riesgos de Seguridad operacional (SRM) en relación al año anterior. Número de nuevos peligros identificados a través del sistema de notificación interno al año y la tendencia por cada 10 peligros identificados. Reducción de un _____% de los incumplimientos de las auditorías externas relacionados con peligros que no habían sido percibidos por el personal / gestión previamente en comparación con el año anterior. Incremento del _____% del número de notificaciones de seguridad operacional recibidas del personal al año y la tendencia en relación al año anterior.
EFECTIVIDAD DEL SMS	Controles de riesgo	Número de nuevos controles de riesgo validados por año en los últimos dos años. Incremento en un _____% del presupuesto total asignado a nuevos controles de riesgo en relación al año anterior.
EFECTIVIDAD DEL SMS	Gestión y desarrollo de las competencias de recursos humanos	Incremento en un _____% de la plantilla para la que se ha establecido una evaluación de competencias en los últimos dos años. Incremento en un _____ % de personal que ha tenido formación en gestión de la seguridad operacional en los últimos dos años (instrucción continua). Incremento en un _____% la frecuencia de revisión de los perfiles de competencias en los últimos dos años. Incremento en un _____% la frecuencia de revisión del alcance, contenido y calidad de los programas de formación en comparación con el año anterior. Número de cambios realizados en los programas de capacitación a raíz de la retroalimentación del personal al año en relación a las 10 últimas revisiones efectuadas. Numero de cambios realizados en los programas de formación a raíz del análisis de las notificaciones de seguridad operacional internas por año en relación a los 10 últimos cambios.
EFECTIVIDAD DEL SMS	Gestión del cambio	Número de cambios organizacionales en los que se ha realizado una evaluación formal de riesgos de seguridad operacional al mes / trimestre / año y la tendencia en relación a los 10 últimos cambios

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
EFECTIVIDAD DEL SMS		Número de cambios en los procedimientos para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al mes/trimestre/año y la tendencia en relación a los 10 últimos cambios. Número de cambios técnicos (por ejemplo: nuevos equipos, nuevas instalaciones, nuevo hardware) para los que se ha realizado una evaluación formal de riesgos de seguridad operacional al mes/trimestre/año y tendencia en relación a los 10 últimos cambios. Número de controles de riesgo implementados por los cambios al mes/trimestre/año y tendencia en relación a los 10 últimos cambios. % de cambios organizacionales/procedimientos/técnicos, etc.) que han sido objeto de evaluación de riesgos en relación a los 10 últimos cambios.
	Gestión de contratistas	Incremento del _____ % de contratistas cuyo rendimiento en materia de seguridad operacional se ha evaluado en relación a la cantidad de contratistas que se tuvo el año anterior. Reducción del _____ % de la frecuencia con la que se determina el rendimiento en materia de seguridad operacional de los contratistas en relación a la del año anterior. Reducción en un ____% del tiempo de demora para impartir capacitación (formación) de los contratistas en seguridad operacional en relación al año anterior. Incremento de un _____ % de los contratistas que han implementado procedimientos de control de la formación en temas de seguridad operacional en relación al año anterior. Incremento en un _____% de los contratistas que tienen establecido un sistema de información (o seguimiento) sobre cuestiones de seguridad operacional con sus clientes en relación al año anterior. Número de notificaciones de seguridad operacional recibidas de los contratistas por año y tendencia en relación a la cantidad de contratistas que tiene la OMA. Número de acciones de seguridad operacional iniciadas debido a la evaluación del rendimiento en materia de seguridad operacional o de las notificaciones de seguridad operacional recibidas al año y tendencia en relación a la cantidad de contratistas que tiene la OMA.
EFECTIVIDAD DEL SMS	Planificación de respuesta ante emergencia	Número de simulacros de emergencia cumplidos por año en relación a la cantidad planificada. Frecuencia de la revisión del ERP en relación a la cantidad simulacros de ERP realizadas. Número de cursos de formación en ERP realizados por mes / trimestre / año en relación a los cursos programados. % de personal formado en el ERP dentro de un cuarto de año en relación al total del personal de la OMA. Número de reuniones con los socios principales y contratistas para coordinar el ERP al mes / trimestre /

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
		año en relación a todas las reuniones planificadas al año.
EFECTIVIDAD DEL SMS	Promoción de la seguridad operacional	Incremento en un _____% del grado en que el personal considera la seguridad operacional como un valor que guía su trabajo diario, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un _____% del grado en que el personal considera que la seguridad operacional es muy valorada por sus gestores, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un ____% del grado en que se aplican los principios de actuación humana, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un _____% del grado en que toma iniciativas el personal para mejorar las prácticas organizacionales o notificar u problema a la gestión, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un _____% del grado en el que el comportamiento consciente de la seguridad operacional es apoyado, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un _____% del grado en el que el personal y la gestión son conscientes de los riesgos de sus operaciones y lo que implican para ellos mismos y para los demás, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior.