CIRCULAR DE ASESORAMIENTO

CA :		**OPS-119-002**
FECHA	**:**	**6/01/16**
REVISIÓN	**:**	**Original**
EMITIDA POR	**:**	**DGAC**

ASUNTO: IMPLANTACIÓN Y ACEPTACIÓN DEL SISTEMA DE GESTION DE LA SEGURIDAD OPERACIONAL – SMS

1. PROPÓSITO

Esta circular de asesoramiento (CA) provee información de orientación para el desarrollo, implantación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS) para explotadores de servicios aéreos 121 y 135, y establece los métodos aceptables de cumplimiento (MAC) de los requisitos RAB 121.110 y 135.055.

Un explotador puede utilizar métodos alternos de cumplimiento, siempre que dichos métodos sean aceptables para la Administración de Aviación Civil (AAC).

La utilización del futuro del verbo o del término debe, se aplica a un explotador que elige cumplir los criterios establecidos en esta CA.

2. SECCIONES RELACIONADAS DE LA REGLAMENTACION AERONÁUTICA BOLIVIANA (RAB) O EQUIVALENTE

RAB 121: Sección 121.110 o equivalente

RAB 135: Sección 135.055 o equivalente

3. DOCUMENTOS RELACIONADOS

Anexo 6	Operación de aeronaves
Anexo 19	Gestión de la seguridad operacional
ICAO Doc. 9859	Manual de gestión de la seguridad operacional

4. DEFINICIONES Y ABREVIATURAS

4.1 Definiciones

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

b) **Ejecutivo responsable.-** Persona única e identificable que es responsable del rendimiento eficaz y eficiente del SSP del Estado o del SMS del explotador.

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

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

e) **Indicadores de alto impacto.-** Indicadores de rendimiento en materia de seguridad operacional relacionados con el control y la medición de sucesos de alto impacto, como

accidentes o incidentes graves. A menudo, los indicadores de alto impacto se conocen como indicadores reactivos.

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

g) **Meta de rendimiento en materia de seguridad operacional.-** El objetivo proyectado o que se desea conseguir, en cuanto a los indicadores de rendimiento en materia de seguridad operacional, en un período de tiempo determinado.

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

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

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

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

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

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

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

4.2 Abreviaturas

a)	AAC	Administración de Aviación Civil/Autoridad de Aviación Civil
b)	ALoSP	Nivel aceptable del rendimiento en materia de seguridad operacional
c)	AOC	Certificado de explotador de servicios aéreos
d)	ERP	Plan de respuesta ante emergencias
e)	HIRA	Identificación de peligros y evaluación de riesgos
f)	HIRM	Identificación de peligros y mitigación de riesgos
g)	IFSD	Parada de motor en vuelo
h)	LSI	Inspección de la estación de línea
i)	ORP	Perfil de riesgo de la organización
j)	OSC	Cultura de seguridad operacional de la organización
k)	POI	Inspector principal de operaciones
l)	QM	Gestión de la calidad
m)	QMS	Sistema de gestión de la calidad

n)	RAB	Reglamentacion Aeronautica Boliviana
o)	SAG	Grupo de acción de seguridad operacional
p)	SDCPS	Sistema de recopilación y procesamiento de datos sobre seguridad operacional
q)	SMS	Sistema de gestión de la seguridad operacional
r)	SPI	Indicador de rendimiento en materia de seguridad operacional
s)	SRC	Comité de revisión de seguridad operacional
t)	SSP	Programa estatal de seguridad operacional

5. ORGANIZACIÓN Y CONTENIDO DE ESTA CIRCULAR

5.1 La presente circular de asesoramiento está organizada en 6 partes. La primera parte, compuesta por los Numerales 1 al 5, contiene los aspectos formales de la circular. La segunda parte, compuesta por el Numeral 6 describe el sistema de gestión de la seguridad operacional. La tercera parte, correspondiente al Numeral 7, contiene una descripción individual de cada uno de los elementos del SMS, y provee orientación y métodos aceptables para su cumplimiento por parte de los explotadores de servicios aéreos. La cuarta parte, correspondiente a los Numerales 8 y 9, describe el proceso de aceptación del SMS para explotadores nuevos, y el proceso de implantación por fases para explotadores certificados. Finalmente la quinta y última parte contiene en Adjuntos la información complementaria, los formularios y las ayudas de trabajo requeridas para las distintas actividades relacionadas con el desarrollo, implantación y mantenimiento de un SMS.

5.2 Esta circular contiene orientación sobre los aspectos prácticos relacionados con la implantación de un SMS. Se recomienda usar la misma junto con el manual de SMS de la OACI, Documento 9859 3ra edición.

5.3 Para aquellas empresas que cuenten con un AOC emitido antes del 31 de diciembre de 2015, o que en dicha fecha se encuentren en la Fase 3 o mayor de su proceso de certificación, se aplicará el proceso de implantación por etapas descrito en el Numeral 8. Los procesos que se encuentren en las Fases I o II, y todos los procesos de certificación para la obtención de un AOC según el RAB 121 o 135 cuya solicitud se presente a partir del 1 de enero de 2016, deberán contar con un SMS aceptado por la AAC en el momento de la emisión de su AOC de acuerdo con los criterios contenidos en el Numeral 9 de la presente circular.

6. INTRODUCCIÓN A LA GESTION DE LA SEGURIDAD OPERACIONAL

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

6.2 La seguridad es una característica dinámica del sistema de aviación, por el cual los riesgos de seguridad operacional deben mitigarse continuamente. Siempre y cuando los riesgos de seguridad operacional se mantengan en un nivel de control adecuado, un sistema tan abierto y dinámico como la aviación podrá seguir gestionándose para mantener el equilibrio correcto de producción y protección.

6.3 Desde de la Sección 6.4 hasta la Sección 6.10 se desarrollan algunos conceptos fundamentales para la adecuada comprensión e implantación del SMS, tales como la recopilación y el análisis de datos de seguridad operacional, indicadores de seguridad operacional y control de rendimiento, y los requisitos basados en rendimiento. El Documento 9859 de la OACI ofrece también información detallada sobre estos conceptos.

6.4 Recopilación de datos de seguridad operacional

6.4.1 La toma de decisiones basada en datos es una de las facetas más importantes de cualquier sistema de gestión. El tipo de datos de seguridad operacional que se recopila puede incluir accidentes e incidentes, eventos, no cumplimientos o desvíos e informes de peligros. Desafortunadamente, muchas bases de datos carecen de la calidad de datos necesaria para ofrecer una base confiable a fin de evaluar las prioridades y la eficacia de las medidas de mitigación de riesgos. Si no se consideran las limitaciones de los datos usados para respaldar las funciones de la gestión de riesgos de seguridad operacional y el aseguramiento de la seguridad operacional, se generarán resultados erróneos del análisis, los que, a su vez, pueden producir decisiones incompletas y desacreditación del proceso de gestión de la seguridad.

6.4.2 Es fundamental para el correcto funcionamiento del SMS del explotador, contar con medios adecuados para la recolección y análisis de la información de seguridad operacional.

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

a) datos de la investigación de accidentes;

b) datos de la investigación de incidentes obligatoria;

c) datos de la notificación voluntaria;

d) datos de la notificación de la aeronavegabilidad continua;

e) datos del control de rendimiento operacional;

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

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

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

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

6.4.4 En la **Figura 1** se muestra una vista esquemática del sistema de datos de seguridad operacional de un Estado, indicando las entradas, los procesos y los resultados relacionados con la recopilación, el análisis y el intercambio de datos de seguridad operacional.

Figura 1 – Vista esquemática del sistema de datos de la seguridad operacional

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

6.5 Análisis de datos de la seguridad operacional

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

a) ayudar a decidir qué hechos son necesarios;

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

c) ayudar a alcanzar conclusiones válidas; y

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

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

6.6 Métodos y herramientas analíticas

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

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

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

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

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

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

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

6.7 Gestión de la información de seguridad operacional

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

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

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

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

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

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

d) operar a un costo relativamente bajo.

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

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

a) registrar eventos de seguridad operacional en varias categorías;

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

c) controlar tendencias;

d) compilar análisis, gráficos e informes;

e) revisar registros históricos;

f) compartir datos de seguridad operacional con otras organizaciones;

g) controlar investigaciones de eventos; y

h) controlar la implementación de medidas correctivas.

6.8 Protección de los datos de seguridad operacional

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

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

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

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

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

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

6.9 Indicadores de seguridad operacional y control de rendimiento

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

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

6.9.3 El análisis usado para controlar continuamente la seguridad operacional debe estar en la forma de una extracción de datos periódica para generar un diagrama o gráfico de tendencia, actualizado de forma mensual o trimestral, como se muestra en la Figura 3. Este diagrama de datos proporciona información sobre la tasa de incidentes de notificación mensual, considerando la cantidad de horas de vuelo (FH) acumuladas por la flota del explotador. Una carga periódica (mensual) de los datos de la tasa de incidentes permitirá que el gráfico sirva como un indicador de control de tendencia continua. Luego de aplicar el diagrama del indicador de control de tendencia continuo, el siguiente paso será transformarlo en un indicador de medición del rendimiento en materia de seguridad operacional al configurar los niveles de objetivos y alertas dentro del diagrama. Este paso se debe hacer de preferencia donde los puntos de datos históricos ya se hayan generado en el diagrama. Estos puntos de datos históricos (rendimiento histórico) será la base para configurar o definir niveles de tendencia inaceptables, así como también, cualquier nivel de mejora deseado que se deba lograr dentro de un período especificado. En el Párrafo 3.1 de la Sección 7 así como en el Adjunto G se incluye la orientación para el desarrollo de los indicadores de rendimiento en materia de seguridad operacional y la configuración de objetivos y alertas asociadas.

Figura 2 - Diagrama de análisis de datos básico (captura de pantalla)

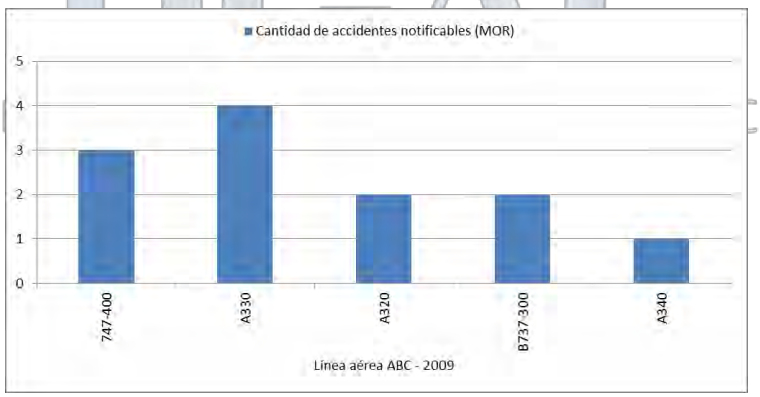
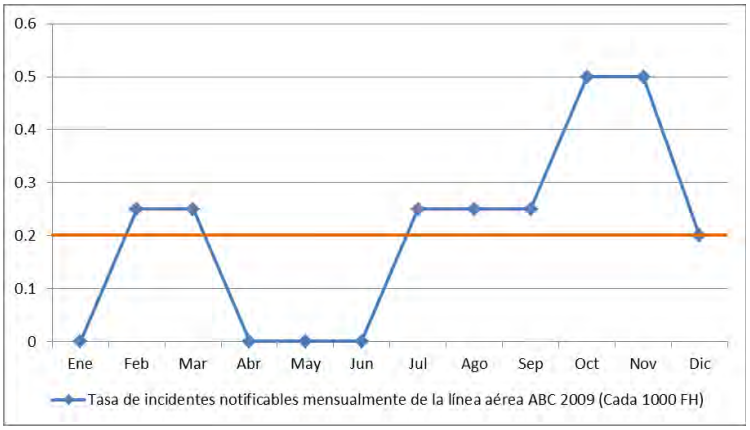


Figura 3 - Diagrama del indicador de seguridad operacional de control continuo



6.10 Requisitos basados en rendimiento

6.10.1 Comprensión de requisitos basados en rendimiento

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

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

6.10.1.3 En un entorno de seguridad operacional mejorado, basado en rendimiento, ciertos elementos basados en rendimiento se introducen dentro de un marco de trabajo prescriptivo. Esto permitirá que el aspecto de “cumplimiento” de un reglamento tenga espacio para un rendimiento más flexible basado en riesgos (y, por lo tanto, más dinámico).

6.10.1.4 Como resultado, algunos elementos dentro de los marcos de trabajo de SMS y SSP pueden administrarse en un enfoque cada vez más basado en rendimiento que tan solo prescriptivo. Estos elementos basados en rendimiento están bajo los componentes del aseguramiento de la seguridad operacional y la gestión de riesgo de seguridad operacional de los marcos de trabajo respectivos.

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

6.10.2 Requisitos previos para los requisitos basados en rendimiento

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

6.10.3 Línea base y nivel equivalente de seguridad operacional

6.10.3.1 El resultado del rendimiento en materia de seguridad operacional de la introducción de los elementos basados en rendimiento, dentro o complementarios a un marco de trabajo de SMS, no debe ser peor que el de un marco de trabajo reglamentario existente solo prescriptivo. Para evaluar o controlar que tal “equivalencia” sea de hecho el caso, deben existir indicadores de seguridad operacional para controlar el resultado general de los eventos (sucesos de no cumplimiento) del sistema/proceso pertinente para el cual se introducirá el elemento basado en rendimiento.

6.10.3.2 Como ejemplo, la tasa de incidentes promedio de la planificación de vuelo y gestión de combustible (FPFM) general luego de la introducción de las disposiciones basadas en rendimiento no debe ser peor que la tasa de incidentes antes de la introducción de las disposiciones de FPFM basadas en rendimiento. Mediante un proceso de comparación, el rendimiento de "línea base" previo a la implementación puede verificarse si se compara con el rendimiento posterior a la implementación, para ver si se ha mantenido un nivel de rendimiento “equivalente”. Si el rendimiento posterior a la implementación resulta ser mejor, entonces se ha manifestado realmente un "mejor" nivel de rendimiento. Donde exista una degradación del rendimiento del sistema, el explotador debe trabajar junto con el regulador para verificar los factores causativos y tomar medidas según corresponda, las que pueden incluir la modificación del requisito basado en rendimiento o, donde corresponda, la restauración de los requisitos preceptivos básicos. En el Párrafo 3.1 de la Sección 7 y en el Adjunto G de esta circular se señalan detalles de cómo se puede medir el rendimiento del sistema mediante indicadores de rendimiento en materia de seguridad operacional.

6.10.4 Control y medición basada en rendimiento

6.10.4.1 El control y la medición de un proceso basado en rendimiento se deben llevar a cabo mediante indicadores de rendimiento, calidad o seguridad operacional adecuados que rastreen continuamente el rendimiento de dicho proceso. Los parámetros de dicho seguimiento de rendimiento pueden ser resultados de sucesos, desviaciones o cualquier tipo de evento que refleje el nivel de seguridad operacional, calidad o riesgo del proceso. Se debe usar un diagrama de tendencia de datos para rastrear tales resultados. Los sucesos del resultado deben rastrearse normalmente como tasas de sucesos en lugar de números absolutos. Junto con tales indicadores, se deben ajustar los niveles de alertas al igual que los niveles perseguidos de mejora que desee para cada indicador, donde corresponda.

6.10.4.2 Estos sirven como marcadores para definir qué es una tasa de sucesos anormal/inaceptable, así como también, la tasa (mejora) de objetivos deseada del indicador. La configuración del nivel de alerta servirá eficazmente como la línea demarcada entre la región de tendencia aceptable y la región inaceptable para un indicador de seguridad operacional.

6.10.4.3 Así que, mientras la tasa de sucesos de un proceso no presente una tendencia que vaya más allá o viole los criterios del nivel de alerta establecidos, la cantidad de tales sucesos se

considerará aceptable (no anormal) para ese período de control. Por otra parte, el propósito de un nivel de mejora objetivo es lograr el nivel de mejora deseado dentro de un hito futuro definido o período de control. Con tal configuración de alertas y objetivos, se vuelve aparente que el resultado del rendimiento cualitativo/cuantitativo puede derivarse al final de un período de control dado. Esto se puede hacer al contar la cantidad de violaciones de alertas o la cantidad de objetivos logrados para un indicador individual o un paquete de indicadores de seguridad operacional. Los ejemplos de los indicadores de rendimiento en materia de seguridad operacional y las metodologías de configuración de objetivos/alertas se abordan más a fondo en el Párrafo 3.1 de la Sección 7 y en el Adjunto G.

6.10.5 Vigilancia de los requisitos basados en rendimiento

6.10.5.1 A diferencia de la auditoría de requisitos prescriptivos independientes, la evaluación de un proceso basado en rendimiento requeriría que el asesor tomara en cuenta el contexto de dicho proceso/elemento dentro de su marco de trabajo reglamentario general, así como también, dentro de la complejidad de la organización auditada.

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

7. ELEMENTOS DE UN SMS Y CRITERIOS DE ACEPTABILIDAD

7.1 Se debe tener presente que la dimensión del marco de trabajo debe ser proporcional a la envergadura de la organización y la complejidad de los productos o servicios proporcionados.

7.2 El marco de trabajo incluye cuatro componentes y doce elementos, los que representan los requisitos mínimos para la implementación y aceptación del SMS. Los cuatro componentes de un SMS son:

a) política y objetivos de seguridad operacional;

b) gestión de riesgos de seguridad operacional;

c) aseguramiento de la seguridad operacional; y

d) promoción de la seguridad operacional.

7.3 Las políticas y objetivos de seguridad operacional crean el marco de referencia para el SMS. El objetivo del componente de gestión de riesgos de seguridad operacional es identificar peligros, evaluar los riesgos relacionados y desarrollar mitigaciones adecuadas en el contexto de la entrega de los productos y servicios de la organización. Se logra el aseguramiento de la seguridad operacional mediante procesos constantes que controlan el cumplimiento de las normas internacionales y los reglamentos nacionales. Es más, el proceso de aseguramiento de la seguridad operacional proporciona confianza en que el SMS funciona como fue diseñado y es eficaz. La promoción de la seguridad operacional proporciona la toma de conciencia y capacitación necesarias.

7.4 El marco de trabajo consta de cuatro componentes y doce elementos que constituyen los requisitos mínimos para la implantación de un SMS:

1. Política y objetivos de seguridad operacional

1.1 Responsabilidad funcional y compromiso de la dirección

1.2 Obligación de rendición de cuentas sobre la 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

7.5 A continuación se describen cada uno de los elementos del SMS, y se acompañan orientaciones sobre los medios aceptables de cumplimiento así como los criterios de aceptabilidad por parte de la AAC.

1. Política y objetivos de seguridad operacional

La política de seguridad operacional describe los principios, procesos y métodos del SMS de la organización para lograr los resultados deseados de la seguridad operacional. La política establece el compromiso de la administración superior para incorporar y mejorar continuamente la seguridad operacional en todos los aspectos de sus actividades. La administración superior desarrolla objetivos de seguridad operacional a nivel de la organización medibles y asequibles que puedan alcanzarse.

1.1 Responsabilidad funcional y compromiso de la dirección

1.1.1 El explotador deberá definir su política de seguridad operacional de acuerdo con requisitos internacionales y nacionales. La política de seguridad operacional deberá:

a) reflejar el compromiso institucional acerca de la seguridad operacional;

b) incluir una clara declaración sobre la disposición de los recursos necesarios para la implementación de la política de seguridad operacional;

c) incluir procedimientos de notificación de seguridad operacional;

d) indicar claramente qué tipos de comportamientos son inaceptables, en relación con las actividades de aviación del explotador e incluir las circunstancias según las cuales no se aplicaría una medida disciplinaria;

e) tener la firma de un ejecutivo responsable de la organización;

f) comunicarse, con un respaldo visible, en toda la organización; y

g) revisarse periódicamente para garantizar que sigue siendo pertinente y adecuado para el explotador.

1.1.2 En la Adjunto A se muestra un ejemplo de una declaración de política de seguridad operacional.

1.1.3 Luego de haber desarrollado una política de seguridad operacional, la administración superior deberá:

a) respaldar visiblemente la política;

b) comunicar la política a todo el personal correspondiente;

c) establecer objetivos de seguridad operacional para el SMS y la organización (de acuerdo con 1.1.4); y

d) establecer objetivos de seguridad operacional que identifiquen lo que intenta alcanzar la organización en términos de gestión de la seguridad operacional (de acuerdo con 1.1.4).

1.1.4 Los objetivos de seguridad operacional del explotador son declaraciones de alto nivel que describen el contexto general de lo que el SMS pretende lograr. Los objetivos de seguridad operacional deben ser específicos, medibles, alcanzables y realistas. Algunos ejemplos de estos objetivos son los siguientes:

- Minimizar las consecuencias y la gravedad de los accidentes e incidentes cuando ocurran.
- Reducir la cantidad de accidentes e incidentes.
- Incorporar la seguridad operacional en todas las actividades operativas, de mantenimiento e instrucción.
- Evitar daños y lesiones a la propiedad y el personal de la empresa.
- Considerar las implicaciones en materia de seguridad operacional cuando se incorporan nuevos equipos de vuelo, instalaciones o procedimientos.
- Cumplir con las leyes, reglamentos y políticas y procedimientos internos relacionados con la seguridad operacional.
- Etc.

1.1.5 Los objetivos de rendimiento en materia de seguridad operacional (SPI) que se detallan en el Párrafo 3.1 de la Sección 7 y en el Adjunto G de esta circular, están directamente relacionados y se derivan de los objetivos de seguridad operacional.

1.1.6 La responsabilidad funcional y compromiso de la dirección será aceptable para la AAC si se han observado los siguientes criterios:

- *Se ha desarrollado la política de acuerdo con el Adjunto A y está firmada por el ejecutivo responsable.*
- *La alta dirección ha respaldado abiertamente esta política, por ejemplo con asignación de una partida presupuestaria adecuada para las actividades relacionadas con el SMS.*
- *Existe evidencia objetiva de que se ha comunicado la política y es accesible a todo el personal del explotador.*
- *Se han establecido y publicado en el manual del SMS o documento equivalente los objetivos de seguridad operacional del explotador, según el Párrafo 1.1.4, y están alineados a los ALoSP del Estado si éstos han sido desarrollados.*

1.2 Obligación de rendición de cuentas sobre la seguridad operacional

1.2.1 El explotador:

a) identificará al directivo que, independientemente de sus otras funciones, tenga la responsabilidad funcional y obligación de rendición de cuentas definitivas, en nombre de la organización, respecto de la implantación y el mantenimiento del SMS;

b) definirá claramente las líneas de obligación de rendición de cuentas sobre la seguridad operacional para toda la organización, incluida la obligación directa de rendición de cuentas sobre seguridad operacional de la administración superior;

c) determinará la obligación de rendición de cuentas de todos los miembros de la administración, independientemente de sus otras funciones, así como la de los empleados, en relación con el rendimiento en materia de seguridad operacional del SMS;

d) documentará y comunicará la información relativa a las responsabilidades funcionales, la obligación de rendición de cuentas y las atribuciones de seguridad operacional de toda la organización; y

e) definirá los niveles de gestión con atribuciones para tomar decisiones sobre la tolerabilidad de riesgos de seguridad operacional.

1.2.2 En el contexto de SMS, responsabilidad significa ser el responsable final del rendimiento en materia de la seguridad operacional, ya sea a nivel de SMS general (ejecutivo responsable) o a niveles específicos del producto/proceso (miembros del equipo de gestión). Esto incluye ser responsable de garantizar que se tomen medidas correctivas adecuadas para abordar los peligros y errores notificados, así como también, responder ante accidentes e incidentes.

1.2.3 Al exigir que el explotador identifique al ejecutivo responsable, la responsabilidad del rendimiento en materia de seguridad operacional general se ubica en un nivel en la organización que tenga la autoridad para tomar medidas a fin de garantizar que el SMS sea eficaz. En el contexto del SMM, el término “responsabilidades” puede considerarse como aquellas responsabilidades que no pueden delegarse.

1.2.4 El ejecutivo responsable que identificó el explotador es la única persona con total responsabilidad del SMS, incluida la responsabilidad de proporcionar los recursos esenciales para su implementación y mantenimiento. Las autoridades y responsabilidades del ejecutivo responsable incluyen, entre otras:

a) la disposición y asignación de recursos humanos, técnicos, financieros y de otro tipo necesarios para el rendimiento eficaz y eficiente del SMS;

b) la responsabilidad directa de la conducta de los asuntos de la organización;

c) la autoridad final sobre las operaciones con certificación/aprobación de la organización;

d) el establecimiento y la promoción de la política de seguridad operacional;

e) el establecimiento de los objetivos de seguridad operacional de la organización;

f) actuar como promotor de la seguridad operacional de la organización;

g) tener la responsabilidad final para la resolución de todos los problemas de seguridad operacional; y

h) el establecimiento y mantenimiento de la competencia de la organización para aprender del análisis de los datos recopilados mediante sus sistemas de notificación de seguridad operacional.

1.2.5 Las responsabilidades descritas anteriormente no pueden delegarse.

1.2.6 Según la envergadura, estructura y complejidad de la organización, el ejecutivo responsable puede ser:

a) el funcionario ejecutivo principal de la organización del explotador;

b) el presidente del consejo de directores;

c) un socio principal; o

d) el propietario.

1.2.7 Todos los puestos, las responsabilidades y las autoridades relacionadas con la seguridad operacional de la aviación deben definirse, documentarse y comunicarse en toda la organización. Las responsabilidades de la seguridad operacional de cada gerente superior (líder de departamento o persona responsable de una unidad funcional) son componentes integrales de sus descripciones laborales. Dado que la gestión de la seguridad operacional es una función comercial principal, cada gerente superior tiene un grado de participación en la operación del SMS.

1.2.8 El explotador es responsable del rendimiento en materia de seguridad operacional de los productos o servicios que proporcionan los subcontratistas que no requieren una certificación o aprobación de seguridad operacional por separado.

1.2.9 Si bien es cierto que no se requiere que todos los subcontratistas tengan necesariamente un SMS, sigue siendo la responsabilidad del explotador garantizar que se cumplan sus propios requisitos de rendimiento en materia de seguridad operacional. En cualquier caso, es fundamental que el SMS del explotador interactúe lo más perfectamente posible que se pueda con los sistemas de seguridad operacional o los subcontratistas que proporcionan productos o servicios pertinentes para la operación segura de la aeronave. La interfaz entre el SMS de la organización y aquel del sistema de seguridad operacional del proveedor de subproductos o subservicios debe abordar la identificación de peligros, la evaluación de riesgos y el desarrollo de estrategias de mitigación de riesgos, donde corresponda. El explotador debe garantizar que:

a) haya una política que establezca claramente un flujo de responsabilidad y autoridad de seguridad operacional entre el explotador y el subcontratista;

b) el subcontratista tenga un sistema de notificación de seguridad operacional proporcional a su envergadura y complejidad, que facilite la identificación temprana de peligros y averías sistémicas de interés para el explotador;

c) el consejo de revisión de seguridad operacional del explotador incluya la representación del subcontratista, donde corresponda;

d) se hayan creado indicadores de seguridad operacional/calidad para controlar el rendimiento del subcontratista, donde corresponda;

e) el proceso de promoción de la seguridad operacional del explotador garantiza que los empleados del subcontratista cuenten con las comunicaciones de seguridad operacional correspondientes de la organización; y

f) se haya desarrollado y probado cualquier papel, responsabilidad y función del subcontratista pertinente para el plan de respuesta ante emergencias del explotador.

1.2.10 Las responsabilidades y autoridades relacionadas con SMS de todos los gerentes superiores correspondientes deben describirse en el manual del SMS de la organización. Las funciones de seguridad operacional obligatorias que realiza el gerente de seguridad operacional, la oficina de seguridad operacional, los grupos de acción de seguridad operacional, etc., pueden incorporarse en las descripciones, los procesos y los procedimientos de trabajo existentes.

1.2.11 La función del gerente de seguridad operacional se describe en detalle en la Sección

1.2.12 A partir de una perspectiva de responsabilidad, la persona que realiza la función del gerente de seguridad operacional es responsable del rendimiento del SMS ante el ejecutivo responsable y de la entrega de servicios de seguridad operacional a los otros departamentos en la organización.

1.2.13 La obligación de rendición de cuentas sobre la seguridad operacional será aceptable para la AAC si se han observado los siguientes criterios:

- *El ejecutivo responsable está plenamente identificado y ha sido designado observando la orientación de 1.2.3 y 1.2.6.*
- *Las obligaciones en materia de seguridad operacional así como las líneas de obligación de rendición de cuentas sobre la seguridad operacional, para toda la organización, incluidos la de la administración superior, el encargado o gerente del SMS y los gerentes o responsables de área están claramente definidas, documentadas y disponibles.*
- *Los niveles de atribución para la toma de decisiones sobre la tolerabilidad de los riesgos de seguridad operacional están claramente definidas, documentadas y disponibles.*
- *La autoridad y responsabilidades del ejecutivo responsable incluyen al menos aquellas señaladas en 1.2.4.*
- *Existe una declaración expresa de que las responsabilidades del ejecutivo responsable en materia de seguridad operacional no pueden delegarse.*
- *Los puestos, las responsabilidades y las autoridades relacionadas con la seguridad operacional han sido definidas, publicadas y comunicadas a toda la organización.*
- *Existe una declaración expresa de que el explotador es responsable del rendimiento en materia de seguridad operacional de los productos o servicios que proporcionan los subcontratistas.*
- *Se han establecido y publicado los procedimientos del explotador que garantizan el cumplimiento de 1.2.9 con relación a los subcontratistas.*
- *Todos los puntos anteriores están documentados en el manual de SMS del explotador.*

1.3 Designación del personal clave de seguridad operacional

1.3.1 El explotador designará un gerente de seguridad operacional que será responsable de la implantación y el mantenimiento de un SMS eficaz.

1.3.2 El nombramiento de un gerente de seguridad operacional calificado es clave para la implementación y el funcionamiento eficaces de una oficina de servicios de seguridad operacional. Las funciones del gerente de seguridad operacional incluyen, entre otras:

a) gestionar el plan de implementación del SMS en nombre del ejecutivo responsable;

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

c) controlar las medidas correctivas y evaluar sus resultados;

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

e) mantener registros y documentación de la seguridad operacional;

f) planificar y facilitar una capacitación de seguridad operacional para el personal;

g) proporcionar consejos independientes sobre asuntos de seguridad operacional;

h) controlar las preocupaciones de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones de la organización orientadas a la entrega de servicios;

i) coordinarse y comunicarse (en nombre del ejecutivo responsable) con la autoridad de vigilancia del Estado y otras entidades estatales, según sea necesario, sobre temas relacionados con la seguridad operacional; y

j) coordinarse y comunicarse (en nombre del ejecutivo responsable) con organizaciones internacionales sobre temas relacionados con la seguridad operacional.

1.3.3 Los criterios de selección de un gerente de seguridad operacional deben incluir, entre otros, los siguientes:

a) experiencia de gestión de seguridad operacional/calidad;

b) experiencia operacional;

c) antecedentes técnicos para comprender los sistemas que respaldan las operaciones;

d) habilidades para relacionarse con las personas;

e) habilidades analíticas y de solución de problemas;

f) habilidades de gestión de proyectos; y

g) habilidades de comunicaciones oral y escrita.

1.3.4 El gerente de seguridad operacional es la persona responsable de la recopilación y el análisis de los datos de seguridad operacional y la distribución de información de seguridad operacional asociada a los gerentes de línea.

1.3.5 El Adjunto B de este capítulo contiene una muestra de descripción de trabajo de un gerente de seguridad operacional. El personal adicional, cuando corresponde, designado para apoyar las actividades que realiza el gerente de seguridad operacional dependerá de la dimensión y complejidad del explotador. Para las organizaciones pequeñas, puede ser viable combinar las funciones de gestión de calidad y seguridad operacional dentro de la misma oficina.

1.3.6 El gerente de seguridad operacional es la persona responsable de la recopilación y el análisis de los datos de seguridad operacional y la distribución de información de seguridad operacional asociada a los gerentes de línea. La distribución de la información de seguridad operacional mediante la oficina de servicios de seguridad operacional es el primer paso en el proceso de gestión de riesgos de seguridad operacional. Esta información la deberán usar los gerentes de línea para mitigar los riesgos de seguridad operacional, que inevitablemente requieren la asignación de los recursos. Los recursos necesarios podrían estar disponibles fácilmente para los gerentes de línea para este propósito.

1.3.7 Además, se requiere de un proceso formal para evaluar la eficacia y eficiencia de cualquier estrategia de mitigación usada para lograr los objetivos de rendimiento en materia de seguridad operacional acordados de la organización. Es recomendable la creación de un comité de revisión de seguridad operacional (SRC). El SRC proporciona la plataforma para lograr los objetivos de la asignación de recursos y para evaluar la eficacia y eficiencia de las estrategias de mitigación de riesgos. El SRC es un comité de muy alto nivel, liderado por un ejecutivo responsable y se compone de gerentes superiores, lo que incluye gerentes de línea responsables de las áreas funcionales, así como también, de aquellos departamentos administrativos pertinentes. El gerente de seguridad operacional participa en el SRC solo en una función de asesoría. El SRC puede reunirse con poca frecuencia, a menos que circunstancias excepcionales indiquen lo contrario. El SRC:

a) controla la eficacia del SMS;

b) controla que se tome cualquier medida correctiva necesaria de forma oportuna;

c) controla el rendimiento en materia de seguridad operacional en comparación con la política y los objetivos de seguridad operacional de la organización;

d) controla la eficacia de los procesos de gestión de seguridad operacional de la organización, la que respalda la prioridad empresarial declarada de la gestión de seguridad operacional como otro proceso comercial principal;

e) controla la eficacia de la supervisión de seguridad operacional de las operaciones subcontratadas; y

f) garantiza que los recursos correspondientes estén asignados para lograr el rendimiento en materia de seguridad operacional más allá de lo que requiere el cumplimiento reglamentario.

1.3.8 El SRC es estratégico y aborda temas de alto nivel relacionados con políticas, la asignación de recursos y el control del rendimiento institucional. Luego que el SRC desarrolla una dirección estratégica, se deben coordinar las estrategias de seguridad operacional en toda la organización. Esto puede lograrse al crear un grupo de acción de seguridad operacional (SAG). Los SAG se componen de gerentes de línea y personal de primera línea, y los lidera normalmente un gerente de línea designado.

1.3.9 Los SAG son entidades tácticas que abordan problemas de implementación específicos según la dirección del SRC. Los SAG:

a) supervisan el rendimiento en materia de seguridad operacional dentro de las áreas funcionales de la organización y garantizan que se lleven a cabo las actividades de gestión de riesgos de seguridad operacional correspondientes, con participación del personal, según sea necesario, para generar conciencia de la seguridad operacional;

b) coordinan la resolución de las estrategias de mitigación para las consecuencias de peligros identificadas y garantizan que existan disposiciones satisfactorias para la captura de los datos de seguridad operacional y los comentarios del empleado;

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

d) coordinan la implementación de planes de medidas correctivas y garantizan que se tome la medida correctiva de forma oportuna;

e) revisan la eficacia de las recomendaciones de seguridad operacional anteriores; y

f) supervisan las actividades de promoción de la seguridad operacional, según sea necesario, para aumentar la conciencia de los empleados sobre temas de seguridad operacional y para garantizar que se les proporcione oportunidades adecuadas para participar en las actividades de la gestión de seguridad operacional.

1.3.10 *La designación del personal clave de seguridad operacional será aceptable para la AAC si se han observado los siguientes criterios:*

- *El explotador ha definido los requisitos y ha designado un gerente de seguridad operacional que será responsable de la implantación y el mantenimiento de un SMS eficaz debidamente calificado según la orientación de 1.3.3 y del Adjunto B.*
- *En el manual del SMS se describen las funciones del gerente de seguridad operacional que incluyen como mínimo los criterios de 1.3.2 y del Adjunto B.*
- *Se han establecido y documentado en el manual del SMS el comité de revisión de seguridad operacional (SRC) y el grupo de acción de seguridad operacional (SAG), incluyendo la descripción de sus funciones, sus miembros, la frecuencia y circunstancias de sus reuniones, etc. según la orientación de 1.3.7 y 1.3.9.*

1.4 Coordinación de la planificación de respuestas ante emergencias

1.4.1 El explotador garantizará que el plan de respuesta ante emergencias se coordine en forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que deba interactuar al suministrar sus servicios o productos.

1.4.2 Un plan de respuesta ante emergencias (ERP) describe por escrito lo que se debe hacer después de un accidente o una crisis de aviación y quién es responsable de cada medida.

1.4.3 Un plan de respuesta ante emergencias (ERP) documenta las medidas que deberá tomar todo el personal responsable durante las emergencias relacionadas con la aviación. El propósito de un ERP es garantizar que exista una transición ordenada y eficiente de operaciones normales a operaciones de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de la autoridad. En el plan también se incluye la autorización de las medidas realizadas por personal clave, así como también, los medios para coordinar esfuerzos necesarios para hacer frente a la emergencia. El objetivo general es salvar vidas, la continuación segura de las operaciones y el retorno a las operaciones normales, lo antes posible. Véase el Adjunto C para guía detallada sobre ERP.

1.4.4 Una respuesta satisfactoria ante una emergencia comienza con la planificación eficaz. Un ERP representa la base de un enfoque sistemático para gestionar los asuntos de la organización durante las consecuencias de un evento no planificado importante, en el peor de los casos, un accidente importante.

1.4.5 El propósito de un plan de respuesta ante emergencias es para garantizar:

a) la delegación de la autoridad de emergencia;

b) la asignación de responsabilidades de emergencia;

c) la documentación de procedimientos y procesos de emergencia;

d) la coordinación de esfuerzos de emergencia de forma interna y con partes externas;

e) la continuación segura de las operaciones fundamentales, mientras se gestiona la crisis;

f) la identificación proactiva de todos los posibles eventos/escenarios de emergencia y sus medidas de mitigación correspondientes, etc.

1.4.6 Para ser eficaz, un ERP debe:

a) ser adecuado según la envergadura, naturaleza y complejidad de la organización;

b) estar fácilmente accesible para todo el personal pertinente y otras organizaciones, donde corresponda;

c) incluir listas de verificación y procedimientos pertinentes a las situaciones de emergencia específicas;

d) tener detalles de contacto de referencia rápida de todo el personal pertinente;

e) probarse regularmente mediante ejercicios;

f) revisarse y actualizarse periódicamente cuando cambian los detalles, etc.

1.4.4 *La coordinación de la planificación de respuestas ante emergencias será aceptable para la AAC si se han observado los siguientes criterios:*

- *El explotador ha desarrollado y documentado una planificación de respuesta ante emergencias de acuerdo con 1.4.6 y con la orientación del Adjunto C.*
- *La planificación de respuesta ante emergencias puede ser parte integral del manual del SMS o puede desarrollarse como un manual independiente.*

1.5 Documentación SMS

1.5.1 La documentación del SMS está compuesta por el manual del SMS, los registros del SMS y el plan de implantación.

1.5.2 El componente principal de la documentación del SMS adopta la forma de un manual del SMS en el que se describe:

a) su política y objetivos de seguridad operacional;

b) sus requisitos del SMS;

c) todos los procesos y procedimientos del SMS;

d) sus obligaciones de rendición de cuentas, responsabilidades funcionales y las atribuciones relativas a los procesos y procedimientos del SMS; y

e) sus resultados esperados del SMS. Véase el Adjunto D para más información sobre el desarrollo y contenido del manual del SMS del explotador.

1.5.3 El desarrollo, control y mantenimiento de la documentación relacionada con el SMS son esenciales para una eficiente gestión de la seguridad operacional. En este sentido el explotador deberá establecer un proceso de control de la documentación del SMS para asegurar que ésta se revisa y actualiza continuamente, y que la versión disponible sea siempre la más reciente.

1.5.4 En el caso de explotadores certificados o que se encuentren en proceso de certificación al 31 de diciembre de 2015, la documentación del SMS, además del manual, deberá incluir un plan de implantación del SMS, aprobado formalmente por la organización, en el que se definirá el enfoque de la organización respecto de la gestión de la seguridad operacional, de manera que se cumplan los objetivos de la organización en materia de seguridad operacional. Véanse las Secciónes 8 y 9 para más información sobre el proceso de implantación.

1.5.5 Otro aspecto de la documentación de SMS es la compilación y el mantenimiento de registros que corroboran la existencia y operación continua del SMS. Tales registros deben organizarse de acuerdo con los elementos de SMS respectivos y los procesos asociados.

1.5.6 La documentación de SMS aborda todos los elementos y procesos del SMS y normalmente incluye:

a) una descripción consolidada de los componentes y elementos de SMS, como por ejemplo:

   1) gestión de documentos y registros;

   2) requisitos del SMS reglamentarios;

   3) marco de trabajo, alcance e integración;

   4) política y objetivos de seguridad operacional;

   5) responsabilidades de la seguridad operacional y personal clave;

   6) sistema de notificación de peligros voluntaria;

   7) procedimientos de notificación e investigación de incidentes;

   8) procesos de identificación de peligros y evaluación de riesgos;

   9) indicadores de rendimiento en materia de seguridad operacional;

   10) capacitación y comunicación de seguridad operacional;

   11) mejora continua y auditoría de SMS;

   12) gestión de cambio; y

13) planificación de contingencia de emergencia u operaciones;

b) una compilación de registros y documentos relacionados con SMS actuales, como por ejemplo:

1) registro del informe de peligros y muestras de los informes reales;

2) indicadores de rendimiento en materia de seguridad operacional y gráficos relacionados;

3) registros de evaluaciones de seguridad operacional completadas o en progreso;

4) registros de revisión o auditoría internas de SMS;

5) registros de promoción de seguridad operacional;

6) registros de capacitación de SMS/seguridad operacional del personal;

7) actas de la reunión del comité de SMS/seguridad operacional; y

8) plan de implementación del SMS (durante el proceso de implementación).

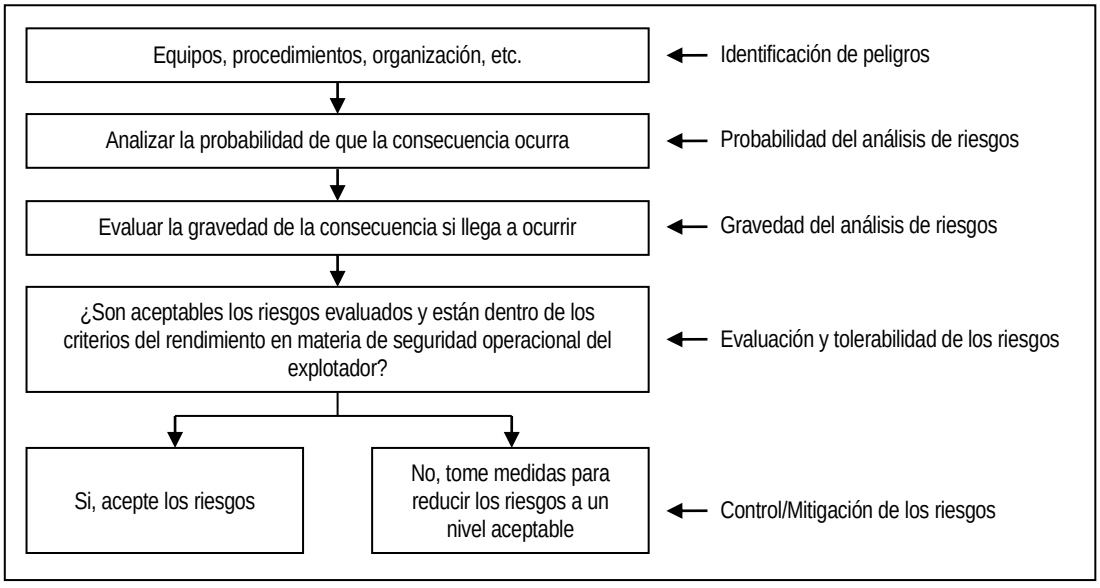
1.5.7 *La documentación SMS será aceptable para la AAC si se han observado los siguientes criterios:*

- *El explotador ha desarrollado un manual del SMS de acuerdo con 1.5.2, 1.5.6 (a) y con el Adjunto D.*
- *El explotador mantiene un sistema de registros adecuado, de acuerdo con 1.5.6 (b).*
- *El explotador ha desarrollado un plan de implantación de acuerdo con las Secciónes 8 o 9, según corresponda.*

2. Gestión de riesgos de seguridad operacional

Los proveedores de servicios deben garantizar que los riesgos de seguridad operacional encontrados en las actividades de aviación están bajo control para alcanzar sus objetivos de eficacia de la seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional e incluye la identificación de peligros, la evaluación de riesgos de seguridad operacional y la implementación de medidas de solución adecuadas. El proceso de gestión de riesgos de seguridad operacional se ilustra en la Figura 4.

Figura 4 – Proceso de gestión de riesgos de la seguridad operacional



2.1 Identificación de peligros

2.1.1 Los peligros existen en todos los niveles en la organización y son detectables mediante el uso de sistemas de notificación, inspecciones o auditorías. Los contratiempos ocurren cuando los peligros interactúan con ciertos factores activadores. Como resultado, los peligros deben identificarse antes de que produzcan accidentes, incidentes u otros sucesos relacionados con la seguridad operacional.

2.1.2 El explotador definirá y mantendrá un proceso que garantice la identificación de los peligros asociados a sus productos o servicios de aviación.

2.1.3 La identificación de los peligros se basará en una combinación de métodos reactivos, preventivos y de predicción para recopilar datos sobre seguridad operacional, como se describe en el Párrafo 2.1.3.

2.1.4 Las tres metodologías para identificar peligros son:

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

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

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

2.1.5 La gestión de riesgos de seguridad operacional requiere que el explotador desarrolle y mantenga un proceso formal para identificar peligros que pueden contribuir con los sucesos relacionados con la aviación. Los peligros pueden existir en las actividades de aviación continuas o introducirse accidentalmente en una operación cada vez que se producen cambios al sistema de aviación. En este caso, la identificación de peligros es una parte integral de los procesos de la gestión de cambio, como se describe en el Elemento 3.2 del SMS — La gestión de cambio.

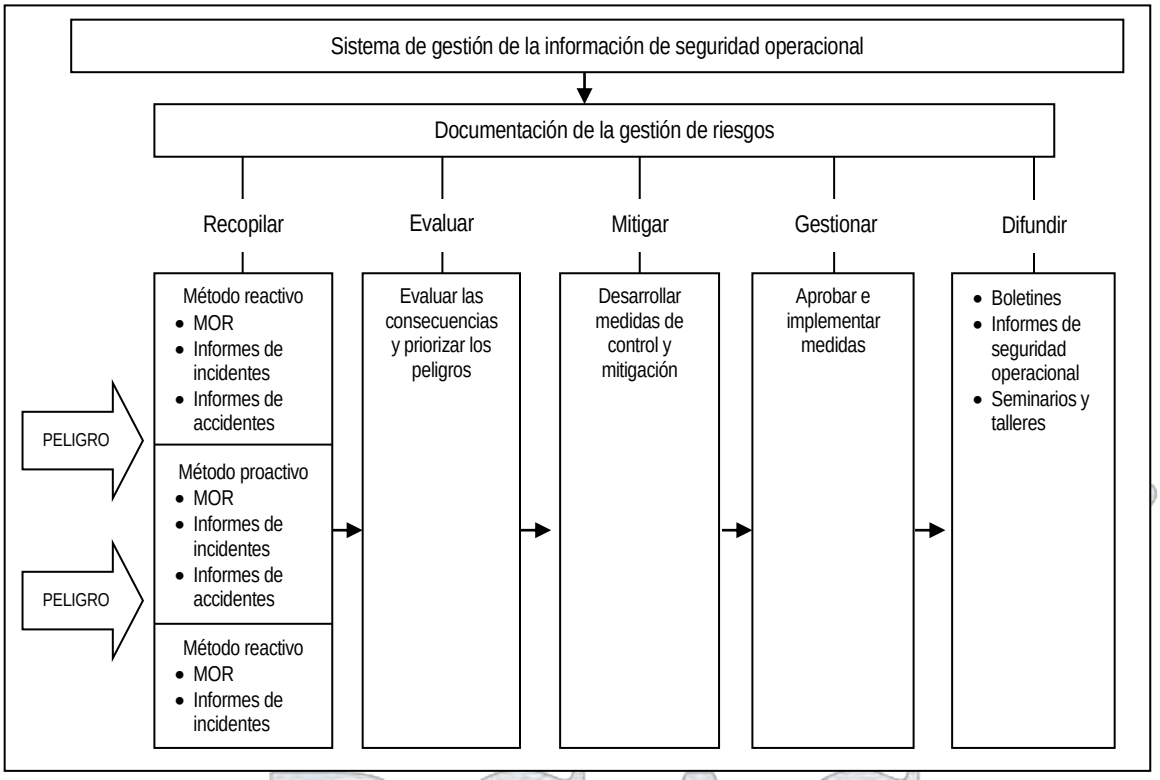
2.1.6 La identificación de peligros es el primer paso en el proceso de gestión de riesgos de la seguridad operacional. Los riesgos de seguridad operacional correspondientes se evalúan dentro del contexto de las consecuencias potencialmente dañinas relacionadas con el peligro. Donde se evalúe que los riesgos de seguridad operacional son inaceptables, se deben incorporar controles de riesgos de seguridad operacional adicionales en el sistema.

2.1.7 El sistema de gestión de la información de la seguridad operacional del explotador debe incluir la documentación de la evaluación de seguridad operacional que contiene descripciones de peligros, las consecuencias relacionadas, la probabilidad evaluada y la gravedad de los riesgos de seguridad operacional, además de los controles de riesgos de la seguridad operacional necesarios. Las evaluaciones de la seguridad operacional existentes deben revisarse cada vez que se identifican peligros nuevos y se anticipan propuestas para otros controles de riesgos de la seguridad operacional.

2.1.7 La Figura 5 ilustra la documentación de peligros y el proceso de gestión de riesgos de seguimiento. Los peligros se identifican constantemente mediante varias fuentes de datos. Se espera que el explotador identifique peligros, elimine estos peligros o mitigue los riesgos asociados. En el caso de peligros identificados en los productos o servicios suministrados mediante subcontratistas,

una mitigación podría ser el requisito del explotador para que tales organizaciones tengan un SMS o un proceso equivalente para la identificación de peligros y la gestión de riesgos.

Figura 5 - Documentación de peligros y seguimiento del proceso de gestión de riesgos



2.1.8 El sistema de información de la gestión de seguridad operacional se convierte en una fuente de conocimientos de seguridad operacional que se usará como referencia en los procesos de toma de decisiones de la seguridad operacional institucional. Este conocimiento de la seguridad operacional proporciona el material para el análisis de tendencia de la seguridad operacional, así como también, para la educación de la seguridad operacional.

2.1.9 Los peligros pueden identificarse mediante las metodologías proactivas y predictivas o como resultado de investigaciones de accidentes o incidentes. Existe una variedad de fuentes de datos de identificación de peligros que pueden ser internos o externos a la organización. Entre los ejemplos de fuentes de datos de la identificación de peligros internos se incluyen:

a) diagramas de control de operación normal (por ejemplo, análisis de datos en vuelo para los explotadores de aeronaves);

b) sistemas de notificación voluntaria y obligatoria;

c) estudios de seguridad operacional;

d) auditorías de seguridad operacional;

e) comentarios de la capacitación; y

f) investigación e informes de seguimiento sobre accidentes/incidentes.

Entre los ejemplos de fuentes de datos externos para la identificación de peligros se incluyen:

a) informes de accidentes industriales;

b) sistemas de notificación de incidentes obligatoria estatal;

c) sistemas de notificación de incidentes voluntaria estatal;

d) auditorías de vigilancia estatal; y

e) sistemas de intercambio de información.

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

2.1.11 El tipo de tecnologías usadas en el proceso de identificación de peligros dependerá de la envergadura y complejidad del explotador y sus actividades de aviación. En todos los casos, el proceso de identificación de peligros del explotador se describe claramente en la documentación de SMS/seguridad operacional de la organización. El proceso de identificación de peligros considera todos los peligros posibles que puedan existir dentro del alcance de las actividades de aviación del explotador, como las interfaces con otros sistemas, tanto dentro como fuera de la organización.

2.1.12 El Programa de análisis de datos de vuelo (FDAP) es parte integral del SMS y es una herramienta adicional para la identificación de peligros. La orientación para la implementación de un FDAP, así como los medios aceptables de cumplimiento, se encuentran detallados en la CA-119-003.

2.1.13 La Identificación de peligros será aceptable para la AAC si se han observado los siguientes criterios:

- *El explotador ha definido de manera clara y detallada en su manual del SMS los medios y procedimientos que garanticen la identificación de los peligros asociados a sus productos o servicios de aviación.*
- *La identificación de peligros del explotador está compuesta por una combinación de métodos reactivos, preventivos y de predicción para recopilar datos sobre seguridad operacional.*
- *El explotador ha establecido y documentado un sistema de notificación voluntaria y obligatoria, incluyendo las situaciones que requieren ser reportadas en cada uno de estos sistemas, los procedimientos de notificación, los formularios, y la garantía de protección de la información.*
- *El explotador ha establecido un Programa de análisis de datos de vuelo de acuerdo con LA CA-OPS-119-003.*
- *Existe un método adecuado para la documentación y registro de los peligros identificados.*

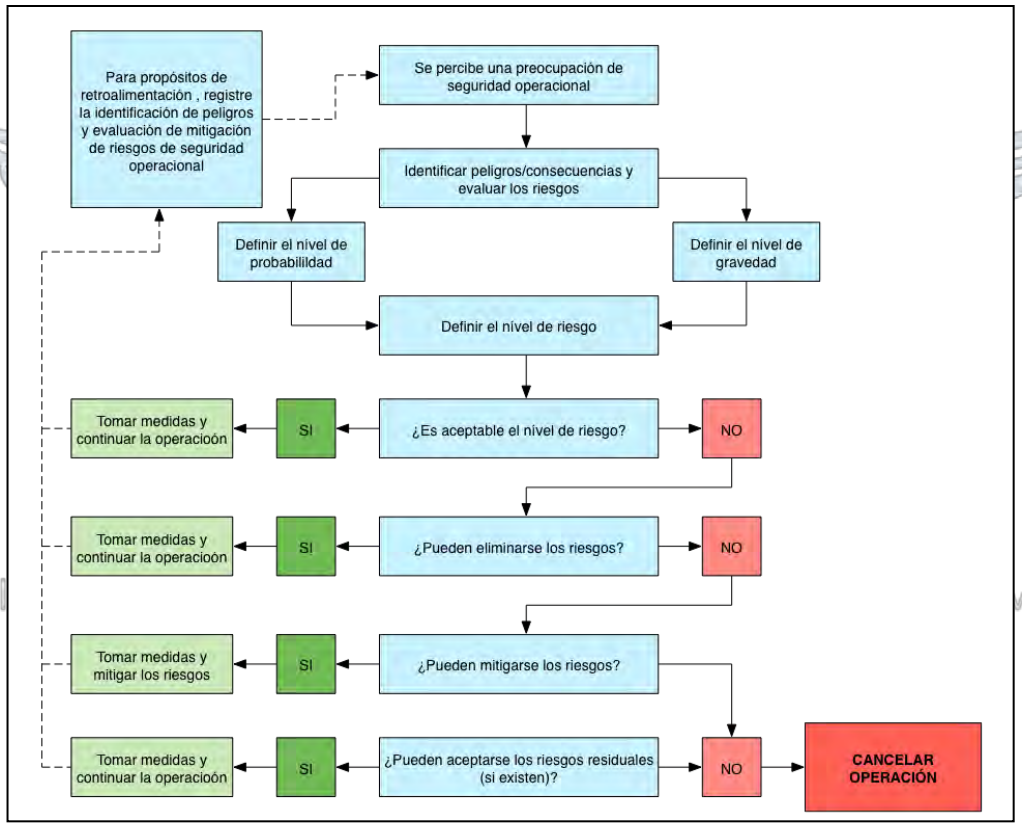
2.2 Evaluación y mitigación de riesgos de seguridad operacional

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

2.2.2 El explotador definirá y mantendrá un proceso que garantice el análisis, la evaluación y el control de riesgos de seguridad operacional asociados a los peligros identificados.

2.2.3 La Figura 6 presenta el proceso de gestión de riesgos de seguridad operacional por completo. El proceso comienza con la identificación de los peligros y sus posibles consecuencias. Los riesgos de seguridad operacional se evalúan en términos de probabilidad y gravedad, para definir el nivel de riesgos de seguridad operacional (índice de riesgo de seguridad operacional). Si los riesgos de seguridad operacional evaluados se consideran tolerables, se debe tomar una medida adecuada y la operación puede continuar. La identificación de peligros completada y el proceso de evaluación y mitigación de riesgos de seguridad operacional se documentan y aprueba como corresponda y forma parte del sistema de gestión de información de seguridad operacional. Luego de identificar los peligros, se deben determinar sus consecuencias (es decir, cualquier evento o resultado específico).

Figura 6 - Proceso de gestión de riesgos de la seguridad operacional



2.2.4 En muchos casos será necesario priorizar los peligros de acuerdo con la gravedad/probabilidad de sus consecuencias proyectadas. Esto facilita la priorización de las estrategias de mitigación de riesgos, tanto como para usar recursos limitados de la forma más eficaz. La Figura 7 presenta un ejemplo de un procedimiento de priorización de peligros.

Figura 7 – Ejemplo de un procedimiento de priorización de peligros

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

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

c) concluir que la priorización del peligro es:

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

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

c) concluir que la priorización del peligro es:

<table><tr><th>Índice de riesgo proyectado</th><th>Nivel de peligro</th></tr><tr><td>Intolerable/alto riesgo</td><td>Nivel 1</td></tr><tr><td>Tolerable/riesgo moderado</td><td>Nivel 2</td></tr><tr><td>Aceptable/bajo riesgo</td><td>Nivel 3</td></tr></table></td></tr>
<tr><td>Observaciones</td><td>La Opción 1 considera solo la gravedad de la consecuencia proyectada del peligro.</td><td>La Opción 2 considera la gravedad y probabilidad de la consecuencia proyectada del peligro; este es un criterio más completo que la Opción 1.</td></tr>
</table>

2.2.5 La evaluación de riesgos de seguridad operacional implica un análisis de peligros identificados que incluye dos componentes:

a) la gravedad de un resultado de seguridad operacional; y

b) la probabilidad que sucederá.

2.2.6 El proceso de controlar los riesgos de seguridad operacional comienza al evaluar la probabilidad de que las consecuencias de los peligros se materialicen durante las actividades de aviación realizadas por la organización. La probabilidad de riesgo de seguridad operacional se define como la probabilidad o frecuencia de que pueda suceder una consecuencia o un resultado de la seguridad operacional. Con las siguientes preguntas se puede ayudar a determinar dicha probabilidad:

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

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

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

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

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

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

2.2.8 La Figura 8 presenta una tabla de probabilidad de riesgo de seguridad operacional típica, en este caso, una tabla de cinco puntos. La tabla incluye cinco categorías para denotar la

probabilidad relacionada con un evento o una condición inseguros, la descripción de cada categoría y una asignación de valor a cada categoría.

Figura 8 – Tabla de probabilidad de riesgo de seguridad operacional

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

2.2.9 Luego de completar la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional, considerando las posibles consecuencias relacionadas con el peligro. La gravedad del riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La evaluación de la gravedad puede basarse en:

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

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

2.2.10 La evaluación de gravedad debe considerar todas las posibles consecuencias relacionadas con una condición o un objeto inseguros, considerando la peor situación predecible. La Figura 9 presenta una tabla de gravedad de riesgo de seguridad operacional típico. Incluye cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada categoría. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla solo es un ejemplo.

Figura 9 – Tabla de gravedad de riesgo de seguridad operacional

Gravedad	Significado	Valor
Catastrófico	• Equipo destruido • Varias muertes	5
Peligroso	• Una gran reducción de los márgenes de seguridad operacional estrés físico o una carga de trabajo tal que ya no se pueda confiar en los explotadores para que realicen sus tareas con precisión o por completo • Lesiones graves • Daño importante al equipo	4
Grave	• Una reducción importante de los márgenes de seguridad operacional, una reducción en la capacidad de los explotadores para tolerar condiciones de operación adversas como resultado de un aumento en la carga de trabajo o como resultado de condiciones que afecten su eficiencia • Incidente grave • Lesiones para las personas	3
Leve	• Molestias • Limitaciones operacionales • Uso de procedimientos de emergencia • Incidente leve	2
Insignificante	• Pocas consecuencias	1

2.2.11 El proceso de evaluación de la probabilidad y gravedad del riesgo de seguridad operacional puede usarse para derivar un índice de riesgo de seguridad operacional. El índice que se crea mediante la metodología descrita anteriormente consta de un identificador alfanumérico, que indica los resultados combinados de las evaluaciones de probabilidad y gravedad. Las combinaciones de gravedad/probabilidad respectivas se presentan en la matriz de evaluación del riesgo de seguridad operacional en la Figura 10.

Figura 10 – Ejemplo de una matriz de evaluación (índice) de riesgos de seguridad operacional.

PROBABILIDAD DEL RIESGO	GRAVEDAD DEL RIESGO				
	Catastrófico A	Peligroso B	Importante C	Leve D	Insignificante E
Frecuente 5	5A	5B	5C	5D	5E
Ocasional 4	4A	4B	4C	4D	4E
Remoto 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Sumamente Improbable 1	1A	1B	1C	1D	1E

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

2.2.13 El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a una matriz de tolerabilidad del riesgo de seguridad operacional (véase la Figura 11) que describe los criterios de tolerabilidad para una organización en particular. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B cae en la categoría “inaceptable bajo las circunstancias existentes”. En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por tanto, la organización debe:

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

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

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

2.2.14 La pirámide invertida en la Figura 11 refleja un esfuerzo constante para impulsar el índice de riesgo hacia el vértice inferior de la parte inferior de la pirámide. La Figura 12 proporciona un ejemplo de una matriz de tolerabilidad de riesgo de seguridad operacional alternativa.

Figura 11 – Matriz de tolerabilidad del riesgo de seguridad operacional

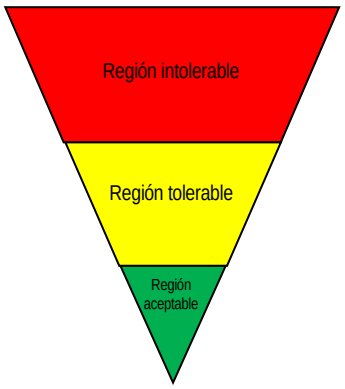
Descripción de la tolerabilidad	Índice de riesgo evaluado	Criterios sugeridos
	5A, 5B, 5C, 4A, 4B, 3A	Inaceptable según las circunstancias existentes
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Aceptable según la mitigación de riesgos. Puede necesitar una decisión de gestión.
	3E, 2D, 2E, 1B, 1C,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

Figura 12 – Matriz de tolerabilidad del riesgo de seguridad operacional alternativa

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

2.2.15 Al usar esta matriz, los riesgos pueden categorizarse de acuerdo con una evaluación de su posible gravedad y probabilidad. La matriz de evaluación de riesgos puede personalizarse para reflejar el contexto de cada estructura institucional y actividades de aviación del explotador y puede estar sujeta al acuerdo de su autoridad reglamentaria. Según este ejemplo de matriz, los riesgos reflejados como inaceptables (categorías roja y amarilla) deben mitigarse para reducir su gravedad o probabilidad. El explotador debe considerar la suspensión de cualquier actividad que siga exponiendo a la organización a riesgos de seguridad operacional intolerables en la ausencia de medidas de mitigación que reduzcan los riesgos a un nivel aceptable.

2.2.16 Después de evaluar los riesgos de seguridad operacional, se pueden implementar medidas de mitigación adecuadas. Debe describirse una estrategia de mitigación de riesgos, y alguna forma de retroalimentación para asegurarse que funciona correctamente. Esto es necesario para garantizar la integridad, eficiencia y eficacia de las defensas según las nuevas condiciones operacionales.

2.2.17 Cada ejercicio de mitigación de riesgos se documentará de manera progresiva. Esto puede lograrse al usar una variedad de aplicaciones, desde hojas de cálculo o tablas básicas hasta software personalizado de mitigación de riesgos comercial. Los documentos de mitigación de riesgos completos deben recibir la aprobación del nivel correspondiente de la administración. Para conocer un ejemplo de una hoja de cálculo de mitigación de riesgos de peligros básica, véase el Adjunto F.

2.2.18 *La evaluación y mitigación de riesgos de seguridad operacional será aceptable para la AAC si se han observado los siguientes criterios:*

- *El explotador ha establecido y documentado en su manual del SMS un proceso de evaluación y mitigación de los riesgos que garantice el análisis, la evaluación y el control de los riesgos de seguridad operacional asociados a los peligros identificados.*
- *El proceso de evaluación y mitigación de los riesgos incluye los procedimientos para :*
  - *la priorización de los peligros;*
  - *la evaluación del nivel de riesgos asociados a los peligros identificados en términos de probabilidad y gravedad;*
  - *la determinación de la tolerabilidad del riesgo;*
  - *la definición de las medidas adecuadas y las estrategias de mitigación de riesgos; y*
  - *alguna forma de retroalimentación.*
- *Existe un método y procedimientos adecuados para la documentación y archivo de la identificación de peligros y la evaluación y mitigación de los riesgos. De acuerdo con 2.2.17.*
- *El explotador ha desarrollado tablas de probabilidad y severidad para identificar los valores y definiciones respectivas, de acuerdo con 2.2.8, 2.2.9 y 2.2.10.*
- *El explotador ha desarrollado una matriz de evaluación del riesgo de seguridad operacional de acuerdo con 2.2.11.*
- *El explotador ha desarrollado una matriz de tolerabilidad de riesgo de acuerdo con 2.2.13 y 2.2.14.*
- *Como parte de la estrategia de control de riesgos, está considerada la posibilidad de cancelar la operación cuando la mitigación no fuera posible.*

3. Aseguramiento de la seguridad operacional

El aseguramiento de la seguridad operacional consta de procesos y actividades realizadas por el explotador para determinar si el SMS funciona de acuerdo con las expectativas y los requisitos. El explotador controla continuamente sus procesos internos, así como también, su entorno de operación para detectar cambios o desviaciones que puedan introducir riesgos de seguridad operacional emergentes o la degradación de los controles de riesgos existentes. Tales cambios o desviaciones podrían abordarse entonces con el proceso de gestión de riesgos de seguridad operacional.

3.1 Observación y medición del rendimiento en materia de seguridad operacional

3.1.1 El explotador desarrollará y mantendrá los medios para verificar el rendimiento en materia de seguridad operacional de la organización y para confirmar la eficacia de los controles de riesgo de seguridad operacional.

3.1.2 El rendimiento en materia de seguridad operacional del explotador se verificará en referencia a los indicadores y las metas de rendimiento en materia de seguridad operacional del SMS.
La información usada para medir el rendimiento en materia de seguridad operacional de la

organización se genera mediante sus sistemas de notificación de la seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional se analizan en detalle a partir del Párrafo 3.1.8 de esta sección y en el Adjunto G de esta circular.

3.1.3 Existen dos tipos de sistemas de notificación:

a) sistemas de notificación de incidentes obligatoria; y

b) sistemas de notificación de incidentes voluntaria.

3.1.4 Los sistemas de notificación voluntaria pueden ser confidenciales, lo que requiere que cualquier información que dé la identidad del notificador la sepan solo los "puntos de entrada" para permitir una medida de seguimiento. Los sistemas de notificación de incidentes confidencial facilitan la divulgación de peligros que generan errores humanos, sin miedo a retribuciones o dificultades. Los informes de incidentes voluntarios pueden archivarse y su identidad eliminarse luego de haber tomado cualquier medida de seguimiento necesaria. Los informes sin identidad pueden respaldar futuros análisis de tendencias para rastrear la eficacia de la mitigación de riesgos y para identificar los peligros emergentes.

3.1.5 Para ser eficaces, las herramientas de notificación de seguridad operacional deben estar accesible fácilmente para el personal operacional.

3.1.6 Otras fuentes de información de seguridad operacional para respaldar el control y la medición del rendimiento en materia de seguridad operacional pueden incluir:

a) revisiones de seguridad operacional;

b) estudios de seguridad operacional;

c) auditorías; e

d) investigaciones internas.

3.1.7 El resultado final del control y la medición del rendimiento en materia de seguridad operacional es el desarrollo de indicadores de rendimiento en materia de seguridad operacional, basado en el análisis de los datos recopilados mediante las fuentes nombradas anteriormente. El proceso de control y medición implica el uso de indicadores de rendimiento en materia de seguridad operacional seleccionados y niveles de objetivos y alertas del rendimiento en materia de seguridad operacional correspondientes. A partir del párrafo 3.1.8 de esta sección y en el Adjunto G podrá encontrar una guía sobre la selección de indicadores de rendimiento en materia de seguridad operacional y su configuración de objetivos y alertas.

3.1.8 Un SMS define los resultados del rendimiento medible para determinar si el sistema funciona verdaderamente en acuerdo con las expectativas de diseño y no cumplen simplemente con requisitos reglamentarios. Los indicadores de rendimiento en materia de seguridad operacional se usan para controlar los riesgos de seguridad operacional conocidos, detectar riesgos de seguridad operacional emergentes y para determinar cualquier medida correctiva necesaria.

3.1.9 Los indicadores de rendimiento en materia de seguridad operacional también proporcionan evidencia objetiva para que la AAC evalúe la eficacia del SMS del explotador y controle el logro de sus objetivos de seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional del explotador consideran factores como la tolerancia de los riesgos de seguridad operacional de la organización, el costo/beneficios que conlleva la implementación de las mejoras al sistema, los requisitos reglamentarios y las expectativas públicas. Se deben seleccionar y desarrollar indicadores de rendimiento en materia de seguridad operacional en coordinación y con el asesoramiento de la AAC. Este proceso es necesario para facilitar la agregación de la AAC y la armonización de los indicadores de rendimiento en materia de seguridad operacional del explotador

para el mismo sector de aviación. Aún en caso que la AAC no hubiera implementado su SSP o no hubiera definido los indicadores y objetivos de seguridad operacional del Estado, el explotador deberá establecer sus propios indicadores, alertas y objetivos de seguridad operacional en estrecha coordinación con la AAC.

3.1.10 Algunos ejemplos típicos de indicadores de rendimiento de seguridad operacional (SPI) para explotadores de servicios aéreos son los siguientes:

- Declaraciones de emergencia relacionadas con baja cantidad de combustible por cada (XX) horas de vuelo o ciclos de operación.
- Ocurrencias o incidentes en tierra ocurridos en la plataforma o en las calles de rodaje que podrían haber resultado en daños a la aeronave o a equipos en tierra o lesiones a personas, por cada (XX) horas de vuelo o ciclos de operación.
- Incursiones de pista por cada (XX) ciclos de operación.
- Excursiones de pista por cada (XX) ciclos de operación.
- Despegues interrumpidos por encima de 80 kt por cada (XX) ciclos de operación.
- Retorno en vuelo al aeropuerto de origen por fallas mecánicas por cada (XX) ciclos de operación.
- Cortes de motor en vuelo (INSD) por cada (XX) ciclos de operación.
- Desviaciones de velocidad, altitud o rumbo no intencionales que resulten en una activación de alerta, alarma o llamada del ATC, por cada (XX) ciclos de operación.
- Incapacitación de algún miembro de la tripulación por cada (XX) ciclos de operación.
- Daño estructural, pérdida de altitud mayor a 300 pies, lesiones a pasajeros o dificultad para controlar la aeronave provocada por turbulencia u otros factores meteorológicos por cada (XX) ciclos de operación.
- Activación de TCAS/RA por cada (XX) ciclos de operación.
- Aproximaciones no estabilizadas por cada (XX) ciclos de operación.
- Activación del EGPWS por cada (XX) ciclos de operación.
- Aterrizajes bruscos (*Hard landing*) por cada (XX) ciclos de operación.
- Mercancías peligrosas no declaradas por cada (XX) ciclos de operación.
- Eventos relacionados con fuego o humo por cada (XX) ciclos de operación.
- Etc.

3.1.11 Los indicadores de rendimiento en materia de seguridad operacional y los objetivos asociados debe aceptarlos la AAC del explotador. Los indicadores de rendimiento en materia de seguridad operacional son complementarios a cualquier requisito legal o reglamentario y no exime al explotador de sus obligaciones reglamentarias.

3.1.12 En la práctica, el rendimiento en materia de seguridad operacional de un SMS se expresa mediante indicadores de rendimiento en materia de seguridad operacional (SPI) y sus valores de alertas y objetivos correspondientes.

3.1.13 El proveedor de servicios debe controlar el rendimiento de los indicadores actuales en el contexto de tendencias históricas para identificar cambios anormales en el rendimiento en materia de seguridad operacional. De igual forma, la configuración de objetivos y alertas debe considerar el rendimiento histórico reciente para un indicador determinado. Los objetivos de mejora deseados deben ser realistas y alcanzables para el explotador y el sector de aviación asociado.

3.2.14 En el caso de un explotador nuevo, que carece de datos históricos, los indicadores se generarán a partir de la experiencia operativo una vez que se inicien las operaciones y el explotador almacene y analice la información sobre seguridad operacional. Sin embargo, un explotador nuevo puede utilizar inicialmente indicadores genéricos y objetivos de seguridad operacional de fuentes externas. Estas fuentes pueden ser organizaciones internacionales como la OACI, IATA, ALTA, FSF, etc., el SSP de su Estado, u otros explotadores que operan en el mismo segmento y contexto operacional. A medida que el explotador reúne experiencia mediante su operación, irá reuniendo información de seguridad operacional por medio de sus propias fuentes y podrá migrar gradualmente hacia indicadores, objetivos y niveles de alerta propios. El período de transición deberá ser acordado con la AAC en función a la dimensión y complejidad del explotador. En el Adjunto G se incluyen ejemplos de objetivos de seguridad operacional, indicadores de seguridad operacional y niveles de alerta.

3.1.15 El establecimiento de un nivel de alerta para un indicador de seguridad operacional es pertinente desde una perspectiva de control de riesgos. Un nivel de alerta es un criterio común para delinear las regiones de rendimiento aceptable de aquellas inaceptables para un indicador de seguridad operacional particular. Según los libros de métricas genéricas de seguridad operacional, un método objetivo básico para ajustar los criterios de alertas fuera de control (OOC) es el uso del principio de desviación estándar. Este método considera la desviación estándar y los valores promedio de los puntos de datos históricos previos para un indicador de seguridad operacional determinado. Estos dos valores se usan entonces para establecer el nivel de alerta para el siguiente período de control del indicador.

3.1.16 Una gama de indicadores de rendimiento en materia de seguridad operacional de alto y bajo impacto proporcionan una comprensión más integral acerca del rendimiento en materia de seguridad operacional del proveedor de servicios. Esto garantiza que se aborden los resultados de alto impacto (por ejemplo, accidentes e incidentes graves), así como también, los eventos de bajo impacto (por ejemplo, incidentes, informes de no cumplimiento, desviaciones). Los indicadores de rendimiento en materia de seguridad operacional son básicamente diagramas de tendencias de datos que rastrean los sucesos en términos de tasas de eventos (por ejemplo, cantidad de incidentes cada 1 000 horas de vuelo). En el Adjunto G se incluyen ejemplos de objetivos de seguridad operacional, indicadores de seguridad operacional y niveles de alerta.

3.1.17 Los indicadores de alto impacto deben abordarse primero, mientras que los indicadores de bajo impacto pueden desarrollarse más adelante.

3.1.18 Luego de definir los indicadores de rendimiento en materia de seguridad operacional y su configuración de objetivos y alertas correspondiente, el resultado del rendimiento de cada indicador debe actualizarse y controlarse de forma regular. Puede rastrearse el estado de rendimiento respectivo del nivel de objetivos y alertas para cada indicador.

3.1.19 También se puede compilar/agregar un resumen consolidado del resultado de rendimiento general de objetivos y alertas de todo el paquete de indicadores de rendimiento en materia de seguridad operacional para un período de control determinado. Se pueden asignar valores cualitativos (satisfactorio/insatisfactorio) para cada “objetivo logrado” y cada “nivel de alerta no violado”. O bien, se pueden usar valores numéricos (puntos) para proporcionar una medición cuantitativa del rendimiento general del paquete de indicadores. En el Adjunto G de esta circular se ofrecen ejemplos de los indicadores de rendimiento en materia de seguridad operacional y sus criterios de configuración de objetivos y alertas.

3.1.18 La observación y medición del rendimiento en materia de seguridad operacional será aceptable para la AAC si se han observado los siguientes criterios:

- *El explotador ha desarrollado métodos y procedimientos para verificar el rendimiento en materia de seguridad operacional para confirmar la eficacia de los controles de riesgo de la seguridad operacional que incluya al menos:*
  - *Los indicadores, objetivos y alertas de seguridad operacional en base a datos históricos del explotador o a los criterios de 3.2.13 y 3.2.14, de acuerdo con esta sección y con el Adjunto G.*
  - *Los indicadores, objetivos y alertas de seguridad operacional alineados con los del SSP del Estado si están disponibles.*
  - *Procedimientos para el monitoreo continuo del Estado de los indicadores y para las acciones a tomar frente a la activación de los niveles de alerta.*
  - *Procedimientos para el control y actualización regular de los indicadores, alertas y objetivos de seguridad operacional.*
  - *Procedimientos para la producción y emisión de resúmenes consolidados para períodos determinados de tiempo (Por ejemplo, meses, años, etc.)*

3.2 Gestión del cambio

3.2.1 El explotador definirá y mantendrá un proceso para identificar los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus productos o servicios de aviación, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios. Un ejemplo de los cambios que deben gestionarse es la incorporación de un nuevo tipo de aeronaves, la apertura de una nueva ruta, modificaciones importantes en la dimensión del explotador, la incorporación de un nuevo tipo de operación o tecnología, las adquisiciones o funciones entre empresas, cambio de base principal de operaciones, etc.

3.2.2 Un proceso de análisis de los riesgos es un aspecto fundamental de la gestión de los cambios.

3.2.3 El proceso de gestión de cambio de la organización debe considerar las siguientes tres consideraciones:

a) Criticidad.- Las evaluaciones de criticidad determinan los sistemas, los equipos o las actividades que son fundamentales para la operación segura de la aeronave. Aunque la criticidad se evalúa normalmente durante el proceso de diseño del sistema, también es relevante durante una situación de cambio. Los sistemas, los equipos y las actividades que tengan una criticidad de seguridad operacional más alta deben revisarse después del cambio para asegurarse de que las medidas correctivas se tomaron para controlar los riesgos de seguridad operacional potencialmente emergentes.

b) Estabilidad de los sistemas y entornos operacionales.- Los cambios pueden ser planificados y estar bajo el control directo de la organización. Dichos cambios incluyen el crecimiento y la contracción institucional, la expansión de los productos o servicios suministrados o la introducción de nuevas tecnologías. Los cambios no planificados pueden incluir aquellos relacionados con ciclos económicos, descontento laboral, así como también, cambios en los entornos políticos, reglamentarios u operacionales.

c) Rendimiento pasado.- El rendimiento pasado de los sistemas críticos y el análisis de tendencias en el proceso de aseguramiento de la seguridad operacional debe usarse para anticipar y controlar el rendimiento en materia de seguridad operacional bajo situaciones de

cambio. El control del rendimiento pasado también garantiza la eficacia de las medidas correctivas tomadas para abordar deficiencias de seguridad operacional identificadas como resultado de auditorías, evaluaciones, investigaciones o informes.

3.2.4 La gestión del cambio será aceptable para la AAC si se han observado los siguientes criterios:

- *El explotador ha desarrollado y publicado en su manual del SMS un proceso para identificar los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus productos o servicios de aviación, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios, teniendo en cuenta las consideraciones de 3.2.4.*
- *El proceso de identificación y efecto de los cambios también incluye los arreglos que deberán incorporarse con anterioridad a la implementación de los cambios, así como los controles y mitigación de riesgos que ya no serán necesarios o efectivos una vez que el cambio haya surtido efecto.*
- *La gestión del cambio incluye un análisis de los riesgos asociados a dicho cambio.*

3.3 Mejora continua del SMS

3.3.1 El explotador observará y evaluará la eficacia de sus procesos SMS para permitir el mejoramiento continuo del rendimiento general del SMS.

3.3.2 La mejora continua se mide mediante el control de los indicadores de rendimiento en materia de seguridad operacional de la organización y se relaciona con la madurez y eficacia de un SMS. Los procesos del aseguramiento de la seguridad operacional respaldan las mejoras al SMS mediante la verificación continua y las medidas de seguimiento. Estos objetivos se logran mediante la aplicación de evaluaciones internas y auditorías independientes del SMS.

3.3.3 Las evaluaciones internas implican la evaluación de las actividades de aviación del explotador que pueden proporcionar información útil a los procesos de toma de decisiones de la organización. Es aquí donde se realiza la actividad clave del SMS, la identificación de peligros y mitigación de riesgos (HIRM). Las evaluaciones realizadas a raíz de este requisito deben realizarlas personas u organizaciones que sean funcionalmente independientes de los procesos técnicos evaluados. La evaluación interna incluye la evaluación de las funciones de la gestión de la seguridad operacional, el diseño de políticas, la gestión de riesgos de la seguridad operacional, el aseguramiento de la seguridad operacional y la promoción de la seguridad operacional en toda la organización.

3.3.4 Las auditorías internas implican la examinación sistemática y programada de las actividades de aviación del explotador, lo que incluye aquellas específicas para la implementación del SMS. Para lograr la máxima eficacia, las auditorías internas las llevan a cabo personas o departamentos que son independientes de las funciones que se evalúan. Tales auditorías proporcionan al ejecutivo responsable, así como también, a los funcionarios de administración superior responsables del SMS, la capacidad de rastrear la implementación y eficacia del SMS, al igual que sus sistemas de respaldo.

3.3.5 La AAC como responsable de la aceptación del SMS del explotador, puede realizar las auditorías externas del SMS. Adicionalmente, las auditorías pueden realizarlas asociaciones industriales u otros terceros que selecciona el explotador. Estas auditorías externas mejoran el sistema de auditoría interna, así como también, proporcionan vigilancia independiente.

3.3.6 En resumen, los procesos de evaluación y auditoría contribuyen con la capacidad del explotador de lograr una mejora continua en el rendimiento en materia de seguridad operacional. El

control continuo del SMS, sus controles de seguridad operacional relacionados y los sistemas de respaldo garantizan que el proceso de gestión de la seguridad operacional logre sus objetivos.

3.3.7 *La mejora continua del SMS será aceptable para la AAC si se han observado los siguientes criterios:*

- *El explotador ha establecido las políticas, características, frecuencia y procedimientos (incluidas las ayudas de trabajo) relacionados con las evaluaciones internas y auditorías independientes de su SMS.*
- *Existen en el manual del SMS disposiciones relativas a que las evaluaciones internas serán realizadas por personas u organizaciones funcionalmente independientes de los procesos técnicos evaluados.*
- *Las evaluaciones internas incluyen al menos la evaluación de:*
    - *las funciones de la gestión de la seguridad operacional;*
    - *el diseño de las políticas;*
    - *la gestión de los riesgos;*
    - *el aseguramiento de la seguridad operacional; y*
    - *la promoción de la seguridad operacional en toda la organización*
- *El explotador ha establecido la frecuencia y las circunstancias para recibir auditorías externas de asociaciones industriales, u otras empresas seleccionadas por el explotador para la evaluación de su SMS.*
- *Las políticas y procedimientos relacionados con las auditorías externas incluyen los criterios de selección de las organizaciones auditoras, y el compromiso y procedimientos para el tratamiento de los hallazgos y no conformidades.*

4. Promoción de la seguridad operacional

La promoción de la seguridad operacional alienta una cultura de seguridad operacional positiva y crea un entorno que propicia el logro de los objetivos de seguridad operacional del explotador. Esto se logra mediante la combinación de competencias técnicas que mejoran continuamente con la capacitación y educación, las comunicaciones eficaces y la distribución de información. La administración superior proporciona el liderazgo para promover la cultura de seguridad operacional en toda la organización.

El explotador debe establecer e implementar procesos y procedimientos que faciliten la comunicación eficaz en todos los niveles de la organización. Los proveedores de servicios deben comunicar sus objetivos de seguridad operacional, así como también, el estado actual de cualquier actividad o evento relacionado. Los proveedores de servicios también deben alentar la comunicación "jerárquica ascendente", lo que ofrece un entorno que permite a la administración superior recibir comentarios abiertos y constructivos del personal de operaciones.

4.1 Instrucción y educación

4.1.1 El explotador creará y mantendrá un programa de instrucción en seguridad operacional que garantice que el personal cuente con la instrucción y las competencias necesarias para cumplir sus funciones en el marco del SMS.

4.1.2 El alcance del programa de instrucción en seguridad operacional será apropiado para el tipo de participación que cada persona tenga en el SMS.

4.1.3 El gerente de seguridad operacional debe proporcionar información actual y facilitar la

capacitación pertinente para los temas de seguridad operacional específicos que encuentran las unidades institucionales. La entrega de la capacitación al personal adecuado, sin importar su nivel en la organización, es un indicio del compromiso de la gestión con un SMS eficaz. El programa de capacitación y educación de seguridad operacional debe constar de lo siguiente:

a) políticas de seguridad operacional institucional, metas y objetivos;

b) funciones de seguridad operacional institucional y responsabilidades relacionadas con la seguridad operacional;

c) principios básicos de la gestión de riesgos de la seguridad operacional;

d) sistemas de notificación de la seguridad operacional;

e) respaldo de la gestión de la seguridad operacional (lo que incluye los programas de evaluación y auditoría);

f) líneas de comunicación para la diseminación de información de seguridad operacional;

g) un proceso de validación que mide la eficacia de la capacitación; y

h) adoctrinamiento inicial documentado y requisitos de capacitación recurrente.

4.1.4 Los requisitos de capacitación coherentes con las necesidades y la complejidad de la organización deben documentarse para cada área de actividad. Se debe desarrollar un archivo de capacitación para cada empleado, incluida la administración.

4.1.5 La capacitación de seguridad operacional dentro de una organización debe garantizar que el personal sea competente para realizar tareas relacionadas con la seguridad operacional. Los procedimientos de capacitación deben especificar normas de capacitación de seguridad operacional inicial y periódica para el personal de operaciones, los gerentes y supervisores, los gerentes superiores y el ejecutivo responsable. La cantidad de capacitación de seguridad operacional debe ser adecuada para la responsabilidad y participación de la persona en el SMS. La documentación de capacitación del SMS también debe especificar las responsabilidades para el desarrollo del contenido y programación de la capacitación, así como también, la gestión de los registros de la capacitación.

4.1.6 La capacitación debe incluir la política de seguridad operacional y las funciones y responsabilidades de la seguridad operacional de la organización, los principios de SMS relacionados con la gestión de riesgos de la seguridad operacional y el aseguramiento de la seguridad operacional, así como también, el uso y los beneficios de los sistemas de notificación de seguridad operacional de la organización.

4.1.7 La capacitación de la seguridad operacional para los gerentes superiores debe incluir el contenido relacionado con el cumplimiento de los requisitos de seguridad operacional nacionales e institucionales, la asignación de recursos y la promoción activa del SMS, lo que incluye la comunicación eficaz de seguridad operacional entre los departamentos. Además, la capacitación de seguridad operacional para los gerentes superiores debe incluir material acerca del establecimiento de niveles de objetivos y alertas del rendimiento en materia de seguridad operacional.

4.1.8 Finalmente, el programa de capacitación de la seguridad operacional debe incluir una sesión diseñada específicamente para el ejecutivo responsable. Esta sesión de capacitación debe estar en un alto nivel, dándole al ejecutivo responsable una comprensión del SMS y su relación con la estrategia comercial general de la organización.

4.1.9 *La instrucción y educación será aceptable para la AAC si se han observado los siguientes criterios:*

- *El explotador ha establecido dentro de su programa de instrucción, la instrucción inicial y periódica del SMS para todas las personas involucradas en actividades de seguridad operacional que garantice el nivel de competencia de su personal. El programa establece que la instrucción de SMS debe ser recibida al menos por:*
    - *el gerente responsable*;*
    - *los gerentes superiores y supervisores; y*
    - *el personal de operaciones*
- *El alcance y duración de cada curso de instrucción del SMS es apropiado para cada área de actividad.*
- *El contenido de la instrucción aborda al menos lo establecido por 4.1.3.*
- *Está claramente establecida la responsabilidad por el desarrollo de los contenidos de los cursos, la programación y el mantenimiento de los registros de capacitación.*
- **La capacitación del ejecutivo responsable ha sido especialmente diseñada para ser una sesión de alto nivel, que asegure la comprensión sus responsabilidades con relación al SMS, así como la descripción general del SMS y su relación con la estrategia comercial de la organización.*

4.2 Comunicación de la seguridad operacional

4.2.1 El explotador creará y mantendrá un medio oficial de comunicación en relación con la seguridad operacional que:

a) garantice que el personal conozca el SMS, con arreglo al puesto que ocupe;

b) difunda información crítica para la seguridad operacional;

c) explique por qué se toman determinadas medidas de seguridad operacional; y

d) explique por qué se introducen o modifican procedimientos de seguridad operacional.

4.2.2 El explotador debe comunicar los objetivos y procedimientos del SMS de la organización a todo el personal de operaciones. El gerente de seguridad operacional debe comunicar regularmente información sobre las tendencias de rendimiento en materia de seguridad operacional y temas de seguridad operacional específicos mediante los boletines y las sesiones informativas. El gerente de seguridad operacional también debe garantizar que las lecciones aprendidas a partir de las investigaciones, las historias de casos o las experiencias, ya sean internas o de otras organizaciones, se distribuyan ampliamente. El rendimiento en materia de seguridad operacional será más eficiente si se alienta activamente para que el personal de operaciones identifique e informe los peligros.

4.2.3 Entre los ejemplos de iniciativas de comunicación institucional se incluye:

a) la diseminación del manual del SMS;

b) los procesos y procedimientos de seguridad operacional;

c) los folletos informativos, las noticias y los boletines de seguridad operacional; y

e) sitios web o correo electrónico.

4.2.4. La comunicación de la seguridad operacional será aceptable para la AAC si se han observado los siguientes criterios:

- *El explotador ha establecido un método oficial de comunicación sobre seguridad operacional que cumpla con 4.2.1 y 4.2.3.*
- *Se han comunicado debidamente a todo el personal de operaciones los objetivos y procedimientos del SMS.*
- *Se han desarrollado y documentado procedimientos para la comunicación regular de información sobre tendencias de rendimiento en materia de seguridad operacional y temas de seguridad relevantes, incluyendo la responsabilidad por la preparación y publicación de esta información.*
- *Se han determinado los medios apropiados para distribuir la información del punto anterior, de tal forma de garantizar su amplia distribución.*
- *Se han establecido mecanismos para alentar al personal de operaciones que identifique e informe sobre los peligros.*
- *Todo el personal del explotador está familiarizado con el acceso y el uso de los medios de notificación de peligros.*

8. PROCESO DE IMPLANTACIÓN DEL SMS POR ETAPAS PARA EXPLOTADORES CERTIFICADOS

8.1 A partir del 1 de enero de 2016, todos los procesos nuevos de certificación para la obtención de un certificado de explotador de servicios aéreos (AOC) o aquellos que en dicha fecha se encontraran en las Fases I o II del proceso de certificación, deberán incluir el desarrollo de un manual del SMS como parte del manual de operaciones del explotador (OM), y la implementación de todos los elementos según la Sección 7 de esta circular, con excepción de los aquellos aspectos identificados en el Figura 14, que deberán ser incluídos en un plan de implementación, que deberá ser aceptado por la AAC junto con el manual del SMS.

8.2 Para aquellos explotadores que obtuvieron su AOC con anterioridad al 1 de enero del 2016, o que en aquella fecha se encuentren en las Fases III o IV del proceso de certificación, se prevé un proceso de adecuación o implantación del SMS por etapas, en virtud a que la mayor parte de los elementos del SMS descritos en la Sección 7 ya forman parte del programa de prevención de accidentes, sistema de calidad y otros procesos anteriores al desarrollo del concepto de los SMS. En este sentido, lo que hace falta es en primer lugar identificar los elementos que ya están desarrollados y ajustarlos a los criterios del SMS, y lógicamente, desarrollar aquellos elementos que no estuvieran todavía desarrollados. El contenido de estas etapas se detalla en la Figura 13. Una descripción en detalle se incluye a partir del Numeral 8.11. **Las 4 etapas de implementación se aplican solamente a explotadores certificados.**

8.3 El proceso de transición o adaptación, también llamado de implantación del SMS puede durar desde algunos meses hasta varios años, **dependiendo del tamaño, complejidad y naturaleza de las operaciones del explotador, y el resultado del análisis de los elementos faltantes**. Para facilitar la implantación, la misma se ha dividido en etapas. El número de etapas y la duración de cada una de estas dependerán del resultado del análisis de brecha, y del tamaño, naturaleza y complejidad de las operaciones del explotador. En el Adjunto H se ofrece una lista de las preguntas del análisis de brechas para facilitar que los explotadores evalúen sistemáticamente sus procesos existentes.

8.4 Un plan de implementación de SMS se desarrolla con el asesoramiento del ejecutivo responsable y los gerentes responsables del suministro de productos y servicios relacionados con la operación segura de la aeronave o en respaldo de esta. Luego de completarse, el ejecutivo responsable apoya el plan. El plan de implementación del SMS incluye cronologías e hitos

coherentes con los requisitos identificados en el proceso de análisis de brechas, la envergadura del proveedor de servicios y la complejidad de sus productos o servicios. El plan debe abordar la coordinación con organizaciones o contratistas externos, donde corresponda, y deberá ser aceptado por la AAC.

8.5 El plan de implantación del explotador puede documentarse de diferentes formas, lo que varía de una simple hoja de cálculos hasta software especializado de gestión de proyectos. El plan de implantación debe abordar las brechas mediante la finalización de medidas e hitos específicos de acuerdo con la cronología determinada. La asignación de cada tarea garantiza una responsabilidad en todo el proceso de implementación. El plan debe revisarse y actualizarse regularmente, según sea necesario. En el Adjunto H se muestra un ejemplo de formato de un plan/programa de implementación del SMS.

8.6 A partir del párrafo siguiente, se presenta una descripción genérica de un proceso de implantación por etapas, es fundamental comprender que dicho texto se presenta solamente como una orientación y recalcar que: **el número de etapas y la duración de cada una de estas dependerán del resultado del análisis de brecha, y del tamaño, naturaleza y complejidad de las operaciones del explotador.** En este sentido se recuerda que las referencias de las etapas y la duración de las mismas que se incluyen en los párrafos siguientes son solamente de muestra.

8.7 La implementación de un SMS es un proceso sistemático. Sin embargo, este proceso puede resultar ser una tarea bastante desafiante dependiendo de los factores, como la disponibilidad del material guía y recursos necesarios para la implementación, así como también, el conocimiento preexistente del proveedor de servicios de los procesos y procedimientos del SMS.

8.8 Entre los motivos para un enfoque en etapas para la implementación de SMS se incluyen:

a) la disposición de una serie de pasos gestionables que se deban seguir para la implementación de un SMS, como la asignación de recursos;

b) la necesidad de permitir la implementación de elementos del marco de trabajo del SMS en varias secuencias, según los resultados de cada análisis de brechas del proveedor de servicios;

c) la disponibilidad inicial de los datos y procesos analíticos para respaldar las prácticas de gestión de la seguridad operacional reactiva, proactiva y predictiva; y

d) la necesidad de un proceso metodológico para garantizar la implementación de SMS eficaz y sustentable.

8.9 El enfoque en etapas reconoce que la implementación de un SMS completamente maduro es un proceso que toma varios años. Un enfoque de implementación en etapas permite que el SMS sea mucho más sólido a medida que se completa cada etapa de implementación. Se completan los procesos de gestión de la seguridad operacional fundamentales antes de pasar a etapas sucesivas que impliquen procesos de mayor complejidad.

8.10 Se describen como ejemplo cuatro etapas de implementación para un SMS. Cada etapa se asocia con varios elementos (o subelementos) según el marco de trabajo del SMS. Resulta aparente que la configuración particular de los elementos en este material guía no esté diseñada para ser absoluta. La AAC y el explotador deben hacer estos ajustes como mejor se considere según las circunstancias. En la **Figura 13** se muestra el contenido de las cuatro etapas de la implantación del SMS y sus elementos correspondientes para explotadores certificados, y en la **Figura 14** se muestran los elementos que deben ser incluídos en el plan de implementación del SMS de un explotador nuevo.

Figura 13 – Contenido de las cuatro etapas de la implementación del SMS en un explotador existente

Etapa 1 (12 meses*)	Etapa 2 (12 meses)	Etapa 3 (18 meses)	Etapa 4 (18 meses)
1. Elemento 1.1 del SMS (i): a) identificar al ejecutivo responsable del SMS; b) establecer un equipo de implementación del SMS; c) definir el alcance del SMS; d) realizar un análisis de brechas de SMS. 2. Elemento 1.5 del SMS (i): a) desarrollar un plan de implementación del SMS. 3. Elemento 1.3 del SMS: a) establecer una persona/oficina clave responsable de la administración y el mantenimiento del SMS. 4. Elemento 4.1 del SMS (i): a) establecer un programa de capacitación de SMS para el personal, con prioridad para el equipo de implementación del SMS. 5. Elemento 4.2 del SMS (i): a) iniciar canales de comunicación del SMS/seguridad operacional.	1. Elemento 1.1 del SMS (ii): a) establecer la política y los objetivos de seguridad operacional, 2. Elemento 1.2 del SMS: a) definir las responsabilidades de la gestión de la seguridad operacional en los departamentos pertinentes de la organización; b) establecer un mecanismo/comité de coordinación de SMS/seguridad operacional; c) establecer SAG por departamento/divisional, donde corresponda. 3. Elemento 1.4 del SMS: a) establecer un plan de respuesta ante emergencias. 4. Elemento 1.5 del SMS (ii): a) iniciar el desarrollo progresivo de un documento/manual de SMS y otra documentación de respaldo.	1. Elemento 2.1 del SMS (i): a) establecer un procedimiento de notificación de peligros voluntaria. 2. Elemento 2.2 del SMS: a) establecer procedimientos de gestión de riesgos de la seguridad operacional. 3. Elemento 3.1 del SMS (i): a) establecer procedimientos de notificación e investigación de sucesos; b) establecer un sistema de recopilación y procesamiento de datos de seguridad operacional para los resultados de alto impacto; c) desarrollar SPI de alto impacto y una configuración de objetivos y alertas asociada. 4. Elemento 3.2 del SMS: a) establecer un procedimiento de gestión de cambio que incluye la evaluación de riesgos de seguridad operacional. 5. Elemento 3.3 del SMS (i): a) establecer un programa interno de auditoría de la calidad; b) establecer un programa externo de auditoría de la calidad.	1. Elemento 1.1 del SMS (iii): a) mejorar el procedimiento disciplinario/la política existentes con una debida consideración de los errores o las equivocaciones accidentales de las infracciones deliberadas o graves. 2. Elemento 2.1 del SMS (ii): a) integrar los peligros identificados a partir de los informes de investigación de sucesos con el sistema de notificación de peligros voluntaria; b) integrar procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o el cliente, donde corresponda. 3. Elemento 3.1 del SMS (ii): a) mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto; b) desarrollar SPI de bajo impacto y una configuración de objetivos/alertas asociada. 4. Elemento 3.3 del SMS (ii): a) establecer programas de auditoría de SMS o integrarlos en programas de auditoría internos y externos existentes; b) establecer otros programas de revisión/estudio de SMS operacional, donde corresponda. 5. Elemento 4.1 del SMS (ii): a) garantizar que se haya completado el programa de capacitación de SMS para todo el personal pertinentes. 6. Elemento 4.2 del SMS (ii): a) promover la distribución e intercambio de información de la seguridad operacional de forma interna y externa.
Elemento 1.5 del SMS: documentación del SMS (Etapas 1 a 4) >>			
Elementos 4.1 y 4.2 del SMS: capacitación, educación y comunicación de SMS (Etapas 1 y posteriores) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			
Nota 1.— El período de implementación indicado es una aproximación. El período de implementación real depende del alcance de las medidas necesarias para cada elemento asignado y la envergadura/complejidad de la organización. *Nota 2.— Los números de elementos del SMS indicados corresponden a los números de elementos del SMS de la OACI. Los sufijos como a), b) y c) indican que el elemento se ha subdividido para facilitar el enfoque de implementación en etapas.*			

Figura 14 – Contenido del plan de implementación del SMS en un explotador nuevo

1. Elemento 1.1 del SMS (i): a) identificar al ejecutivo responsable del SMS; b) establecer un equipo de implementación del SMS; c) definir el alcance del SMS; d) realizar un análisis de brechas de SMS. 2. Elemento 1.5 del SMS (i): a) desarrollar un plan de implementación del SMS. 3. Elemento 1.3 del SMS: a) establecer una persona/oficina clave responsable de la administración y el mantenimiento del SMS. 4. Elemento 4.1 del SMS (i): a) establecer un programa de capacitación de SMS para el personal, con p[illegible] implementación del SMS. 5. Elemento 4.2 del SMS (i): a) iniciar canales de comunicación para 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 [illegible] de SMS y otra [illegible] establecido.	1. Elemento 2.1 del SMS (i): a) establecer un procedimiento de notificación de peligros voluntaria. 2. Elemento 2.2 del SMS: a) establecer procedimientos de gestión de riesgos de la seguridad operacional. 3. Elemento 3.1 del SMS (i): a) establecer procedimientos de notificación e investigación de sucesos; b) establecer un sistema de recopilación y procesamiento de datos de seguridad operacional para los resultados de alto impacto; c) desarrollar SPI de alto impacto y una configuración de objetivos y alertas asociada. 4. Elemento [illegible] del SMS: a) establecer un procedimiento de gestión del cambio que [illegible] evaluación de riesgos [illegible] operacional. 5. Elemento [illegible] del SMS: a) establecer [illegible] auditoría [illegible] b) establecer un programa externo de [illegible] de la calidad.	1. Elemento 1.1 del SMS (iii): a) mejorar el procedimiento disciplinario/la política existentes con una debida consideración de los errores o las equivocaciones accidentales de las infracciones deliberadas o graves. 2. Elemento 2.1 del SMS (ii): a) integrar los peligros identificados a partir de los informes de investigación de sucesos con el sistema de notificación de peligros voluntaria; b) integrar procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o el cliente, donde corresponda. 3. Elemento 3.1 del SMS (ii): a) mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto; b) desarrollar SPI de bajo impacto y una configuración de objetivos/alertas asociada. 4. Elemento 3.3 del SMS (ii): a) establecer programas de auditoría de SMS o integrarlos en programas de auditoría internos y externos existentes; b) establecer otros programas de revisión/estudio de SMS operacional, donde corresponda. 5. Elemento 4.1 del SMS (ii): a) garantizar que se haya completado el programa de capacitación de SMS para todo el personal pertinente. 6. Elemento 4.2 del SMS (ii): a) promover la distribución e intercambio de información de la seguridad operacional de forma interna y externa.
Nota 1.— Los elementos en negro oscuro, son aquellos que no pueden ser implementados por un nuevo explotador durante el proceso de certificación y que serán desarrollados de acuerdo con el plan de implementación una vez que el explotador inicie sus operaciones. *Nota 2. — Los elementos en gris claro son auqellos que deben desarrollarse y establecerse antes de la emisión del AOC.* *Nota 2.— El plan de implementación debe ser aceptado por la AAC antes de la emisión del AOC.*			

8.11 **Etapa 1**

8.11.1 El objetivo de la Etapa 1 de la implementación de SMS es proporcionar un plano de cómo se cumplirán los requisitos de SMS y se integrarán en los sistemas de control de la organización, así como también, un marco de trabajo de responsabilidad para la implementación del SMS.

8.11.2 Durante la Etapa 1, se establece una planificación básica y la asignación de responsabilidades. Un aspecto central en la Etapa 1 es el análisis de brechas. A partir del análisis de brechas, una organización puede determinar el estado de sus procesos de gestión de la seguridad operacional existentes y puede comenzar a planificar el desarrollo de otros procesos de gestión de la seguridad operacional. El resultado importante de la Etapa 1 es el plan de implementación del SMS.

8.11.3 Al finalizar la Etapa 1, se deben finalizar las siguientes actividades de tal forma que cumplan las expectativas de la autoridad de vigilancia de la aviación civil, como se establece en los requisitos y el material guía pertinentes:

Compromiso y responsabilidad de la gestión — Elemento 1.1 (i)

a) Identificar al ejecutivo responsable y las responsabilidades de seguridad operacional de los gerentes. Esta actividad se basa en los Elementos 1.1 y 1.2 del marco de trabajo del SMS.

b) Establecer un equipo de implementación del SMS. El equipo debe componerse de representantes de los departamentos pertinentes. El papel del equipo es impulsar la implementación de SMS desde la etapa de planificación hasta la implementación final. Otras funciones del equipo de implementación incluirán, entre otras:

   1) desarrollar el plan de implementación del SMS;

   2) garantizar la capacitación adecuada del SMS y experiencia técnica del equipo para implementar eficazmente los elementos del SMS y los procesos relacionados; y

   3) controlar y notificar el progreso de la implementación del SMS, proporcionar actualizaciones regulares y coordinar con el ejecutivo responsable del SMS.

c) Definir el alcance de las actividades de la organización (departamentos/divisiones) según el cual el SMS será aplicable. El alcance de la aplicabilidad del SMS de la organización se deberá describir posteriormente en el manual del SMS, según corresponda. Esta actividad se basa en el Elemento 1.5 del marco de trabajo del SMS.

d) Realizar un análisis de brechas de los sistemas y procesos actuales de la organización en relación con los requisitos del marco de trabajo del SMS (o los requisitos reglamentarios de SMS pertinentes). En el Adjunto H de este capítulo se encuentra una guía sobre un análisis de brechas de SMS para un proveedor de servicios.

Plan de implementación del SMS — Elemento 1.5 (i)

a) Desarrollar un plan de implementación del SMS acerca de cómo la organización implementará el SMS sobre la base del sistema identificado y las brechas del proceso que se generan del análisis de brechas. En el Adjunto H de este capítulo se muestra un ejemplo de un plan de implementación de SMS básico.

Nombramiento del personal de seguridad operacional clave — Elemento 1.3

a) Identificar la persona de SMS clave (seguridad operacional/calidad/función) dentro de la organización que será responsable de administrar el SMS en nombre del ejecutivo responsable.

b) Establecer la oficina de servicios de seguridad operacional.

Capacitación y educación — Elemento 4.1 (i)

a) Realizar un análisis de las necesidades de capacitación.

b) Organizar y configurar programas para la capacitación correcta de todo el personal, de acuerdo con sus responsabilidades individuales y su participación en el SMS.

c) Desarrollar la capacitación de la seguridad operacional, considerando:

1) la capacitación inicial (seguridad operacional general) específica del trabajo; y

2) la capacitación periódica.

d) Identificar los costos asociados con la capacitación.

e) Desarrollar un proceso de validación que mide la eficacia de la capacitación.

f) Establecer un sistema de registros de capacitación de la seguridad operacional.

Comunicación de la seguridad operacional — Elemento 4.2 (i)

a) Iniciar un mecanismo o medio para una comunicación de seguridad operacional.

b) Establecer un medio para transferir información de seguridad operacional mediante cualquiera de las siguientes opciones:

1) folletos informativos, noticias y boletines de seguridad operacional;

2) sitios web;

3) correo electrónico.

8.12 **Etapa 2**

8.12.1 El objetivo de la Etapa 2 es implementar procesos de gestión de seguridad operacional fundamentales, mientras que al mismo tiempo de corrigen las posibles deficiencias en los procesos de gestión de seguridad operacional existentes. La mayoría de las organizaciones tendrán implementadas ciertas actividades de gestión de seguridad operacional básicas, en diferentes niveles de implementación. Esta etapa está orientada a consolidar las actividades existentes y desarrollar aquellas que todavía no existen.

Compromisos y responsabilidades de la gestión — Elemento 1.1 (ii)

a) Desarrollar una política de seguridad operacional.

b) Solicitar que el ejecutivo responsable firme la política de seguridad operacional.

c) Comunicar la política de seguridad operacional en toda la organización.

d) Establecer un programa de revisión de la política de seguridad operacional para garantizar que sigue siendo pertinente y adecuada para la organización.

e) Establecer objetivos de seguridad operacional para el SMS mediante el desarrollo de normas de rendimiento en materia de seguridad operacional en términos de:

1) indicadores de rendimiento en materia de seguridad operacional;

2) niveles de objetivos y alertas de rendimiento en materia de seguridad operacional; y

3) planes de acción.

f) Establecer los requisitos del SMS para los subcontratistas:

1) establecer un procedimiento para escribir requisitos del SMS en el proceso contratante;

2) establecer los requisitos del SMS en la documentación de licitación.

Responsabilidades de la seguridad operacional — Elemento 1.2

a) Definir las responsabilidades de la seguridad operacional y comunicarlas en toda la organización.

b) Establecer el grupo de acción de seguridad operacional (SAG).

c) Establecer el comité de coordinación de la seguridad operacional/SMS.

d) Definir las funciones claras para el SAG y el comité de coordinación de la seguridad operacional/SMS.

e) Establecer líneas de comunicación entre la oficina de servicios de seguridad operacional, el ejecutivo responsable, el SAG y el comité de coordinación de la seguridad operacional/SMS.

f) Asignar un ejecutivo responsable como el líder del comité de coordinación de seguridad operacional/SMS.

g) Desarrollar un programa de reuniones para la oficina de servicios de seguridad operacional para reunirse con el comité de coordinación de seguridad operacional/SMS y el SAG, según sea necesario.

Coordinación de la planificación de respuesta ante emergencias — Elemento 1.4

a) Revisar la descripción del ERP relacionado con la delegación de autoridad y asignación de responsabilidades de emergencia.

c) Establecer procedimientos de coordinación para medidas mediante el personal clave durante la emergencia y volver a las operaciones normales.

c) Identificar entidades externas que interactuarán con la organización durante situaciones de emergencia.

d) Evaluar los ERP respectivos de las entidades externas.

e) Establecer la coordinación entre los diferentes ERP.

f) Incorporar información acerca de la coordinación entre los diferentes ERP en la documentación de SMS de la organización.

Nota.- Véase el Adjunto C para una guía detallada sobre ERP.

Documentación del SMS — Elemento 1.5 (ii)

a) Crear un sistema de documentación del SMS para describir, guardar, recuperar y archivar toda la información y los registros relacionados con SMS al:

1) desarrollar un documento de SMS que sea un manual independiente o una sección distinta dentro de un manual institucional controlado existente (véase el Adjunto D) para una guía sobre el desarrollo de un manual de SMS);

2) establecer un sistema de archivo de SMS para recopilar y mantener los registros actuales en relación con los procesos de SMS constantes de la organización;

3) mantener registros para proporcionar una referencia histórica, así como también, el estado actual de todos los procesos de SMS, como por ejemplo: un registro de peligros; un índice de evaluaciones de seguridad operacional completadas; registros de capacitación de SMS/ seguridad operacional; los SPI actuales y los objetivos de seguridad operacional asociados; informes de auditoría interna de SMS; actas de la reunión del comité de SMS/seguridad operacional y el plan de implementación de SMS;

4) mantener registros que servirán como evidencia de la operación de SMS y las actividades durante la evaluación o auditoría internas o externas del SMS.

8.13 **Etapa 3**

8.13.1 El objetivo de la Etapa 3 es establecer procesos de gestión de riesgos de la seguridad operacional. Hacia el final de la Etapa 3, la organización estará lista para recopilar datos de seguridad operacional y realizar los análisis de seguridad operacional basados en la información obtenida mediante diversos sistemas de notificación.

Identificación de peligros — Elemento 2.1 (i)

a) Establecer un procedimiento de notificación voluntaria. Véase el Adjunto E para guía.

b) Establecer un programa/plan para la revisión sistemática de todos los procesos/equipos relacionados con la seguridad operacional de aviación aplicables que sean idóneos para el proceso de HIRM.

c) Establecer un proceso para la priorización y asignación de peligros identificados para la mitigación de riesgos.

Evaluación y mitigación de riesgos de seguridad operacional — Elemento 2.2

a) Establecer un procedimiento de gestión de riesgos de la seguridad operacional que incluya su aprobación y un proceso de revisión periódico.

b) Desarrollar y adoptar matrices de riesgos de seguridad operacional pertinentes para los procesos operacionales y de producción de la organización.

c) Incluir matrices de riesgos de seguridad operacional adoptados e instrucciones asociadas en el material de capacitación de la gestión de riesgos o SMS de la organización.

Control y medición del rendimiento en materia de seguridad operacional — Elemento 3.1 (i)

a) Establecer un procedimiento interno de notificación e investigación de sucesos. Esto puede incluir informes obligatorios de defectos (MDR) o informes importantes, donde corresponda.

b) Establecer la recopilación, el procesamiento y el análisis de los datos de seguridad operacional de los resultados de alto impacto.

c) Establecer indicadores de seguridad operacional de alto impacto (ALoSP inicial) y su configuración de objetivos y alertas asociados. Entre los ejemplos de indicadores de seguridad operacional de alto impacto se incluyen tasas de accidentes, tasas de incidentes graves y el control de los resultados de no cumplimiento de alto riesgo. Véase el Adjunto G para guía sobre los indicadores de rendimiento en seguridad operacional.

d) Lograr un acuerdo con la autoridad de vigilancia del Estado sobre los indicadores de rendimiento en materia de seguridad operacional y objetivos de rendimiento en materia de seguridad operacional.

La gestión de cambio — Elemento 3.2

a) Establecer un proceso formal para la gestión de cambio que considera:

   1) la vulnerabilidad de los sistemas y actividades;

   2) la estabilidad de los sistemas y entornos operacionales;

   3) rendimiento pasado;

   4) cambios reglamentarios, industriales y tecnológicos.

b) Garantizar que los procedimientos de la gestión de cambio aborden el impacto de los registros existentes de rendimiento en materia de seguridad operacional y de mitigación de riesgos antes de implementar nuevos cambios.

c) Establecer procedimientos para garantizar que se lleve a cabo (o se considere) la evaluación de seguridad operacional de las operaciones, los procesos y los equipos relacionados con la seguridad operacional de la aviación, según corresponda, antes de ponerlos en servicio.

Mejora continua del SMS — Elemento 3.3 (i)

a) Desarrollar formularios para las evaluaciones internas.

b) Definir un proceso de auditoría interna.

c) Definir un proceso de auditoría externa.

d) Definir un programa para la evaluación de instalaciones, equipos, documentación y procedimientos que se deben completar mediante auditorías y estudios.

e) Desarrollar documentación pertinente para el aseguramiento de la seguridad operacional.

8.14 **Etapa 4**

8.14.1 La Etapa 4 es la etapa final de la implementación de SMS. Esta etapa implica la implementación madura de la gestión de riesgos de la seguridad operacional y el aseguramiento de la seguridad operacional. En esta etapa, el aseguramiento de la seguridad operacional se evalúa mediante la implementación de control periódico, retroalimentación y una medida correctiva continua para mantener la eficacia de los controles de riesgos de seguridad operacional.

Compromiso y responsabilidad de la gestión — Elemento 1.1 (iii)

a) Mejorar el procedimiento disciplinario/la política existentes con una debida consideración de errores/equivocaciones accidentales de las infracciones deliberadas/graves.

Identificación de peligros — Elemento 2.1 (ii)

a) Integrar los peligros identificados en los informes de investigación de sucesos con el sistema de notificación voluntaria.

b) Integrar los procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o del cliente, donde corresponda.

c) Si fuera necesario, desarrollar un proceso para priorizar peligros recopilados para la mitigación de riesgos según las áreas de mayor necesidad o preocupación.

Control y medición del rendimiento en materia de seguridad operacional — Elemento 3.1 (ii)

a) Mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto.

b) Establecer indicadores de seguridad operacional/calidad de bajo impacto con el control del nivel de objetivos/alertas, según corresponda (ALoSP maduro).

c) Lograr un acuerdo con la autoridad de vigilancia del Estado sobre indicadores de rendimiento en materia de seguridad operacional de bajo impacto y niveles de objetivos/alertas de rendimiento en materia de seguridad operacional.

Mejora continua del SMS — Elemento 3.3 (ii)

a) Establecer auditorías de SMS o integrarlas en los programas de auditoría interna o externa existentes.

b) Establecer otros programas de revisión/estudio de SMS operacional, donde corresponda.

Capacitación y educación — Elemento 4.1 (ii)

a) Completar un programa de capacitación de SMS para todo el personal pertinente.

Comunicación de seguridad operacional — Elemento 4.2 (ii)

a) Establecer mecanismos para promover la distribución y el intercambio de información de seguridad operacional de forma interna y externa.

8.15 Elementos del SMS implementados progresivamente a través de las Etapas 1 a 4. En la implementación del enfoque en etapas, los siguientes tres elementos clave se implementan progresivamente en cada una de las etapas:

Documentación del SMS — Elemento 1.5

8.15.1 A medida que el SMS madura progresivamente, el manual del SMS pertinente y la documentación de la seguridad operacional deben revisarse y actualizarse en conformidad. Esta actividad será inherente a todas las etapas de la implementación del SMS y también deberá mantenerse después de la implementación.

Capacitación y educación — Elemento 4.1 y comunicación de la seguridad operacional — Elemento 4.2

8.15.2 Al igual que con la documentación de SMS, la capacitación, la educación y la comunicación de seguridad operacional son actividades continuas importantes en todas las etapas de la implantación del SMS. A medida que evoluciona el SMS, pueden entrar en vigencia nuevos procesos, procedimientos o reglamentos o los procedimientos existentes pueden cambiar para proveer los requisitos del SMS. Para garantizar que todo el personal que participa en las tareas relacionadas con la seguridad operacional comprenden e implementan realmente estos cambios, es vital que la capacitación y comunicación sigan siendo actividades continuas en toda la implementación del SMS y luego de completarse.

9. PROCESO DE ACEPTACIÓN INCIAL DEL SMS PARA EXPLOTADORES NUEVOS

9.1 El proceso de aceptación del SMS forma parte integral del proceso de certificación del explotador 121 o 135. La aceptación del SMS es un requisito previo a la otorgación del AOC y las OpSpecs, dado que los procedimientos del SMS deben ser aplicados desde el primer día de operaciones. A continuación se describen las acciones que debe llevar a cabo el explotador, durante el proceso de certificación para obtener la aprobación oportuna del su SMS.

9.2 Fase 1 – Pre solicitud

9.2.1 El solicitante de un AOC debe recibir una copia de esta circular durante la Fase 1 del proceso de certificación. Es muy importante que esté familiarizado con su contenido antes de la reunión de pre-solicitud de tal manera de tener listas todas sus preguntas e inquietudes con relación a la implantación del SMS que necesita aclarar con la AAC. Al culminar la Fase I el solicitante debe comprender a cabalidad todo el contenido de esta circular, así como ser capaz de interpretar correctamente cada uno de los Adjuntos.

9.2.2 En la reunión de pre-solicitud y durante las reuniones sucesivas que podrían requerirse antes de pasar a la Fase II, deben acordarse con la AAC el alcance del SMS en función del tipo y complejidad de las operaciones propuestas. Este es el primer paso para la planificación adecuada del SMS. También es importante adelantar los criterios que serán utilizados para definir los indicadores y objetivos de seguridad operacional. Es este sentido un factor clave es determinar si la AAC ya ha establecido ciertos indicadores y objetivos como parte del programa estatal de seguridad operacional (SSP) que deben ser tomados en cuenta por el explotador.

9.2.3 No es posible iniciar el desarrollo del manual del SMS del explotador si no se ha acordado con la AAC el alcance del SMS del explotador y los criterios para el establecimiento de indicadores y metas de seguridad operacional.

9.3 **Fase 2 – Solicitud formal**

9.3.1 Durante la Fase II y con anterioridad a la presentación de la carta de solicitud formal, el explotador deberá desarrollar el contenido de todos los elementos descritos en la Sección 7 de esta circular según los criterios del Numeral 8.1 de esta circular. Esto incluirá, entre otros, el desarrollo del manual del SMS, el establecimiento de una base de datos, el desarrollo de los formularios de notificación de peligros, el establecimiento de los indicadores y objetivos de seguridad operacional con sus correspondientes niveles de alerta, el programa de instrucción del SMS, etc. El solicitante puede llevar adelante el análisis de brecha del Adjunto H para asegurarse que todos los elementos del SMS están en su lugar. El análisis del faltante no es requerido para un explotador nuevo, pero es una referencia útil durante esta etapa.

9.3.2 El manual del SMS y el plan de implementación deberán ser presentados a la AAC junto con la carta de solicitud formal y el resto de los documentos del explotador. Es importante recordar que el manual del SMS forma parte del manual de operaciones del explotador, aún si se ha desarrollado como un documento separado. Una vez que se ha presentado la carta de solicitud formal, la AAC llevará adelante una revisión superficial del manual del SMS para verificar que se han cumplido todos los aspectos formales, y notificará la admisión o rechazo del documento. La AAC tiene un plazo de 10 días para pronunciarse con relación al documento. Esta eventual admisión no implica de ninguna manera la aceptación del SMS del explotador ni de su manual, sólo indica que aparentemente está completo y que puede iniciarse su revisión en detalle como parte de la Fase III del proceso de certificación.

9.3.3 En caso de que el documento sea rechazado por la AAC, el explotador deberá proceder a revisar las observaciones y subsanarlas en el menor tiempo posible. Los ejemplos y formatos incluidos en esta circular representan medios aceptables de cumplimiento (MAC) para la AAC por lo que se recomienda que los explotadores los utilicen como guía para la confección de su SMS.

9.4 **Fase 3 – Análisis de la documentación**

9.4.1 Una vez que los documentos han sido admitidos como parte de la solitud formal, a la AAC le corresponde revisar el manual del SMS y el plan de implemetación en detalle, utilizando como referencia la ayuda de trabajo del Adjunto D. Durante esta fase, es muy importante que el explotador mantenga una comunicación fluida con la AAC para poder resolver oportunamente cualquier observación que surja durante la revisión del manual.

9.4.2 Algunos aspectos complementarios al manual, así como la aplicación de éstos, serán verificados en la Fase IV del proceso de certificación del explotador durante las inspecciones y demostraciones.

9.4.3 Una vez que el explotador haya subsanado todas las observaciones de la AAC con relación al manual el SMS y al plan de implementación, le corresponde a la AAC aceptar dichos documentos como parte del manual de operaciones (OM) del explotador.

9.4.4 Durante esta etapa la AAC revisará el contenido del curso de SMS del explotador como parte de su programa de instrucción y le otorgará, si corresponde, una aprobación inicial para que el explotador proceda a impartir esta capacitación. Es muy probable que los primeros cursos sean cercanamente vigilados por la AAC para comprobar que se están impartiendo en armonía con el programa aprobado.

9.5 **Fase 4 – Inspección y demostración**

9.5.1 La Fase IV del proceso de certificación ofrece a la AAC una excelente oportunidad para evaluar el establecimiento del SMS. En este momento del proceso de certificación, el explotador ya debería encontrarse prácticamente listo para iniciar sus operaciones comerciales, hecho que será demostrado mediante las pruebas de demostración y las inspecciones.

9.5.2 En esta etapa los inspectores de la AAC utilizarán el contenido del Adjunto H para verificar que todos los elementos del SMS que se detallan en la Sección 7 de esta circular han sido debidamente desarrollados e incorporados por el explotador.

9.5.3 La AAC revisará y verificará el correcto funcionamiento del sistema de base de datos y registros del SMS del explotador para asegurarse que cumplen con los criterios de aceptabilidad y que son adecuados para el tipo de operaciones que se pretende realizar.

9.5.4 Como parte de las demostraciones, la AAC podrá solicitar la simulación de un proceso completo de gestión de los riesgos, desde la identificación y reporte de un peligro, hasta la determinación de las medidas adecuadas y los medios para hacerle seguimiento.

9.5.5 Si la AAC queda satisfecha con las inspecciones y demostraciones del SMS, emitirá un informe interno sobre la aceptación inicial del SMS del explotador, que se consolidará con el resto de aceptaciones y aprobaciones que forman parte del proceso principal de certificación. En caso de que la AAC tenga algunas observaciones o que hubiera determinado que alguno de los elementos del SMS no cumplen con los criterios de aceptación, comunicará al explotador los detalles por escrito para que sean subsanados oportunamente. La Fase IV no puede darse por concluida hasta que el explotador haya solucionado, a satisfacción de la AAC, todas las observaciones.

9.6 **Fase 5 – Aceptación**

9.6.1 La **aceptación inicial** del SMS por parte de la AAC es un requisito previo a la emisión del AOC y las especificaciones relativas a las operaciones (OpSpecs) del explotador. Dicha aceptación estará de acuerdo con lo establecido en la Figura 14 de esta circular de asesoramiento. Una vez que el explotador haya superado satisfactoriamente las cuatro primeras fases del proceso de certificación, le corresponderá a la AAC la emisión del OAC y de las OpSpecs.

9.6.2 A partir del primer día de las operaciones, el explotador implementará su SMS, poniendo en funcionamiento todos los procesos y procedimientos establecidos y aceptados por la AAC durante el proceso de certificación. A partir de este día, el explotador recopilará datos de seguridad operacional, identificará peligros, determinará sus consecuencias, gestionará los riesgos e implemetará las medidas de mitigación correspondientes. Al cabo de un período determinado, el explotador procederá a acordar con la AAC sus indicadores y niveles de objetivos y alertas, una vez que cuente con suficiente información de seguridad operacional, con lo cual se dará por finalizado el proceso de aceptación del SMS del explotador y se continuará con la vigilancia del mismo. Durante el período de implementación, el explotador revisará su sistema para hacer las mejoras en sus procesos y procedimientos y completará los ítems referidos en la Etapa IV.

9.6.3 Una vez que el explotador cumpla con el contenido del plan de implementación, de acuerdo con el plazo fijado, la AAC procederá a emitir la aceptación final del SMS del explotador.

.

ADJUNTO A

EJEMPLO DE DECLARACION DE POLITICA DE SEGURIDAD OPERACIONAL DEL EXPLOTADOR

La seguridad operacional es una de nuestras funciones comerciales centrales. Estamos comprometidos a desarrollar, implementar, mantener y mejorar constantemente las estrategias y los procesos para garantizar que todas nuestras actividades de aviación se lleven a cabo a partir de una correcta asignación de recursos institucionales, orientados a alcanzar el más alto nivel de rendimiento en materia de seguridad operacional y cumplir con requisitos reglamentarios, mientras prestamos nuestros servicios.

Todos los niveles de administración y todos los empleados son responsables de proporcionar el más alto nivel de rendimiento en materia de seguridad operacional, comenzando con [Funcionario ejecutivo principal director ejecutivo/o lo que corresponda para la organización].

Nuestro compromiso es para:

• *respaldar* la gestión de la seguridad operacional mediante la disposición de los recursos correspondientes que generarán una cultura institucional que fomenta prácticas seguras, alienta una notificación y comunicación eficaces de la seguridad operacional y gestiona activamente la seguridad operacional con la misma atención a los resultados como la atención a los resultados de otros sistemas de gestión de la organización;

• *garantizar* que la gestión de la seguridad operacional sea una de las responsabilidades principales de todos los gerentes y empleados;

• *definir claramente,* para todo el personal, gerentes y empleados por igual, sus responsabilidades para la entrega del rendimiento en materia de seguridad operacional de la organización y el rendimiento de nuestro sistema de gestión de la seguridad operacional;

• *establecer y operar* los procesos de identificación de peligros y gestión de riesgos, incluido un sistema de notificación de peligros, para eliminar o mitigar los riesgos de seguridad operacional de las consecuencias de peligros que se generen de nuestras operaciones o actividades, para alcanzar una mejora continua en nuestro rendimiento en materia de seguridad operacional;

• *garantizar* que no se tome ninguna medida en contra de ningún empleado que divulgue una preocupación de seguridad operacional mediante el sistema de notificación de peligros, a menos que dicha divulgación indique, más allá de cualquier duda razonable, una negligencia grave o una despreocupación deliberada o consciente de los reglamentos y procedimientos;

• *cumplir* con y, cuando sea posible, superar los requisitos y las normas reglamentarias y legislativas;

• *garantizar* que estén disponibles suficientes recursos humanos cualificados y capacitados para implementar las estrategias y los procesos de seguridad operacional;

• *garantizar* que todo el personal disponga de información y capacitación adecuadas y correspondientes de la seguridad operacional de la aviación, sea competente en asuntos de seguridad operacional y tengan asignadas solo tareas proporcionales a sus habilidades;

• *establecer y medir* nuestro rendimiento en materia de seguridad operacional en contraste con indicadores de rendimiento en materia de seguridad operacional realistas y objetivos de rendimiento en materia de seguridad operacional;

• *mejorar continuamente* nuestro rendimiento en materia de seguridad operacional mediante un control y una medición continuos, revisión y ajuste regulares de los objetivos y las metas de seguridad operacional y el logro diligente de estos; y

• *garantizar* que se implementen los sistemas y servicios suministrados de forma externa para respaldar nuestras operaciones y que cumplan nuestras normas de rendimiento en materia de seguridad operacional.
(Firmado)

_____
Director ejecutivo/o quien corresponda

ADJUNTO B

MUESTRA DE DESCRIPCION DE TRABAJO DE UN GERENTE DE SEGURIDAD OPERACIONAL

1. PROPÓSITO GENERAL

El gerente de seguridad operacional es responsable ante el ejecutivo responsable de proporcionar una guía e instrucciones para la planificación, implementación y operación del sistema de gestión de la seguridad operacional (SMS) de la organización. El gerente de seguridad operacional proporciona servicios relacionados con el SMS a áreas de la organización certificadas, no certificadas y de terceros que se incluyen en el SMS y podría haber delegado responsabilidades en nombre de las personas que están en los cargos que requieren los reglamentos.

2. FUNCIONES CLAVE

Defensor de la seguridad operacional

- Demuestra una excelente conducta y actitud de seguridad operacional, sigue las prácticas y reglas reglamentarias, reconoce e informa los peligros y promueve la notificación eficaz de la seguridad operacional.

Líder

- Modela y promueve una cultura institucional que impulsa las prácticas de seguridad operacional mediante un liderazgo eficaz.

Comunicador

- Actúa como un conducto de información para llevar temas de seguridad operacional a la atención de la administración y para entregar información de seguridad operacional al personal, los contratistas o los accionistas de la organización.
- Proporciona y articula la información acerca de temas de seguridad operacional dentro de la organización.

Desarrollador

- Ayuda en la mejora continua de los diagramas de la evaluación de identificación de peligros y gestión de riesgos de seguridad operacional y el SMS de la organización.

Creador de relaciones

- Construye y mantiene una excelente relación de trabajo con el grupo de acción de seguridad operacional (SAG) de la organización y dentro de la oficina de servicios de seguridad operacional (SSO).

Embajador

- Representa a la organización ante comités industriales, gubernamentales y de organizaciones internacionales (por ejemplo, OACI, IATA, CAA, AIB, etc.).

Analista

- Analiza datos técnicos en busca de tendencias relacionadas con peligros, eventos y sucesos.

Gestión del proceso

- Usa eficazmente los procesos y procedimientos correspondientes para satisfacer las funciones y responsabilidades.
- Investiga las oportunidades de aumentar la eficiencia de los procesos.
- Mide la eficacia y busca mejorar continuamente la calidad de los procesos.

3. RESPONSABILIDADES

Entre otras tareas, el gerente de seguridad operacional es responsable de:

- gestionar la operación del sistema de gestión de seguridad operacional;
- recopilar y analizar la información de la seguridad operacional de forma oportuna;
- administrar cualquier estudio relacionado con la seguridad operacional;
- controlar y evaluar los resultados de las medidas correctivas;
- garantizar que las evaluaciones de riesgos se lleven a cabo cuando corresponda;
- controlar la industria en busca de preocupaciones de seguridad operacional que pudiesen afectar a la organización;
- participar en las respuestas ante emergencias reales o prácticas;
- participar en el desarrollo y actualización del plan y procedimientos de respuesta ante emergencias; y
- garantizar que la información relacionada con la seguridad operacional, como las metas y los objetivos institucionales, esté disponible para todo el personal mediante los procesos de comunicación establecidos.

4. NATURALEZA Y ALCANCE

El gerente de seguridad operacional debe interactuar con el personal de operaciones, los gerentes superiores y los líderes de departamento en toda la organización. El gerente de seguridad operacional también debe fomentar relaciones positivas con las autoridades, las agencias y los proveedores de servicios y productos reglamentarios fuera de la organización. Otros contactos se establecerán en niveles de trabajo, según sea necesario.

5. CALIFICACIONES

Para calificar como gerente de seguridad operacional, una persona debe tener:

- experiencia de tiempo completo en la seguridad operacional de la aviación, en capacidad de un investigador de seguridad operacional de la aviación, gerente de seguridad operacional/calidad o gerente de riesgos de la seguridad operacional;
- conocimientos sólidos de las operaciones, procedimientos y actividades de la organización;
- un amplio conocimiento técnico de aviación;
- un extenso conocimiento de los sistemas de gestión de la seguridad operacional (SMS) y haber completado la capacitación de SMS correspondiente;
- una comprensión de los principios y las técnicas de la gestión de riesgos para respaldar al SMS;
- experiencia en la implementación o gestión de un SMS;

- experiencia y calificaciones en la investigación de accidentes/incidentes de la aviación y factores humanos;
- experiencia y calificaciones en la realización de auditorías e inspecciones de seguridad operacional/ calidad;
- un conocimiento sólido de los marcos de trabajo reglamentarios de la aviación, incluidas las normas y métodos recomendados (SARPS) de la OACI y los reglamentos de aviación civil pertinentes;
- la capacidad de comunicarse en todos los niveles tanto dentro como fuera de la empresa;
- la capacidad de tener una postura firme, promover una “cultura justa e imparcial” y aun así fomentar una atmósfera abierta y no punitiva para la notificación;
- la capacidad y confianza de comunicarse directamente con el ejecutivo responsable como su asesor o confidente;
- habilidades de comunicación bien desarrolladas y habilidades interpersonales demostradas de alto orden, con la capacidad de vincularse con una variedad de personas y representantes institucionales, como aquellos de diferentes entornos culturales;
- alfabetización computacional y habilidades analíticas superiores.

6. AUTORIDAD

6.1 Acerca de los temas de seguridad operacional, el gerente de seguridad operacional tiene acceso directo con el ejecutivo responsable y la administración superior y de cargo medio correspondiente.

6.2 El gerente de seguridad operacional tiene autorización, según las instrucciones del ejecutivo responsable, de realizar auditorías de seguridad operacional, estudios e inspecciones de cualquier aspecto de la operación, de acuerdo con los procedimientos especificados en la documentación del sistema de gestión de seguridad operacional.

6.3 El gerente de seguridad operacional tiene autorización, según las instrucciones del ejecutivo responsable, de realizar investigaciones de los eventos de seguridad operacional internos, de acuerdo con los procedimientos especificados en la documentación del SMS de la organización.

6.4 El gerente de seguridad operacional no debe tener otros cargos ni responsabilidades que puedan entrar en conflicto o perjudicar su función como un gerente de seguridad operacional de SMS. Este debe ser un cargo administrativo superior que no sea inferior jerárquicamente o subordinado a las funciones de producción u operacionales de la organización.

ADJUNTO C

ORIENTACION PARA LA PLANIFICACION DE LA RESPUESTA ANTE EMERGENCIAS

1. Generalidades

1.1 Tal vez, dado que los accidentes de aviación son eventos raros, pocas organizaciones están preparadas cuando uno sucede. Muchas organizaciones no tienen planes eficaces implementados para gestionar eventos durante o después de una emergencia o crisis. La forma en que una organización lidia con las consecuencias de un accidente u otra emergencia puede depender de cuán bien controla las primeras horas o días después de un evento de seguridad operacional importante. Un plan de respuesta ante emergencias (ERP) describe por escrito lo que se debe hacer después de un accidente o una crisis de aviación y quién es responsable de cada medida.

1.2 Entre los diferentes explotadores, tal planificación de emergencia podría conocerse con diferentes términos, como plan de contingencia, plan de gestión de crisis, etc. En este Adjunto, el término genérico "plan de respuesta ante emergencias (ERP)" se usa para abordar los planes de contingencia pertinentes que se esperan de los explotadores, cuyos productos/servicios podrían tener un impacto en la seguridad operacional de la aviación.

1.3 Donde exista la posibilidad de que las operaciones o actividades de aviación de la organización estén comprometidas a causa de otras crisis o emergencias que se originan de fuentes externas, como emergencias de salud/pandémicas, estos casos también deben abordarse en este ERP de aviación, según corresponda. Por lo tanto, un ERP es básicamente un componente integral del procedimiento de gestión de riesgos de seguridad operacional de una organización para abordar todas las emergencias, las crisis o los eventos posibles relacionados con la seguridad operacional o la calidad con los cuales este producto o servicio pueda contribuir o asociarse.

1.4 El ERP debe abordar todos los escenarios posibles/probables y tener medidas o procesos de mitigación adecuados implementados para que la organización, sus clientes, el público o la industria en toda su extensión puedan tener un mejor nivel de aseguramiento de la seguridad operacional, así como también, la continuidad de servicio.

1.5 Una respuesta satisfactoria ante una emergencia comienza con la planificación eficaz. Un ERP representa la base de un enfoque sistemático para gestionar los asuntos de la organización durante las consecuencias de un evento no planificado importante, en el peor de los casos, un accidente importante.

1.6 El propósito de un plan de respuesta ante emergencias es garantizar:

a) la delegación de la autoridad de emergencia;

b) la asignación de responsabilidades de emergencia;

c) la documentación de procedimientos y procesos de emergencia;

d) la coordinación de esfuerzos de emergencia de forma interna y con partes externas;

e) la continuación segura de las operaciones fundamentales, mientras se gestiona la crisis;

f) la identificación proactiva de todos los posibles eventos/escenarios de emergencia y sus medidas de mitigación correspondientes, etc.

1.7 Para ser eficaz, un ERP debe:

a) ser adecuado según la envergadura, naturaleza y complejidad de la organización;

b) estar fácilmente accesible para todo el personal pertinente y otras organizaciones, donde corresponda;

c) incluir listas de verificación y procedimientos pertinentes a las situaciones de emergencia específicas;

d) tener detalles de contacto de referencia rápida de todo el personal pertinente;

e) probarse regularmente mediante ejercicios;

f) revisarse y actualizarse periódicamente cuando cambian los detalles, etc.

2. Contenido del ERP

2.1 Un ERP normalmente estaría documentado en el formato de un manual que debiera establecer las responsabilidades, las funciones y las medidas de las diversas agencias y el personal que participan abordando emergencias específicas. Un ERP debe considerar lo siguiente:

a) *Políticas gobernantes.* El ERP debe proporcionar las instrucciones para responder a emergencias, como leyes y reglamentos gobernantes para las investigaciones, acuerdos con autoridades locales, políticas empresariales y prioridades.

b) *Organización.* El ERP debe describir las intenciones de la gestión en relación con las organizaciones que dan respuesta al:

1) designar quién liderará y quién estará asignado a los equipos de respuesta;

2) definir las funciones y responsabilidades del personal asignado a los equipos de respuesta;

3) clarificar las líneas de notificación de la autoridad;

4) configurar un centro de gestión de emergencia (EMC);

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

6) designar al vocero empresarial para tratar con los medios;

7) definir qué recursos estarán disponibles, lo que incluye a las autoridades financieras para actividades inmediatas;

8) designar al representante de la empresa para cualquier investigación formal que lleven a cabo los funcionarios del Estado;

9) definir un plan de llamada para el personal clave.

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

c) *Notificaciones.* El plan debe especificar a quién, en la organización, se le notificará de una emergencia, quién realizará las notificaciones externas y mediante qué medios. Se deben considerar las necesidades de notificación de lo siguiente:

1) la gestión;

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

3) los servicios de respuesta ante emergencias locales (autoridades del aeródromo, bomberos, policía, ambulancia, instituciones médicas, etc.);

4) los familiares de las víctimas (un tema delicado que, en muchos Estados, está a cargo de la policía);

5) el personal de la empresa;

6) los medios de comunicación; y

7) el área legal, contabilidad, aseguradores, etc.

d) *Respuesta inicial.* Dependiendo de las circunstancias, un equipo de repuesta inicial puede despacharse al sitio del accidente o crisis para aumentar los recursos locales y supervisar

los intereses de la organización. Entre los factores que deben considerarse para dicho equipo se incluyen:

1) ¿Quién debe liderar el equipo de respuesta inicial?

2) ¿Quién debe incluirse en el equipo de respuesta inicial?

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

4) ¿Qué se necesitará en cuanto a equipo especial, ropa, documentación, transporte, hospedaje, etc.?

e) *Ayuda adicional.* Los empleados con una capacitación y experiencia adecuadas pueden proporcionar un respaldo útil durante la preparación, el ejercicio y la actualización del ERP de una organización. Su experiencia puede resultar útil en la planificación y ejecución de tales tareas como:

1) actuar como pasajeros o clientes en los ejercicios;

2) abordar a los supervivientes o partes externas;

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

f) *Centro de gestión de emergencia (EMC).* Un EMC (normalmente en modo de espera) puede establecerse en la sede de la organización luego de cumplir los criterios de activación. Además, se puede establecer un puesto de mando (CP) cerca o en el sitio de la crisis. El ERP debe abordar cómo se cumplirán los siguientes requisitos:

1) personal (tal vez por 24 horas al día, los 7 días de la semana, durante el período de respuesta inicial);

2) equipo de comunicaciones (teléfonos, fax, Internet, etc.);

3) requisitos de documentación, mantenimiento de los registros de actividad de emergencia;

4) incautar los registros empresariales relacionados;

5) muebles y suministros de oficina; y

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

El explotador puede contratar los servicios de un centro de crisis para que resguarde los intereses del proveedor de servicios ante una crisis lejos de la base de domicilio. Por lo general, el personal de la empresa complementaría dicho centro contratado lo antes posible.

g) *Registros.* Además de la necesidad de la organización de mantener registros de los eventos y las actividades, la organización también necesitará proporcionar información a cualquier equipo de investigación del Estado. El ERP debe abordar los siguientes tipos de información que requieran los investigadores:

1) todos los registros pertinentes acerca del producto o servicio de interés;

2) listas de puntos de contacto y cualquier personal asociado con el suceso;

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

4) cualquier evidencia fotográfica o de otro tipo.

h) *Sitio del accidente.* Para un accidente importante, los representantes de muchas jurisdicciones tienen motivos legítimos para acceder al sitio: por ejemplo, la policía; bomberos; médicos; autoridades del aeródromo; forenses (funcionarios encargados de examen médico) para abordar las fatalidades; investigadores de accidentes del Estado; agencias de ayuda como la Cruz Roja e incluso los medios de comunicación. Aunque la coordinación de las actividades de estos accionistas es la responsabilidad de la autoridad de investigación o la policía del

Estado, el explotador debe clarificar los siguientes aspectos de las actividades en el sitio del accidente:

1) nominar a un representante superior de la empresa en el sitio del accidente si:

— se está en la base de domicilio;

— se está lejos de la base de domicilio;

— se está en mar abierto o en un Estado extranjero;

2) gestión de las víctimas supervivientes;

3) las necesidades de los familiares de las víctimas;

4) la seguridad de los restos de la aeronave;

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

6) preservación de la evidencia;

7) disposición de ayuda (según sea necesario) a las autoridades de la investigación;

8) retiro y eliminación de los restos de la aeronave; etc.

i) *Medios de prensa.* La forma como responde la empresa a los medios de comunicación puede afectar cuán bien la empresa se recupera del evento. Se requiere una clara instrucción acerca de, por ejemplo:

1) qué información está protegida por un estatuto (datos de FDR, registros de CVR y ATC, declaraciones de testigos, etc.);

2) quién puede hablar en nombre de la organización matriz en la oficina principal y en el sitio del accidente (gerente de relaciones públicas, funcionario ejecutivo principal u otro ejecutivo superior, gerente, propietario);

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

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

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

6) disposiciones de actualizaciones regulares a los medios de comunicación.

j) *Investigaciones formales.* Se debe proporcionar una guía acerca del personal de la empresa que trata con los investigadores del accidente y la policía del Estado.

k) *Ayuda para la familia.* El ERP también debe incluir una guía sobre el enfoque de la organización para ayudar a las víctimas de las crisis o las organizaciones del cliente. Esta guía puede incluir factores como:

1) Requisitos del Estado para la disposición de servicios de ayuda;

2) arreglos de viajes y hospedaje para visitar el sitio de la crisis;

3) coordinador del programa y puntos de contacto para las víctimas/clientes;

4) disposición de información actualizada;

5) ayuda temporal a las víctimas y los clientes.

l) *Revisión posterior al suceso.* Se deben proporcionar instrucciones para garantizar que, después de una emergencia, el personal clave realice una sesión informativa completa y el registro de todas las lecciones significativas aprendidas, que pueden producir enmiendas al ERP y procedimientos asociados.

3. Listas de verificación

3.1 Todos los que participan en la respuesta inicial a un evento de aviación importante sufrirán de algún grado de desorientación. Por lo tanto, el proceso de respuesta ante emergencias se presta para el uso de las listas de verificación. Estas listas de verificación pueden formar una parte integral del manual de operaciones de la empresa o el manual de respuesta ante emergencias. Para ser eficaces, las listas de verificación deben regularmente:

a) revisarse y actualizarse (por ejemplo, la actualidad de las listas de llamada y los detalles de contacto); y

b) probarse mediante ejercicios realistas.

4. Capacitación y ejercicios

4.1 Un ERP es un indicio de intento en papel. Con suerte, gran parte del ERP no se probará nunca bajo condiciones reales. Se requiere de capacitación para garantizar que estas intenciones reciban el respaldo de capacidades operacionales. Dado que la capacitación tiene una corta “vida útil”, se recomienda llevar a cabo ensayos regulares y ejercicios. Algunas partes del ERP, como el plan de llamadas y comunicaciones, pueden probarse mediante ejercicios de "escritorio". Otros aspectos, como las actividades "en terreno" que implican a otras agencias, necesitan practicarse en intervalos regulares. Tales ejercicios tienen la ventaja de demostrar deficiencias en el plan, las que pueden rectificarse antes de una emergencia real. Para ciertos proveedores de servicios, como aeropuertos, puede que sea obligatorio usar pruebas periódicas de la idoneidad del plan y la conducta de un ejercicio de emergencia a escala completa.

ADJUNTO D

ORIENTACION PARA EL DESARROLLO DEL MANUAL DEL SMS DEL EXPLOTADOR

1. GENERALIDADES

1.1 Este apéndice sirve para guiar a las organizaciones en su compilación de un manual (o documento) de SMS para definir su marco de trabajo de SMS y sus elementos asociados. Puede ser un manual de SMS independiente o puede integrarse como una sección/capítulo del manual de operaciones (OM) del explotador. La configuración real puede depender de la expectativa reglamentaria.

1.2 Al usar el formato sugerido y los elementos del contenido en este apéndice y adaptarlos como corresponda, es una forma en que la organización puede desarrollar su propio manual de SMS. Los elementos del contenido real dependerán del marco de trabajo de SMS específico y los elementos de la organización según la naturaleza y la complejidad de las operaciones propuestas por el explotador. La descripción debajo de cada elemento será proporcional al alcance y la complejidad de los procesos de SMS de la organización.

1.3 El manual servirá para comunicar el marco de trabajo de SMS de la organización de forma interna, así como también, con las organizaciones externas pertinentes. El manual debe someterse para su aceptación por parte de la CAA como evidencia de la aceptación del SMS.

Nota.— Se debe hacer una distinción entre un manual de SMS y sus registros y documentos de respaldo operacional. El último hace referencia a registros y documentos históricos y actuales generados durante la implementación y operación de los diversos procesos del SMS. Estos constituyen evidencia documental de las actividades constantes de SMS de la organización.

2. FORMATO DEL MANUAL DE SMS

2.1 El manual de SMS puede asumir un formato de la siguiente manera:

a) encabezado de sección;

b) objetivo;

c) criterios;

d) documentos de referencia cruzada.

2.2 Debajo de cada “encabezado de sección” numerado se incluye una descripción del “objetivo” de esa sección, seguido de sus “criterios” y “documentos de referencia cruzada”. El “objetivo” es lo que intenta lograr la organización al hacer lo que se describe en esa sección. Los "criterios" definen el alcance de lo que se debe considerar al escribir esa sección. Los “documentos de referencia cruzada” vinculan la información con otros manuales pertinentes o SOP de la organización, los que contienen detalles del elemento o proceso, según corresponda.

3. CONTENIDO DEL MANUAL

3.1 Entre los contenidos del manual se pueden incluir las siguientes secciones:

1. Control de documentos;
2. Requisitos reglamentarios del SMS;
3. Alcance e integración del sistema de gestión de la seguridad operacional;
4. Política de seguridad operacional;

5. Objetivos de seguridad operacional;
6. Responsabilidades de la seguridad operacional y personal clave;
7. Notificación de seguridad operacional y medidas correctivas;
8. Identificación de peligros y evaluación de riesgos;
9. Control y medición del rendimiento en materia de seguridad operacional;
10. Investigaciones relacionadas con la seguridad operacional y medidas correctivas;
11. Capacitación y comunicación de seguridad operacional;
12. Mejora continua y auditoría de SMS;
13. Gestión de los registros de SMS;
14. Gestión de cambio; y
15. Plan de respuesta ante emergencias/contingencia.

3.2 A continuación se indica un ejemplo del tipo de información que puede incluirse en cada sección mediante el formato descrito en 2.2.

1. Control de documentos

Objetivo

Describir cómo los manuales se mantendrán actualizados y cómo garantizará la organización que el personal que participa en las tareas relacionadas con la seguridad operacional tenga la versión más actual.

Criterios

a) Copia impresa o medio electrónico controlado y lista de distribución.

b) La correlación entre el manual de SMS y otros manuales existentes, como el manual de control de mantenimiento (MCM) o el manual de operaciones.

c) El proceso de revisión periódica del manual y sus formularios/documentos relacionados para garantizar su sustentabilidad, suficiencia y eficacia constantes.

d) El proceso de administración, aprobación y aceptación reglamentaria del manual.

Documentos de referencia cruzada

Manual de la calidad, manual de ingeniería, etc.

2. Requisitos reglamentarios de SMS

Objetivo

Abordar los reglamentos de SMS y el material guía actuales para obtener una referencia necesaria y toma de conciencia de todos los interesados.

Criterios

a) Explicar en detalle los reglamentos/normas actuales de SMS. Incluir el marco de tiempo del cumplimiento y las referencias del material de asesoramiento, según corresponda.

b) Donde corresponda, elaborar o explicar la importancia y las implicaciones de los reglamentos para la organización.

c) Establecer una correlación con otros requisitos o normas relacionados con la seguridad operacional, donde corresponda.

Documentos de referencia cruzada

Referencias de reglamentos/requisitos de SMS, referencias de documentos de guía de SMS, etc.

3. Alcance e integración del sistema de gestión de la seguridad operacional

Objetivo

Describir el alcance y extensión de las operaciones e instalaciones relacionadas con la aviación de la organización, dentro de las cuales se aplicará el SMS. También se debe abordar el alcance de los procesos, los equipos y las operaciones consideradas idóneas para el programa de identificación de peligros y mitigación de riesgos (HIRM) de la organización.

Criterios

a) Explicar la naturaleza del negocio de aviación de la organización y su posición o función dentro de la industria como un todo.

b) Identificar las áreas, los departamentos, los talleres y las instalaciones principales de la organización, dentro de las cuales se aplicará el SMS.

c) Identificar los procesos, las operaciones y los equipos principales que se consideran idóneos para el programa HIRM de la organización, especialmente aquellos que son pertinentes para la seguridad operacional de la aviación. Si el alcance de los procesos, las operaciones y los equipos idóneos de HIRM es demasiado detallado o extenso, se puede controlar de acuerdo con un documento complementario, según corresponda.

d) Donde se espera que el SMS se opere o administre en un grupo de organizaciones o contratistas interconectados, defina y documente dicha integración y las responsabilidades asociadas, según corresponda.

e) Donde hayan otros sistemas de control/gestión relacionados dentro de la organización, como QMS, OSHE y SeMS, identifique su integración pertinente (donde corresponda) dentro del SMS de la aviación.

Documentos de referencia cruzada

Manual de la calidad, manual de ingeniería, etc.

4. Política de seguridad operacional

Objetivo

Describir las intenciones de la organización, sus principios de gestión y su compromiso con la mejora de la seguridad operacional de la aviación, en términos del proveedor servicios. Una política de seguridad operacional debe ser una descripción corta, parecida a una declaración de la misión.

Criterios

a) La política de seguridad operacional debe ser adecuada para la envergadura y complejidad de la organización.

b) La política de seguridad operacional señala las intenciones de la organización, sus principios de gestión y el compromiso con la mejora continua en la seguridad operacional de la aviación.

c) El ejecutivo responsable aprueba y firma la política de seguridad operacional.

d) El ejecutivo responsable y el resto de los gerentes promueven la política de seguridad operacional.

e) La política de seguridad operacional se revisa periódicamente.

f) El personal en todos los niveles participa en el establecimiento y mantenimiento del sistema de gestión de la seguridad operacional.

g) La política de seguridad operacional se comunica a todos los empleados con la intención de crear conciencia de sus obligaciones de seguridad operacional individuales.

Documentos de referencia cruzada

Política de seguridad operacional de OSHE, etc.

5. Objetivos de seguridad operacional

Objetivo

Describir los objetivos de seguridad operacional de la organización. Los objetivos de seguridad operacional deben ser una declaración corta que describa a grandes rasgos lo que espera lograr la organización.

Criterios

a) Se hayan establecido los objetivos de seguridad operacional.

b) Los objetivos de seguridad operacional se expresan como una declaración de nivel superior que describe el compromiso de la organización para lograr la seguridad operacional.

c) Existe un proceso formal para desarrollar un conjunto coherente de objetivos de seguridad operacional.

d) Los objetivos de seguridad operacional se difunden y distribuyen.

e) Se han asignado recursos para lograr los objetivos.

f) Los objetivos de seguridad operacional se vinculan con los indicadores de seguridad operacional para facilitar el control y la medición, como corresponda.

Documentos de referencia cruzada

Documento de indicadores de rendimiento en materia de seguridad operacional, etc.

6. Funciones y responsabilidades

Objetivo
Describir las autoridades y responsabilidades de la seguridad operacional para el personal que participa en el SMS.

Criterios

a) El ejecutivo responsable se encarga de garantizar que el sistema de gestión de la seguridad operacional se implemente correctamente y se desempeñe según los requisitos en todas las áreas de la organización.

b) Se asignó un gerente (oficina) de seguridad operacional correspondiente, un comité de seguridad operacional o grupos de acción de seguridad operacional, según corresponda.

c) Las autoridades y responsabilidades de seguridad operacional del personal en todos los niveles de la organización están definidos y documentados.

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

e) Se dispone de un diagrama de responsabilidades institucionales del SMS.

Documentos de referencia cruzada

Manual de exposición de la empresa, manual de SOP, manual de administración, etc.

7. Notificación de seguridad operacional

Objetivo

Un sistema de notificación debe incluir medidas reactivas (informes de accidentes/incidentes, etc.) y proactivas/predictivas (informes de peligros). Describir los sistemas de notificación respectivos. Entre los factores que se deben considerar se incluyen: el formato del informe, la confidencialidad, los destinatarios, los procedimientos de investigación/evaluación, las medidas correctivas/preventivas y la divulgación del informe.

Criterios

a) La organización tiene un procedimiento que proporciona la captura de sucesos internos, como accidentes, incidentes y otros sucesos pertinentes para el SMS.

b) Se debe hacer una distinción entre los informes obligatorios (accidentes, incidentes graves, defectos importantes, etc.) que se deben notificar a la CAA y otros informes de sucesos de rutina, que permanecen dentro de la organización.

c) También existe un sistema de notificación de peligros/sucesos voluntaria y confidencial, que incorpora la protección de identidad/datos adecuada, según corresponda.

d) Los procesos de notificación respectivos son simples, accesibles y proporcionales a la envergadura de la organización.

e) Los informes de alto impacto y las recomendaciones asociadas se abordan y revisan según el nivel de gestión correspondiente.

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

8. Identificación de peligros y evaluación de riesgos

Objetivo

Describir el sistema de identificación de peligros y cómo se recopilan tales datos. Describir el proceso para la categorización de peligros/riesgos y su posterior priorización para una evaluación de seguridad operacional documentada. Describir cómo se lleva a cabo el proceso de evaluación de seguridad operacional y cómo se implementan planes de acción preventiva.

Criterios

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

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

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

d) El proceso de evaluación de riesgos usa hojas de cálculo, formularios o software correspondientes a la complejidad de la organización y las operaciones involucradas.

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

f) Existe un proceso para evaluar la eficacia de las medidas correctivas, preventivas y de recuperación que se han desarrollado.

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

9. Control y medición del rendimiento en materia de seguridad operacional

Objetivo

Describir el componente de control y medición del rendimiento en materia de seguridad operacional del SMS. Esto incluye los indicadores de rendimiento en materia de seguridad operacional (SPI) del SMS de la organización.

Criterios

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

b) Correlación establecida entre los SPI y los objetivos de seguridad operacional de la organización, donde corresponda, y el proceso de aceptación reglamentaria de los SPI, donde sea necesario.

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

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

10. Investigaciones relacionadas con la seguridad operacional y las medidas correctivas

Objetivo

Describir cómo se investigan y procesan los accidentes/incidentes/sucesos dentro de la organización, incluida la correlación con el sistema de identificación de peligros y gestión de riesgos del SMS de la organización.

Criterios

a) Procedimientos para garantizar que se investiguen de forma interna los accidentes e incidentes notificados.

b) Divulgación interna de los informes de investigación completados al igual que a la CAA, según corresponda.

c) Un proceso para garantizar que se lleven a cabo las medidas correctivas tomadas o recomendadas y para evaluar sus resultados/eficacia.

d) Procedimiento sobre la consulta y las medidas disciplinarias asociadas con los resultados del informe de investigación.

e) Condiciones definidas claramente según las cuales se podrían considerar medidas disciplinarias punitivas (por ejemplo, actividad ilegal, imprudencia, negligencia grave o conducta impropia deliberada).

f) Un proceso para garantizar que las investigaciones incluyan la identificación de averías activas, así como también, factores y peligros que contribuyen.

g) El procedimiento y el formato de la investigación proporcionan hallazgos sobre factores o peligros contribuyentes que se procesarán para la medida de seguimiento con el sistema de identificación de peligros y gestión de riesgos de la organización, donde corresponda.

Documentos de referencia cruzada

11. Capacitación y comunicación de seguridad operacional

Objetivo

Describir el tipo de SMS y otra capacitación relacionada con la seguridad operacional que reciba el personal y el proceso para garantizar la eficacia de la capacitación. Describir cómo se documentan tales procedimientos de capacitación. Describir los procesos/canales de comunicación de seguridad operacional dentro de la organización.

Criterios

a) Se documenta el programa de capacitación, la idoneidad y los requisitos.

b) Existe un proceso de validación que mide la eficacia de la capacitación.

c) La capacitación incluye capacitación inicial, recurrente y de actualización, donde corresponda.

d) La capacitación de SMS de la organización es parte del programa de capacitación general de la organización.

e) Se incorpora la toma de conciencia de SMS en el programa de empleo o adoctrinamiento.

f) Los procesos/canales de comunicación de la seguridad operacional dentro de la organización.

12. Mejora continua y auditoría de SMS

Objetivo

Describir el proceso para la revisión y mejora continuas del SMS.

Criterios

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

b) Describir cualquier otro programa que contribuya con la mejora continua del SMS de la organización y el rendimiento en materia de seguridad operacional, por ejemplo, MEDA, estudios de seguridad operacional, sistemas ISO.

13. Gestión de los registros de SMS

Objetivo

Describir el método de almacenamiento de todos los registros y documentos relacionados con SMS.

Criterios

a) La organización tiene registros de SMS o un sistema de archivo que garantiza la conservación de todos los registros generados en conjunto con la implementación y operación del SMS.

b) Los registros que deben guardarse incluyen informes de peligros, informes de evaluación de riesgos, notas de grupos de acción de seguridad operacional/reuniones de seguridad operacional, diagramas de indicadores de rendimiento en materia de seguridad operacional, informes de auditoría del SMS y registros de la capacitación de SMS.

c) Los registros deben permitir que se rastreen todos los elementos del SMS y que estén accesibles para la administración de rutina del SMS, así como también, para propósitos de auditorías internas y externas.

14. Gestión de cambio

Objetivo

Describir el proceso de la organización para gestionar los cambios que pueden tener un impacto en los riesgos de la seguridad operacional y cómo tales procesos se integran con el SMS.

Criterios

a) Procedimientos para garantizar que los cambios institucionales y operacionales sustanciales consideran cualquier impacto que puedan tener en los riesgos existentes de la seguridad operacional.

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

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

Documentos de referencia cruzada

SOP de la empresa relacionado con la gestión de cambio, etc.

15. Plan de respuesta ante emergencias/contingencia

Objetivo

Describir las intenciones de la organización acerca de situaciones de emergencia y sus controles de recuperación correspondientes, además de su compromiso para abordar dichas situaciones.

Describir las funciones y responsabilidades del personal clave. El plan de respuesta ante emergencias puede ser un documento separado o puede ser parte del manual de SMS.

Criterios (como corresponda para la organización)

a) La organización tiene un plan de emergencia que describe las funciones y responsabilidades en caso de un incidente, una crisis o un accidente importante.

b) Existe un proceso de notificación que incluye una lista de llamadas de emergencia y un proceso de movilización interno.

c) La organización tiene disposiciones con otras agencias para recibir ayuda y la disposición de servicios de emergencia, según corresponda.

d) La organización tiene procedimientos para las operaciones del modo de emergencia, donde corresponda.

e) Existe un procedimiento para vigilar el bienestar de todas las personas afectadas y para notificar al familiar más cercano.

f) La organización ha establecido procedimientos para tratar con los medios de comunicación y temas relacionados con el seguro.

g) Existen responsabilidades de investigación de accidentes definidas dentro de la organización.

h) El requisito para preservar la evidencia, asegurar el área afectada y la notificación obligatoria/gubernamental está claramente declarada.

i) Existe una capacitación de preparación y respuesta ante emergencias para el personal afectado.

j) La organización desarrolló un plan de evacuación en caso de una aeronave o un equipo averiado con el asesoramiento de propietarios de aeronaves/equipos, explotadores de aeródromo u otras agencias, según corresponda.

k) Existe un procedimiento para registrar las actividades durante una respuesta ante emergencias.

Documentos de referencia cruzada

Manual de ERP, etc.

ADJUNTO E

SISTEMAS DE NOTIFICACION VOLUNTARIA Y CONFIDENCIAL

El sistema de notificación voluntaria y confidencial de una organización debe, como mínimo, definir:

a) el objetivo del sistema de notificación;

Ejemplo:

El objetivo clave del sistema de notificación voluntaria y confidencial de [Nombre de la organización] es mejorar la seguridad operacional de nuestras actividades de aviación de la empresa mediante la recopilación de informes sobre deficiencias reales y posibles de la seguridad operacional que, de lo contrario, no se informarían mediante otros canales.

Tales informes pueden implicar sucesos, peligros o amenazas pertinentes para la seguridad operacional de nuestras actividades de aviación. Este sistema no elimina la necesidad de la notificación formal de accidentes e incidentes, de acuerdo con los SOP de nuestra empresa, ni tampoco, el envío de los informes obligatorios de sucesos a las autoridades reglamentarias pertinentes.

El [Nombre del sistema] es un sistema de notificación de sucesos y peligros voluntario, no punitivo y confidencial que administra [Nombre del departamento/oficina]. Proporciona un canal para la notificación voluntaria de sucesos y peligros de aviación pertinentes para las actividades de seguridad operacional de nuestra organización, mientras protege la identidad del notificador.

Nota.— Al establecer dicho sistema, la organización tendrá que decidir si integra o segrega su sistema de notificación de seguridad, salud y ambiente en el trabajo (OSHE) del sistema de notificación de seguridad operacional de la aviación. Esto puede depender de las expectativas o los requisitos de las autoridades de OSHE y aviación respectivas. Donde exista un sistema de notificación de OSHE separado en la empresa, se debe destacar en conformidad en este párrafo para guiar al notificador, según sea necesario.

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

Ejemplo:

El [Nombre del sistema] aborda áreas como:

a) operaciones de vuelo;

b) mantenimiento de la aeronave en el hangar;

d) gestión de la flota técnica;

e) gestión técnica del inventario;

g) servicios técnicos;

h) registros técnicos;

i) mantenimiento de línea;

j) etc.

c) quien pueda hacer un informe voluntario;

Ejemplo:

Si pertenece a cualquiera de estas áreas o departamentos operacionales, puede contribuir con la mejora de la seguridad operacional de la aviación mediante [Nombre del sistema] al notificar los sucesos, los peligros o las amenazas pertinentes para las actividades de aviación de nuestra organización:

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

b) controladores de tránsito aéreo;

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

e) explotadores de servicios de escala del aeropuerto;

f) etc.

d) cuando se debe hacer dicho informe;

Ejemplo:

Debe hacer un informe cuando:

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

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

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

e) cómo se procesan los informes;

Ejemplo:

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

Cuando el gerente esté satisfecho con que la información obtenida es completa y coherente, omitirá la identidad de quien entrega la información e ingresará los datos en la base de datos del [Nombre del sistema]. En caso que se deba buscar aportes de cualquier tercero, solo se usarán datos no identificados. El formulario del [Nombre del sistema], con la fecha de retorno anotada, será devuelto finalmente al notificador. El gerente intentará completar el procesamiento dentro de diez (10) días hábiles si no se necesita información adicional. En los casos donde el gerente debe conversar con el notificador o consultar a un tercero, se necesitará más tiempo.

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

Distribución de información de seguridad operacional dentro de la empresa y la comunidad de la aviación

Se pueden compartir informes y extractos no identificados pertinentes dentro de la empresa, así como también, con accionistas de aviación externa, según se considere adecuado. Esto permitirá que todo el personal y los departamentos interesados dentro de la empresa, además de los accionistas de aviación externos, revisen sus propias operaciones y respalden la mejora de la seguridad operacional de la aviación como un todo.

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

f) comunicación con el gerente de [Nombre del sistema];

Ejemplo:

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

Administrador del [Nombre del sistema]

El Sr. ABC
Tel.:
Administrador suplente
El Sr. XYZ
Tel.:

ADJUNTO F

HOJA DE CÁLCULO PARA LA MITIGACION DE RIESGOS

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

Tabla 1 – Peligro y consecuencia

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

Tabla 2 – Índice de riesgo y tolerabilidad de la consecuencia

	Índice del riesgo y tolerabilidad ACTUAL (Teniendo en cuenta cualquier PC/RM/EC existente)				Índice del riesgo y tolerabilidad RESULTANTE (teniendo en cuenta cualquier PC/RM/EC nuevo)		
	Gravedad	Probabilidad	Tolerabilidad		Gravedad	Probabilidad	Tolerabilidad
Evento inseguro							
Consecuencia final							

Tabla 3 – Mitigación de riesgos

Peligro (H)	*Control preventivo (PC)*	*Factor de intensificación (EF)*	*Control de intensificación (EC)*		*Medida de recuperación (RM)*	*Factor de intensificación (EF)*	*Control de intensificación (EC)*	
H	PC1 (existente)	EF (Existente)	EC1 (Existente) EC2 (Nuevo)		RM1	EF (del RM1)	EC (del EF)	CONSECUENCIA FINAL (UC)
	PC2 (Existente)	EF1 (Nuevo) EF2 (Nuevo)	EC (Nuevo) EC (Nuevo)		RM2	EF (del RM2)	EC (del EF)	
	PC3 (Nuevo)	EF (Nuevo)	EC (Nuevo)		RM3	EF (del RM3)	EC (del EF)	

Notas explicativas. —

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

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

3. *Evento inseguro (UE).* Posible evento inseguro intermedio antes de cualquier consecuencia final, accidente o resultado más creíble. La identificación de un evento inseguro corresponde solo cuando existe la necesidad de distinguir y establecer medidas mitigadoras corriente arriba y corriente abajo de dicho evento intermedio (antes de la consecuencia final/accidente) (por ejemplo, “evento de sobretemperatura” antes de una “falla de motor”). Si este estado de UE

intermedio no corresponde para una operación en particular, entonces puede excluirse según corresponda.

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

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

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

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

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

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

TABLAS DE EJEMPLO DE GRAVEDAD, PROBABILIDAD, INDICE DE RIESGO Y TOLERABILIDAD

Tabla 4 – Tabla de gravedad (Básica)

Nivel	Descriptor	Descripción de la gravedad
1	Insignificante	Sin efecto con relación a la seguridad operacional
2	Leve	Efecto o degradación de las operaciones, rendimiento o procedimientos normales de la aeronave
3	Moderado	Pérdida parcial de un sistema significativo de la aeronave, o la aplicación de procedimientos de vuelo anormales
4	Grave	Falla completa de un sistema significativo de la aeronave, o la aplicación de procedimientos de emergencia
5	Catastrófico	Pérdida de vidas o destrucción de la aeronave

Tabla 5 – Tabla de gravedad (alternativa)

Nivel	Descriptor	Descripción de la gravedad					
		Estado de la aeronave	**Lesiones a personas**	**Daños a bienes**	**Pérdida potencial de ingresos**	**Daño al medio ambiente**	**Daño a la reputación corporativa**
1	Insignificante	Sin efecto con relación a la seguridad operacional	Sin lesiones	Sin daños	Sin pérdida de ganancias	Sin efectos	Sin implicancias
2	Menor	Efecto o degradación de las operaciones, rendimiento o procedimientos normales de la aeronave	Lesione leve	Daño leve menor que $:	Pérdida leve menor que $:	Efecto leve	Implicancia localizada y limitada
3	Moderado	Pérdida parcial de un sistema significativo de la aeronave, o la aplicación de procedimientos de vuelo anormales	Lesión grave	Daño sustancial menor que $:	Pérdida sustancial menor que $:	Efecto contenido	Implicancia regional
4	Grave	Falla completa de un sistema significativo de la aeronave, o la aplicación de procedimientos de emergencia	Un caso mortal	Daño importante menor que $:	Pérdida importante menor que $:	Efecto importante	Implicancia nacional
5	Catastrófico	Pérdida de vidas o destrucción de la aeronave	Varios casos mortales	Daño catastrófico mayor que $:	Pérdida masiva mayor que $:	Efecto masivo	Implicancia internacional

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

Tabla 6 – Tabla de probabilidad

Nivel	Descriptor	Descripción de la probabilidad
A	Seguro/frecuente	Se espera que ocurra en casi todas las circunstancias
B	Probable/ocasional	Probablemente ocurrirá en algún momento
C	Remoto/posible	Podría ocurrir en algún momento
D	Poco probable/improbable	Muy improbable que ocurra
E	Excepcional	Extremadamente improbable que ocurra. Sólo ocurrirá en circunstancias excepcionales

Tabla 7 – Matriz de riesgo (Gravedad x probabilidad)

Probabilidad	Severidad				
	1. Insignificante	2. Leve	3. Moderado	4. Grave	5. Catastrófico
A. Frecuente	Moderado (1A)	Moderado (2A)	Alto (3A)	Extremo (4A)	Extremo (5A)
B. Ocasional	Bajo (1B)	Moderado (2B)	Moderado (3B)	Alto (4B)	Extremo (5B)
C. Remoto	Bajo (1C)	Bajo (2C)	Moderado (3C)	Moderado (4C)	Alto (5C)
D. Improbable	Insignificante (1D)	Bajo (2D)	Bajo (3D)	Moderado (4D)	Moderado (5D)
E. Excepcional	Insignificante (1E)	Insignificante (2E)	Bajo (3E)	Bajo (4E)	Moderado (5E)

Tabla 8 – Tabla de aceptabilidad (tolerabilidad) de riesgos

Índice de riesgo	Tolerabilidad	Acciona requerida
5A, 5B, 4A	Riesgo extremo	PARAR LA OPERACIÓN O MITIGAR INMEDIATAMENTE. El riesgo es inaceptable bajo las circunstancias actuales. No permita ninguna operación hasta que se hayan implementado suficientes medidas de control para reducir los riesgos a un nivel aceptable. Se requiere la aprobación de la alta gerencia.
5C, 4B, 3A	Riesgo alto	PRECAUCION. Asegúrese que la evaluación del riesgo se ha completado satisfactoriamente y que se han aplicado controles preventivos. Se requiere la aprobación de la evaluación del riesgo por parte de la de la alta gerencia antes del inicio de las operaciones.
1A, 2A, 2B, 3B, 3C, 4C, 4D, 5D, 5E	Riesgo moderado	Si es necesario mitigue los riesgos o revise las medidas de mitigación existentes. El jefe o gerente de área debe aprobar la evaluación de riesgo.
1B, 1C, 2C, 2D, 3D, 3E, 4E	Riesgo bajo	La mitigación del riesgo es opcional.
1D, 1E, 2E	R. Insignificante	Aceptable tal cual. No necesita mitigación de riesgos.

EJEMPLO DE LLENADO DE LA HOJA DE CALCULO PARA LA MITIGACION DE RIESGOS (Tablas 1, 2 y 3)

Tabla 1 – Peligro y consecuencia

OPERACIÓN/PROCESO:	*Operación nocturna al aeropuerto XXXX*
PELIGRO (H):	*Luces PAPI pista 32 inoperativas*
EVENTO INSEGURO (UE):	*Aproximación no estabilizada*
CONSECUENCIA FINAL (UC):	*Salida de pista/Contacto anormal con la pista*

Tabla 2 – Índice de riesgo y tolerabilidad de la consecuencia

	Índice del riesgo y tolerabilidad ACTUAL (Teniendo en cuenta cualquier PC/RM/EC existente)				*Índice del riesgo y tolerabilidad RESULTANTE (teniendo en cuenta cualquier PC/RM/EC nuevo)*		
	Gravedad	Probabilidad	Tolerabilidad		Gravedad	Probabilidad	Tolerabilidad
Evento inseguro	*Moderado (3)*	*Remoto (C)*	*Riesgo moderado (3C)*		*Moderado (3)*	*Improbable (D)*	*Riesgo bajo (3D)*
Consecuencia final	*Catastrófico (5)*	*Remoto (C)*	*Riesgo alto (5C)*		*Catastrófico (5)*	*Improbable (D)*	*Riesgo moderado (5D)*

Tabla 3 – Mitigación de riesgos

Peligro (H)	Control preventivo (PC)	Factor de intensificación (EF)	Control de intensificación (EC)		Medida de recuperación (RM)	Factor de intensificación (EF)	Control de intensificación (EC)	
Luces PAPI pista 32 inoperativas	*SOP sobre aproximaciones estabilizadas*	*Incumplimiento de los SOP*	*Inspecciones en línea*		*SOP sobre aproximaciones estabilizadas*	*Incumplimiento de los SOP*	*FOQA*	*Salida de pista/Contacto anormal con la pista*
			FOQA					
	Restricción de operación al sólo PIC (Nuevo)	*Incumplimiento de la restricción*	*FOQA*		*Instrucción CRM*	*Incumplimiento de las políticas CRM*	*Inspecciones en línea*	
		Pista corta	.					
	Incremento de los mínimos meteorológicos (Nuevo)		.					

ADJUNTO G

INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DEL SMS

1. Las **Tablas 1** (ejemplos de indicadores de seguridad operacional) proporciona ejemplos ilustrativos de los indicadores de rendimiento en materia de seguridad operacional (SPI) colectivos del Estado y sus criterios de configuración de alertas y objetivos correspondientes. Los SPI del SMS se reflejan en el lado derecho de las tablas. Los criterios del nivel de alerta y objetivos correspondientes para cada indicador se deben explicar como se muestra. Los indicadores de rendimiento en materia de seguridad operacional del SSP a la izquierda de las tablas aparecen para indicar la correlación necesaria entre los indicadores de seguridad operacional de SMS y SSP. Los proveedores de productos y servicios deben desarrollar los SPI del SMS con el asesoramiento de sus organizaciones reglamentarias estatales respectivas. Sus SPI propuestos deberán ser coherentes con los indicadores de seguridad operacional de SSP del Estado; por lo tanto, se debe obtener un acuerdo/aceptación necesario. Adicionalmente, la **Tabla 5** proporciona una amplia lista de ejemplos de insdicadores de seguridad operacional (SPI), los mismos que pueden ser utilizados como tal, o personalizados de acuerdo a las necesidades de cada proveedor de servicios.

2. La **Tabla 2** (ejemplo de un diagrama del indicador de rendimiento en materia de seguridad operacional del SMS) es un ejemplo de cómo luce un diagrama del indicador de rendimiento en materia de seguridad operacional del SMS de alto impacto. En este caso, es la tasa de incidentes que pueden notificarse/obligatorios del explotador de una línea aérea. El diagrama de la izquierda es el rendimiento del año anterior, mientras que el diagrama de la derecha representa las actualizaciones de datos constantes del año actual. La configuración del nivel de alerta se basa en criterios de desviación estándar de la métrica de seguridad operacional básica. La fórmula de la hoja de cálculo Excel es “=STDEVP”. Para propósitos del cálculo de desviación estándar manual, la fórmula es:

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

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

3. La configuración de objetivos es una mejora porcentual deseada (en este caso el 5%) en el promedio del punto de datos del año anterior. Este diagrama se genera con la hoja de datos de la Tabla 6.

4. La hoja de datos en la Tabla 6 se usa para generar el diagrama del indicador de rendimiento en materia de seguridad operacional que aparece en la **Tabla 5-A6-5**. Lo mismo puede usarse para generar cualquier otro indicador de rendimiento en materia de seguridad operacional con la entrada de datos adecuada y la enmienda del descriptor del indicador de rendimiento en materia de seguridad operacional.

5. La **Tabla 7** (ejemplo del resumen de rendimiento de un SMS) proporciona un resumen de todos los indicadores de seguridad operacional del SMS de los explotadores, con sus resultados del nivel de alertas y objetivos respectivos anotados. Tal resumen podrá compilarse al final de cada período de control para proporcionar una descripción general del rendimiento del SMS. Si se desea una medición del resumen del rendimiento más cuantitativa, se pueden asignar puntos adecuados para cada resultado Sí/No para cada resultado de objetivos y alertas. Ejemplo:

Indicadores de alto impacto:

Nivel de alerta no violado (Si=4, No=0)

Objetivo alcanzado
(Si=3, No=0)

Indicadores de bajo impacto:

Nivel de alerta no violado (Si=2, No=0)

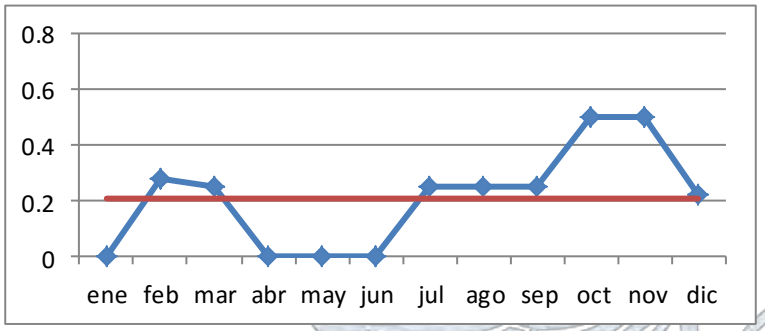
Objetivos alcanzada
(Si=1, No=0)

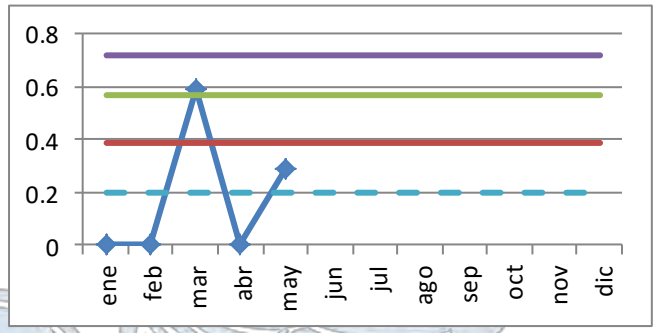
Gracias a esto se puede obtener una puntuación (o porcentaje) de resumen para indicar el rendimiento en materia de seguridad operacional general del SMS al final de cualquier período de control determinado.

Tabla 1 – Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores aéreos

Indicadores de seguridad operacional del SSP (Estado)						Indicadores de rendimiento en materia de seguridad operacional del SMS (Explotador)					
Indicadores de alto impacto (basado en sucesos//resultados)			Indicadores de bajo impacto (basados en eventos/Actividad)			Indicadores de alto impacto (basados en sucesos/Resultados)			Indicadores de bajo impacto (basados en Eventos/Actividad)		
Indicador de seguridad operacional	Criterios del Nivel de alerta	Criterios del nivel de Objetivos	Indicador de seguridad operacional	Criterios del Nivel de alerta	Criterios del nivel de Objetivos	Indicador de rendimiento en materia de seguridad operacional	Criterios del Nivel de alerta	Criterios del nivel de objetivos	Indicador de rendimiento en materia de seguridad operacional	Criterios del nivel de alerta	Criterios del nivel de objetivos
Tasa mensual de accidentes / incidentes graves de todos los explotadores (ej: por/1000HV)	Promedio + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de resultados de la vigilancia anual LEI% o tasa de hallazgos (hallazgos por auditoría)	Por definir	Por definir	Tasa mensual de incidentes graves por flota (ej: por/1000HV)	Promedio + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa mensual de incidentes combinada de todas las flotas (ej: por/1000HV)	Promedio + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.
Tasa trimestral de incidentes relacionados con paradas de motor en vuelo (engine IFSD) (Ej: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de resultados de la inspección anual de estación LEI% o tasa de hallazgos (hallazgos por auditoría)	Por definir	Por definir	Tasa mensual de incidentes graves combinada de todas las flotas (ej: por/1000HV)	Promedio + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de hallazgos o LEI% de la auditoría interna anual de SMS/QMS (ej: hallazgos por auditoría)	Por definir	Por definir
			Inspecciones anuales en rampa a explotadores extranjeros. Promedio LEI% (Para cada operador extranjero)	Por definir	Por definir	Tasa de incidentes de paradas de motor en vuelo (IFSD) (ej: por/1000HV)	Promedio + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de informes voluntarios de peligros del explotador (ej: por/1000HV)	Por definir	Por definir
			Tasa de informes sobre incidentes con mercancías peligrosas (ej: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.				Tasa de informes de incidentes con mercancías peligrosas (ej: por/1000HV)	Promedio + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.
ETC.											

Tabla 2 – Ejemplos de indicadores de rendimiento en materia de seguridad operacional

<table>
<tr>
<td> 

Tasa de incidentes notificables mensualmente de la línea ABC del año anterior (cada 1000 FH)
Promedio del año anterior</td>
<td> 

Tasa de incidentes notificables mensualmente de la línea aérea ABC del año actual (cada 1 000 FH)
Promedio del objetivo del año actual</td>
</tr>
<tr>
<td>a) Ajuste del nivel de alerta:

El nivel de alerta de un nuevo período de control (año actual) se basa en la 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.</td>
<td>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.</td>
</tr>
<tr>
<td>b) Activador 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.</td>
<td>d) Logro de los objetivos

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 objetivos: 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.</td>
</tr>
</table>

Tabla 3 – Ejemplo de indicador de alto nivel de la eficacia de la seguridad operacional (Con el criterio de ajuste de objetivos y alertas)

Año anterior				
Mes	Aerolínea ABC Total HV	Número de incidentes MOR reportables	Tasa de inc.*	Ave
Ene	3,992	-	0.00	0.21
Feb	3,727	1.00	0.27	0.21
Mar	3,900	1.00	0.26	0.21
Abr	3,870	-	0.00	0.21
May	3,976	-	0.00	0.21
Jun	3,809	-	0.00	0.21
Jul	3,870	1.00	0.26	0.21
Ago	3,904	1.00	0.26	0.21
Sep	3,864	1.00	0.26	0.21
Oct	3,973	2.00	0.50	0.21
Nov	3,955	2.00	0.51	0.21
Dic	3,369	1.00	0.23	0.21
		Ave	**0.21**	
		SD	**0.18**	

*Cálculo de la tasa (por 1000 HV)

Ave+1SD	Ave+2SD	Ave+3SD
0.39	0.57	0.76

*El criterio para el ajuste del **nivel de alerta del año actual**, está basado en (Ave+1/2/3 SD) del año anterior.*

Presente año							
Mes	Aerolínea ABC Total HV	Número de incidentes MOR reportables	Tasa de inc.*	Ave+1SD Año anterior	Ave+2SD Año anterior	Ave+3SD Año anterior	Objetivo promedio año actual
Dic	3,396	1.00	0.23	0.39	0.57	0.76	0.21
Ene	4,090	0.00	0.00	0.39	0.57	0.76	0.20
Feb	3,316	0.00	0.00	0.39	0.57	0.76	0.20
Mar	3,482	2.00	0.57	0.39	0.57	0.76	0.20
Abr	3,549	0.00	0.00	0.39	0.57	0.76	0.20
May	3,633	1.00	0.28	0.39	0.57	0.76	0.20
Jun				0.39	0.57	0.76	0.20
Jul				0.39	0.57	0.76	0.20
Ago				0.39	0.57	0.76	0.20
Sep				0.39	0.57	0.76	0.20
Oct				0.39	0.57	0.76	0.20
Nov				0.39	0.57	0.76	0.20
Dic				0.39	0.57	0.76	0.20
	Promedio						
	SD						

*Cálculo de la tasa (por 1000 HV)

El objetivo del presente año** es de mejora en el promedio (Ave) de 5% con relación al año anterior, lo que corresponde a: **0.20

INTENCIONALMENTE EN BLANCO

Tabla 4 – Ejemplo de la medición de rendimiento en materia de seguridad operacional del SMS de la línea aérea Alfa (digamos, para el año 2010)

Indicador de rendimiento en materia de seguridad operacional de alto impacto					
Descripción del indicador (SPI)		Criterio/Nivel de alerta del SPI (Para 2010)	Nivel de alerta violado? (Si/No)	Criterios del nivel de objetivos del SPI (para 2010)	Objetivo alcanzado (Si/no)
1	Tasa de incidentes graves mensual de la flota A320 de la línea aérea Alfa (por ejemplo, cada 1 000 FH)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)	Si	5% de mejora en la tasa promedio con relación al año anterior	No
2	Tasa de incidentes de IFSD de la flota A320 de la línea aérea Alfa (por ejemplo, cada 1 000 FH)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)	Si	3% de mejora en la tasa promedio con relación al año anterior	Si
3	Etc.				

Indicador de rendimiento en materia de seguridad operacional de bajo impacto					
Descripción del indicador (S.I.)		Criterio/Nivel de alerta del S.I.	Nivel de alerta superado? (Si/No)	Criterio/Objetivo S.I.	Objetivo alcanzado /Si/no)
1	Tasa combinada de incidentes de todas las flotas (por/1000 HV)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)	Si	5% de mejora en la tasa promedio con relación al año anterior	No
2	LEI% o tasa de hallazgos de la auditoría interna anual QMS (hallazgos por auditoría)	>25% LEI promedio; O cualquier hallazgo de nivel 1; O >5 hallazgos de nivel 2 por auditoría	Si	5% de mejora en la tasa promedio con relación al año anterior	Si
3	Tasa de informes voluntarios de peligros (ej: por/1000 HV)	TBD		TBD	
4	Tasa de incidentes con mercancías peligrosas (ej: por/1000 HV)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)		5% de mejora en la tasa promedio con relación al año anterior	Si
5	ETC				

Tabla 4 – Ejemplos de la indicadores de rendimiento de seguridad operacional (SPI) de alto y bajo impacto para proveedores de servicios aéreos

Ejemplos de la indicadores de rendimiento de seguridad operacional (SPI) de alto y bajo impacto para proveedores de servicios aéreos	
Indicador	**Nivel de impacto**
Número de salidas de pista por cada 1000 aterrizajes	Alto
Número de incidentes grave por flota de aeronaves por cada 1000 horas de vuelo	Alto
Número de cortes de motor en vuelo (IFSD) por flota de aeronaves por cada 1000 horas de vuelo	Alto
Incendio o humo producido en la cabina de pasajeros, en los compartimientos de carga o en los motores, aun cuando tales incendios se hayan apagado mediante agentes extintores por cada 10000 horas de vuelo	Alto
Número de TCAS RA por cada 1000 horas de vuelo	Alto
Número de avisos GPWS y EGPWS por cada 1000 horas de vuelo	Alto
Número de aterrizajes con menos combustible que el mínimo reglamentario requerido por cada 1000 aterrizajes	Alto
Número de errores de cálculo de combustible por cada 1000 vuelos	Alto
Cantidad de combustible que obligue al piloto a declarar una situación de emergencia por cada 1000 vuelos	Alto
Sucesos que obliguen a la tripulación de vuelo a utilizar el oxígeno de emergencia por cada 1000 vuelos	Alto
Despegues abortados por cada 1000 despegues debido a problemas técnicos	Alto
Número de incidentes en que requirieron asistencia en tierra por cada 1000 vuelos	Alto
Número de retornos en vuelo (IFTB) por cada 1000 despegues	Alto
Número de contactos anormales con la pista, fuera de la pista o fuera de las áreas de la pista disignadas para el aterrizaje por cada 1000 aterrizajes	Alto
Incursiones en pista por 1.000 operaciones	Alto
Mal funcionamiento de uno o más sistemas de la aeronave que afecten gravemente el funcionamiento de ésta por cada 1000 vuelos	Alto
Incapacitación de un tripulante de vuelo por cada 1000 vuelos	Alto
Cuasi colisiones que requieren una maniobra evasiva para evitar la collision por cada 1000 horas de vuelo	Alto
Impacto con aves en vuelo por cada 1000 horas de vuelo	Alto
Despegues efectuados desde una pista cerrada o comprometida con una separación apenas suficiente respecto a los obstáculos por cada 1000 despegues	Alto
Excursiones del nivel de vuelo asignado por cada 1000 vuelos	Alto
Descenso por debajo de la DA o MDA por cada 1000 aterrizajes	Alto

Eventos relacionados con actitudes inusuales de vuelo por cada 1000 vuelos	Alto
Accidentes o incidentes de pérdida de control en tierra por cada 1000 operaciones	Alto
Número de activaciones del “Stick shacker” u otros sistemas equivalents de protección al vuelo por cada 1000 horas de vuelo	Alto
Incapacidad grave de lograr los desempeños previstos durante el recorrido de despegue o el ascenso inicial por cada 1000 despegues	Alto
Número de casos en los que la preparación del vuelo tuvo que hacerse en menos tiempo del normalmente asignado por cada 1000 vuelos	Bajo
Tiempo de espera promedio para completar las acciones correctivas de no conformidades detectadas durante inspecciones por cada año	Bajo
Número de extensiones de los períodos de servicio del vuelo por cada trimestre	Bajo
Número de incumplimientos significativos descubiertos a través de las auditorías externas	Bajo
Número de reuniones de gestión dedicadas a la seguridad operacional al año	Bajo
Número de casos en que los supervisores expresaron feedback positivo sobre el comportamiento consciente en materia de seguridad operacional de su personal al año	Bajo
Número de nuevos peligros identificados a través del sistema de notificación interno al año	Bajo
Número de notificaciones voluntarias recibidas al trimestre	Bajo
Frecuencia con la que se determina el rendimiento en materia de seguridad operacional de los contratistas	Bajo
Número de cambios organizativos para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al año	Bajo
Número de cambios en los Procedimientos Operativos Estándar (SOPs) para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al año	Bajo
Porcentaje de la plantilla para la que se ha establecido un perfil de competencias	Bajo
Número de notificaciones de seguridad operacional recibidas de los contratistas por año	Bajo
Número de simulacros de emergencia por año	Bajo
Número de cursos de formación en ERP por año	Bajo
Porcentaje de personal formado en el ERP en el año	Bajo
Número de reuniones con los socios principales y contratistas para coordinar el ERP al año	Bajo
Número de comunicaciones de seguridad operacional publicadas por año	Bajo
Número de sesiones informativas (o briefings) de seguridad operacional realizadas por año	Bajo
Porcentaje de los contratistas integrados en el sistema de notificación de seguridad operacional de la empresa	Bajo
Porcentaje de los contratistas para las cuales se ha impartido formación en seguridad operacional	Bajo
Porcentaje de los contratistas cuyo rendimiento en materia de seguridad operacional se ha	Bajo

evaluado al año	
Porcentaje de personal que ha tenido formación en gestión de la seguridad	Bajo
Número de cambios realizados en los programas de instrución a raíz de la retroalimentación del personal o de los resultados del programa de instrucción al año	Bajo
Número de retrasos superiores a 15 minutos, debido a problemas técnicos por cada 1000 despegues	Bajo
Número de cancelaciones por cada 100 vuelos programados debido a problemas técnicos	Bajo
Número de diferidos por flota de aeronaves por cada trimestre	Bajo
Número de errores de cálculo de peso y balance por cada trimestre	Bajo
Número de aproximaciones estabilizadas por cada 1000 aterrizajes	Bajo

ADJUNTO H

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

1. LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHAS INICIAL (TABLA 5-A7-1)

1.1 La lista de verificación del análisis de brechas inicial en la Tabla 5-A7-1 puede usarse como una plantilla para realizar el primer paso de un análisis de brechas del SMS. Este formato con sus respuestas generales “Sí/No/Parcial” proporcionará una indicación inicial del amplio alcance de las brechas y, por lo tanto, la carga de trabajo general que puede esperarse. El cuestionario puede ajustarse para adaptarse a las necesidades de la organización y a la naturaleza del producto o servicio suministrado. Esta información inicial debe ser útil para que la administración superior anticipe la escala del esfuerzo de implementación del SMS y, por lo tanto, los recursos que se proporcionarán. Esta lista de verificación inicial necesitaría de seguimiento con un plan de implementación adecuado, según las Tablas 5-A7-2 y 5-A7-3.

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

No.	*Aspecto a ser analizado o pregunta por responder*	*Respuesta*	*Estado de implantación*
Componente 1 – POLÍTICA DE SEGURIDAD Y OBJETIVOS			
Elemento 1.1 – Responsabilidad y compromiso de la dirección			
1	¿Está implementada una política de seguridad operacional?	Si No Parcial	
2	¿Refleja la política de seguridad operacional el compromiso de la administración superior acerca de la gestión de la seguridad operacional?	Si No Parcial	
3	¿Es adecuada la política de seguridad operacional según la envergadura, naturaleza y complejidad de la organización?	Si No Parcial	
4	¿Es pertinente la política de seguridad operacional para la seguridad operacional de la aviación?	Si No Parcial	
5	¿Ha firmado el ejecutivo responsable la política de seguridad operacional?	Si No Parcial	
6	¿Se comunica la política de seguridad operacional, con un respaldo visible, en toda la Organización]?	Si No Parcial	
7	¿Se revisa periódicamente la política de seguridad operacional para garantizar que siga siendo pertinente y adecuada para la [Organización]?	Si No Parcial	
Elemento 1.2 – Obligación de rendición de cuentas sobre la seguridad operacional			
1	¿Ha identificado [Organización] a un ejecutivo responsable que, sin importar otras funciones, tenga la máxima responsabilidad, en nombre de [Organización], de la implementación y mantenimiento del SMS?	Si No Parcial	
2	¿Tiene el ejecutivo responsable total control de los recursos financieros y humanos necesarios para las operaciones autorizadas que se realizarán según el certificado de operaciones?	Si No Parcial	

No.	Aspecto a ser analizado o pregunta por responder	Respuesta	Estado de implantación
3	¿Tiene el ejecutivo responsable la autoridad final sobre todas las actividades de aviación de su organización?	Si No Parcial	
4	¿Ha identificado y documentado [Organización] las responsabilidades de seguridad operacional de la gestión, así como también, del personal de operaciones, en relación con el SMS?	Si No Parcial	
5	¿Existe un comité de seguridad operacional o consejo de revisión para el propósito de revisión del SMS y el rendimiento en materia de seguridad operacional?	Si No Parcial	
6	¿Lidera al comité de seguridad operacional un ejecutivo responsable o un delegado asignado correctamente, confirmado debidamente en el manual del SMS?	Si No Parcial	
7	¿Incluye el comité de seguridad operacional a líderes de departamento u operacionales pertinentes, según corresponda?	Si No Parcial	
8	¿Existen grupos de acción de seguridad operacional que trabajan junto con el comité de seguridad operacional (en particular para las organizaciones grandes/complejas)?	Si No Parcial	
Elemento 1.3 – Designación del personal clave de seguridad operacional			
1	¿Ha asignado [Organización] a una persona calificada para gestionar y vigilar la operación diaria del SMS?	Si No Parcial	
2	¿Tiene la persona calificada acceso o notificación directa al ejecutivo responsable, acerca de la implementación y operación del SMS?	Si No Parcial	
3	¿Tiene el gerente responsable de administrar el SMS otra responsabilidad más que pueda entrar en conflicto o perjudicar su papel como gerente de SMS?	Si No Parcial	
4	¿Es el puesto de gerente de SMS un puesto administrativo superior que no es inferior jerárquicamente o subordinado a otros puestos operacionales o de producción?	Si No Parcial	
Elemento 1.4 – Coordinación de la planificación de respuesta ante emergencias			
1	¿Tiene [Organización] un plan de respuesta ante Emergencias/contingencia adecuado para la envergadura, naturaleza y complejidad de la organización?	Si No Parcial	
2	¿Aborda el plan de emergencia/contingencia todos los escenarios de emergencia/crisis posibles o probables, en relación con los suministros de productos o servicios de aviación de la organización?	Si No Parcial	
3	¿Incluye el ERP procedimientos para la producción, la entrega y el respaldo seguros y continuos de los productos o servicios de la aviación durante tales emergencias o contingencias?	Si No Parcial	
4	¿Existe un plan y registro para los ensayos o ejercicios en relación con el ERP?	Si No Parcial	
5	¿Aborda el ERP la coordinación necesaria de sus procedimientos de respuesta ante emergencias/contingencia con los procedimientos de contingencia de emergencia/respuesta de otras organizaciones, donde corresponda?	Si No Parcial	
6	¿Tiene [Organización] un proceso para distribuir y comunicar el ERP a todo el personal pertinente, incluidas las organizaciones externas pertinentes?	Si No Parcial	
7	¿Existe un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continuas?	Si No Parcial	
Elemento 1.5 – Documentación SMS			
1	¿Existe un resumen de SMS de nivel superior o documento de exposición que esté aprobado por el gerente responsable y aceptado por la CAA?	Si No Parcial	
2	¿Aborda la documentación del SMS el SMS de la organización y sus componentes y elementos asociados?	Si No Parcial	

No.	*Aspecto a ser analizado o pregunta por responder*	*Respuesta*	*Estado de implantación*
3	¿Está el marco de trabajo de SMS de [Organización] en alineación con el marco de trabajo del SMS reglamentario?	Si No Parcial	
4	¿Mantiene [Organización] un registro de documentación de respaldo pertinente para la implementación y operación del SMS?	Si No Parcial	
5	¿Tiene [Organización] un plan de implementación de SMS para establecer su proceso de implementación de SMS, incluidas las tareas específicas y sus hitos de implementación pertinentes?	Si No Parcial	
6	¿Aborda el plan de implementación de SMS la coordinación entre el SMS del proveedor de servicios y el SMS de las organizaciones externas, donde corresponde?	Si No Parcial	
7	¿Respalda el ejecutivo responsable el plan de implementación de SMS?	Si No Parcial	
Componente 2 – GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL			
Elemento 2.1 – Identificación de peligros			
1	¿Existe un proceso para la notificación de peligros/amenazas voluntaria de todos los empleados?	Si No Parcial	
2	¿Es simple la notificación de peligros/amenazas voluntaria, está disponible a todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios?	Si No Parcial	
3	¿Incluye el SDCPS de [Organización] procedimientos para la notificación de incidentes/accidentes mediante personal operacional o producción?	Si No Parcial	
4	¿Es simple la notificación de incidentes/accidentes, es accesible para todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios?	Si No Parcial	
5	¿Tiene [Organización] procedimientos para la investigación de todos los incidentes/accidentes notificados?	Si No Parcial	
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	
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	
Elemento 2.2 – Evaluación y mitigación de riesgos de seguridad operacional			
1	¿Existe un procedimiento de identificación de peligros y mitigación de riesgos (HIRM) documentado que implique el uso de herramientas de análisis de riesgos objetivas?	Si No Parcial	
2	¿Aprobaron los gerentes de departamento o un nivel superior los informes de evaluación de riesgos, donde corresponda?	Si No Parcial	
3	¿Existe un procedimiento para la revisión periódica de los registros de mitigación de riesgos existentes?	Si No Parcial	
4	¿Existe un procedimiento para explicar las medidas de mitigación cada vez que se identifican niveles de riesgos inaceptables?	Si No Parcial	
5	¿Existe un procedimiento para priorizar los peligros identificados para las medidas de mitigación de riesgos?	Si No Parcial	
6	¿Existe un programa para la revisión sistemática y progresiva de todas las operaciones, los procesos, las instalaciones y los equipos relacionados con la seguridad operacional de la aviación sujetos al proceso de HIRM, como lo identificó la organización?	Si No Parcial	

No.	Aspecto a ser analizado o pregunta por responder	Respuesta	Estado de implantación
Componente 3 – ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL			
Elemento 3.1 – Observación y medición del rendimiento en materia de seguridad			
1	¿Existen indicadores de rendimiento en materia de seguridad operacional identificados para medir y controlar el rendimiento en materia de seguridad operacional de las actividades de aviación de la organización?	Si No Parcial	
2	¿Son los indicadores de rendimiento en materia de seguridad operacional relevantes con la política de seguridad operacional así como con los objetivos y metas de seguridad asumidos por el ejecutivo responsable?	Si No Parcial	
3	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional alertas y objetivos de seguridad operacional que definan las regiones de rendimiento inaceptable y las metas de mejora establecidas?	Si No Parcial	
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	
5	Incluyen los indicadores de rendimiento en materia de seguridad operacional un control cuantitativo de resultados de seguridad operacional de alto impacto (por ejemplos, tasas de incidentes de accidentes e incidentes graves), así como también, eventos de bajo impacto (por ejemplo, tasa de no cumplimiento, desviaciones)?	Si No Parcial	
6	¿Están los indicadores de rendimiento en materia de seguridad operacional y su configuración de rendimiento asociada desarrollados en función del acuerdo de la autoridad de aviación civil y sujetos a este?	Si No Parcial	
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	
8	¿Se revisan periódicamente los indicadores de rendimiento en materia de seguridad operacional?	Si No Parcial	
Elemento 3.2 – La gestión del cambio			
1	¿Existe un procedimiento para la revisión de instalaciones y equipos existentes relacionados con la seguridad operacional de la aviación (incluidos los registros de HIRM) cada vez que haya cambios pertinentes a aquellas instalaciones y equipos?	Si No Parcial	
2	Existe un procedimiento para revisar las operaciones y los procesos existentes relacionados con la seguridad operacional de la aviación pertinente (como cualquier registro de HIRM) cada vez que haya cambios a aquellas operaciones o procesos?	Si No Parcial	
3	¿Existe un procedimiento para revisar las nuevas operaciones y los procesos relacionados con la seguridad operacional de la aviación en busca de peligros/riesgos antes de implementarlos?	Si No Parcial	
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	
Elemento 3.3 – Mejora continua del SMS			
1	¿Existe un procedimiento para la evaluación/auditoría interna periódica del SMS?	Si No Parcial	
2	¿Existe un plan actual de la auditoría/evaluación de SMS interna?	Si No Parcial	
3	¿Incluye la auditoría de SMS la toma de muestras de las evaluaciones existentes completadas/de riesgos de seguridad operacional?	Si No Parcial	
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	Si No Parcial	

No.	*Aspecto a ser analizado o pregunta por responder*	*Respuesta*	*Estado de implantación*
	rendimiento de su configuración de objetivos/alertas?		
5	¿Aborda el plan de auditoría de SMS la interfaz de SMS con los subcontratistas o clientes, donde corresponda?	Si No Parcial	
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	
Componente 4 – PROMOCIÓN DE LA SEGURIDAD OPERACIONAL			
Elemento 4.1 – Instrucción y educación			
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	
2	¿Ha tomado el ejecutivo responsable un curso de familiarización, sesión informativa o capacitación de SMS adecuado?	Si No Parcial	
3	¿Se brinda al personal que participa en la evaluación de riesgos capacitación o familiarización adecuadas de la gestión de riesgos?	Si No Parcial	
4	¿Existe evidencia de esfuerzos de educación o toma de conciencia del SMS a nivel de la organización?	Si No Parcial	
Elemento 4.2 – Comunicación de la seguridad operacional			
1	¿Participa [Organización] en la distribución de información de seguridad operacional a proveedores de productos y servicios u organizaciones industriales externos pertinentes, incluidas las organizaciones reglamentarias de aviación pertinentes?	Si No Parcial	
2	¿Existe evidencia de una publicación, un circular o un canal de seguridad operacional (SMS) para comunicar la seguridad operacional y asuntos de SMS a los empleados?	Si No Parcial	
3	¿Hay un manual de SMS de [Organización] y material guía relacionado accesible o distribuido a todo el personal pertinente?	Si No Parcial	

2. ANÁLISIS DE BRECHAS DE SMS DETALLADO Y TAREAS DE IMPLEMENTACIÓN (TABLA 2)

2.1 La lista de verificación del análisis de brechas inicial en la Tabla 1 debe seguirse mediante el "plan de identificación del análisis de brechas y tarea de implementación del SMS" descrito en la Tabla 2. Una vez completada, la Tabla 2 debe proporcionar un análisis de seguimiento sobre los detalles de las brechas y ayudar a traducir esto en tareas y subtareas necesarias reales en el contexto específico de los procesos y procedimientos de la organización.

2.2 Entonces, cada tarea se asignará en conformidad a las personas adecuadas o grupos de acción. Es importante que en la Tabla 2 se proporcione la correlación del desarrollo del elemento/tarea individuales con sus apoderados descriptivos en el documento del SMS para activar la actualización progresiva del borrador de documento de SMS a medida que se implementa o mejora cada elemento. (Las críticas iniciales del elemento en los documentos del SMS tienden a ser anticipativas en lugar de ser declarativas).

3. PROGRAMA DE IMPLEMENTACIÓN DE MEDIDAS/TAREAS (TABLA 3)

3.1 La Tabla 3 mostrará los hitos (fechas de inicio y fin) programados para cada tarea/medida. Para un enfoque de implementación en etapas, estas tareas/acciones se deberán organizar de acuerdo con la asignación de la etapa de sus elementos relacionados. Véase la Sección 8 de esta circular para la priorización en etapas de los elementos del SMS, como corresponda. La Tabla 3 puede ser

una consolidación por separado de todas las acciones/tareas pendientes o, si se prefiere, ser una continuación de la Tabla 2 en la forma de una hoja de cálculo. Donde se anticipa que la cantidad real de tareas/medidas y sus hitos son lo suficientemente voluminosos y complejos como para requerir el uso de un software de gestión de proyectos para administrarlas, se puede hacer al usar un software como MS Project/diagrama Gantt, como corresponda.

Tabla 2 – Ejemplo de un plan de identificación de análisis de brechas y tareas de implementación del SMS

Ref. PAC	Pregunta del análisis de brechas	Respuesta: Si/ No/ Parcial	Descripción de la brecha	Acción/tarea requerida para subsanar la brecha	Persona o grupo asignado	Ref. manual SMS	Estado de la acción (Abierta/ en proceso/ Cerrada)
1. 1-1	*¿Se ha introducido y se aplica una política de seguridad operacional?*	*Parcial*	*La política de seguridad existente contempla solamente los aspectos OSHE*	*a) Mejorar la política de seguridad existente para incluir las políticas y los objetivos del SMS, o desarrollar una nueva política de seguridad.* *b) Hacer aprobar y firmar la política de seguridad por el ejecutivo responsable.*	*Grupo de acción 1*	*Capítulo 1, Sección 1.3*	*Abierta*
Etc.							

Tabla 3 – Ejemplo de un programa de implementación de SMS

Acción/tarea requerida para subsanar la brecha	Ref. manual SMS	Persona o grupo asignado	Estado de la acción	Cronograma												
				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 existente para incluir las políticas y los objetivos del SMS, o desarrollar una nueva política de seguridad.	*Capítulo 1, Sección 1.3*	*Grupo de acción 1*	*Abierta*													
1. 1-1 b) Hacer aprobar y firmar la política de seguridad por el ejecutivo responsable.																
Etc.																