DGAC
DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

CIRCULAR DE ASESORAMIENTO

CA N°	:	**ATM-211-001**
Revisión	:	**00 (Original)**
Fecha	:	**01/05/2025**
Emitida por	:	**DGAC**

ASUNTO: "Implementación y mantenimiento del Sistema de Gestión de Seguridad Operacional (SMS) para el proveedor de Servicios de Tránsito Aéreo ATSP"

a) OBJETIVO:

Brindar orientación a los Proveedores de Servicios de Tránsito Aéreo (ATSP) para la implementación y mantenimiento de un Sistema de Gestión de la Seguridad Operacional (SMS) que cumpla con los requisitos establecidos en la RAB 211 y el Manual para la Gestión de Tránsito Aéreo PANS ATM respecto a las evaluaciones y exámenes de seguridad operacional.

b) APLICABILIDAD:

Esta Circular de Asesoramiento aplica al Proveedor de Servicios de Tránsito Aéreo.

c) FECHA DE EFECTIVIDAD:

01 de mayo de 2025.

d) CANCELACIÓN:

No aplica.

e) APROBACIÓN DE LA CA:

	NOMBRE Y CARGO	FECHA DE APROBACION	FIRMA
APROBADO POR	Ing. MSc. José Iván F. García Terceros **DIRECTOR EJECUTIVO a.i.**	23 ABR. 2025	Ing. MSc. Jose Ivan F. Garcia Terceros DIRECTOR EJECUTIVO a.i Dirección General de Aeronáutica Civil

PAGINA INTENCIONALMENTE DEJADA EN BLANCO

INDICE DE CONTENIDOS

IMPLEMENTACIÓN Y MANTENIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD OPERACIONAL (SMS) PARA EL PROVEEDOR DE SERVICIOS DE TRÁNSITO AÉREO ATSP

1. PROPOSITO:

El propósito de esta Circular de Asesoramiento (CA) es proporcionar una orientación para la implementación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS) por parte de los Proveedores de Servicios de Tránsito Aéreo (ATSP) que sea aceptable por la Autoridad Aeronáutica en conformidad con los requisitos establecidos en la RAB211 Gestión de Tránsito Aéreo, como también, el Manual para la Gestión de Tránsito Aéreo PANS ATM respecto a la realización de evaluaciones y exámenes de seguridad operacional.

Esta CA no es de cumplimiento obligatorio y no constituye un reglamento, más al contrario, describe un proceso aceptable pero no único, para demostrar el cumplimiento del requisito conforme a normativa vigente, por lo tanto, el ATSP puede utilizar otros métodos alternos de cumplimiento, siempre que dichos medios sean aceptables para la AAC.

2. REFERENCIA NORMATIVA Y DOCUMENTOS RELACIONADOS:

Referencia Normativa:
RAB 211 – Reglamento sobre la Gestión del Tránsito Aéreo.
PANS ATM – Manual de Procedimientos para la Gestión de Tránsito Aéreo.

Documentos Relacionados:
Anexo 11 – Servicios de Tránsito Aéreo.
Anexo 19 – Gestión de la Seguridad Operacional.
Doc. 4444 – Procedimientos para los Servicios de Navegación Aérea, Gestión de Tránsito Aéreo.
Doc. 9859 – Manual de Gestión de Seguridad Operacional.

3. DEFINICIONES Y ABREVIATURAS:

Aseguramiento de la seguridad operacional: Procesos dentro del SMS que funcionan sistemáticamente para garantizar el rendimiento y la eficacia de los controles de riesgos de seguridad operacional y que la organización cumple o supera sus objetivos de seguridad operacional a través de la recopilación, análisis y evaluación de información. (Fuente: NAS2297).

Cultura de seguridad operacional: Un conjunto de valores, comportamientos y actitudes duraderos con respecto a la gestión de la seguridad operacional, compartido por todos los miembros en todos los niveles de una organización.

Nota. *El objetivo de la cultura de seguridad operacional es mejorar la comprensión de los empleados de la organización sobre su papel en la seguridad operacional, compartir y promover los valores de seguridad operacional y fomentar el comportamiento positivo y la mentalidad para abordar cualquier pregunta o inquietud relacionada con la seguridad operacional identificada en un entorno de confianza y respeto mutuo. Una cultura de seguridad operacional sólida va más allá del mero cumplimiento de las reglas y regulaciones (es decir, requisitos de aeronavegabilidad inicial y continua*).

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

(i) Dichos datos sobre seguridad operacional se recopilan a través de actividades preventivas o reactivas relacionadas con la seguridad operacional, incluyendo, entre otros, los siguientes:

(A) investigaciones de accidentes o incidentes;
(B) notificaciones de seguridad operacional;
(C) notificaciones sobre el mantenimiento de la aeronavegabilidad;

(D) supervisión de la eficiencia operacional;
(E) inspecciones, auditorías, constataciones; o
(F) estudios, investigaciones y exámenes de seguridad operacional.

Defensas: Medidas de mitigación específicas, controles preventivos o medidas de recuperación aplicadas para evitar que suceda un peligro o que aumente a una consecuencia no deseada.

Descripción del sistema: Una descripción de un sistema organizacional incluyendo su estructura, políticas, comunicaciones, procesos, productos y operaciones para determinar el alcance y perímetro del sistema sujeto a la SRM. Esto permite la comprensión de factores o características críticos con el propósito de identificar peligros. Se actualiza cada vez que hay un elemento introducido recientemente o un cambio en la situación interna o externa que podría afectar la seguridad operacional (Fuente: NAS2297)

Ejecutivo responsable: Persona única e identificable que es responsable del rendimiento eficaz y eficiente del SSP del Estado o del SMS del proveedor de servicio.

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

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

Gestión de riesgo: Identificación análisis y eliminación (o mitigación a un nivel aceptable o tolerable) de los peligros, y los consiguientes riesgos, que amenazan la viabilidad de un aeropuerto o aeródromo.

Incidente grave: Incidentes en el que intervienen circunstancias que indican que casi ocurrió un accidente.

Nota 1. *La diferencia entre accidente e incidente grave estriba solamente en el resultado.*
Nota 2. *El Adjunto C del Anexo 13 OACI y el Manual de notificación de accidentes / incidentes muestran ejemplos de incidentes graves.*

Indicadores de rendimiento en materia de seguridad operacional: Parámetro de seguridad basado en datos, que se utiliza para observar y evaluar el rendimiento en materia de seguridad operacional.

Indicadores avanzados: Son medidas que proporcionan información sobre la situación actual que puede afectar al rendimiento futuro.

Indicadores de resultados: Son métricas que miden los eventos de seguridad operacional que ya han ocurrido, incluyendo los eventos se seguridad operacional no deseados y que se están tratando de evitar.

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

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

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

rendimiento en materia de seguridad operacional.

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

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

Peligro: Condición un objeto con el potencial de causar la muerte, lesiones al personal, daños al equipo o estructuras, pérdida de material, o la reducción de la capacidad de realizar una función determinada.

Política de seguridad operacional: El enfoque fundamental de una organización para la gestión de la seguridad operacional que se adoptará dentro de una organización y define además el compromiso de la dirección de la organización con la seguridad operacional y la visión de seguridad operacional general.

Procedimiento: Una forma específica de realizar una actividad o un proceso.

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

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

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

SMS corporativo: La gobernanza, la estructura y los procesos corporativos para cubrir algunos o todos los elementos comunes en todos los dominios (como la responsabilidad, la política de seguridad operacional, la identificación de peligros y los principios de gestión de los riesgos de seguridad operacional, la recopilación y evaluación de datos de seguridad operacional, la conciencia e instrucción en seguridad operacional)

Los SMS corporativos no son obligatorios, pero podrían facilitar la implementación consistente de SMS en empresas que tienen múltiples aprobaciones y/o certificados.

Suceso: Cualquier acontecimiento relacionado con la seguridad operacional que ponga en peligro o que, en caso de no ser corregido o abordado, pueda poner en peligro una aeronave, sus ocupantes o cualquier otra persona. Incluye específicamente: Accidentes, Incidentes graves, Incidentes y Otros eventos relacionados con la seguridad operacional.

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

Para los efectos de la presenta Circular de Asesoramiento, se consideran las siguientes abreviaturas:

AAC	Autoridad de Aeronáutica Civil
ALoSP	Nivel aceptable del rendimiento en materia de seguridad operacional
ANSP	Proveedor de Servicios a la Navegación Aérea.
ATS	Servicios de Tránsito Aéreo.
ATSP	Proveedor de Servicios de Tránsito Aéreo.
CA	Circular de Asesoramiento.

CAST	Equipo de seguridad operacional de la aviación comercial.
CICTT	Equipo de taxonomía común CAST/OACI.
HJ	Desde la salida hasta la puesta del sol
OACI	Organización de Aviación Civil Internacional
OSHE	Seguridad ocupacional, salud y medio ambiente
OHSMS	Sistema de Gestión sobre cuestiones de salud y seguridad en el trabajo
PAC	Plan de Acción Correctiva
QMS	Sistema de gestión de calidad
SAG	Grupo de acción de seguridad operacional
SDCPS	Sistemas de recopilación y procesamiento de datos de seguridad operacional
MSMS	Manual de gestión de la seguridad operacional
SMS	Sistema de gestión de la seguridad operacional
SSP	Programa estatal de seguridad operacional

4. **IMPLEMENTACIÓN DEL SMS:**

El ATSP implementará un sistema de gestión de la seguridad operacional para los servicios de tránsito aéreo que sea aceptable para la AAC, a fin de garantizar la seguridad operacional en el suministro de los Servicios de Tránsito Aéreo dentro de la FIR La Paz.

El proveedor de servicios deberá elaborar un plan para facilitar la implementación del SMS; esta implementación estará de acuerdo con el tamaño de la organización y la complejidad de los servicios prestados.

El ATSP deberá alcanzar y mantener un nivel aceptable de seguridad y los objetivos de la seguridad, establecidos por la AAC y que son aplicables al suministro de ATS dentro del espacio aéreo. De ser aplicable, se establecerán los niveles de seguridad y los objetivos de seguridad mediante acuerdos regionales de navegación aérea.

El SMS del proveedor ATS será objeto de lo establecido para la aceptación y evaluación de madurez del SMS por la AAC, con la finalidad de verificar que el ATSP cumpla con lo requerido por la AAC en materia de seguridad operacional y la mejora continua del mismo.

El SMS del proveedor ATS deberá describir la estructura de la organización, los deberes, facultades y responsabilidades de los empleados de la estructura de la organización, con miras a asegurar que las operaciones se realizaran en una forma controlada y que se mejoren cuando sea necesario.

Estructura y Contenido.
El marco para la implementación y la mejora continua de un SMS consta de los requisitos mínimos siguientes:

COMPONENTE	ELEMENTO
1. Política y objetivos de seguridad operacional	1.1. Compromiso de la dirección
	1.2. Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional
	1.3. Designación del personal clave de seguridad operacional
	1.4. Coordinación de la planificación de respuestas ante emergencias
	1.5. Documentación SMS
2. Gestión de riesgos de	2.1 Identificación de peligros

seguridad operacional	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

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

El segundo componente proporciona un marco para ayudar a las organizaciones a gestionar sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional (SRM), que incluye la identificación de peligros, la evaluación de riesgos y la gestión de riesgos.

El tercer componente proporciona los medios para verificar el rendimiento de seguridad operacional de la organización y para validar la eficacia de los controles de riesgos de seguridad operacional.

El cuarto componente fomenta una cultura de seguridad operacional positiva y ayuda a la organización a lograr sus metas y objetivos de seguridad operacional a través de la combinación de competencia técnica que se mejora continuamente, comunicaciones efectivas e Intercambio de información. El Gerente Responsable proporciona el liderazgo para promover la cultura de seguridad operacional en toda la organización.

Ninguno de los componentes y elementos puede considerarse independiente, ya que existen múltiples interacciones dentro del sistema.

Gestión de proveedores.
Las actividades de aviación son realizadas y respaldadas por una multitud de servicios interconectados. El ATSP es responsable de administrar y monitorear cómo interactúan con esas organizaciones y/o servicios. Es probable que el nivel general de seguridad operacional en la industria de la aviación aumente cuando se comprendan y controlen mejor los riesgos de seguridad operacional relacionados con esas conexiones.

Un SMS no solo se aplica al ATSP, se extiende a terceros (personas y organizaciones) que suministran productos y servicios para que el ATSP brinde el servicio y a terceros que son suministrados con productos. Es posible que algunos de estos terceros no tengan (o requieran) un SMS, pero todos tienen el potencial de afectar los riesgos de seguridad operacional para el ATSP. Al identificar y administrar estas interfaces, la organización tendrá más control sobre los riesgos de seguridad operacional relacionados con las interfaces. Estas interfaces de terceros deben definirse y describirse en el sistema de gestión de seguridad operacional de la organización (descripción del sistema).

Escalabilidad del SMS.
Una de las características de los SMS es que ningún sistema se adapta a todas las organizaciones. Se requiere que el SMS de un proveedor de servicios sea proporcional al tamaño y la complejidad del ATSP. La industria se caracteriza por una amplia variedad de organizaciones y servicios. Cada ATSP tiene características únicas relacionadas con los servicios que presta y los riesgos de seguridad operacional asociados, por lo tanto, un SMS debe adaptarse para satisfacer las necesidades de la organización.

Independientemente del tamaño de la organización, la escalabilidad también deberá ser una función del riesgo de seguridad operacional inherente de las actividades realizadas. Incluso los ATSP pequeños pueden participar en actividades que pueden entrañar importantes riesgos para la seguridad operacional de la aviación. Por lo tanto, la capacidad de gestión de la seguridad operacional debe estar en consonancia con el riesgo de seguridad operacional a gestionar.

El tamaño, la estructura y la complejidad del SMS deberán ser apropiados al proveedor ATS dependiendo del tipo de servicio, así como la cultura de seguridad operacional y el entorno en que se desarrollan las operaciones. El Sistema de Gestión de Seguridad Operacional debe tener presente en todo momento dos aspectos:

a) Los aspectos organizacionales respecto a la cultura de Seguridad Operacional
b) Los factores humanos en la prestación de los servicios.

Los términos “dimensión y complejidad”, que determinaran el SMS a aplicar se refieren:

1. **Dimensión:** Magnitud o tamaño del proveedor ATS, en la cual debe considerarse la cantidad de personas y la naturaleza del servicio que ofrece la organización.
2. **Complejidad:** Esta referenciada al tipo de servicio ATC, horario de atención, cantidad de operaciones y tipos de aeronaves que pueden afectar la provisión del servicio ATS.

La siguiente tabla hace la distinción de ATSP entre organizaciones complejas y no complejas, teniendo en cuenta factores de escalabilidad, con un tamaño aproximado en términos de empleados equivalentes a tiempo completo. A medida que se acumula la experiencia, la familiaridad con la gestión de varios tipos de aeronaves, la aplicación de nuevos procedimientos y utilización de nuevos sistemas los ATSP crecen, por lo que cambia el nivel de riesgo y pueden surgir otros riesgos. Es importante reconocer estas relaciones, que son fundamentales para el enfoque de SMS basado en riesgos.

CRITERIOS	CATEGORIZACION DEL ATSP		
	PEQUEÑO	MEDIANO	GRANDE
Personal Controladores Tránsito Aéreo	Hasta 4	Hasta 10	Más de 10
Tipos de Servicio	Aeródromo y/o Aproximación		Aeródromo / Aproximación incluye área de control terminal o Centro de Control de Área
Complejidad	Cantidad de operaciones menor a 10 por día, solo operaciones VFR en horario de atención HJ	Cantidad de operaciones menor a 20 por día, combinación de operaciones IFR/VFR en horario de atención HJ y operaciones nocturnas a solicitud	Cantidad de operaciones mayor a 20 por día, tipo de operaciones IFR/VFR en horario de atención H24

Nota 1. Si bien el tamaño de la organización puede ser un punto de partida, la naturaleza y complejidad de sus operaciones y sistemas (por ejemplo, sistema para informes de seguridad operacional, sistema para listar, etc.) deben considerarse igualmente al evaluar los riesgos de seguridad operacional y la complejidad general de la organización.

Nota 2. Para determinar la cantidad mínima de persona, se deberá tener en cuenta ciertas consideraciones en el servicio ATS sumado del personal disponible en la provisión de otros servicios ANS.

El proveedor de servicios de tránsito aéreo y el operador de aeródromo que se encuentren bajo una misma razón social pueden optar por aplicar un único sistema de gestión de la seguridad operacional.

Esta forma es opcional y supeditada a la aceptación por parte de la AAC. Permitirá que el sistema de gestión de la seguridad operacional que se ha diseñado pueda cumplir con los requisitos reglamentarios de ambos requerimientos. Esto asegurara que el SMS sea un sistema completamente integrado y no sistemas separados que operen independientemente uno del otro. Esto no implica que los requisitos reglamentarios dentro de cada servicio se combinen. Cada servicio debe seguir cumpliendo con sus requisitos reglamentarios. Por lo tanto, los indicadores de rendimiento del ATSP no son los mismos que los del operador de aeródromo, las metas y las alertas son propias del ATSP y no deben confundirse con los del operador de aeródromo. Sin embargo, ambos servicios pueden estar sujetas a un solo SMS.

Asimismo, un proveedor de servicios ATS categorizado como mediano o grande debe tener un responsable de la gestión de la seguridad operacional para el proveedor de servicios ATS y un responsable de seguridad operacional para el explotador de aeródromos, nombrados por el gerente responsable.

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

Desafíos para proveedores más pequeños.
Para los ATSP pequeños, el bajo volumen de datos generados por el proveedor puede significar que es más difícil identificar tendencias o cambios en el rendimiento de la seguridad operacional. Puede ser más apropiado utilizar reuniones para plantear y discutir problemas de seguridad operacional con la experiencia adecuada. Esto puede ser más cualitativo que cuantitativo, pero ayudará a identificar peligros y riesgos para el ATSP. La colaboración con otras organizaciones, grupos de usuarios o asociaciones de la industria puede ser útil, ya que estos pueden tener datos que la organización no tiene, como información sobre riesgos de seguridad operacional y tendencias de rendimiento de seguridad operacional identificadas. Otra fuente útil son los perfiles de riesgo del sector, cuando sea aplicable, publicados por AAC. Las organizaciones deben analizar y procesar adecuadamente sus datos internos, aunque sean limitados.

El ATSP debe hacerse las siguientes preguntas en todas las etapas del desarrollo, implementación y funcionamiento de su SMS:

- ¿Es apropiado para el tamaño de la organización y la naturaleza y complejidad de las actividades realizadas?
- ¿Está en su lugar: presente y adecuado?
- ¿Es operativo y se está utilizando?
- ¿Es eficaz y produce los resultados esperados?

El desarrollo e implementación de un SMS es parte de impulsar una mejor integridad operativa. Una vez que el SMS está en su lugar, se necesita un programa de mejora continua, para garantizar un compromiso continuo con la seguridad operacional.

Integración de los sistemas de gestión.
El Proveedor de servicios de tránsito aéreo debe definir la mejor manera de integrar o segregar su SMS para que éste se adecúe a su modelo de servicio, siempre y cuando cumpla con los requisitos reglamentarios y otros impuestos por la AAC.

Generalmente el proveedor de servicios ATS tendrá previamente implementadas varias funciones del SMS por cumplimiento con las reglamentaciones nacionales existentes o por adopción de las mejores prácticas del sistema. El SMS debe desarrollarse alrededor de las estructuras organizacionales y los sistemas de control existentes. El SMS del proveedor ATS también puede, de ser necesario, estar integrado con los sistemas de gestión de seguridad de la aviación, salud ocupacional, medio ambiente y gestión de la fatiga.

El ATSP deberá decidir cuáles son los mejores medios para integrar o segregar el SMS para

ajustarlos a sus necesidades de negocio u organizacionales.

Un sistema típico de gestión integrado puede incluir:

a) sistema de gestión de la calidad (QMS);
b) sistema de gestión de la seguridad operacional (SMS);
c) sistema de gestión de la seguridad de la aviación (SeMS);
d) sistema de gestión ambiental (EMS);
e) sistema de gestión de la seguridad operacional y salud ocupacional (OHSMS);
f) sistema de gestión financiera (FMS);
g) sistema de gestión de la documentación (DMS); y
h) sistema de gestión del riesgo de la fatiga (FRMS)

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

Beneficios y desafíos de la integración de sistemas de gestión.

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

a) reducción de la duplicación y superposición de procesos y recursos.
b) reducción de las responsabilidades y relaciones potencialmente conflictivas.
c) consideración de los impactos más amplios de los riesgos y las oportunidades en todas las actividades; y
d) permitir un seguimiento y una gestión eficaces del rendimiento en todas las actividades

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

a) los sistemas existentes pueden tener diferentes gerentes funcionales quienes se resisten a la integración, esto podría generar conflictos;
b) podría haber resistencia al cambio para el personal afectado por la integración, ya que esto requerirá una mayor cooperación y coordinación;
c) impacto en la cultura general de seguridad operacional dentro de la organización ya que puede haber diferentes culturas con respecto a cada sistema que crea conflictos;
d) las reglamentaciones pueden impedir tal integración o los diferentes reguladores y organismos de normalización pueden tener expectativas divergentes sobre cómo se deben cumplir sus requisitos; y
e) la integración de diferentes sistemas de gestión (como QMS y SMS) puede crear trabajo adicional para poder demostrar que se cumplen los requisitos de cada sistema de gestión.

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

Integración del SMS y el QMS.

La eficacia de la seguridad organizacional depende de la integración efectiva de estos sistemas para apoyar la producción de bienes y servicios. En el contexto del SMS el aspecto más significante de integración es con el sistema de gestión de la calidad (QMS) del proveedor de servicios ATS. El QMS comúnmente se define como la estructura organizacional, las responsabilidades, recursos, procesos y procedimientos necesarios para establecer y promover un sistema de garantía de la calidad y mejoramiento continuo, mientras se producen los bienes o servicios.

El SMS y el QMS utilizan herramientas similares. Los profesionales en seguridad y calidad están esencialmente enfocados en la misma meta de proveer productos y servicios seguros y confiables a sus clientes. Los profesionales tanto en seguridad como en calidad son entrenados en varios métodos analíticos incluyendo el análisis de causa raíz y análisis de información estadística.

La relación entre el SMS y el QMS permite a la contribución complementaria de ambos sistemas al

logro de los objetivos de seguridad y calidad de la organización. Una comparación resumida puede reflejarse de la siguiente manera:

QMS	SMS
Aseguramiento de la calidad	Aseguramiento de la seguridad operacional
Control de la calidad	Identificación de peligros y control de riesgos
Cultura de calidad	Cultura de seguridad operacional
Cumplimiento de requisitos	Nivel aceptable de rendimiento en materia de seguridad operacional
Prescriptivo	Basado en rendimiento
Normas y especificaciones	Factores institucionales y humanos
Reactivó > proactivo	Proactivo > predictivo

4.1. Cultura de la seguridad operacional.

Introducción.

La cultura de seguridad operacional es el conjunto de valores, comportamientos y actitudes perdurables con respecto a la seguridad operacional, compartido por todos los miembros en todos los niveles de una organización.

La forma en que la gerencia y el personal incorporan los valores de seguridad operacional en la práctica afecta directamente cómo se establecen y mantienen los elementos clave del SMS. Como consecuencia, la cultura de la seguridad operacional tiene un impacto directo en el rendimiento de la seguridad operacional. Si alguien en la organización cree que la seguridad no es tan importante, el resultado puede ser soluciones alternativas, tomar atajos o tomar decisiones o juicios inseguros, especialmente cuando el riesgo se percibe como bajo y no hay consecuencias o peligros aparentes.

Por lo tanto, la cultura de seguridad operacional de una organización influye significativamente en cómo se desarrolla su SMS y cómo se vuelve efectivo. Podría decirse que la cultura de la seguridad operacional es la influencia más importante en la gestión de la seguridad operacional. Si una organización ha instituido todos los requisitos de gestión de seguridad operacional necesarios, pero no tiene una posible cultura de seguridad operacional, es probable que tenga un rendimiento inferior.

Cuando la organización tiene una cultura de seguridad operacional positiva y esto es visiblemente respaldado por el Gerente Responsable y el personal clave, el personal de primera línea tiende a sentir un sentido de responsabilidades compartidas hacia el logro de los objetivos de seguridad operacional de la organización. La gestión de seguridad operacional eficaz también respalda los esfuerzos para impulsar una cultura de seguridad operacional cada vez más positiva al aumentar la visibilidad del apoyo de la dirección y mejorar la participación activa del personal en la gestión de riesgos de seguridad operacional.

En términos simples, la cultura de la seguridad operacional es cómo las personas se comportan hacia la seguridad operacional cuando nadie los está mirando.

SMS + Cultura = Rendimiento en seguridad operacional
(marco) + (comportamientos) = (logro)

La cultura de seguridad operacional puede describirse mediante seis características de alto nivel, como se muestra a continuación y se amplía en la sección Desarrollo de una cultura de seguridad operacional positiva:

Cultura de seguridad operacional y notificaciones de seguridad operacional.
La cultura de la presentación de notificaciones surge de las creencias personales y las actitudes hacia los beneficios y desventajas asociados con los sistemas de presentación de notificaciones.

Una cultura de notificaciones saludable se basa en una cultura justa, que tiene como objetivo diferenciar entre desviaciones intencionales y no intencionales, con un enfoque en los comportamientos exhibidos más que en los resultados. Fomenta la determinación del mejor curso de acción tanto para la organización en su conjunto como para las personas involucradas.

El personal debe saber que se mantendrá la confidencialidad y que la información que presenten se actuará de manera justa y equitativa. De lo contrario, determinarán que hay poco o ningún beneficio en presentar una notificación.

Toma de decisiones basada en datos.
Una cultura de seguridad operacional positiva es esencial para un SMS eficaz. Crea una franqueza que anima a las personas a notificar sobre problemas de seguridad operacional. Esto, a su vez, ayudará a la gerencia a tomar decisiones informadas basadas en lo que realmente está sucediendo, al tener:

- ✓ cultura de presentación de notificaciones: ¿la organización fomenta la presentación de notificaciones?
- ✓ cultura de aprendizaje: ¿la organización trata la información como una oportunidad para hacer crecer su cultura de seguridad operacional?
- ✓ cultura flexible: ¿la organización actúa sobre la información para mejorar la seguridad operacional?

Desarrollo de una cultura de seguridad operacional positiva.
Debemos tener cuidado con los intentos de "implementar" o "crear" una cultura como se haría con un

interruptor. Las culturas no se transforman de la noche a la mañana, pero puede cambiar el entorno de trabajo y la forma en que las personas trabajan juntas, y explicar claramente los comportamientos que se esperan de todos. Puede evaluar actitudes y comportamientos, pero las personas no cambiarán a menos que las nuevas formas se acepten como una mejora.

El Gerente Responsable necesita crear el ambiente de trabajo, proporcionar las herramientas y una política clara, y demostrar comportamientos que fomenten los comportamientos de seguridad operacional deseables. Las acciones del Gerente Responsable, el personal clave y el personal del ATSP pueden ayudar a impulsar su cultura de seguridad operacional para que sea más positiva.

La siguiente tabla proporciona ejemplos de los tipos de acciones de administración y personal que habilitarán o inhabilitarán una cultura de seguridad operacional positiva en una organización. Las organizaciones deben centrarse en proporcionar habilitadores y eliminar los inhabilitadores para promover y lograr una cultura de seguridad operacional positiva.

CARACTERISTICAS	HABILITADORES	DESHABILITADORES
COMPROMISO		
El compromiso con la seguridad operacional refleja el grado en que la administración superior de la organización tiene una actitud positiva respecto de la seguridad operacional y reconoce su importancia. La administración superior debería estar genuinamente comprometida con el logro y mantenimiento de un alto nivel de seguridad operacional y motivar a sus empleados dándoles los medios para hacerlo.	La administración conduce una cultura de seguridad operacional y motiva activamente a sus empleados para que se preocupen por la misma, no sólo con palabras sino actuando como ejemplo. La administración proporciona recursos para muchas tareas relacionadas con la seguridad operacional (p. ej., instrucción) Se establece una vigilancia continua de la gestión de la seguridad operacional y gobernanza conexa	La administración demuestra claramente que el lucro, la reducción de costos y la eficiencia son lo primero. Las inversiones para mejorar la seguridad operacional se efectúan a menudo solo cuando lo exigen los reglamentos o después de accidentes. No hay vigilancia ni gobernanza establecidas con respecto a la gestión de la seguridad operacional.
ADAPTABILIDAD		
La adaptabilidad refleja el grado en que los empleados y la administración están dispuestos a aprender de experiencias pasadas y en condiciones de tomar las medidas necesarias para mejorar el nivel de seguridad operacional de la organización.	Se fomenta activamente la contribución de los empleados al tratar problemas de seguridad operacional. Todos los incidentes y constataciones de auditorías se investigan y se actúa en consecuencia. Los procesos y procedimientos institucionales se cuestionan en cuanto a su impacto en la seguridad operacional (alto grado de autocrítica). Se demuestra y aplica un enfoque proactivo claro de la seguridad operacional.	No se fomenta la contribución de los empleados en problemas de seguridad operacional a todos los niveles del personal. A menudo las medidas se adoptan solo después de accidentes o cuando lo exigen los reglamentos. Los procesos y procedimientos institucionales se consideran adecuados en la medida en que no ocurren accidentes (complacencia o falta de autocrítica). Aun cuando ocurre un accidente la organización no se auto cuestiona.

		Se demuestra y aplica un enfoque reactivo de la seguridad operacional.
CONCIENCIA		
La conciencia refleja el grado en que empleados y administradores son conscientes de los riesgos de aviación que enfrentan la organización y sus actividades. Desde la perspectiva del Estado el personal es consciente de los riesgos de seguridad operacional inducidos por sus propias actividades y las organizaciones que supervisan. Los empleados y la administración deberían mantener constantemente un alto grado de vigilancia con respecto a la seguridad operacional.	Se ha establecido una forma eficaz de identificar peligros. Las investigaciones procuran establecer las causas básicas. La organización está siempre al tanto de importantes mejoras de la seguridad operacional y se adapta a las mismas según sea necesario. La organización evalúa sistemáticamente si se aplican y funcionan según lo previsto las mejoras de la seguridad operacional. Los miembros apropiados de la organización están bien conscientes de los riesgos de seguridad operacional inducidos por sus acciones individuales y las operaciones o actividades de la compañía.	No se realizan esfuerzos para identificar peligros. Las investigaciones se detienen en la primera causa viable sin procurar determinar la causa básica. La organización no está al tanto de importantes mejoras de seguridad operacional. La organización no evalúa si se implantan adecuadamente las mejoras de seguridad. Cuando corresponde, los miembros de la organización no están conscientes de los riesgos de seguridad operacional inducidos por sus acciones individuales y operaciones de la compañía. Los datos de seguridad operacional se recopilan, pero no se analizan ni se toman medidas al respecto.
COMPORTAMIENTO		
El comportamiento con respecto a la seguridad operacional refleja el grado en que todos los niveles de la organización se comportan para mantener y mejorar el nivel de seguridad operacional. La importancia de la seguridad operacional debería reconocerse y se deberían instituir procesos y procedimientos necesarios para mantenerla.	Los empleados se auto motivan para actuar en forma segura y como ejemplos. Se practica la observación continua del comportamiento de seguridad operacional. El comportamiento inseguro intencional no es tolerado por la administración y los colegas. Las condiciones de trabajo apoyan la seguridad operacional de la aviación en todo momento.	Los empleados no son castigados por el comportamiento inseguro intencional en beneficio de sus propios intereses o los de terceros. Las condiciones de trabajo provocan comportamientos y acciones alternativas que van en detrimento de la seguridad operacional de la aviación. No se vigila la seguridad operacional de la aviación dentro de los productos al servicio de la organización. No se ven con agrado las críticas constructivas para beneficiar la seguridad operacional de la aviación.
INFORMACION		
La información refleja el grado en que se distribuyen los	Existe un entorno abierto y justo para notificar problemas de	Es evidente un entorno de notificación de seguridad

conocimientos y datos a todas las personas necesarias dentro de la organización. Debería permitirse y fomentarse que los empleados notifiquen preocupaciones de seguridad operacional de la aviación y reciban comentarios sobre sus informes. La información laboral relacionada con la seguridad operacional de la aviación debe comunicarse correctamente a las personas adecuadas para evitar malas interpretaciones que podrían contribuir a situaciones y consecuencias peligrosas para el sistema aeronáutico El Estado se muestra abierto a compartir información relacionada con la seguridad operacional de la aviación con todos los proveedores de servicios.	seguridad operacional. Se brinda a los empleados información sobre seguridad operacional en forma oportuna para permitir la realización de operaciones o la toma de decisiones seguras. La administración y los supervisores verifican regularmente si la información de seguridad operacional es comprendida y se actúa sobre la misma. Se practica activamente la transferencia de conocimientos y la instrucción con respecto a la seguridad operacional de la aviación (p. ej., se comparten las experiencias adquiridas).	operacional con asignación de culpas. Se retiene la información sobre seguridad Operacional. No se vigila la eficacia de las comunicaciones de seguridad operacional. No se proporciona transferencia de conocimientos o instrucción
CONFIANZA		
La contribución de los empleados a la seguridad operacional es favorecida por un entorno de notificación que fomente la confianza de que sus acciones u omisiones, acordes con su instrucción y experiencia, no serán castigadas. Un enfoque viable es aplicar una prueba de sensatez – es decir, si es razonable que una persona con el mismo nivel de experiencia e instrucción podría hacer la misma cosa. Un entorno de este tipo es fundamental para la notificación eficaz y eficiente de la seguridad operacional. Los sistemas eficaces de notificación de seguridad operacional contribuyen a asegurar que las personas están dispuestas a notificar sus errores y experiencias, de modo que los Estados y los proveedores del servicio tengan acceso a datos e información pertinente necesarios para tratar deficiencias y peligros de seguridad operacional tanto	Hay una diferencia entre el comportamiento aceptable e inaceptable, conocida por todos los empleados. Las investigaciones de sucesos (incluyendo accidentes e incidentes) consideran factores individuales, así como institucionales. Se reconoce y recompensa con carácter continuo el buen rendimiento en materia de seguridad operacional de la aviación. Hay buena disposición de los empleados y personal de operaciones para notificar sucesos en los que han estado involucrados.	No hay diferencias identificables entre comportamiento aceptable e inaceptable. Los empleados son sistemática y rigurosamente castigados por los errores humanos. Las investigaciones de accidentes e incidentes se concentran solamente en factores individuales. Se da por descontado un buen rendimiento y un buen rendimiento en materia de seguridad operacional.

existente como posible. Estos sistemas crean un entorno en el que las personas pueden confiar en que su información y datos de seguridad operacional se utilizarán exclusivamente para mejorar la misma.		

Monitoreo de la cultura de seguridad operacional.

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

- ✓ comprender cómo se sienten las personas acerca de la organización y qué tan importante se percibe la seguridad operacional
- ✓ identificar fortalezas y debilidades
- ✓ identificar diferencias entre varios grupos (subculturas) dentro de una organización
- ✓ examinar los cambios a lo largo del tiempo (por ejemplo, en respuesta a cambios organizacionales importantes, como después de un accidente, un cambio en el personal clave o acuerdos de relaciones laborales alterados).

Hay una serie de herramientas que se pueden utilizar para evaluar la madurez de la cultura de seguridad operacional, generalmente en combinación:

- ✓ cuestionarios
- ✓ entrevistas y grupos focales
- ✓ observaciones
- ✓ revisiones de documentos.

La evaluación de la cultura de seguridad operacional y la maduración de la organización en esta área puede proporcionar información valiosa, lo que lleva a acciones por parte de la gerencia que fomentarán los comportamientos de seguridad operacional deseados.

La evaluación de la cultura de seguridad operacional plantea desafíos, y las organizaciones deberán centrarse inicialmente en iniciar iniciativas para recibir respuestas de la organización, en lugar de preguntarse cuál es el método "correcto". Cabe señalar que existe un cierto grado de subjetividad con tales evaluaciones y pueden reflejar las opiniones y percepciones de las personas involucradas solo en un momento particular. Además, puntuar la madurez de la cultura de seguridad operacional puede tener consecuencias no deseadas al alentar inadvertidamente a la organización a esforzarse por lograr la puntuación "correcta", en el lugar de trabajar juntos para comprender y mejorar la cultura de seguridad operacional.

4.2. Planificación para la implementación.

Para permitir al ATSP y a la AAC verificar el avance de los diferentes elementos que soportan la implementación del SMS, y por la conveniencia de establecer un orden y control, se deberá utilizar la herramienta de evaluación del SMS que se menciona en el Apéndice 2 de esta circular de asesoramiento.

Inicialmente el ATSP junto con los miembros del equipo de implementación del SMS, deberán establecer el alcance de su SMS, en base a un análisis de su accionar, procedimientos, política y objetivos del SMS, y fundamentalmente establecer las interfaces del sistema con otras organizaciones o contratistas. Con el alcance, será posible establecer las brechas existentes entre los requisitos del SMS y las capacidades, procesos y procedimientos que posee el ATSP, a fin de determinar la magnitud del trabajo a realizar, la envergadura y los costos del proceso de implementación del SMS a realizar, y la manera como este trabajo será efectuado en un plazo definido (plan de implementación).

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

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

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

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

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

También, es el momento de incorporar al sistema toda aquella información que el ATSP posee de los accidentes e incidentes en los que ha estado involucrado previamente, con sus correspondiente evaluaciones y acciones correctivas, las acciones de prevención desarrolladas. Esta información permitirá el desarrollo de indicadores de alta gravedad/baja probabilidad y alta probabilidad/baja gravedad, y empezar a completar las bases de información o de datos de seguridad operacional del ATSP. La AAC deberá aceptar los indicadores presentados por el ATSP, desarrollados en base a la experiencia y sustentados en datos de seguridad operacional.

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

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

Una vez completado el plan de implementación aceptado por la AAC se culminará el proceso de aceptación, al demostrar a la AAC que se ha completado en forma efectiva y eficiente la implementación del SMS, de acuerdo a la dimensión y complejidad del ATSP.

Descripción del sistema
La descripción del sistema incluye las interfaces del SMS dentro de la organización, así como las interfaces pertinentes con organizaciones externas. Un resumen de la descripción del sistema, las responsabilidades, la estructura, la cadena de mando y comunicación debe incluirse en la documentación del SMS. En organizaciones muy grandes y complejas una descripción básica del sistema y sus procedimientos organizacionales están contenidos en sus manuales administrativos, si este fuera el caso, un breve resumen, junto con un diagrama de flujo de la organización, con sus respectivas referencias cruzadas puede ser adecuado como una descripción del sistema.

Es posible que algunos de estos terceros no tengan (o requieran) un SMS, pero todos tienen el potencial de afectar los riesgos de seguridad operacional para el ATSP. Al identificar y administrar estas interfaces, la organización tendrá más control sobre los riesgos de seguridad operacional relacionados con las interfaces. Estas interfaces de terceros deben definirse y describirse en la descripción del sistema.

Dado que cada organización se debe comportar como un sistema, es necesario generar un “plano” de la organización, en el que se identifiquen entradas/procesos/salidas/canales para la mejor comprensión y sus elementos interactúales.

Esta identificación permitirá al equipo de implementación del SMS, comprender la organización y manejar los asuntos de su competencia en tal sentido, un sistema no puede permitir elementos aislados. Por otra parte, al identificar la organización como un sistema, apoya al análisis de faltantes de la estructura completa para que puedan ser tomados en cuenta dentro de la implementación del SMS. Para tal efecto, se podría aplicar el modelo SHELL para describir los siguientes elementos:

- Las interacciones del ATSP con otros sistemas de aviación
- Las funciones del sistema
- Las consideraciones de rendimiento humano requeridas para la operación del sistema
- Los componentes hardware del sistema
- Los componentes software del sistema
- Los procedimientos que definen las guías para la operación y el uso del sistema
- El medio ambiente operacional
- Los productos o servicios contratados o adquiridos

5. ELEMENTOS Y COMPONENTES DEL SMS.

5.1. Componente 1 – Política y objetivos de seguridad operacional.

Compromiso de la dirección.

Política de seguridad operacional.

Comprensión.
La política de seguridad operacional de la organización constituye la base de su SMS. La seguridad operacional deberá identificarse como una prioridad y un valor máximos para la organización.

El Responsable de seguridad operacional es responsable de desarrollar una declaración de compromiso y visión, mediante la participación directa en la elaboración de la redacción. El Gerente Responsable, el personal clave y, cuando proceda, los órganos representativos del personal (foros de empleados, asociaciones) deben ser consultados en el desarrollo de la política de seguridad para promover un sentido de responsabilidad compartida.

La política no deberá ser solo una pintura en la pared, debe vincular la política de la organización a la cultura que se desea inculcar en el ATSP. Es importante que la voz del Gerente Responsable se pueda escuchar a través de las palabras que se elijan, no solo frases impersonales estándar, y debe quedar claro que harán lo que sea necesario para cumplir con ese compromiso, incluida la asignación de recursos para respaldar los objetivos de seguridad operacional y objetivos.

La política de seguridad operacional define los objetivos de la organización, asigna responsabilidades y establece estándares. La política de seguridad operacional deberá describir en términos amplios la

visión de la organización para la gestión de la seguridad operacional; cómo se propone abordar los temas relacionados con la seguridad operacional; y cómo reaccionará y fomentará una cultura de seguridad operacional en todos los niveles de la estructura organizativa, con un compromiso activo y visible.

Teniendo en cuenta cada requisito de todos los elementos del SMS, significa que la política de seguridad operacional:

a) Transmite el compromiso de la administración con el rendimiento de seguridad operacional de la organización hacia sus empleados.
b) Aborda la provisión de recursos materiales, humanos y financieros suficientes para realizar las actividades planificadas del SMS.
c) Incluye (pero no se limita a) los procedimientos de notificaciones de seguridad operacional relacionados con la seguridad operacional de los servicios que ofrece el ATSP, incluida la recopilación continua de incidentes ATS y los informes de sucesos que se hayan producido en la provisión del servicio, así como los informes internos de la organización sobre problemas y riesgos de seguridad operacional, como notificaciones voluntarias de empleados.
d) Incluye el establecimiento de una política de "Cultura Justa". Las personas no son sancionadas por acciones, omisiones o decisiones erróneas acordes con su experiencia, formación y procedimientos internos. Sin embargo, no se toleran la negligencia grave, las infracciones deliberadas y los actos destructivos. Otras organizaciones pueden considerar esta definición al establecer políticas para comportamientos que son inaceptables y las circunstancias bajo las cuales no se aplicarían medidas disciplinarias.

   Si bien un sistema de notificaciones es una parte necesaria de un SMS, las organizaciones pueden adaptar su sistema de notificaciones confidenciales de empleados, según el nivel de madurez de su cultura de seguridad operacional.

e) Estará firmada por el Gerente Responsable como el líder de seguridad operacional de la organización y por el Responsable de seguridad operacional.

   El estar firmada evidencia que se cuenta con el respaldo visible del Gerente Responsable y del Responsable de seguridad operacional. "Respaldo visible" se refiere a hacer que el apoyo activo de la administración a la política de seguridad operacional sea visible para el resto de la organización. Esto se puede hacer a través de cualquier medio de comunicación y mediante la alineación de actividades con la política de seguridad operacional.

f) Es visible a todos los niveles, desde un punto de vista positivo. La política de seguridad operacional debe promoverse entre todos los empleados con la participación activa de la alta y media dirección. El propósito es fomentar una cultura de seguridad operacional dentro de la organización.

g) Se revisa periódicamente para verificar su validez y relevancia para el rendimiento real de seguridad operacional de la organización. La mejora continua del SMS puede conducir a revisiones de la política de seguridad operacional para adaptar las prioridades y objetivos de seguridad operacional.

Medios de cumplimiento.

La política de seguridad operacional es un documento de alto nivel que establece principios y objetivos generales. Esta deberá mantenerse simple y directa, con detalles del ATSP y los procesos y procedimientos de SMS que se describen en el manual del sistema de gestión de seguridad operacional (MSMS), o un documento equivalente. La política de seguridad operacional podría ser un documento independiente o integrarse en la documentación del sistema de gestión existente.

La seguridad operacional deberá destacarse como una responsabilidad principal de todo el personal clave (los gerentes) con un compromiso fuerte y claro de cumplir con los requisitos legales relevantes y los reglamentos aplicables.

Para (b) y (e) anteriores, dependiendo de la estructura y gobernanza del ATSP, las decisiones finales sobre la asignación de recursos pueden tomarse en varios niveles. El Responsable de la seguridad

operacional puede ser designado por el Gerente Responsable para todas las actividades de seguridad operacional y ser responsable de la asignación y gestión de los recursos para estas actividades. Si el Responsable de la seguridad operacional no tiene esta responsabilidad, el nivel más alto de administración debe mostrar su compromiso. La(s) persona(s) que toman las decisiones finales sobre los recursos asignados al SMS deben firmar conjuntamente la política de seguridad operacional junto con el Responsable de la seguridad operacional o utilizar otro método que muestre un compromiso conjunto.

Para los literales (c) y (d), referente a la “Cultura Justa” puede ser necesaria una evaluación de los comportamientos caso por caso. En consecuencia, la declaración de la política de seguridad operacional deberá realizarse teniendo en cuenta las reglas aplicables del ATSP.

Para el literal (f) anterior, el documento de política de seguridad operacional necesitará ser comunicado a toda la organización. Deberá proporcionar un alto nivel de información, ser convincente y fácil de entender.

Algunos puntos a considerar al desarrollar una política de seguridad operacional:

- ✓ la voz del Gerente Responsable se puede escuchar a través de las palabras que se eligen
- ✓ mantenga la política lo suficientemente breve para que el lector pueda comprender y recordar a qué se ha comprometido el Gerente Responsable.
- ✓ compromiso e intenciones de la alta dirección con respecto a la seguridad operacional y promoción de una cultura de seguridad operacional positiva.
- ✓ cómo la organización trata la seguridad operacional como un valor fundamental
- ✓ un compromiso con la mejora continua del rendimiento del SMS
- ✓ reconocimiento de que el cumplimiento de los procedimientos, normas y reglas es deber de todo el personal.

Objetivos de seguridad operacional.

Comprensión.
Los objetivos de seguridad operacional deberán respaldar la política de seguridad operacional. Hay varios objetivos posibles que difieren en alcance y plazo.

Los objetivos de seguridad operacional se establecen para mejorar continuamente la seguridad de las operaciones de las aeronaves y el rendimiento de la organización con respecto a la seguridad operacional del servicio que se ofrece. Estos objetivos de seguridad operacional deben ser significativos para la organización y, por lo tanto, adaptarse al tipo de negocio y al volumen de datos de seguridad operacional recopilados.

Otros objetivos están relacionados con el desarrollo y rendimiento del propio ATSP.

Los objetivos de seguridad operacional deberán ser lo suficientemente detallados para garantizar que se pueda demostrar su cumplimiento, en la medida de lo posible mediante un mecanismo de medición (cualitativo o cuantitativo). El propósito del monitoreo del rendimiento de seguridad operacional es evaluar apropiadamente el logro de los objetivos de seguridad operacional de la organización.

Por ejemplo, si dentro de la declaración de la política de la organización era promover una cultura de seguridad operacional positiva, esto podría estar respaldado por un objetivo que aborde las características de la cultura de seguridad operacional descritas en la sección anterior. Con el objetivo de llevar a los inhabilitadores a una cultura positiva y promover los habilitadores, durante un período de tiempo, la organización podría crear un programa con indicadores mensurables de su progreso.

Los objetivos de seguridad operacional deben ser significativos, realistas y proporcionales a la organización y a la madurez de su SMS.

Se presenta un ejemplo de cómo podría desarrollarse un objetivo de seguridad operacional:

Objetivo de Seguridad Operacional	Meta	Indicador de Rendimiento de Seguridad Operacional
Implementar un SMS con el que todo el personal esté plenamente comprometido.	Asegúrese de que el personal esté capacitado y sea competente en el sistema de notificaciones de seguridad operacional.	Instrucción y evaluación de todo el personal nuevo dentro del mes siguiente a su incorporación.
		El personal puede demostrar el uso del sistema de notificaciones (entrevista de auditoría).
	Promover las características de la cultura de seguridad operacional a través del compromiso de la gerencia y la cultura justa a lo largo del año 202X.	Las reuniones mensuales incluyen la revisión liderada por el Gerente Responsable de las actividades de mejora de la seguridad operacional (se toman actas).
		Incremento del número de notificaciones de seguridad operacional donde el personal identifica sus propios actos inseguros.
Gestionar activamente los riesgos de seguridad operacional para que el personal y clientes, el equipo y los trabajos que realiza el ATSP no sufra ningún daño.	Completar los talleres (workshops) de identificación proactiva de peligros para los trabajos que realiza el ATSP a fines del año 202X	Talleres (workshops) completados para planificar +/- 10% de variación
		Los peligros y riesgos asociados están documentados para evaluación.
		Los controles de riesgo están establecidos y monitoreados para todos los riesgos tolerables e intolerables.
	Todos los cambios significativos están gestionados a través de nuestro proceso formal de gestión del cambio lo que son documentados y comunicados.	Las actas de las reuniones muestran la consulta y la comunicación con las partes interesadas.
		El personal involucrado conoce los controles de riesgo aplicables (entrevistas de auditoría).

Medios de cumplimiento.

a) El ATSP deberá definir objetivos de seguridad operacional que reflejen el rendimiento de seguridad operacional en el servicio que proporciona, así como objetivos relacionados con la función del SMS mismo. Estos objetivos deberían incluir el seguimiento del correcto despliegue del SMS, la medición de su actividad y la asignación de los medios y competencias del personal adecuados. Estos objetivos de seguridad operacional deberán reflejar la mejora de seguridad operacional identificada, con base en la situación actual. Deberán definirse como específicos, medibles, alcanzables, pertinentes y de duración determinada (SMART).

Los objetivos de seguridad operacional pueden considerar la gestión de interfaces dentro de la organización, así como con otras organizaciones.

Los objetivos de seguridad operacional se podrían presentar como un documento independiente para constituir la representación gráfica (dashboard) de rendimiento de la seguridad operacional del ATSP, que también se puede utilizar para notificar los resultados del rendimiento de

seguridad operacional.

b) El establecimiento de objetivos debe tener como objetivo impulsar la mejora continua del rendimiento de seguridad operacional de la organización. Puede ser apropiado establecer metas y objetivos estratégicos (a largo plazo) y tácticos (a corto o medio plazo) para permitir revisiones periódicas y evaluaciones del rendimiento.

c) Durante el proceso de comunicación de la política de seguridad operacional y los objetivos asociados a todo el ATSP, se debería tener cuidado de describir el flujo descendente de los objetivos generales a nivel de la organización en relación con los objetivos de seguridad operacional "locales". Estos objetivos locales tienen como objetivo mostrar la contribución a la seguridad operacional de un individuo/grupo de empleados. Cada empleado debe ser consciente de las posibles consecuencias de sus acciones y comportamiento y de su contribución positiva al SMS mediante la comprensión de los objetivos de seguridad operacional.

d) El SMS debería incluir una revisión periódica de los objetivos de seguridad operacional, por ejemplo, una vez al año, o con una frecuencia adaptada a las especificidades, cambios y logros de seguridad operacional de la organización. Esta revisión debe estar alineada con la publicación de los resultados de rendimiento de seguridad operacional en términos de lograr los objetivos.

Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional.

Comprensión.
El “Gerente Responsable” es una persona que rinde cuentas (que tiene la responsabilidad final) del SMS dentro del ATSP. La autoridad y las responsabilidades de esta persona pueden incluir, pero no se limitan a:

a) Proporcionar y asignar recursos humanos, técnicos, financieros o de otro tipo necesarios para el rendimiento eficaz y eficiente del SMS.
b) Responsabilidad directa por la conducción de los asuntos de la organización.
c) Autoridad final sobre las operaciones bajo el certificado y lista de capacidades de la organización.
d) Establecer y promover la política de seguridad operacional.
e) Establecer los objetivos y las metas de seguridad operacional de la organización.
f) Actúa como el líder de la seguridad operacional de la organización.
g) Responsabilidad final por la resolución de todos los problemas de seguridad operacional.
h) Establecer y mantener la competencia de la organización para aprender del análisis de los datos recopilados a través de su sistema de notificaciones de seguridad operacional.

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

La rendición de cuentas de la seguridad operacional define la obligación de la persona responsable de demostrar la ejecución satisfactoria de sus responsabilidades de seguridad operacional.

La responsabilidad de la seguridad operacional se puede delegar (es decir, de arriba hacia abajo) dentro del alcance de las responsabilidades laborales definidas, siempre que dicha delegación esté documentada.

Para asegurar la conciencia y el compromiso de seguridad operacional necesarios de todo el personal involucrado en las tareas relacionadas con la seguridad operacional, la rendición de cuentas y las responsabilidades de seguridad operacional en el ATSP deberán definirse, documentarse y comunicarse de forma clara y completa en toda la organización.

Al identificar las responsabilidades del personal de gestión y los empleados, las organizaciones deberán considerar qué empleados están incluidos en las tareas y actividades relacionadas con la seguridad operacional.

Todas las responsabilidades de rendición de cuenta, responsabilidades y autoridades definidas deben indicarse en la documentación de SMS del ATSP y deben comunicarse a toda la organización. Las responsabilidades de rendición de cuenta y responsabilidades de seguridad operacional de cada gerente senior son componentes integrales de sus descripciones de trabajo. Esto también debería capturar las diferentes funciones de gestión de la seguridad operacional entre los gerentes de línea y el Responsable de seguridad operacional.

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

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

Para mayor eficiencia, una empresa que tenga varios certificados/aprobaciones de organización (por ejemplo, explotador aéreo, ATSP, operador de aeródromo) puede organizar las responsabilidades a través de diferentes esquemas de acuerdo con la complejidad, necesidades y limitaciones de cada empresa. Tal esquema sería aceptable siempre que cada titular del ATSP cumpla con los requisitos para las responsabilidades de seguridad operacional.

Los ejemplos de esquemas incluyen, pero no se limitan a:
- ✓ Un Responsable de la seguridad operacional para cada servicio (por ejemplo, operador de aeródromo y ATSP).
- ✓ Un solo Responsable de seguridad operacional en un nivel de gestión adecuado para cubrir el SMS general de la empresa.

Rendición de cuentas y responsabilidades con respecto a las organizaciones externas.
El ATSP es responsable del rendimiento de seguridad operacional de las organizaciones externas donde hay una interfaz de SMS. El ATSP puede ser responsable de la rendición de cuentas de seguridad operacional de los productos o servicios proporcionados por organizaciones externas que respaldan sus actividades, incluso si las organizaciones externas no están obligadas a tener un SMS. Es esencial que los SMS del ATSP interactúen con los sistemas de seguridad operacional de cualquier organización externa que contribuya a la entrega segura de sus productos o servicios.

Designación de personal clave de seguridad operacional.

Medios de cumplimiento.
La asignación de responsabilidades de gestión de SMS queda a discreción del proveedor de servicios.

Esto incluye el nombramiento de personal directamente responsable ante el Gerente Responsable para brindar orientación, dirección y apoyo para la planificación, implementación y operación del SMS del proveedor de servicios. Esta podría ser su única función, actuar como personal asignado a la seguridad operacional dedicados a dicha área, o combinada con otras tareas, siempre que esas tareas no den lugar a ningún conflicto de intereses.

En organizaciones pequeñas/simples, estas responsabilidades también podrían ser asumidas por el Gerente Responsable.

La organización es responsable de:
- ✓ Asegurarse de que el SMS funcione según lo definido y sea eficaz.
- ✓ Recopilar y analizar información de seguridad operacional de manera oportuna.
- ✓ Administrar encuestas relacionadas con la seguridad operacional.
- ✓ Seguimiento y evaluación de los resultados de las acciones correctivas.

- ✓ Asegurar que se lleven a cabo evaluaciones de riesgo, cuando corresponda;
- ✓ Monitorear los problemas de seguridad operacional reportadas en otras organizaciones que podrían afectar al ATSP o sus productos / servicios.
- ✓ Garantizar que la información relacionada con la seguridad operacional, incluidas los logros y los objetivos de la organización, esté disponible para todo el personal a través de los procesos de comunicación establecidos.
- ✓ Proporcionar notificaciones periódicas sobre el rendimiento en seguridad operacional.

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

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

a) administrar el plan de implementación de SMS en nombre del Gerente Responsable (en la implementación inicial);
b) realizar/ facilitar la identificación de peligros y el análisis de riesgos de seguridad operacional;
c) monitorear acciones correctivas y evaluar sus resultados;
d) proporcionar informes periódicos sobre el rendimiento de seguridad operacional de la organización;
e) mantener documentación y registros de SMS;
f) planificar y facilitar la instrucción de seguridad operacional del personal;
g) proporcionar asesoramiento independiente sobre problemas de seguridad operacional;
h) monitorear las preocupaciones de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones del ATSP dirigidas a la entrega de productos y servicios; y
i) coordinar y comunicar (en nombre del Gerente Responsable) con la AAC del Estado y otras autoridades estatales, según sea necesario, acerca de problemas relacionados con la seguridad operacional.

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

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

a) competencia por la financiación (por ejemplo, el gerente financiero es el Responsable de seguridad operacional);
b) prioridades conflictivas para los recursos; y
c) cuando el Responsable de seguridad operacional tiene una función operativa y su capacidad para evaluar la efectividad de SMS de las actividades operacionales en las que está involucrado.

En los casos donde la función se asigna a un grupo de personas (por ejemplo, cuando el ATSP extiende su SMS a través de múltiples actividades) una de las personas debe ser designada como Responsable de seguridad operacional "principal" para mantener una línea directa e inequívoca con el Gerente Responsable.

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

a) egresado de una carrera universitaria en una especialidad a fin a la aeronáutica o poseer una licencia como controlador de tránsito aéreo;
b) cualificación en el sistema de gestión de seguridad operacional;

Nota. La cualificación corresponde a haber seguido la formación del SMS y haberla aprobado en una organización reconocida y aceptable por la AAC para desempeñarse en temas de gestión de la seguridad operacional.

c) conocimiento del reglamento aeronáutico (RAB211);
d) una comprensión de los factores humanos.
e) experiencia en el sistema de gestión de seguridad operacional o sistema de calidad en la industria aeronáutica;
f) experiencia operacional relacionada con el producto o servicio proporcionado por el ATSP;
g) antecedentes técnicos para garantizar la comprensión de los sistemas que respaldan las operaciones o producto / servicio proporcionado por el ATSP;
h) habilidades de gestión de proyectos;
i) habilidades analíticas y de resolución de problemas;
j) habilidades interpersonales;
k) habilidades de comunicación oral y escrita; y

Nota. Si el ATSP lo considera necesario los requisitos de competencia los puede desarrollar en el documento/manual de SMS.

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

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

El Consejo de revisión de seguridad operacional (SRC), incluye al Gerente Responsable y los gerentes senior (personal clave) con el Responsable de seguridad operacional participante en carácter de asesor. El SRC es estratégico y se ocupa de cuestiones de alto nivel relacionadas con las políticas, la asignación de recursos y el monitoreo del rendimiento organizacional. La SRC monitorea:

a) La efectividad del SMS;
b) respuesta oportuna de las acciones de control de riesgos de seguridad operacional necesarias;
c) el rendimiento de seguridad operacional contra la política y los objetivos de seguridad operacional de la organización;
d) La efectividad general de las estrategias de mitigación de riesgos de seguridad operacional;
e) La eficacia de los procesos de gestión de la seguridad operacional del ATSP que apoyan:
    1) la prioridad organizativa declarada de la gestión de la seguridad operacional; y
    2) la promoción de la seguridad operacional en toda la organización.

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

a) monitorea el rendimiento de la seguridad operacional dentro de las áreas funcionales de la organización y asegura que se lleven a cabo las actividades adecuadas de la gestión de riesgos de seguridad operacional (SRM);
b) revisa los datos de seguridad operacional disponibles e identifica la implementación de las

estrategias apropiadas de control de riesgos de seguridad operacional y asegura que se brinde retroalimentación a los empleados;
c) evalúa el impacto de seguridad operacional relacionado con la introducción de cambios operacionales o nuevas tecnologías;
d) coordina la implementación de cualquier acción relacionada con los controles de riesgos de seguridad operacional y asegura que las acciones se tomen con prontitud; y
e) revisa la efectividad de los controles de riesgo de seguridad operacional.

Coordinación de la planificación de respuestas ante emergencias.

Comprensión.
La coordinación de la planificación de respuestas ante emergencias documenta las acciones que debe tomar todo el personal responsable durante las emergencias. El propósito de la coordinación de la planificación de respuestas ante emergencias es garantizar que haya una transición ordenada y eficiente hacia y desde las operaciones de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de autoridad.

La coordinación de la planificación de respuestas ante emergencias también contiene la autorización para la acción del personal clave, así como los medios para coordinar los esfuerzos necesarios para hacer frente a la emergencia.

El objetivo general es la continuación segura de las operaciones. La coordinación de la planificación de respuestas ante emergencias se aplica al ATSP en la provisión de asistencia a aeronaves en vuelo y coordinación con el operador de aeródromo.

También se puede utilizar ante contingencias cuando se produce una interrupción significativa en la provisión de los servicios, para garantizar la continuidad de las operaciones y la gestión de crisis.

Con respecto a la seguridad operacional del ATSP está implementando disposiciones para respuestas ante emergencia que pueden identificarse bajo diferentes títulos en diferentes organizaciones (por ejemplo, reglas de gestión de crisis, política de respuesta a crisis, plan de respuesta a accidentes, entre otros). Estas actividades deben coordinarse con todas las partes involucradas en caso de accidente o incidente grave.

Medios de cumplimiento.
El plan de respuesta ante emergencias (ERP) se aplica solo a los proveedores de servicios requeridos a establecer y mantener un ERP como es el caso de los aeropuertos, explotadores aéreos y ATSP. Para ello, se deberán establecer los procedimientos en donde se detallen funciones y responsabilidades que deberán cumplirse en caso de un accidente o incidente grave en el cual se solicite su colaboración.

Documentación SMS.

Comprensión.
El alcance de la documentación de SMS puede diferir de un ATSP a otro debido a:
- Dimensión (tamaño) de la organización y tipo de actividades.
- Complejidad de procesos y sus interacciones.

Cada ATSP debe garantizar el control y actualización adecuada de estos documentos. Deberán revisarse periódicamente y actualizarse según sea necesario (por ejemplo, anualmente).

a) Política y objetivos de seguridad operacional
La política de seguridad operacional tal como se entiende en la sección compromiso de la dirección, determina los objetivos de seguridad operacional. Los objetivos deben ser prácticos, alcanzables, revisados y reevaluados periódicamente y comunicados al personal.

La política de seguridad operacional y los objetivos de seguridad operacional deberán estar documentados y pueden ser documentos independientes o estar incluidos en el manual de SMS.

b) Requisitos de SMS

Como parte de la documentación de SMS, debe documentarse una lista de todos los requisitos de SMS, tanto internos (por ejemplo, organización, corporativos) como externos (por ejemplo, autoridades, clientes).

c) Procesos y procedimientos de SMS

Los procesos y procedimientos deben incluir los pasos y métodos que se utilizarán para cumplir con los requisitos aplicables y lograr los resultados esperados.

La estructura y el formato de los procesos y procedimientos documentados, y su método de resguardo (copia impresa, medios digitales o ambos) deben ser definidos por la organización.

d) Rendición de cuentas, responsabilidades y autoridades para los procesos y procedimientos de SMS

La documentación deberá identificar qué gerente superior tiene la rendición de cuentas del SMS e identificar las responsabilidades y autoridades de las partes interesadas clave con respecto al rendimiento de seguridad operacional de la organización.

La responsabilidad, la autoridad y las interrelaciones pueden indicarse por medios tales como organigramas, diagramas de flujo o descripciones de puestos o ambos (sin limitarse a los altos directivos o las partes interesadas clave).

e) Manual de SMS

La documentación de SMS puede incluir un documento de nivel superior (Manual de SMS o similar), que describe la implementación de SMS del ATSP de los cuatro componentes y doce elementos.

Cuando los detalles de los procesos de SMS de la organización ya se abordan en documentos existentes, es suficiente la referencia cruzada adecuada a dichos documentos.

Medios de cumplimiento.

La forma y el formato de la documentación quedan a discreción del ATSP. Puede integrarse en la documentación existente de cualquier otro sistema de gestión implementado por la organización.

En el Apéndice 3 se proporciona una guía del contenido del Manual SMS.

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

a) registro de peligros y notificaciones de peligros/seguridad operacional;
b) SPI y gráficos relacionados;
c) registro de evaluaciones de riesgos de seguridad operacional completados;
d) revisión interna del SMS o registros de auditoría;
e) registros de auditoría interna;
f) registros de SMS / registros de instrucción de seguridad operacional;
g) actas de reuniones del SRC/SMS;
h) plan de implementación de SMS (durante la implementación inicial); y
i) análisis de brechas para apoyar el plan de implementación.

5.2. Componente 2 – Gestión de riesgos de seguridad operacional (SRM).

El objetivo de la gestión de riesgos de seguridad operacional (SRM) es prevenir la ocurrencia de incidentes graves o accidentes. Con ese fin, SRM identifica peligros, analiza, evalúa y controla los riesgos de seguridad operacional.

La gestión de riesgos de seguridad operacional es un componente clave de la gestión de seguridad operacional e incluye una combinación de procesos para la identificación de peligros, evaluación de

riesgos de seguridad operacional, mitigación de riesgos de seguridad operacional y aceptación de riesgos. La SRM es una actividad continua porque el sistema de aviación cambia constantemente, pueden surgir nuevos peligros y algunos peligros y sus riesgos asociados pueden cambiar con el tiempo. Además, es necesario monitorear la efectividad de las estrategias de mitigación de riesgos de seguridad operacional implementadas para determinar si se requieren más acciones.

En pocas palabras, la gestión de riesgos de seguridad operacional describe el proceso general que utiliza para identificar cosas que pueden o han salido mal, evaluar qué tan grave podría ser esa consecuencia y decidir qué hará para reducir la probabilidad de que suceda o el impacto en su negocio si lo hace. Es muy similar a nivel operacional, a los métodos utilizados para "Gestión de amenazas y errores", como ya lo practican muchos profesionales de la aviación y recreativos por igual.

La descripción del sistema es un requisito previo para la aplicación de la SRM (identificación de peligros, evaluación y mitigación de riesgos de seguridad operacional). Por lo tanto, se requiere una descripción del sistema para proporcionar una descripción general de la organización cubierta por la aplicación del SRM.

En todos los niveles, la organización deberá definir acciones para mantener los riesgos de seguridad operacional a un nivel aceptable.

Identificación de peligros.

Comprensión.
La identificación de peligros es un requisito previo para el proceso de gestión de riesgos de la seguridad operacional. Para el personal involucrado en el proceso de gestión de riesgos de la seguridad operacional, una clara comprensión de los peligros y sus consecuencias asociadas es esencial para la implementación de una adecuada gestión de riesgos de la seguridad operacional.

Para fines de la gestión de riesgos de la seguridad operacional de la aviación, el termino peligro debería centrarse en aquellas condiciones u objetos que podrían causar o contribuir a un accidente o incidente de aviación.

El ATSP debería desarrollar y mantener un proceso formal para la identificación de peligros que podrían tener un impacto en la seguridad operacional de la aviación en todos los sectores de su operación y su actividad. Una comprensión del sistema y de su entorno operacional es también esencial para este proceso. Para ello, ayudaría contar con una descripción detallada del sistema que defina sus interfaces. También es importante considerar los peligros que pudieran ser introducidos a través de las interfaces con las organizaciones externas que pueden o no tener su propio SMS.

La identificación de peligros permite identificar “problemas de seguridad operacional” o “amenazas” (a los que se hace referencia como peligro) que requieren la aplicación de una SRM y aseguramiento de la seguridad operacional (SA). Esto permite a la organización asignar recursos de gestión de la seguridad operacional a fuentes de riesgo potenciales significativos y evitar dedicar recursos a riesgos menores o insignificantes.

Los peligros pueden tener su origen en factores técnicos, ambientales, humanos y organizacionales.

Con respecto a las actividades del ATSP, los peligros son las condiciones que previsiblemente podrían conducir a un servicio no cumplido o no conforme que, si no se abordan, podrían llegar a un nivel de riesgo inaceptable.

Medios de cumplimiento.
La identificación de peligros consiste de:

- ✓ Análisis de las áreas de alto riesgo de las actividades de la organización o cambios organizacionales.
- ✓ Análisis de datos de fuentes internas y externas (por ejemplo, datos de incidentes ATS, comentarios de los explotadores, información de los subcontratistas, peligros identificados por las AAC o datos de notificaciones voluntarias).

Identificación de peligros en la práctica

Los peligros existen en todos los niveles del ATSP y son detectables a través de muchas fuentes, incluidos los sistemas de notificaciones, las inspecciones, las auditorías, las sesiones de intercambio de ideas, el intercambio de información y el juicio de expertos. El objetivo es identificar de forma proactiva los peligros antes de que provoquen accidentes, incidentes u otros sucesos relacionados con la seguridad operacional.

Las dos metodologías principales para identificar peligros son:

- ✓ **Reactivo:** esta metodología implica el análisis de resultados o sucesos pasados. Los peligros se identifican mediante la investigación de sucesos de seguridad operacional o auditorías de calidad. Los incidentes y accidentes son una indicación de deficiencias del sistema y, por lo tanto, se pueden utilizar para determinar qué peligros contribuyeron al suceso. Compartir datos críticos de seguridad operacional puede significar que un suceso para una organización o parte de una organización puede convertirse en un aprendizaje oportunidad para otros.

- ✓ **Proactivo:** esta metodología implica la recopilación de datos de seguridad operacional de sucesos de menor consecuencia o rendimiento del proceso. El análisis de la información de seguridad operacional y la frecuencia de ocurrencia ayudará a la organización a determinar si un peligro podría conducir a un accidente o incidente. La información de seguridad operacional para la identificación proactiva de peligros proviene principalmente de los sistemas de notificaciones de seguridad operacional, las inspecciones de seguridad operacional programadas y la función de aseguramiento de la seguridad operacional.

La identificación proactiva de peligros también se puede lograr mediante revisiones sistemáticas de los procesos y procedimientos organizacionales, así como durante la planificación del cambio que la organización pueda considerar.

Los peligros también se pueden identificar a través del análisis de datos de seguridad operacional que identifica tendencias adversas y hace predicciones sobre peligros emergentes y resultados futuros.

Los peligros pueden identificarse basándose en datos de sucesos que han ocurrido (métodos reactivos) o en anticipación de sucesos potenciales que podrían conducir a un riesgo inaceptable (métodos proactivos).

El ATSP deberá establecer y documentar metodologías y procesos para monitorear eventos y sucesos reportados como los siguientes:

Para actividades del ATSP:

- ➢ Incidentes ATS.
- ➢ Reportes LHD.
- ➢ Errores en las coordinaciones entre dependencias ATC.
- ➢ Fallas en los equipos de comunicación y vigilancia.

Cualquiera de estos tipos de eventos o sucesos podría usarse para identificar peligros para la seguridad operacional de la aviación.

Para mejorar la identificación de peligros, el ATSP deberá implementar un sistema de notificación voluntario de los controladores, basado en la política de cultura justa definida e implementada por la organización.

Probabilidad del riesgo de seguridad operacional.

Para determinar la probabilidad de un riesgo de seguridad operacional, el Gerente de Seguridad Operacional, basándose en estadísticas e información relevante del suceso bajo análisis, debe definir las tablas de clasificación de riesgos. Estas tablas deben ser diseñadas a medida, con categorías adaptadas al entorno específico de la organización, ya que no existe un estándar único aplicable a todos los casos.

Cada categoría en la tabla debe incluir una descripción clara y un valor numérico o rango que la

represente. La definición de la probabilidad debe basarse en una "razón aritmética" con un numerador (cantidad de sucesos) y un denominador (base de comparación).

Ejemplos de definiciones de probabilidad:

- 1 suceso "X" cada 10.000 operaciones.
- 1 suceso cada "n" mil despegues.
- 1 x 10^-7 ciclos.

La organización, con base en la información recopilada, determinará el significado de cada categoría (por ejemplo, frecuente, ocasional, etc.).

A continuación, se presentan tres ejemplos de tablas de probabilidad. Es importante destacar que estas tablas son solo ejemplos y cada organización deberá desarrollar sus propias tablas en función de sus necesidades y características particulares.

Tabla de ejemplo A: (Basada en la frecuencia por número de operaciones)

Probabilidad	Definición cualitativa	Significado	Valor asignado	Índice de Probabilidad Id-Prob
Frecuente	Ocurre cien veces cada 1.000 operaciones	100/1.000	0,1%	1
Ocasional	Ocurre cincuenta veces cada 1.000 operaciones	50/1.000	0,05%	2
Escaso	Ocurre veinte veces cada 1.000 operaciones	20/1.000	0,02%	3
Poco probable	Ocurre cinco veces cada 1.000 operaciones	5/1.000	0,005%	4
Altamente improbable	Ocurre una vez cada 1.000 operaciones	1/1.000	0,001%	5

Tabla de ejemplo B: (Basada en la frecuencia por ciclos)

Probabilidad	Definición cualitativa	Significado	Valor asignado	Índice de Probabilidad Id-Prob
Endémico /persistente	Ocurre una vez cada 1.000 ciclos	1×10^{-3}	1×10^{-3}	1
Probable	Ocurre una vez cada 10.000 ciclos	1×10^{-4}	1×10^{-4}	2
Eventual	Ocurre una vez cada 100.000 ciclos	1×10^{-5}	1×10^{-5}	3
Poco probable	Ocurre una vez cada 1’000.000 ciclos	1×10^{-6}	1×10^{-6}	4
Muy improbable	Ocurre una vez cada 10’000.000 ciclos	1×10^{-7}	1×10^{-7}	5

Tabla de ejemplo C: (Basada en la frecuencia por número de despegues)

Probabilidad	Definición cualitativa	Significado	Valor asignado	Índice de Probabilidad Id-Prob
Constante	10.000 veces por cada 1’000.000 de despegues	10.000/1'000.000	1/100	1
Habitual	1.000 veces por cada 1’000.000 de despegues	1.000/1’000.000	1/1.000	2
Normal	100 veces por cada 1’000.000 de despegues	100/1'000.000	1/10.000	3
Inusitado	10 veces por cada 1’000.000 de despegues	10/1'000.000	1/100.000	4
Insólito	1 vez por cada 1’000.000 de despegues	1/1'000.000	1/1’000.000	5

Recomendaciones para la construcción de la tabla:

- Se recomienda evitar el uso de unidades de tiempo (meses, semestres, años) al definir las probabilidades en las tablas. Esto se debe a que la cantidad de sucesos (numerador) y la base de comparación (denominador) pueden variar significativamente entre diferentes períodos, dificultando la estandarización de los datos.
- Considerar preguntas guía: Para determinar la probabilidad, se pueden utilizar preguntas guía como:
  - ¿Existen antecedentes de sucesos similares al que se está analizando?
  - ¿Se han observado problemas similares en otros equipos o componentes del mismo tipo?

- ¿Cuántos miembros del personal están expuestos al peligro o siguen los procedimientos en cuestión?
- ¿Cuál es el grado de exposición al peligro? (Por ejemplo, ¿durante qué porcentaje de la operación se utiliza el equipo o se realiza la actividad?)

En resumen, la probabilidad del riesgo de seguridad operacional se define como la posibilidad de que ocurra una consecuencia o un resultado de seguridad operacional no deseado.

La tabla 1 presenta una clasificación estándar de la probabilidad de riesgos de seguridad operacional, es importante recordar que el nivel de detalle y la complejidad de las tablas y matrices deben adaptarse a las necesidades y características específicas de cada proveedor de servicios. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un suceso o condición insegura, la descripción de cada categoría y una asignación de valor a cada una. Este ejemplo utiliza términos cualitativos; pero también puede definirse términos cuantitativos a efectos de una evaluación más precisa. Esto dependerá de la disponibilidad de datos de seguridad operacional apropiados y del grado de desarrollo del proveedor de servicios y su operación.

Tabla 1 – Tabla de probabilidad de riesgos de seguridad operacional

Probabilidad	Significado	Valor
Frecuente	Es probable que suceda muchas veces (ha ocurrido frecuentemente)	5
Ocasional	Es probable que suceda algunas veces	4
Remoto	Es probable que ocurra, pero no imposible	3
Improbable	Es poco probable que ocurra	2
Sumamente improbable	Es casi inconcebible que el suceso ocurra	1

Nota. *El nivel de detalle y complejidad de las tablas y matrices debe adaptarse a las necesidades y complejidades particulares de cada proveedor de servicios. También se debe tener presente que los proveedores de servicios pueden incluir criterios tanto cualitativos como cuantitativos, conforme a sus necesidades. Por lo que si el proveedor de servicios emplea otra matriz a la sugerida deberá incluirla en el análisis de riesgos.*

Gravedad del riesgo de seguridad operacional

Una vez completada la evaluación de probabilidad, el siguiente paso es determinar la gravedad del riesgo de seguridad operacional. Esto implica analizar las posibles consecuencias asociadas al peligro identificado. En otras palabras, la gravedad del riesgo se refiere al grado de daño que podría resultar del peligro.

Al clasificar la gravedad, se deben considerar los siguientes aspectos:

a) Muertes o lesiones graves ocurridas:

1. A personas a bordo de la aeronave

2. por contacto directo con cualquier parte de la aeronave, incluyendo partes desprendidas de la misma; o

3. Por exposición directa del chorro de los reactores

b) Daños:

1. Daños o fallas estructurales sufridas por la aeronave que:

i. Afecten adversamente la resistencia estructural, las características de vuelo de la aeronave,

ii. Requieran normalmente importantes reparaciones o sustitución del componente afectado

2. Daños sufridos por el equipo ATS o aeródromo que afecten adversamente:

i. la gestión de la separación de aeronaves; o

ii. la capacidad de aterrizaje.

La evaluación de la gravedad debe considerar todas las posibles consecuencias relacionadas con un peligro, siempre considerando el peor escenario posible.

La tabla 2 presenta una clasificación estándar de la gravedad del riesgo de seguridad operacional. Esta tabla, que se ofrece como referencia, incluye cinco categorías para clasificar el nivel de gravedad, junto con la descripción de cada categoría y la asignación de valor correspondiente.

Tabla 2 – Gravedad del riesgo de seguridad operacional

Gravedad	Significado	Valor
Catastrófico	Aeronave o equipo destruidos Varias muertes	A
Peligroso	Gran reducción de los márgenes de seguridad operacional, estrés físico o una carga de trabajo tal que ya no se pueda confiar en que el personal de operaciones realice sus tareas con precisión o por completo Lesiones graves Lesiones a las personas	B
Grave	Reducción importante de los márgenes de seguridad operacional, reducción en la capacidad del personal de operaciones para tolerar condiciones de operación adversas, como resultado de un aumento en la carga de trabajo o como resultado de condiciones que afecten su eficiencia. Incidente grave Lesiones a las personas	C
Leve	Molestias Limitaciones operacionales Uso de procedimientos de emergencia Incidente leve	D
Insignificante	Pocas consecuencias	E

Es importante recordar que, al igual que con la tabla de probabilidad, esta tabla es solo una guía. Cada organización debe adaptarla a sus necesidades y contexto específicos.

Tolerabilidad del riesgo de seguridad operacional.
Al definir la tabla de gravedad, el Gerente de Seguridad Operacional debe considerar cómo se clasificará el riesgo. La severidad del riesgo se define como las consecuencias potenciales de un suceso o condición insegura, tomando como referencia el peor escenario previsible. La organización debe establecer esta clasificación con base en su tipo de provisión de servicios y los daños potenciales previsibles.

Es fundamental que cada definición cualitativa sea clara, concisa y refleje parámetros reales de severidad, considerando los daños potenciales a personas, equipos, infraestructura o cualquier aspecto de la provisión del servicio que pueda comprometer la seguridad de la operación.

La Tabla 3, denominada "Matriz de evaluación de riesgos de seguridad operacional", combina las variables de probabilidad y gravedad para determinar la tolerabilidad del riesgo. Cada celda de la matriz representa un índice de riesgo de seguridad operacional, formado por la combinación alfanumérica de las evaluaciones de probabilidad y gravedad.

El índice de riesgo de seguridad operacional se obtiene combinando las evaluaciones de probabilidad y gravedad. Por ejemplo, si la probabilidad del riesgo se ha evaluado como "Ocasional" (4) y la gravedad como "Peligrosa" (B), el índice de riesgo resultante sería 4B.

Tabla 3 – Tolerabilidad de riesgo de seguridad operacional

Probabilidad del Riesgo de Seguridad Operacional		Gravedad del Riesgo				
Probabilidad		**Catastrófico A**	**Peligroso B**	**Importante C**	**Leve D**	**Insignificante E**
Frecuente	**5**	**5A**	**5B**	**5C**	**5D**	**5E**
Ocasional	**4**	**4A**	**4B**	**4C**	**4D**	**4E**
Remoto	**3**	**3A**	**3B**	**3C**	**3D**	**3E**
Improbable	**2**	**2A**	**2B**	**2C**	**2D**	**2E**
Sumamente Improbable	**1**	**1A**	**1B**	**1C**	**1D**	**1E**

Nota. *Al determinar la tolerabilidad del riesgo, se debe considerar la calidad y confiabilidad de los datos utilizados para identificar el peligro y la probabilidad del riesgo de seguridad operacional.*

La Tabla 4 clasifica los riesgos en aceptables, tolerables o intolerables, y propone medidas a tomar según el índice de riesgo. Continuando con el ejemplo anterior, donde el índice 4B corresponde a la categoría de "Intolerable". En ese caso, el índice de riesgo de seguridad operacional es inaceptable y la organización debe tomar medidas de control para reducir el nivel de riesgo (mitigarlo), ya sea:

a) Reduciendo la exposición al riesgo: Disminuyendo el componente de probabilidad del índice de riesgo a un nivel aceptable.
b) Reduciendo la gravedad de las consecuencias: Disminuyendo el componente de gravedad del índice de riesgo a un nivel aceptable.
c) Reduciendo tanto la gravedad como la probabilidad: Para que el riesgo pueda gestionarse a un nivel aceptable.

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

Tabla 4 – Tabla de tolerabilidad del riesgo de seguridad operacional

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

Evaluación de riesgos relacionados con factores humanos.
La gestión de riesgos debe considerar el impacto de los factores humanos, ya que las personas pueden ser tanto fuente como solución a los peligros de seguridad operacional. Esto se debe a que:

a) Las personas pueden contribuir a un accidente o incidente debido a limitaciones humanas.
b) Las personas pueden prever y adoptar medidas para evitar situaciones de peligro.
c) Las personas pueden resolver problemas, tomar decisiones y adoptar medidas para mitigar los riesgos.

Por lo tanto, es fundamental involucrar a personas con experiencia en factores humanos en la identificación, evaluación y mitigación de riesgos. La gestión de riesgos efectiva debe abordar todos los aspectos de la seguridad operacional, incluyendo aquellos relacionados con las personas.

La evaluación de riesgos relacionados con el desempeño humano es más compleja que la de los factores de riesgo relacionados con la tecnología y el entorno. Esto se debe a:

- Variabilidad del desempeño humano: El desempeño humano es altamente variable y está influenciado por una amplia gama de factores internos y externos. La interacción entre estas influencias puede ser difícil o imposible de predecir con precisión.
- Dependencia del contexto: Las consecuencias de la variabilidad en el desempeño humano varían según la tarea que se realice y el contexto en el que se lleve a cabo.

Estrategias de mitigación de riesgos de seguridad operacional.
Las estrategias de mitigación de riesgos de seguridad operacional son acciones que generalmente implican cambios en los procedimientos operativos, equipos o infraestructura. Estas estrategias se clasifican en tres categorías principales:

a) Evitar: implica cancelar o evitar completamente la operación o actividad que presenta el riesgo, eliminando así el riesgo de seguridad operacional por completo. Esta estrategia se elige cuando los riesgos superan los beneficios de continuar la operación.
b) Reducir: Consiste en disminuir la frecuencia de la operación o actividad, o implementar medidas para minimizar la magnitud de las consecuencias en caso de que el riesgo se materialice.
c) Segregar: Busca aislar los efectos de las consecuencias del riesgo, por ejemplo, estableciendo barreras físicas o implementando sistemas redundantes de protección.

Una estrategia de mitigación puede involucrar uno o varios de estos enfoques. Es crucial analizar todas las posibles medidas de control para determinar la solución óptima. La eficacia de cada estrategia debe evaluarse cuidadosamente antes de tomar una decisión.

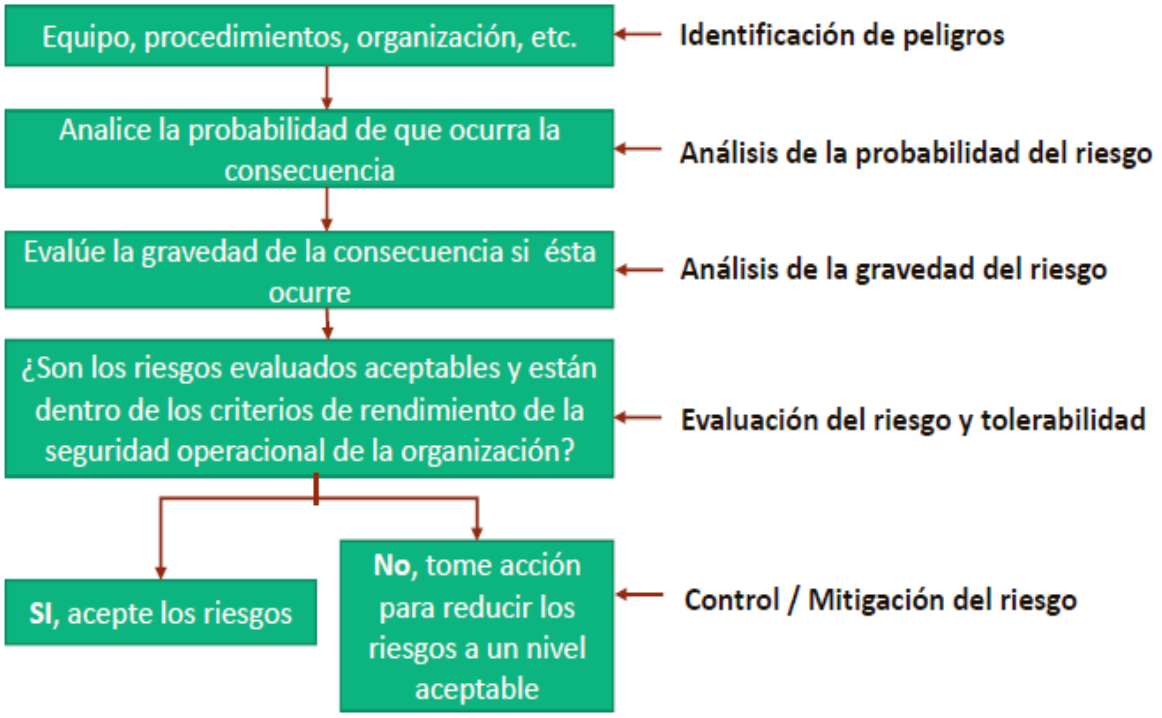
Al evaluar las alternativas de mitigación, se deben considerar los siguientes aspectos:
a) Eficacia: Capacidad de la alternativa para reducir o eliminar los riesgos de seguridad operacional. Se debe analizar cómo las defensas técnicas, de instrucción y normativas contribuyen a la reducción o eliminación del riesgo.
b) Costo/beneficio: Comparación entre los beneficios de la mitigación y los costos asociados a su implementación.
c) Practicidad: Factibilidad de implementar la mitigación considerando los recursos tecnológicos, financieros y administrativos disponibles, así como la legislación vigente, la voluntad política, las realidades operacionales, entre otros.
d) Aceptabilidad: Grado de aceptación de la alternativa por parte del personal que deberá implementarla y cumplirla.
e) Cumplimiento: Capacidad de monitorear/vigilar y garantizar el cumplimiento de las nuevas normas, regulaciones o procedimientos operativos implementados.
f) Duración: Sostenibilidad y eficacia de la mitigación a largo plazo.
g) Riesgo Residual: Nivel de riesgo de seguridad operacional que persiste después de implementar la mitigación inicial. Este riesgo residual puede requerir medidas de control adicionales.
h) Consecuencias Adicionales: Identificación de nuevos peligros y riesgos de seguridad operacional que podrían surgir a raíz de la implementación de la alternativa de mitigación.
i) Tiempo: El tiempo requerido para implementar la alternativa de mitigación de riesgo de seguridad operacional.

Las medidas de mitigación deben tener en cuenta las defensas existentes y su capacidad para alcanzar un nivel de riesgo aceptable.

Documentación de la evaluación de riesgos de la seguridad operacional.
Es fundamental documentar todas las actividades relacionadas con la gestión de riesgos de seguridad operacional. Esto incluye:
- La justificación y los datos utilizados para la evaluación de la probabilidad y la gravedad.
- Las decisiones tomadas durante el proceso.
- Todas las medidas de mitigación de riesgos implementadas.

Esta documentación se puede realizar utilizando hojas de cálculo, tablas o cualquier otro formato que permita un registro claro y organizado. La sección 10 de esta circular de asesoramiento proporciona un formato de gestión de riesgos que incluye los requisitos mínimos para la revisión y análisis de

riesgos de seguridad operacional.



Consultar el Apéndice 1 para conocer las mejores prácticas para la identificación de peligros.

Taxonomías.
Las taxonomías sobre peligros son especialmente importantes. A menudo la identificación de un peligro es la primera etapa en el proceso de gestión de riesgos.

Comenzar con un lenguaje reconocido en común hace que los datos de seguridad tengan más significado, sean más fáciles de clasificar y de procesamiento más sencillo.

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

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

a) Claramente identificable
b) Descrito en el estado deseado (controlable); y
c) Identificado por medio de nombres aceptados.

Algunos ejemplos de taxonomías son los siguientes:

a) Modelo de la aeronave: la organización puede construir una base de datos con todos los modelos certificados para operar.
b) Aeropuerto: la organización puede utilizar los códigos de la OACI. O de la Asociación del Transporte Aéreo Internacional (IATA) para identificar los aeropuertos.
c) Tipo de suceso: la organización puede utilizar taxonomías elaboradas por la OACI y otras organizaciones internacionales para clasificar sucesos.

Las taxonomías más comunes empleadas en la industria aeronáutica son:

a) ADREP: taxonomías de categorías de sucesos que integra el sistema de notificación de

accidentes e incidentes de la OACI. Constituye una recopilación de atributos y valores conexos que permitan realizar análisis de tendencias de seguridad operacional en esas categorías.

b) Equipo de taxonomía común del CAST y OACI por la CICTT

En la tabla 5 se observa un extracto de la taxonomía de peligros elaborada por el CICTT.

Tabla 5 – Ejemplos de taxonomía típica ANSP

Tipo de operación ***Type of operation***	**Tipo de actividad/ infraestructura/sistema** ***Type of activity /infrastructure/system***	**Código inglés**	**Ejemplos de peligros** ***Examples of Hazards***
ANS *ANSP*	Patrón de Tráfico *Traffic Pattern*	TTP-01	Complejidad del tráfico (mezcla de tipos de aeronaves) *Traffic complexity (mixture of aircraft type)*
		TTP-02	Excesivas aeronaves en el patrón o en un espacio aéreo determinado *Excessive aircraft in pattern or given airspace*
		TTP-03	Diseño y flujo del modelo de tráfico ineficaz *Ineffective design and flow of traffic pattern*
		TTP-04	Incursiones en pista de aeronaves o vehículos *Runway incursions by aircraft or vehicles*
		TTP-05	Vuelos no autorizados entrando en el modelo de tráfico *Unauthorized flights entering into traffic pattern*
		TTP-06	Procedimientos no autorizados de las aeronaves *Unauthorized procedures by aircraft*
		TTP-07	Señales que suenan similares o llamadas confusas *Similar sounding or confusing call signs*
		TTP-08	Ausencia de, o deficientes, procedimientos para aeronaves en peligro *Lack of or poor procedures for aircraft in distress*
	Espacio Aéreo *Airspace*	TAS-01	Espacio aéreo insuficiente para el tráfico típico *Insufficient airspace for typical traffic*
		TAS-02	Espacio aéreo distribuido inadecuadamente *Improperly distributed airspace*
		TAS-03	Espacio aéreo combinado durante tráfico excesivo *Airspace combined during excessive traffic*
		TAS-04	Etiquetado confuso de fijos o puntos de paso *Confusing labeling of fixes or way points*
		TAS-05	Procedimientos instrumentales desarrollados de forma inadecuada *Improperly developed instrument procedures*
		TAS-06	Aeronaves que realizan de forma incorrecta procedimientos de aproximación frustrada *Aircraft incorrectly performing missed approach procedures*
		TAS-07	Mezcla de criterios de procedimientos instrumentales nacionales y de la OACI *Intermingling of ICAO and national instrument procedure criteria*
	Acciones del Controlador *Controller Actions*	TCA-01	Autorización incompleta *Incomplete clearances*
		TCA-02	Errores en la identificación de las aeronaves y los objetivos (radar) *Misidentification of aircraft or targets (radar)*

Tipo de operación ***Type of operation***	**Tipo de actividad/ infraestructura/sistema** ***Type of activity /infrastructure/system***	**Código inglés**	**Ejemplos de peligros** ***Examples of Hazards***
		TCA-03	Lectura inadecuada de las instrucciones de autorización *Improper reading of clearance instructions*
		TCA-04	Pérdida de separación entre las aeronaves *Loss of separation between aircraft*
		TCA-05	Pérdida de separación entre la aeronave y el terreno o los obstáculos *Loss of separation between aircraft and terrain or obstacles*
		TCA-06	Mala interpretación de los deseos del piloto *Misinterpretation of pilot desires*
		TCA-07	Juicio incorrecto de las características de la aeronave *Incorrect judgment of aircraft characteristics*
	Comunicaciones *Communications*	TCO-01	Comunicaciones incorrectas, confusas o incompletas entre el personal del ATC y del aeródromo *Incorrect, confusing, or incomplete communications between ATC and aerodrome personnel*
		TCO-02	Comunicaciones incorrectas, confusas o incompletas entre el l ATC y la aeronave *Incorrect, confusing, or incomplete communications between ATC and aircraft*
		TCO-03	Comunicaciones incorrectas, confusas o incompletas entre instalaciones del ATC *Incorrect, confusing, or incomplete coordination between or within ATC facilities*
		TCO-02	Fallos o anomalías de Radio/Frecuencia *Radio/Frequency failures or anomalies*
		TCO-04	Fallos o anomalías en las ayudas a la Navegación (radares, satélites, VOR, ADS-B, etc.) *Navigational aid (radars, satellites, VOR, ADS-B, etc) failures or anomalies*
		TCO-05	Diferencias en la fraseología de OACI y del Control de Tráfico Aéreo nacional *Differences in ICAO and national Air Traffic Control phraseology*
		TCO-06	No utilizar la fraseología estándar de la aviación internacional *Not using the standard international aviation language*
		TCO-07	Barreras lingüísticas (Múltiples lenguas) *Language barriers (Multiple languages)*
		TCO-08	Ausencia de, o errónea, información aeronáutica *Lack of, or wrong aeronautical information*
	Instalaciones *Facilities*	TNF-01	Sistemas defectuosos de suministro de energía eléctrica en aeropuertos o ayudas para la navegación (radares, satélites, VOR, ADS-B, etc.) *Faulty electrical power supply systems on airport or navigational aids (radars, satellites, VOR, ADS-B, etc.)*
		TNF-02	Señalización o iluminación del campo de vuelo defectuosa, incorrecta o incompleta *Faulty, incorrect or incomplete airfield markings or lighting*
		TNF-03	Iluminación de aproximación defectuosa, incorrecta o incompleta *Faulty, incorrect, or incomplete approach lighting*
		TNF-04	Complejidad del sistema de pistas y rodadura *Taxiway and runway system complexity*

Tipo de operación *Type of operation*	Tipo de actividad/ infraestructura/sistema *Type of activity /infrastructure/system*	Código inglés	Ejemplos de peligros *Examples of Hazards*
		TNF-05	Drenaje inadecuado del campo de vuelo o del terreno *Inadequate airfield or terrain drainage*
		TNF-06	Equipamiento, radios, infraestructura o personal, insuficiente *Insufficient equipment, radios, infrastructure, or personnel*

Por lo que el proveedor de servicios podrá ocupar dichas taxonomías para el análisis de riesgos que requiera presentar ante la DGAC.

Medidas de mejora de la seguridad.
Cualquier peligro real o potencial en el sistema ATM debe ser evaluado y clasificado según su riesgo. Si el riesgo es inaceptable, se deben implementar medidas para eliminarlo o reducirlo a un nivel aceptable. La implementación de estas medidas debe ser prioritaria y se debe evaluar su efectividad para mitigar el riesgo.

Nota: *Este contenido subraya la importancia de un enfoque proactivo para la gestión de la seguridad en la ATM. Las evaluaciones de seguridad son cruciales para identificar y mitigar los riesgos asociados a los cambios en el sistema, mientras que las medidas de mejora de la seguridad se implementan para abordar los peligros existentes y garantizar un nivel aceptable de seguridad en las operaciones aéreas.*

Formato para registrar un análisis de riesgos de seguridad operacional.
Para desarrollar una base de datos de análisis de riesgos de seguridad operacional, podrá presentar la tabla 6 cuyo contenido no es limitativo, donde tendrá que estar debidamente llenado; así mismo con evidencia documental para su revisión.

Tabla 6. Formato para la gestión de riesgos.

Peligro genérico	Peligro especifico	Taxonomía del Peligro	Consecuencia (s)	Nivel de Riesgo	Barreras con las que se cuenta	Medidas de Mitigación	Tiempo de implementación	Responsable de Implementación	Nivel de Riesgo Residual
1			2	3	4	5	6	7	8

Nota. En caso de utilizar alguna taxonomía y/o considera dividir el peligro genérico y peligro especifico podrá crear otra columna indicando “Peligro Genérico y Peligro Específico”.

Instructivo de llenado del formato de análisis de riesgos.

a) Debe llenarse a computadora e imprimirse o llenarse a mano con letra legible
b) En caso de no aplicar alguna de las casillas deberán llenarse colocando N/A
c) Debe considerarse la siguiente guía de llenado:

Casilla 1: Definir todos los posibles peligros que pudieran estar inherentes en la operación a desarrollar.
Casilla 2: Determinar las consecuencias de los peligros previamente identificados.
Casilla 3: Analizar en términos de probabilidad y gravedad las consecuencias definidas de los peligros identificados.
Casilla 4: Analizar las barreras con las que se cuenta a fin de disminuir la probabilidad de ocurrencia.
Casilla 5: Definir los controles de seguridad operacional e implementar para cada consecuencia determinada, acordes a los niveles de tolerabilidad establecidos, lo anterior a fin de que permitan desarrollar la actividad dentro de un nivel de riesgo ACEPTABLE.
Casilla 6: Definir un periodo de tiempo para la implementación de los controles de seguridad operacional establecidos.
Casilla 7: Asignar a una persona responsable de llevar a cabo la implementación de los controles seguridad operacional con la finalidad de que estos sean implementados en tiempo y forma.

Casilla 8: Determinar el nivel de riesgo residual toda vez que se hayan establecido las medidas de mitigación, a fin de determinar si los riesgos de las consecuencias de cada peligro identificado se encuentran en un nivel aceptable.

Sistema de notificación de seguridad operacional.

Notificaciones de seguridad operacional.

Un mecanismo importante para la identificación proactiva de peligros es un sistema voluntario de notificación de seguridad operacional. El ATSP ya tiene requisitos de notificaciones obligatorias. Los sistemas de notificación de sucesos obligatorios tienden a recopilar más información técnica (fallas de equipos, incidentes ATS entre otros) que los aspectos relacionados con el rendimiento humano. Para abordar la necesidad de una mayor variedad de notificaciones de seguridad operacional, el ATSP también debe implementar un sistema de notificación voluntario de seguridad operacional. Esto tiene como objetivo adquirir más información, incluidos los aspectos relacionados con los factores humanos, y mejorar la seguridad de la aviación. El alcance de este esquema de notificaciones de seguridad operacional también incluye sucesos que normalmente no se informan a las autoridades. Los objetivos del plan de notificación de sucesos son:

- Permitir una evaluación de las implicaciones para la seguridad operacional de cada incidente y accidente, incluidos sucesos anteriores de naturaleza similar, de modo que se pueda iniciar cualquier acción necesaria; y
- Asegurar que el conocimiento de cuasi-accidentes, incidentes y accidentes relevantes se difunda de manera efectiva, para que otros puedan aprender de ellos.

Los beneficios de que el ATSP tenga una política de presentación de notificaciones es que todos comprendan claramente los valores de la organización con respecto a la presentación de notificaciones de información relacionada con la seguridad operacional y cómo fomenta una cultura de notificación saludable.

La política de notificación podría combinarse con la Política de seguridad operacional y debería:

- animar a los empleados a notificar sobre peligros, incidentes o accidentes; y
- definir las condiciones bajo las cuales se consideraría una acción disciplinaria punitiva (por ejemplo, actividad ilegal, negligencia, mala conducta intencional).

Se debe alentar al personal de todos los niveles y de todas las disciplinas a identificar y notificar peligros y otros problemas de seguridad a través de sus sistemas de notificaciones de seguridad operacional. Para ser efectivos, los sistemas de notificaciones de seguridad operacional deberán ser fácilmente accesibles para todo el personal. Dependiendo de la situación, se puede utilizar un formulario en papel, en la web o de escritorio.

Tener disponibles múltiples métodos de entrada maximiza la probabilidad de participación del personal. Todos deben conocer los beneficios de las notificaciones de seguridad operacional y lo que se debe notificar.

Por lo anterior, una de las principales fuentes para identificar peligros es el sistema de notificaciones de seguridad operacional, especialmente el sistema voluntario de notificación de seguridad operacional. Mientras que el sistema obligatorio se utiliza normalmente para los incidentes que se han producido, el sistema voluntario proporciona un canal de notificación adicional para potenciales problemas de seguridad operacional tales como peligros, cuasi-accidentes o errores.

Es importante que el ATSP brinde las protecciones adecuadas para alentar a las personas a notificar lo que ven o experimentan. Por ejemplo, la obligación de cumplimiento reglamentario puede no aplicarse a las notificaciones de errores o, en algunas circunstancias, a la ruptura de reglas. Debería indicarse claramente que la información presentada se utilizará únicamente para respaldar la mejora de la seguridad operacional. La intención es promover una cultura de notificación efectiva y la identificación proactiva de potenciales deficiencias de seguridad operacional.

Los sistemas de notificación voluntarios de seguridad operacional deberán ser confidenciales, lo que requiere que toda la información de identificación del notificante sea conocida solo por el custodio para permitir el seguimiento de las acciones. El rol del custodio debe mantenerse en unos pocos individuos,

por lo general restringido al Responsable de seguridad operacional y al personal involucrado en la investigación de seguridad operacional.

Mantener la confidencialidad ayudará a facilitar la divulgación de los peligros que conducen al error humano, sin temor a represalias o vergüenza. Las notificaciones voluntarias de seguridad operacional se pueden desidentificar y archivar una vez que se toman las medidas de seguimiento necesarias. Las notificaciones desidentificadas pueden respaldar futuros análisis de tendencias para rastrear la efectividad de la mitigación de riesgos e identificar los peligros emergentes.

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

Cualquiera que envíe una notificación de seguridad operacional debería recibir comentarios sobre qué decisiones o acciones se han tomado. La alineación de los requisitos del sistema de notificación, las herramientas y los métodos de análisis puede facilitar el intercambio de información de seguridad operacional, así como la comparación de ciertos indicadores de rendimiento seguridad operacional. La retroalimentación a los notificadores en los esquemas de notificación voluntario también sirve para demostrar que tales informes se consideran seriamente.

Esto ayuda a promover una cultura de seguridad operacional positiva y estimula las notificaciones futuras.

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

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

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

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

El proceso de identificación de peligros considera todos los peligros posibles que puedan existir dentro del alcance de las actividades de aviación del ATSP, incluidas las interfaces con otros sistemas, tanto dentro como fuera de la organización. Una vez identificados los peligros, se deben determinar sus consecuencias (es decir, cualquier suceso o resultado específico).

Peligros relacionados con las interfaces de SMS con organizaciones externas.
Las organizaciones también deberían identificar los peligros relacionados con sus interfaces de gestión de seguridad operacional. En la medida de lo posible, esto debería llevarse a cabo como un ejercicio conjunto con las organizaciones interconectadas. La identificación de peligros debe

considerar el entorno operativo y las diversas capacidades organizacionales (personas, procesos, tecnologías) que podrían contribuir a la entrega segura del servicio o la disponibilidad, funcionalidad o desempeño del producto.

Por ejemplo, un incidente ATS involucra al personal que provee el servicio como también a las tripulaciones de vuelo que realizaron las maniobras evasivas. Es probable que existan peligros relacionados con las interfaces entre el personal operativo, su equipo y la coordinación en las operaciones aéreas.

Identificación de interfaces de los SMS de terceros.
La realización de un ejercicio o taller de mapeo de la actividad empresarial con las partes interesadas clave a menudo identificará interfaces SMS de las que una organización no necesariamente es plenamente consciente. Estas pueden ser interfaces donde no existe un acuerdo formal, como suministro de energía o servicios de mantenimiento de edificios, por ejemplo. Si la organización ya cuenta con alguna forma de planificación de la continuidad del negocio, este podría ser un buen punto de partida, ya que gran parte del trabajo ya se habrá realizado.

Una vez que se han identificado las interfaces de SMS, la organización debe considerar su importancia relativa. Esto permite a la organización priorizar la gestión de las interfaces más críticas y sus riesgos potenciales de seguridad operacional. Las cosas a considerar son:

- lo que se proporciona
- por qué es necesario
- si la organización involucrada tiene un SMS u otro sistema de gestión implementado, o posee algún tipo de certificación (por ejemplo, de un organismo profesional)
- si la interfaz implica el intercambio de datos/información de seguridad operacional.

Evaluación del impacto de las interfaces en la seguridad operacional.
Luego, la organización debería identificar cualquier peligro para la seguridad operacional relacionado con las interfaces de terceros y llevar a cabo una evaluación de riesgos utilizando sus procesos existentes de identificación de peligros y evaluación de riesgos. Con base en los riesgos de seguridad operacional identificados, puede ser beneficioso considerar trabajar con la (s) otra (s) organización (es) para determinar y definir una estrategia apropiada de control de riesgos de seguridad.

Involucrar a otras organizaciones les permitirá contribuir a identificar peligros, evaluar el riesgo de seguridad operacional, así como determinar el control de riesgo de seguridad operacional adecuado. También es importante reconocer que cada organización tiene la responsabilidad de identificar y gestionar los riesgos que afectan su propio negocio. Esto puede significar que la criticidad de la interfaz es diferente para cada organización, ya que pueden aplicar diferentes clasificaciones de riesgos de seguridad y tener diferentes prioridades de riesgos de seguridad operacional (en términos de rendimiento de seguridad operacional, recursos, tiempo, etc.).

Para ayudar a priorizar los recursos y el nivel de gestión y monitoreo requerido, puede ser beneficioso desarrollar una tabla simple que agrupe a los terceros según el nivel de riesgo de seguridad operacional que traen a la organización (por ejemplo, terceros de aviación, proveedores de servicios comerciales, terceros gubernamentales, etc.).

Gestión y supervisión de interfaces.
El ATSP es responsable de administrar y monitorear las interfaces para garantizar la provisión segura de servicios y productos. Esto garantizará que las interfaces se gestionen de forma eficaz y se mantengan actualizadas y relevantes. Los acuerdos formales, como los contratos y los acuerdos de nivel de servicio, son una forma eficaz de lograr esto, ya que las interfaces y las responsabilidades asociadas pueden definirse claramente.

Además de cualquier consideración comercial, el contrato o acuerdos a nivel servicio debe incluir:

- aclaración de las funciones y responsabilidades de cada organización, incluidas las autoridades encargadas de la toma de decisiones
- acuerdo de decisiones sobre las acciones a tomar (por ejemplo, acciones de control de riesgos de seguridad operacional y escalas de tiempo)
- identificación de qué información de seguridad operacional debe compartirse y comunicarse

(por ejemplo, notificaciones de seguridad operacional, los resultados de las investigaciones y auditorías, etc.)
- cómo y cuándo debe llevarse a cabo la coordinación (reuniones periódicas, reuniones especiales o específicas, requisitos de auditoría, etc.)
- cualquier arreglo de supervisión o instrucción
- objetivos de rendimiento de seguridad operacional, cuando corresponda
- acciones necesarias como resultado de la activación de ERP.

Cualquier cambio en las interfaces y los impactos asociados deben comunicarse a las organizaciones relevantes. Todos los problemas o riesgos de seguridad operacional relacionados con las interfaces deben documentarse y ponerse a disposición de cada organización para compartirlos y revisarlos. Esto permitirá compartir las lecciones aprendidas y la puesta en común de información de seguridad operacional que será valiosa para ambas organizaciones. Los beneficios de la seguridad operacional pueden lograrse mediante una mejora de la seguridad operacional alcanzada por cada organización, como resultado de la propiedad compartida de los riesgos y la responsabilidad de la seguridad operacional.

Existen algunos desafíos asociados con la capacidad de la organización para gestionar los riesgos de seguridad de la interfaz que incluyen:
- Los controles de riesgo de seguridad de una organización no son compatibles con los de la otra organización.
- disposición de ambas organizaciones para aceptar cambios en sus propios procesos y procedimientos
- recursos o experiencia técnica insuficientes disponibles para administrar y monitorear la interfaz
- el número y la ubicación de las interfaces.

Superar estos desafíos, como para cualquier otro desafío empresarial, requiere una combinación de habilidades blandas (como la capacidad de establecer relaciones y comunicarse), habilidades técnicas (como la gestión de riesgos) y un marco o sistema que describa las expectativas y los procesos en uso por las partes interesadas.

Los humanos en el sistema.
Cómo piensan las personas sobre sus responsabilidades hacia la seguridad operacional y cómo interactúan con los demás para realizar sus tareas en el trabajo afectan significativamente el rendimiento de seguridad operacional del ATSP. La gestión de la seguridad operacional debe abordar cómo las personas contribuyen, tanto positiva como negativamente, a la seguridad operacional organizacional. Los factores humanos se tratan de: comprender las formas en que las personas interactúan con el mundo; sus capacidades y limitaciones; e influir en la actividad humana para mejorar la forma en que las personas hacen su trabajo. Como resultado, la consideración de los factores humanos es una parte integral de la gestión de la seguridad operacional, necesaria para comprender, identificar y mitigar los riesgos, así como para optimizar las contribuciones humanas a la seguridad operacional organizacional.

Existen algunas herramientas que ayudan a una organización a reconocer los peligros relacionados al rendimiento humano a ser incluidos en la seguridad operacional:
- El modelo de "queso suizo" (Reason) para la causalidad de accidentes.
- El modelo SHELL utilizado para ilustrar el impacto y la interacción de los diferentes componentes del sistema en el ser humano (Software: procedimientos, instrucción, soporte; Hardware: máquinas y equipos; Medio ambiente: el entorno de trabajo en el que debe funcionar el resto del sistema LHS; Liveware - otras personas en el lugar de trabajo).
- La "Docena Sucia" de Dupont: una lista de doce de las condiciones previas de error humano más comunes, o condiciones que pueden actuar como precursoras de accidentes o incidentes.
- Entre otros.

Investigación de peligros.
La identificación de peligros deberá ser continua y formar parte de las actividades en curso de la organización. Algunas condiciones pueden ameritar una investigación más detallada. Estos pueden incluir:
- instancias en las que el ATSP experimenta un aumento inexplicable de sucesos relacionados

con la seguridad operacional o incumplimiento normativo;
- cambios significativos en la organización o sus actividades.

Desarrollar un proceso de identificación del sistema de peligros.
Un proceso de identificación de peligros permite recopilar, registrar, analizar, actuar y generar retroalimentación sobre los peligros que afectan la seguridad operacional de las actividades realizadas por el ATSP. La alineación en el diseño de los requisitos del sistema de notificaciones, las herramientas y los métodos de análisis puede facilitar el intercambio de información de seguridad operacional, así como las comparaciones de ciertos indicadores de rendimiento de seguridad operacional. En un SMS maduro, la identificación de peligros es un proceso continuo. Los siguientes son algunos pasos para la captura de información identificada como peligros, cuya estructura variará dependiendo de la dimensión y complejidad del ATSP.

Comunicarse y consultar.
Para lograr los objetivos de seguridad operacional del ATSP, se requiere un nivel apropiado de participación de la fuerza laboral. A menudo, los miembros de la fuerza laboral están en la mejor posición para comprender y articular los peligros involucrados en sus tareas diarias. Su participación puede facilitar la identificación efectiva y precisa de peligros nuevos o modificados y riesgos asociados, y la identificación y desarrollo de medidas de control prácticas y efectivas.

La comunicación y la consulta con la fuerza laboral establecerán el marco ideal para que el personal presente notificación de peligros y permita un procesamiento eficiente dentro de los plazos identificados. Según la dimensión y la complejidad del ATSP, se considera lo siguiente:
- los tipos de peligros que probablemente se notificarán y el diseño de un medio de notificación adecuado en torno a este
- cómo hacer que el mecanismo de presentación de notificaciones sea accesible, fácil de usar y lo más intuitivo posible
- cómo el personal puede acceder y enviar notificaciones de la manera más eficiente, dada la tecnología disponible para los informes en línea.

Analizar notificaciones de peligros de seguridad operacional.
El análisis de las notificaciones de seguridad operacional es necesario para validar el contenido de las notificaciones, establecer cualquier tendencia (buena o mala) y evaluar la importancia de la información notificada, es decir, el potencial de causar o contribuir a un incidente o accidente de aeronave. Esto ayudará a la organización a identificar los riesgos de seguridad operacional y sus posibles consecuencias y, por lo tanto, determinará las prioridades para las acciones de seguridad operacional posteriores. La evaluación de las consecuencias del riesgo y las estrategias de control asociadas son parte del proceso de gestión del riesgo (consulte el elemento de evaluación y mitigación de riesgos de seguridad operacional). Por lo tanto, el análisis eficaz de las notificaciones de seguridad operacional se convierte en una fuente clave de información para la gestión de riesgos de seguridad operacional.

Recopilación, almacenamiento y distribución de datos
Los resultados de la identificación de peligros forman la base de los pasos posteriores del proceso de gestión de riesgos, a saber, la evaluación de riesgos y las medidas de control. Los principales requisitos son que para la documentación de identificación el peligro:
- muestre claramente los vínculos entre peligros, eventos peligrosos, causas subyacentes y medidas de control cuando sea apropiado
- contiene un sistema de numeración de peligros y controles para permitir una fácil identificación y seguimiento
- contiene información suficiente para respaldar los pasos posteriores de la gestión de riesgos
- es fácil de administrar
- los registros de identificación de peligros pueden acomodar directamente el proceso de revisión y actualización del conocimiento de peligros, detalles de peligros, incidentes, medidas de control, lecciones de incidentes y accidentes, etc.
- se gestiona bajo un sistema de control de documentos. Dependiendo de la dimensión y la complejidad del ATSP, un sistema electrónico para la gestión de los peligros identificados puede ser más fácil de usar para el mantenimiento de registros.

Si las organizaciones necesitan transmitir o recibir notificaciones de seguridad operacional hacia o desde un tercero, considere utilizar un medio eficaz de transferencia de información que sea apropiado para las necesidades de la organización.

Evaluación y mitigación de riesgos de seguridad operacional.

Comprensión.
La SRM requiere el análisis de los riesgos de seguridad operacional para determinar la gravedad y la probabilidad asociadas con los peligros identificados. Varias orientaciones/métodos se encuentran disponibles para analizar el riesgo.

Se debe evaluar el riesgo de seguridad operacional para determinar su aceptabilidad. Puede utilizarse un método cuantitativo o cualitativo apropiado. Los aspectos a considerar en la evaluación pueden incluir aspectos técnicos, procesos, comportamientos humanos y organizacionales (incluida la gestión de interfaces).

Es necesaria una evaluación de riesgos del producto. Una gran parte de esto podría estar ya controlada en el marco del cumplimiento de otros reglamentos:

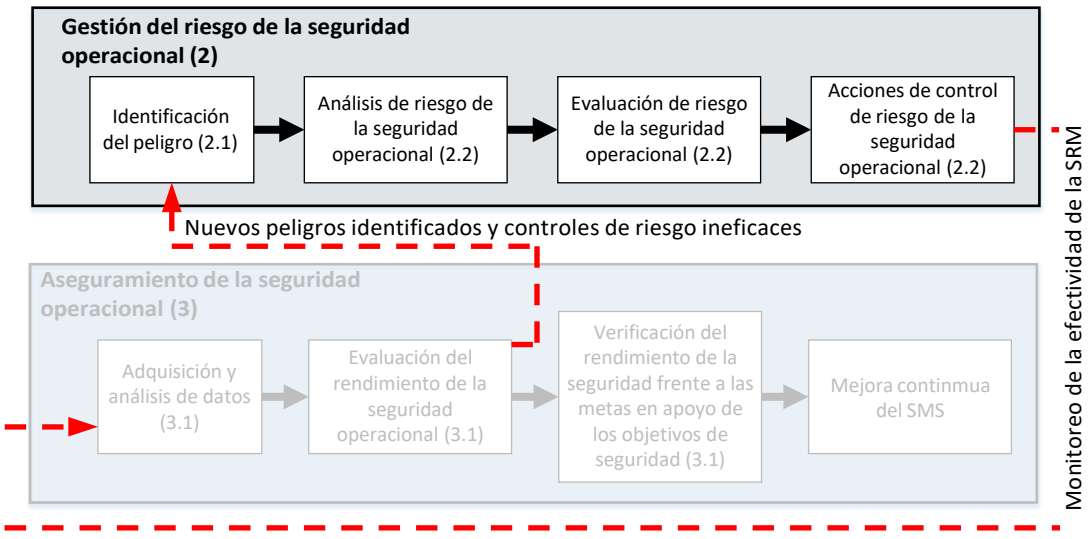
- La aceptabilidad de los riesgos de seguridad operacional durante la provisión de los servicios de tránsito aéreo debe basarse en la consideración de los requisitos ATS aplicables y la garantía de que no existe ninguna condición insegura. Un producto en una condición insegura implica un riesgo de seguridad operacional inaceptable y requiere una gestión de riesgos de seguridad operacional adecuada.

La evaluación de riesgos del producto deberá completarse con una evaluación de riesgos sistémicos con el fin de abordar también los aspectos humanos y organizacionales.

La evaluación y mitigación de riesgos deben incluir las siguientes actividades:

- Descripción del sistema.
- Identificación de peligros y consecuencias.
- Estimación de la gravedad y probabilidad de las consecuencias de la ocurrencia del peligro.
- Evaluación del riesgo y toma de decisiones asociadas.
- Mitigación de riesgos y medidas de seguridad operacional.
- Reclamaciones, argumentos y evidencia de que las acciones de seguridad operacional se han cumplido y documentado en un caso de seguridad operacional.

Pasos de la SRM



Medios de cumplimiento.
Depende de la organización seleccionar los métodos y herramientas que se implementarán con el propósito de la gestión de riesgos de seguridad operacional.

El juicio de ingeniería/evaluación cualitativa deberá considerarse como un medio mínimo aceptable para identificar y evaluar los riesgos de seguridad operacional.

Se pueden utilizar varios métodos, técnicas y herramientas para la identificación de peligros y la evaluación de riesgos. Cualquiera que sea el método seleccionado, la evaluación de riesgos siempre debe centrarse en los impactos sobre la seguridad operacional del producto en funcionamiento:

- Técnicas de evaluación de riesgos (fuente ISO 31010):
  - Lluvia de ideas.
  - Lista de verificación.
  - Análisis de causa raíz.
  - Análisis de modos y efectos de falla (FMEA).
  - Análisis de árbol de fallas (FTA).
  - Árbol de decisiones.
  - Análisis de Bow tie.
  - Simulación de Monte Carlo.
  - Matriz de consecuencias / probabilidades.
- Sistema Europeo de Clasificación de Riesgos (ERCS) (fuente: publicado como vinculado al reglamento de la UE 2015/1018).
- Matriz de evaluación de riesgos de seguridad operacional (fuente CS / FARxx.1309).
- Métodos de análisis de riesgos a nivel de producto (fuente: SAE ARP4761):
  - Evaluación de riesgos funcionales (FHA).
  - Evaluación preliminar de seguridad operacional del sistema (PSSA).
  - Evaluación de la seguridad operacional del sistema (SSA).
  - Diagramas de dependencia.
  - Análisis de Markov.
  - Análisis de seguridad operacional zonal (ZSA).
  - Análisis de causa común (CCA).

Nota. No es posible ni deseable realizar evaluaciones de riesgos de seguridad operacional para todos los cambios. Solo los cambios que potencialmente tengan un impacto sustancial en la seguridad operacional o la gestión de la seguridad operacional están sujeta a la SRM o ambos.

El ATSP ya tiene las bases principales para recolectar, analizar y mitigar los riesgos relacionados con el servicio que ofrecen.

Este proceso, que incluye recopilación de fallas, mal funcionamiento y defectos, análisis de riesgos y acciones para la realización de operaciones aérea seguras, es un factor importante para la SRM y una entrada al proceso de aseguramiento de la seguridad operacional.

5.3. Componente 3 – Aseguramiento de la seguridad operacional.

El aseguramiento de la seguridad operacional (SA) se basa en las siguientes actividades:

- Control y medición del rendimiento de la seguridad operacional.
- Proceso de gestión de cambios.
- Mejora continua del SMS.

El SA deberá lograrse mediante el seguimiento de las actividades del SMS. Por lo tanto, el SA requiere el seguimiento, la recopilación y el análisis de datos, y la evaluación del rendimiento.

La medición del rendimiento de la seguridad operacional se entiende mejor como una evaluación de la capacidad para gestionar el riesgo. Es una determinación del éxito de los procesos en la gestión del riesgo y la eficacia resultante de los controles de riesgo implementados, tanto desde la perspectiva del producto como del ATSP.

El SA también requiere un proceso para gestionar cambios que monitorea cambios sustanciales en el entorno operacional, ya sean planeados o no planeados, autoinducidos o como resultado de

influencias externas, para asegurar que los cambios no conducirán a riesgo inaceptable. Los cambios sustanciales en el SMS también necesitan una evaluación para medir que el rendimiento del SMS no se degrada.

El SA también se utiliza para identificar áreas y para impulsar la mejora continua de los procesos de SMS.

El SA es un proceso reiterativo en el que los requisitos de rendimiento evolucionarán con la madurez de SMS.

El SMS deberá diseñarse de manera que los controles ineficaces, los peligros nuevos o los peligros potenciales identificados por la evaluación del rendimiento de la seguridad operacional se retroalimenten al proceso de SRM para la identificación de peligros, análisis de riesgos, evaluación de riesgos y control de riesgos.

¿Cómo realizar la adquisición de datos?

La adquisición de datos de seguridad operacional en el contexto del control y medición del rendimiento de seguridad operacional es un insumo principal para verificar el nivel de logro del SMS versus los objetivos de seguridad operacional y para mejorar continuamente el SMS. Los medios para la adquisición de datos deberán ser identificados y utilizados por el aseguramiento de la seguridad operacional. Esto puede depender de medios ya implementados, como el sistema de recopilación utilizado para el ATSP cuando lo exigen los reglamentos aplicables, o el monitoreo de las operaciones de la organización en busca de fallas, defectos y fallas de calidad que podrían resultar en un riesgo inaceptable para la seguridad operacional de la aviación. El proceso de adquisición de datos debe incluir datos recopilados en el contexto del seguimiento de proveedores.

Para la adquisición de datos se debe establecer lo siguiente:

- Interfaces con los explotadores aéreos y ATSP, en particular para fomentar el intercambio de datos de seguridad operacional.
- Interfaces con las autoridades
- Canales para recopilar información interna.

Los datos pueden ser:

- Cuantitativo: se utiliza para identificar y proporcionar una imagen más clara del "área" que se mide. Las medidas estadísticas se utilizan generalmente para este esfuerzo.
- Cualitativo: las fuentes de datos, como las notificaciones de seguridad operacional de los empleados y los análisis causales en profundidad en los informes de accidentes, son generalmente cualitativos. Este enfoque es valioso para la identificación de peligros.

Ejemplos de datos relacionados con productos:

- Número de sucesos informados a la organización (de fuentes internas, externas o ambas).
- Número de sucesos notificados a las autoridades.
- Número de sucesos recurrentes.
- Número de fallas en la provisión del servicio, clasificados por criticidad con respecto a la seguridad operacional.
- Número de errores dentro de las instrucciones ATC.

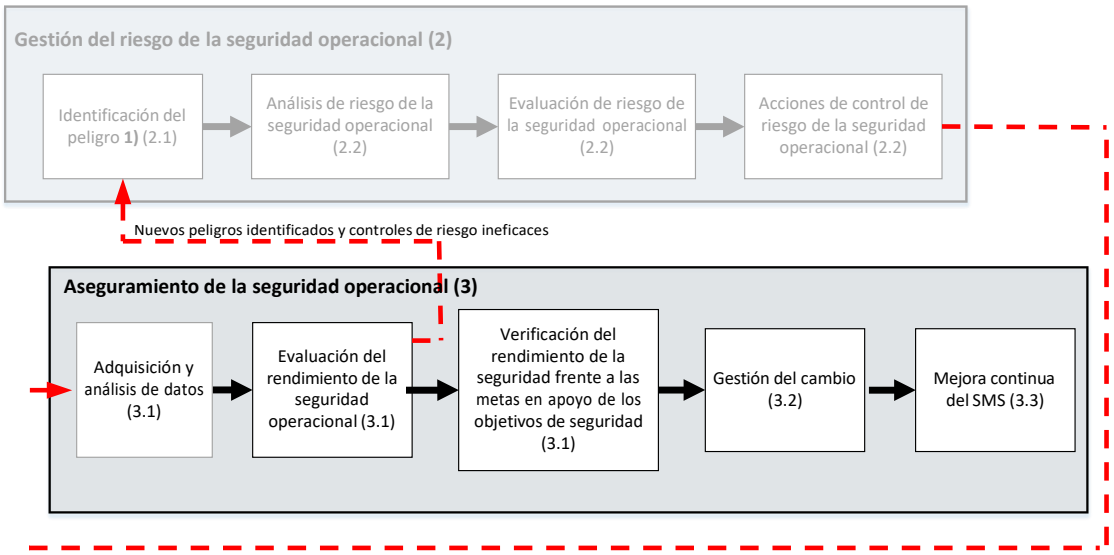
Ejemplos de datos relacionados con el rendimiento del ATSP:

- Estado de las iniciativas en curso que contribuyen a los objetivos de seguridad operacional.
- Estado de las acciones de mitigación de riesgos.
- Asistencia a revisiones de SMS.
- Número de empleados capacitados en temas de seguridad operacional.
- Respuesta a tiempo a los hallazgos relacionados con la seguridad operacional (por ejemplo: auditorías internas; auditorías de la AAC).
- Gestión de recursos o competencias (por ejemplo: cumplimiento de puestos clave de seguridad operacional como personal de gestión de seguridad operacional, personal ATC o ambos).
- Factores relacionados con el entorno operativo (por ejemplo, ruido y ergonomía, temperatura, iluminación y disponibilidad de equipo).
- Deficiencias identificadas en la gestión de interfaces.

Los ejemplos antes mencionados de datos recopilados deben procesarse o analizarse o ambos para establecer indicadores de rendimiento relevantes.

Se requiere que la organización recopile datos para respaldar el aseguramiento de la seguridad operacional. Esto puede incluir, entre otros: notificaciones de datos automáticos, un sistema obligatorio de notificación de sucesos, revisiones sistemáticas o auditorías, o un sistema voluntario de notificación de los empleados, o ambos, según la política de cultura justa y puede ser uno de los medios para adquirir datos. Todos los empleados deben conocer los sistemas que se utilizan que son apropiados para sus funciones y dónde hay sistemas disponibles para permitir la notificación anónima de datos (por ejemplo, peligros potenciales y, si están disponibles, soluciones propuestas o mejoras de seguridad operacional).

Observación y medición del rendimiento en materia de seguridad operacional.
Pasos del aseguramiento de la seguridad operacional



Comprensión.
La intención del SMS del ATSP es lograr una SRM exitoso. El proceso de la SRM no puede ser de bucle abierto; por lo tanto, el proceso de la SA debe incluir medios para monitorear el rendimiento del SMS, tanto en su funcionalidad (operación del SMS) como en la efectividad de los controles de riesgo que produce (seguridad operacional del producto).

La SRM es fundamental para el funcionamiento del SMS. Si se implementa correctamente, proporcionará al ATSP los medios para determinar si sus actividades y procesos están funcionando de manera efectiva para lograr sus objetivos de seguridad operacional. Esto se logra mediante la identificación de indicadores de rendimiento de seguridad operacional (SPI) y (cuando sea apropiado) metas, que se utilizan para monitorear y medir el rendimiento de seguridad operacional. Una vez hecho esto, la organización debería documentar y comunicar los resultados al personal (y a los clientes) Para que tengan clara la relación entre la política de seguridad operacional - los objetivos de seguridad operacional asociados - los objetivos relacionados con cada objetivo - el SPI relacionado con cada objetivo y cualquier meta.

La gestión del rendimiento de la seguridad operacional ayuda al ATSP a formular y responder cuatro preguntas importantes sobre la gestión de la seguridad operacional:

- ¿Cuáles son los principales riesgos de seguridad operacional del ATSP?
- ¿Qué quiere lograr el ATSP en términos de seguridad operacional y cuáles son los principales riesgos de seguridad operacional que deben abordarse? (objetivos de seguridad operacional de la organización).
- ¿Cómo sabrá el ATSP si está progresando hacia sus objetivos de seguridad operacional? (a través de SPI).

- ¿Qué datos e información de seguridad operacional se necesitan para tomar decisiones de seguridad operacional informadas? (incluida la asignación de los recursos de la organización).

Se espera que la organización realice una evaluación sobre cómo está rindiendo el SMS en comparación con los objetivos de seguridad operacional de la organización. Para ello el ATSP deberá desarrollar y mantener indicadores apropiados de rendimiento relacionados con la seguridad operacional.

Medios de cumplimiento.
La adquisición de datos a ser analizados, se realiza de acuerdo con criterios previamente establecidos que deben ser proporcionales a la diversidad, complejidad y criticidad de los servicios de tránsito aéreo. Independientemente de qué parte de la organización esté a cargo de procesar los datos recopilados y de implementar las acciones correctivas, los datos deben informarse a la función del SA con el fin de evaluar el rendimiento de la seguridad operacional.

Los indicadores de rendimiento de seguridad operacional (SPI) se utilizan para ayudar a la alta dirección a saber si es probable que la organización logre su objetivo de seguridad operacional; pueden ser cualitativos o cuantitativos. Los indicadores cualitativos son descriptivos y se miden por calidad, como una imagen descriptiva de la situación de seguridad operacional (¿cómo se ve bien?). Los indicadores cuantitativos pueden expresarse como un número (cantidad de incidentes ATS). Sin embargo, el solo uso de números puede crear una impresión distorsionada de la situación real de seguridad operacional si el nivel de actividad fluctúa.

Por ejemplo, si el explotador aéreo reporta tres (3) incidentes ATS en el mes de julio y cinco (5) en el mes de agosto, puede haber una gran preocupación por el deterioro significativo en el rendimiento de seguridad operacional. Pero en agosto pueden haber realizado el doble de vuelos que en julio, lo que significa que los aumentos de incidentes ATS, o la tasa, han disminuido, no ha aumentado. Esto puede cambiar o no el nivel de escrutinio, pero proporciona otra información valiosa que puede ser vital para la toma de decisiones de seguridad operacional basada en datos.

Los indicadores cuantitativos son preferibles a los cualitativos porque se los puede contar y comparar más fácilmente. La elección del indicador depende de la disponibilidad de datos confiables que se puedan medir cuantitativamente. Importa plantearse si la evidencia necesaria debe estar en forma de datos comparables y generalizables (cuantitativos) o en forma de imágenes descriptivas de la situación de seguridad operacional (cualitativa). Cada opción, cualitativa o cuantitativa, entraña diferentes tipos de SPI que pueden lograrse de mejor manera mediante un proceso reflexivo de selección de SPI. Una combinación de enfoques resulta útil en muchas situaciones y puede resolver muchos de los problemas que pueden surgir de la adopción de un enfoque único.

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

Los SPI de resultados ayudan a la organización a comprender lo que ha sucedido en el pasado y son útiles para determinar tendencias a largo plazo. Se pueden utilizar como indicadores de alto nivel o como una indicación de tipos específicos de sucesos o ubicaciones, como “tipos de accidentes por tipo de aeronave” o “tipos de incidentes específicos por región”. Debido a que los indicadores de resultados miden los resultados de seguridad operacional, pueden medir la efectividad de las medidas de mitigación de la seguridad operacional. También resultan eficaces para validar el rendimiento de seguridad operacional general del sistema.

Los indicadores de resultado se dividen además en dos tipos: baja probabilidad/alta gravedad (accidentes o incidentes graves); alta probabilidad/baja gravedad: resultados que no necesariamente

resultaron en un accidente o incidente grave, también conocidos como indicadores precursores.

Las medidas de seguridad operacional de la aviación han estado históricamente sesgadas hacia los SPI que reflejan resultados de “baja probabilidad/alta gravedad”. Esto es comprensible ya que los accidentes e incidentes graves son sucesos de alto perfil y son fáciles de contar. Sin embargo, desde una perspectiva de gestión de rendimiento en materia de la seguridad operacional, existen inconvenientes en una dependencia excesiva de accidentes e incidentes graves como un indicador fiable del rendimiento en materia de seguridad operacional.

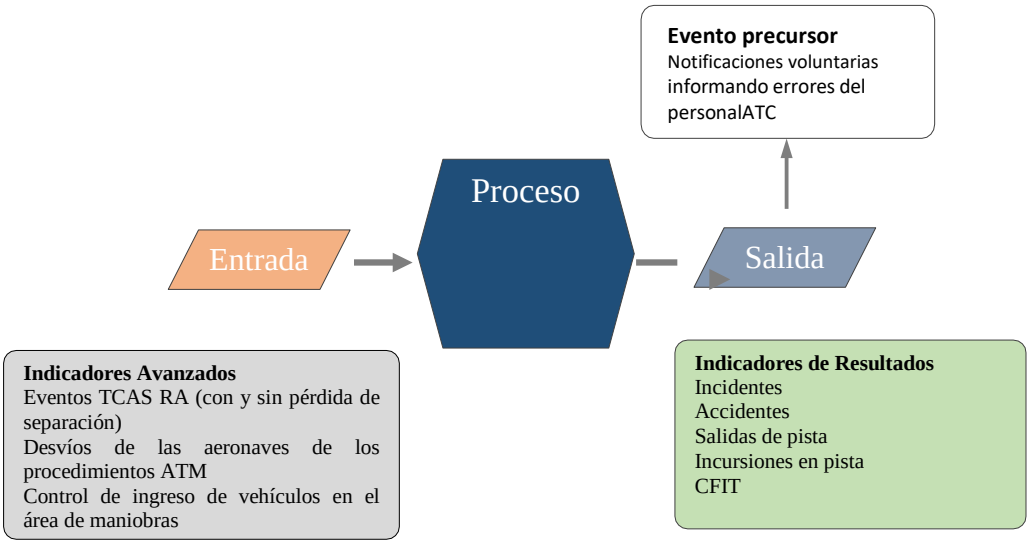
Por ejemplo, los accidentes e incidentes graves son poco frecuentes (puede haber un solo accidente en un año, o ninguno) lo que hace difícil la realización de análisis estadísticos para identificar tendencias. Esto no indica necesariamente que el sistema es seguro. Una consecuencia de confiar en este tipo de datos es un falso sentido de confianza potencial en que el rendimiento en materia de seguridad operacional de una organización o sistema es eficaz, cuando de hecho puede estar peligrosamente cerca de un accidente.

Los indicadores avanzados son medidas que se centran en los procesos y aportes que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como “SPI de actividad o proceso” dado que vigilan y miden las condiciones que tienen el potencial de convertirse en un resultado específico o contribuir al mismo. Los ejemplos de SPI avanzados que impulsan al desarrollo de capacidades organizativas para la gestión proactivo del rendimiento en materia de seguridad operacional comprenden cosas tales como "porcentaje de personal que ha completado con éxito la instrucción en seguridad operacional a tiempo" o "frecuencia de las notificaciones voluntarias".

Los SPI avanzados también pueden informar a la organización sobre cómo su operación se enfrenta al cambio, incluyendo los cambios en su entorno operacional. La atención se centrará en anticipar puntos débiles y vulnerabilidades como resultado del cambio o la supervisión del rendimiento después de un cambio.

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

Indicador avanzado vs indicador de resultado



Es probable que la selección inicial de los SPI se limite a la observación y medición de parámetros

que representan sucesos o procesos que son fáciles o convenientes de captar (datos de seguridad operacional que pueden estar fácilmente disponibles). Idealmente, los SPI deberían enfocarse en parámetros que son indicadores importantes del rendimiento en materia de seguridad operacional, en lugar de aquellos que son fáciles de alcanzar y deberán ser:

- relacionados con el objetivo de seguridad operacional que pretenden indicar;
- seleccionados o desarrollados en base a datos disponibles y mediciones fiables;
- apropiadamente específicos y cuantificables; y
- realistas, teniendo en cuenta las posibilidades y limitaciones de la organización.

Documentar los indicadores de rendimiento de seguridad operacional.
En cuanto a los objetivos de seguridad operacional, los indicadores de rendimiento de seguridad operacional deberán cambiar periódicamente para apoyar la mejora continua. Por esta razón, es mejor documentar el proceso para establecer el SPI y cualquier meta asociada dentro del SMS/Documento de seguridad operacional de la organización, con el SPI real publicado fuera del manual, lo que facilita su actualización.

Metas de rendimiento de seguridad operacional.
Las metas de rendimiento en materia de seguridad operacional (SPT) definen los logros deseados de rendimiento en la materia a corto y mediano plazo. Actúan como “hitos” que proporcionan la confianza de que la organización está en el camino correcto para lograr sus objetivos de seguridad operacional y proporcionan una forma mensurable de verificar la eficacia de las actividades de gestión del rendimiento en materia de seguridad operacional. La configuración de las SPT deberá tener en cuenta factores como el nivel predominante del riesgo de seguridad operacional, la tolerabilidad de los riesgos de seguridad operacional y las expectativas con respecto a la seguridad operacional del sector de la aviación en particular y la madurez del SMS del ATSP.

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

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

Establecimiento de metas con objetivos de seguridad SMART.
Los objetivos de seguridad operacional pueden ser difíciles de comunicar y pueden parecer difíciles de lograr; al dividirlos en metas de seguridad operacional concretos más pequeños, el proceso de entrega es más fácil de gestionar. De esta manera, las metas forman un vínculo crucial entre la estrategia y las operaciones del día a día. Las organizaciones deberán identificar las áreas clave que impulsan el rendimiento en seguridad operacional y establecen una forma de medirlas. Una vez que el ATSP tiene una idea de cuál es su nivel de rendimiento actual mediante el establecimiento de una

línea base de rendimiento en materia de seguridad operacional, puede comenzar a configurar las SPT para proporcionar el ATSP un claro sentido de lo que deberían aspirar a lograr. El ATSP también puede utilizar la evaluación comparativa para ayudar a establecer metas de rendimiento. Esto implica usar información de rendimiento de ATSP similares (siempre que sea posible obtener la información a través de la compartición de la información) que ya han estado midiendo su rendimiento para tener una idea de cómo les está yendo a otros ATSP.

.

Se recomienda que los ATSP comiencen por apuntar a las tasas de tendencia de aumento (por ejemplo, aumento de la tasa de notificación de peligros) o disminución (por ejemplo, reducción de eventos LHD), en lugar de cifras arbitrarias (por ejemplo, reducción del 20%) hasta que el SMS haya estado funcionando durante mucho tiempo. suficiente para proporcionar datos fiables en los que basar objetivos específicos.

Consideraciones adicionales para la selección de SPI y SPT.

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

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

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

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

- Fomento de comportamientos deseados. Las SPT pueden modificar comportamientos y contribuir a resultados deseados. Esto es especialmente importante si el logro de la meta se relaciona con recompensas por parte del ATSP. Las SPT deberían fomentar comportamientos organizacionales e individuales positivos que resulten deliberadamente en decisiones justificables y mejoras del rendimiento en materia de seguridad operacional. Al seleccionar SPI y SPT es igualmente importante tener en cuenta posibles comportamientos no deseados.

- Elección de medidas valiosas. Es fundamental seleccionar SPI útiles, y no solo aquellos cuya medición sea fácil. El ATSP debería decidir cuáles son los parámetros de seguridad operacional más útiles, o sea los que orienten al ATS¨P a la mejora de sus decisiones, gestión del rendimiento en materia de seguridad operacional, y logro de sus objetivos de seguridad operacional.

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

Advertencias para el establecimiento de SPT.

No siempre es necesario o apropiado definir las SPT dado que podría haber SPI más fáciles de

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

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

- Metas operacionales; concentrarse demasiado en el logro de metas operacionales (entregas de aeronaves a tiempo, reducción de costos generales, etc.) sin equilibrar las SPT puede llevar al "logro de metas operaciones" aunque no necesariamente a una mejora del rendimiento en materia de seguridad operacional.

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

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

- Conflicto organizacional; las metas pueden crear conflictos entre dependencias internas del ATSP cuando discuten sobre quién recae la responsabilidad en vez de tratar de trabajar en conjunto.

¿Cómo medir la seguridad operacional?.
El SMS se ocupa de la seguridad operacional de la aviación (es decir, muertes o lesiones de pasajeros y tripulación a bordo, o muertes y lesiones de personas en tierra alrededor de la aeronave, o daños a la aeronave y al medio ambiente).

Debido a múltiples contribuyentes en la cadena de circunstancias que conducen a un suceso de seguridad operacional los datos recopilados para su procesamiento por el SMS de la organización son por naturaleza parciales y limitados.

El monitoreo del rendimiento de seguridad operacional puede necesitar considerar precursores potenciales y señales débiles (sucesos que podrían conducir potencialmente a accidentes / incidentes, pero no lo hicieron) debido a factores como la disminución del número de accidentes y la pequeña cantidad de sucesos de seguridad operacional reconocibles reales que se compensan con el continuo crecimiento del número de vuelos.

Cómo construir indicadores.
La SRM es la herramienta de SMS para estudiar sucesos potenciales. La SRM produce una evaluación de la criticidad relativa a la seguridad operacional de los sucesos que se procesan. Un SPI no puede ser una simple cantidad bruta de incidentes que se procesan, debe incluir un aspecto de evaluación que refleje la criticidad. Los resultados pueden expresarse en proporciones, promedios, tasas o tendencias.

Un tema reconocido es el tiempo necesario para observar los efectos de las medidas de mitigación, nuevamente debido a las bajas probabilidades de que ocurran sucesos reales. Un indicador deberá reflejar un tiempo de observación bastante largo (por ejemplo, promedios móviles durante cinco años), lo que lo hace inconveniente para la gestión a corto plazo del SMS.

Indicadores de rendimiento de seguridad operacional típicos.
El ATSP necesitará definir la categoría de sucesos que se considerarán para la recopilación y el

análisis de datos y los criterios para la evaluación, según su propia actividad (por ejemplo: eventos TCAS a causa de malas autorizaciones por el ATC).

En el Apéndice 4 se ha desarrollado la información correspondiente a los indicadores y metas de rendimiento de seguridad operacional.

Accidentes e incidentes.
El número de accidentes e incidentes graves reales constituye un indicador básico de seguridad operacional.

Se espera que los promedios móviles de 5 a 10 años sean adecuados.

El monitoreo de la aplicación (teniendo en cuenta los tiempos de reacción aceptables en relación con la criticidad) de las recomendaciones de seguridad operacional pertinentes de la AAC y AIG también puede constituir un indicador de seguridad operacional (por ejemplo, tiempo de implementación, cumplimiento del plan).

Clima de SMS.
Una evaluación cualitativa realizada por personas con sólida experiencia en la gestión de SMS del ATSP puede considerarse como un SPI válido (por ejemplo, una evaluación del nivel de implementación de la cultura de seguridad operacional de la organización).

Notificaciones voluntarias.
Las notificaciones voluntarias pueden identificar oportunidades de mejora, además de ser un indicador de una buena cultura de seguridad. Alentar al personal a informar cada peligro percibido permite al ATSP abordar los problemas identificados ("si no se informa, no se puede solucionar"). Múltiples notificaciones voluntarias no son necesariamente un signo de que una organización funciona mal, sino más bien un signo de una cultura de seguridad operacional madura. El número de notificaciones voluntarias se puede utilizar como un SPI.

Indicadores de operaciones de SMS típicos.
El seguimiento del rendimiento operacional del SMS (funcionamiento del SMS) puede requerir una adaptación de los indicadores al estado de implementación real del SMS. Los indicadores también pueden adaptarse al entorno específico del ATSP.

Durante las fases de implementación de SMS, los indicadores pueden ser específicos para medir el progreso del aumento de las actividades de SMS. Ejemplos de tales indicadores son:

- Estado de la nominación del personal clave de seguridad operacional.
- Despliegue y comunicación de políticas y objetivos: ¿A cuántas personas (porcentaje) de la organización se ha llegado?
- ¿Cuántas personas están capacitadas en SMS?
- ¿Cuántos documentos para el SMS se han preparado?
- Disponibilidad y madurez de las herramientas de información tecnológica (IT) necesarias para el SMS (por ejemplo, computadoras y servidores).

Por lo general, los requisitos cuantitativos y cualitativos de los ejemplos mencionados anteriormente deben incluirse en el plan de implementación para permitir la medición regular y el estado de los logros en la hoja de ruta de implementación.

Habiendo alcanzado una cierta madurez del SMS, los datos de SMS adquiridos y los datos de seguridad operacional pueden proporcionar evidencia sobre las operaciones del SMS. Los datos se pueden evaluar con métodos estadísticos que muestran proporción (ratios), promedios, tasas o tendencias. Ejemplos de tales indicadores adicionales son:

- Una tendencia positiva (disminución) en el número de eventos LHD respecto al número de operaciones de cierto periodo.
- Una tendencia positiva (aumento) en el número de notificaciones voluntarias en el ATSP (esto mostrará la adherencia a los principios de SMS).
- El tiempo de procesamiento de incidentes o acciones de mitigación o ambos (esto podría dividirse en la fase de definiciones / investigaciones y la fase de implementación real de las

acciones relacionadas).
- El número de entrada de peligros confirmados al SRM.

Los indicadores anteriores reflejan la madurez del SMS y podrían combinarse en una Matriz de Madurez de SMS para resumir y mapear el rendimiento operacional, y luego usarse para la comunicación.

Necesidad de medición adicional
La auditoría y otros medios de investigación, ya sean internos o externos, contribuyen al monitoreo del rendimiento en seguridad operacional, la adecuación y el cumplimiento de los procesos y procedimientos para garantizar que se sigan y ejecuten correctamente.

El monitoreo de las operaciones de SMS es una técnica complementaria útil para la evaluación diaria de la seguridad operacional, considerando que un sistema con buen rendimiento producirá resultados consistentes.

Las auditorías internas y externas contribuyen a la validación de los procesos de evaluación (y posiblemente a la recopilación de datos). Se espera que estas auditorías vayan más allá del cumplimiento y aborden la eficacia. Estas auditorías no son herramientas para establecer indicadores de seguridad operacional, pero se espera que generen "datos de SMS" para comprender y evaluar las operaciones del sistema.

Como uno de los medios de seguimiento, las auditorías podrían cubrir temas relacionados con:
- Organización (incluido el rendimiento de responsabilidades, gestión de recursos de conocimiento, documentación, medios y herramientas) y el despliegue y madurez de la cultura de seguridad operacional.
- SPI, que representa la efectividad de las mitigaciones y controles de riesgos en el contexto de la SRM.
- Efectividad de los procesos operacionales, tales como:
  - Servicios de control de aeródromo.
  - Servicios de control de aproximación.
  - Servicios de control de área.

Cómo comunicar la medición del rendimiento en seguridad operacional.
Se puede utilizar un dashboard de rendimiento de seguridad operacional para mostrar la medición del rendimiento de seguridad operacional del ATSP.

El dashboard de rendimiento de la seguridad operacional podría contener metas, indicadores, evaluaciones cualitativas o tendencias tanto para el rendimiento de la seguridad operacional del producto como para el rendimiento operacional de la organización de SMS. El contenido y la frecuencia de las actualizaciones del dashboard deben adaptarse a la madurez de la cultura de seguridad operacional del ATSP, a los resultados del rendimiento de la seguridad operacional y a la complejidad del ATSP.

Los indicadores de rendimiento están destinados a medir el progreso frente a los objetivos de seguridad operacional definidos por el ATSP. Deben estar sujetos a revisiones periódicas para garantizar su pertinencia continua.

Gestión del cambio.

Comprensión.
El ATSP experimenta cambios debido a la expansión o contracción, así como modificaciones a los sistemas de gestión existentes que pueden afectar el nivel de riesgo de seguridad operacional asociado con sus servicios. Podrían introducirse peligros inadvertidamente siempre que se produzca un cambio. Además, el cambio puede afectar la eficacia de los controles de riesgo de seguridad operacional existentes.

Si el ATSP elige usar métodos y procesos nuevos o no establecidos, o revisar sustancialmente los

existentes, deberá desarrollar y usar procesos de identificación de peligros para identificar condiciones nuevas o existentes que previsiblemente podrían conducir a un riesgo inaceptable.

No es posible ni deseable implementar un proceso de evaluación de riesgos de seguridad operacional para todos los cambios en el sistema. Solo los cambios que potencialmente tengan un impacto sustancial en la seguridad operacional están sujetos al proceso de SRM.

Medios de cumplimiento.
Aunque cada ATSP es único, una serie de características del entorno operacional son comunes o similares entre los ATSP. Por lo tanto, hay cambios típicos que podrían tener un impacto sustancial en la gestión de la seguridad operacional.

La descripción de un ATSP es fundamental para definir el alcance de la aplicabilidad del SMS y los posibles cambios a los que podría estar sujeto. Según el PANS-ATM, se consideran cambios significativos en un ATSP los siguientes casos, en los cuales se requiere que el ATSP lleve a cabo una gestión del cambio, incluyendo una evaluación de riesgos de seguridad operacional:

a) Modificaciones en la separación mínima entre aeronaves, esto abarca la reducción de la distancia mínima horizontal o vertical;
b) Introducción de un nuevo procedimiento de operación, incluidos los procedimientos de ruta, salida y de llegada por aplicar en determinado espacio aéreo o aeródromo;
c) Reestructuración del espacio áereo, tales como modificaciones en las rutas ATS, la sectorización del espacio aéreo o su clasificación;
d) Una nueva subdivisión por sectores de un determinado espacio aéreo;
e) Cambios en la infraestructura del aeródromo, como modificaciones físicas en la distribución de pistas y calles de rodaje; y
f) Implementación de nuevas tecnologías, como la incorporación de nuevos sistemas y equipo de comunicaciones, vigilancia u otros sistemas críticos para la seguridad, especialmente aquellos que proporcionan nuevas funciones o capacidades.

Nota 1. Se deben considerar no solo los riesgos asociados con el cambio, sino también los riesgos temporales de transición al implementar el cambio.

Nota 2. "cambio" deberá entenderse como un cambio en el sistema (por ejemplo, organización, responsabilidades, procesos) y su entorno operativo asociado y no directamente en el producto. Los cambios en el producto ya están controlados a través de otros requisitos reglamentarios.

Además el PSA ATPS deberá tener en cuentas otros cambios típicos, para los cuales se dan algunos ejemplos de cambios típicos incluyen:

- Cambios en la organización:
  - Cambio de MAE.
  - Reubicación.
  - Prestación de un nuevo servicio
  - Introducción de una nueva tecnología (por ejemplo, máquina, inspección).
  - Cambio en la organización (trabajo compartido internamente entre instalaciones o externamente con socios/proveedores).
  - Cambio en las partes de la organización que contribuyen directamente a la conformidad que se otorga.
  - Cambio a los principios de aseguramiento de la calidad o monitoreo independiente.
  - Cambio de proveedor(es).

- Cambios de responsabilidades:
  - Cambio del Gerente Responsable.
  - Cambio del Responsable de la seguridad operacional.
  - Cambios del personal clave.

- Cambios en los recursos:
  - Reducción sustancial del número, calificaciones y / o experiencia del personal.
  - Aumento sustancial de la plantilla.

La gestión del cambio podría depender del soporte de herramientas o métodos documentados dentro de algunos estándares de la industria, por ejemplo:

- 8 disciplinas para la resolución de problemas (8D);
- metodología de las 5M (mostrar interés, marcar estrategia, movilizar, medir y mantener);
- análisis de modos de fallas y efectos de procesos (PFMEA);

Disponibilidad de expertos en la materia: es importante que el personal clave esté disponible y participe en la gestión de los cambios. Esto puede incluir personas de organizaciones externas.

Muchas organizaciones subestiman la dimensión humana de la gestión del cambio. Esto se demuestra por el rendimiento pasado en la reestructuración y adaptación a diferentes requisitos donde la tasa de fallas es sorprendentemente alta, no debido a la estrategia, sino a la subestimación del factor humano. Las organizaciones también deberán considerar el impacto del cambio en el personal. Esto podría afectar la forma en que los afectados aceptan el cambio. La comunicación y el compromiso tempranos normalmente mejorarán la forma en que se percibe e implementa el cambio.

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

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

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

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

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

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

f. ***plan de aseguramiento***, esto es para determinar qué acción de seguimiento se necesita. Considerar cómo se comunicará el cambio y si se necesitan actividades adicionales (como auditorías) durante o después del cambio. Cualquier suposición hecha necesita ser probada.

El objetivo principal del proceso de gestión del cambio es asegurar que cualquier cambio implementado mantenga o mejore el nivel de seguridad operacional, evitando comprometer la seguridad de las operaciones aéreas.

Esta evaluación se lleva a cabo de forma meticulosa durante las etapas de planificación del espacio aéreo o al identificar desviaciones en la provisión de los Servicios de Tránsito Aéreo. En este último caso, se busca determinar el impacto de dichas desviaciones en relación con lo establecido en la Reglamentación Aeronáutica Boliviana RAB 211.390 y en el documento PANS ATM 2.6 sobre Evaluaciones de la Seguridad Operacional.

La gestión del cambio debe identificar medidas alternativas y de mitigación para garantizar la

seguridad de las operaciones, evaluar la eficacia de cada alternativa y, finalmente, recomendar procedimientos que compensen la desviación.

En este sentido, la implementación de cualquier cambio significativo en la gestión del tránsito aéreo queda supeditada a la demostración a la Autoridad Aeronáutica, a través de la evaluación de riesgos de seguridad operacional, de que los niveles de seguridad operacional se mantienen dentro de los límites aceptables. Es importante destacar que la evaluación de la seguridad operacional no concluye con la implementación de los cambios, sino que debe continuar de forma periódica para monitorear y verificar que los niveles de seguridad operacional se mantienen dentro de los parámetros establecidos. Finalmente, las evaluaciones de riesgos de seguridad operacional son uno de los tópicos considerados como actividades de GSO del ATS y deben estar plenamente documentadas.

Implementación de cambios.
Los cambios propuestos solo se implementarán si la evaluación de seguridad demuestra que se puede mantener un nivel aceptable de seguridad.

Cambios notificables al Gerente Responsable.
Las reglas de funcionamiento individuales especifican los cambios que requieren la aceptación previa del Gerente Responsable; esto incluye cambios en el sistema de gestión de seguridad operacional, si el cambio es un cambio material. Con la excepción de los cambios del responsable de la gestión de la seguridad operacional (ya enumerados en las reglas operativas como un cambio notificable), se considera que los cambios materiales son aquellos que afectan el rendimiento de un proceso o sistema fundamental que sustenta el sistema de gestión de la seguridad operacional, ejemplos de que incluye metodologías para:

- establecer metas, objetivos y medidas de rendimiento de seguridad operacional (nota: solo la metodología del proceso, no las medidas individuales)
- la identificación de peligros y gestión de riesgos
- el desarrollo del programa de auditoría
- la revisión por la dirección.

Cambios en el programa de instrucción en seguridad operacional, p. Ej. cambios de alto nivel en el programa (Silabus) de instrucción en seguridad operacional.

Para las organizaciones con un sistema aceptado para la gestión de la seguridad operacional, las presentaciones que respalden dichas solicitudes de cambio deben incluir evidencia de que se ha aplicado su proceso de gestión del cambio.

Mejora continua del SMS.

Comprensión.
La mejora continua de SMS es un proceso gradual y continuo que se enfoca en aumentar la efectividad y eficiencia de una organización para cumplir con su política y objetivos de seguridad operacional.

La mejora continua deberá aumentar el rendimiento con planes de acción que se basan en el monitoreo y la medición del rendimiento de la seguridad operacional.

Medios de cumplimiento.
Para que el ATSP pueda verificar el cumplimiento de estos procesos, realizará exámenes de la seguridad operacional en las dependencias ATS de forma regular y sistemática, mediante un procedimiento establecido y de conocimiento de la AAC, a cargo de personal calificado mediante la instrucción, experiencia adecuada, conocimientos necesarios y que tenga una comprensión completa de la normativa vigente, procesos internos, y las prácticas de funcionamiento seguras.

Los exámenes de la seguridad operacional realizados por el ATSP deben ser verificados por la AAC, por lo tanto, el ATSP debe asegurarse de la aplicación efectiva y cumplimiento de las acciones de mitigación propuestas, así como la verificación de cumplimiento de lo estipulado en la legislación nacional, lo que quiere decir, que el proceso es similar a una auditoria interna en temas específicos.

La organización debería considerar los resultados de las mediciones del rendimiento de la seguridad operacional al definir acciones de mejora continua para el SMS.

Sobre la base de los datos de seguridad operacional recopilada, el ATSP debería garantizar que:

- se hace análisis de datos a nivel organizacional para establecer un plan de acción, con los grupos de interés a cargo de la implementación de las acciones. El plan de acción debe abordar las causas fundamentales de las fallas o mal funcionamiento a nivel del sistema donde el rendimiento de seguridad operacional no ha alcanzado el nivel esperado.
- se implementan acciones de mejora.
- se consideran las mejores prácticas y lecciones aprendidas para mejorar el SMS. Además, estas mejores prácticas deben difundirse en todo el ATSP mediante actividades de promoción de la seguridad.

En el contexto de la mejora continua, las revisiones de SMS con miembros de la dirección del ATSP deben organizarse con una frecuencia y formato acordes al nivel de riesgos y la complejidad del ATSP. Los resultados de la revisión del SMS deben proporcionarse como entradas a la SRM.

Nota. La revisión de SMS puede ser parte de una "revisión de gestión" según se define en los estándares del sistema de gestión. Dependiendo del ATSP, la revisión de SMS específica podría implementarse como entrada para una revisión de gestión de nivel superior.

La evaluación de la eficacia de un SMS no deberá basarse únicamente en los SPI; las organizaciones deberán utilizar una variedad de métodos para determinar su eficacia, medir los productos y los resultados de los procesos y evaluar la información recopilada a través de estas actividades. Dichos métodos, como se describe con más detalle en "Revisión por la Dirección", puede incluir:

- revisiones de la gestión
- auditorías
- seguimiento de sucesos
- evaluaciones; incluye evaluaciones de la cultura de seguridad operacional y la efectividad del SMS
- encuestas de seguridad operacional
- abordar las lecciones aprendidas.

Los exámenes de la seguridad operacional mediante la identificación de deficiencias aportan a la continua sustentabilidad, suficiencia y eficacia del SMS del ATSP mediante un proceso que permite revisiones internas regulares, por lo tanto, es necesario identificar áreas de posible mejora que garantice el cumplimiento de la normativa vigente y reglamentos internos.

Estos exámenes son requeridos en cada dependencia ATS para conseguir:

- Que el servicio sea siempre de la máxima calidad; y
- Que todas las dependencias y personal apliquen criterios, normas, reglas, procedimientos y mínimas de separación de manera adecuada.

Normalmente, los exámenes ATS abarcan todos o parte de los siguientes aspectos:

- Determinar el servicio proporcionado a los usuarios, en cuanto a aspectos de normalización, calidad, idoneidad, eficiencia y eficacia;
- Conseguir que los procedimientos operacionales se ajusten a las normas nacionales;
- Determinar y hacer recomendaciones concernientes a las exigencias operativas;
- Detectar todo procedimiento o práctica potencialmente insegura, de modo que sea posible tomar medidas correctivas inmediatas;
- Detectar deficiencias, determinar su causa probable y recomendar las medidas correctivas que se juzguen oportunas;
- Examinar la eficacia de las comunicaciones y coordinación entre dependencias y en el interior de estas;
- Examinar las cualificaciones del personal ATC en las dependencias ATS.

En caso de que se identifiquen casos de no cumplimiento y otros problemas, los mismos deben ser investigados y analizados para poder determinar la causa raíz de las deficiencias detectadas, en consecuencia, los exámenes de la seguridad operacional resultan más eficaces cuando estas son

realizadas por personal que no están involucrados en la provisión del servicio, lo que quiere decir, que se recomienda la rotación del personal para realizar los exámenes de la seguridad operacional en las diferentes dependencias ATS.

Por otra parte, para cumplir con la periodicidad de los exámenes de la seguridad operacional, estos plazos deben estar especificados en el procedimiento para la realización de los mismos, como también, se deben tomar en cuenta los resultados de exámenes de seguridad operacional anteriores como las acciones de mitigación propuestas.

La mejora continua solo puede ocurrir con una supervisión constante sobre la implementación y efectividad de las mitigaciones o recomendaciones realizadas. Por lo tanto, una de las principales tareas de este proceso es verificar y controlar los resultados de las mitigaciones del examen de la seguridad operacional.

El personal designado debería realizar los exámenes de la seguridad operacional en base a la frecuencia recomendada mínima de por lo menos cada 2 años, sin embargo, en las dependencias ATS que los encargados de los exámenes de la seguridad operacional tengan base laboral en las mismas, estos exámenes deberían ser parte de un proceso constante, particularmente en relación a la competencia del personal.

Antes de iniciar los exámenes de la seguridad operacional, usualmente se notifica de ello al encargado de la dependencia de que se trate, para que en el caso de ser necesario, se realicen las coordinaciones con otras partes interesadas como ser el personal CNS, jefatura de aeropuerto entre otros. Quizá en algunos casos sea necesario organizar consultas con los explotadores aéreos u organismos militares.

Para la realización de los exámenes de la seguridad operacional, se podría tomar en cuenta lo siguiente, como también, el ATSP podría agregar otros factores que considere necesario:

- ✓ Determinación del cumplimiento
    1. ¿Existe el proceso o procedimiento requerido?
    2. ¿Está documentado el proceso o procedimiento?
    3. ¿Satisface el proceso o procedimiento los requisitos?
    4. ¿Se está aplicando el proceso o procedimiento?
    5. ¿Aplica sistemáticamente el proceso o procedimiento todo el personal afectado?
    6. ¿Se obtienen los resultados definidos?
    7. ¿Se ha documentado e implementado algún cambio en el proceso o procedimiento?

- ✓ Evaluación de la eficacia
    1. ¿Comprenden los usuarios el proceso o procedimiento?
    2. ¿Se logra sistemáticamente el propósito del proceso o procedimiento?
    3. ¿Son los resultados del proceso o procedimiento los que el “cliente” pidió?
    4. ¿Se examina regularmente el proceso o procedimiento?
    5. ¿Se realiza una evaluación de riesgos de seguridad operacional cuando se han introducido cambios en el proceso o procedimiento?
    6. ¿Han producido las mejoras del proceso o procedimiento los beneficios esperados?

Por lo tanto, los procesos de un examen de la seguridad operacional contribuyen a la capacidad del ATSP de lograr la mejora continua en materia de seguridad operacional.

Actividad consistente en un examen y revisión de los procesos y actividades del ATSP, para verificar conformidad respecto a lo establecido en su SMS.

Competencias requeridas del personal.
El personal que va a realizar los exámenes de la seguridad operacional debe contar con los conocimientos y habilidades necesarios de acuerdo a lo siguiente:

- ✓ El tamaño, naturaleza y complejidad del ATSP
- ✓ Parte del sistema al que se va a realizar el examen de seguridad operacional
- ✓ Objetivo y alcance del examen de la seguridad operacional

- ✓ Experiencia adecuada
- ✓ Conocimiento de la normativa vigente
- ✓ Conocimiento de las normas internas de ATSP

Por otra parte, el personal podría contar con cualidades necesarias que les permita actuar de acuerdo a los principios de una auditoria, que pueden ser adoptados para realizar los exámenes de la seguridad operacional, lo que quiere decir un comportamiento profesional como ser:

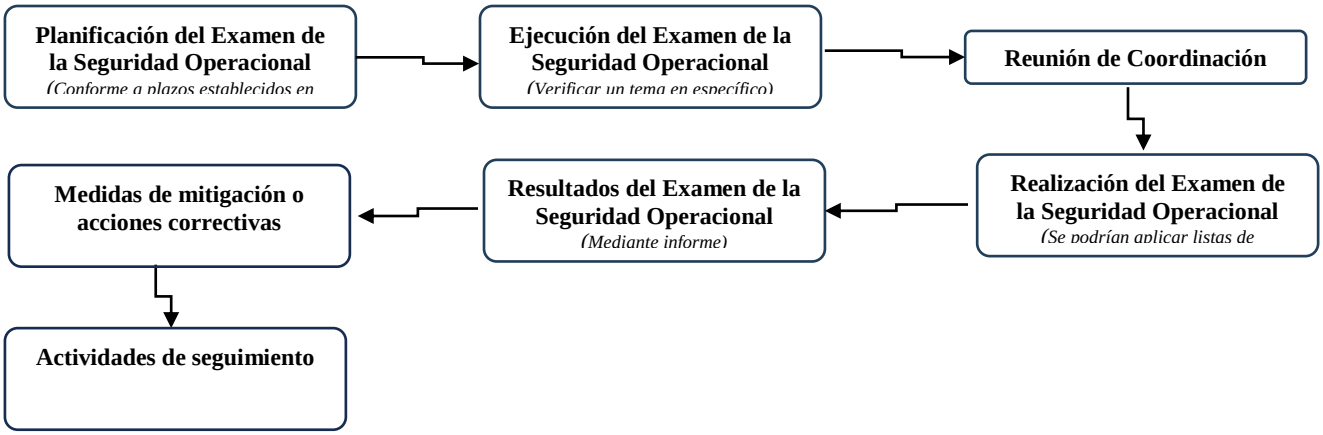
- ✓ Ético, es decir, imparcial, sincero, honesto y discreto;
- ✓ Mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos;
- ✓ Diplomático, es decir, con tacto en las relaciones con las personas;
- ✓ Observador, es decir, activamente consciente del entorno físico y las actividades;
- ✓ Perceptivo, es decir, instintivamente consciente y capaz de entender las situaciones;
- ✓ Tenaz, es decir, persistente, orientado hacia el logro de los objetivos;
- ✓ Decidido, es decir, alcanza conclusiones oportunas basadas en el análisis y razonamiento lógico;
- ✓ Actúa con fortaleza, es decir, es capaz de actuar ética y responsablemente aun cuando dichas acciones no siempre sean populares y a veces puedan resultar en desacuerdo o confrontación;
- ✓ Sensible culturalmente, es decir, observante y respetuosos de la cultura del auditado o inspeccionado;

De la misma manera, es recomendable que este personal demuestre un comportamiento personal de acuerdo a lo siguiente:

- ✓ Aplicar principios, procedimientos y técnicas establecidas;
- ✓ Planificar y organizar el trabajo eficazmente;
- ✓ Llevar a cabo el examen de seguridad operacional dentro del horario acordado;
- ✓ Establecer prioridades y centrarse en los asuntos de importancia;
- ✓ Recopilar información a través de entrevistas eficaces, escuchando, observando y revisando documentos, registros y datos;
- ✓ Entender y considerar las opiniones de los expertos;
- ✓ Verificar la relevancia y exactitud de la información recopilada;
- ✓ Confirmar que la documentación presentada es suficiente y apropiada para apoyar los hallazgos y conclusiones;
- ✓ Utilizar documentos de trabajo para registrar las actividades a ser realizadas;
- ✓ Entender los tipos de riesgos asociados al no cumplimiento de ciertos requisitos.

Examen de seguridad operacional

Un Sistema de Seguridad Operacional requiere retroalimentación y análisis del mismo para identificar deficiencias en el sistema conforme a los establecido en el Documento 4444 de la OACI, por lo tanto, es necesario corregir las fallas que puedan identificarse, las cuales se concentran en evaluar periódicamente el estado de los controles de riesgos y otras herramientas establecidas en el sistema, como también, se utilizan para asegurar que el sistema y el personal que es parte del mismo cumplan los procedimientos adecuados, tenga la capacitación pertinente y tenga una estructura estable y sólida. A continuación, se detallan los pasos para poder realizar los exámenes de la seguridad operacional:



Los procesos del examen de la seguridad operacional respaldan las mejoras al SMS mediante la verificación continua y las medidas de seguimiento, por lo tanto, es recomendable que el ATSP desarrolle un procedimiento para la ejecución de los exámenes de la seguridad operacional.

Estrategia de implementación.
El ATSP una vez tenga seleccionado el personal adecuado para la ejecución de exámenes de la seguridad operacional, funcionalmente independiente como también, el procedimiento requerido que determine los pasos a seguir para la ejecución de esta actividad, se debe establecer un cronograma para la ejecución de exámenes de la seguridad operacional y la periodicidad de los mismos.

La evaluación de las actividades del proveedor de servicios de tránsito aéreo, puede proporcionar información útil a los procesos de toma de decisiones del proveedor.

Planificación del examen de la seguridad operacional.
Dentro de la planificación de las actividades del ATSP, se deben tomar en cuenta un programa de exámenes de la seguridad operacional para verificar el desarrollo de actividades propias del servicio, por lo tanto, el personal que atenderá estas actividades debe contar con el cronograma respectivo.

Para que se puedan lograr resultados adecuados, es conveniente que se comunique la realización de esta actividad oportunamente indicando la fecha, lugar y logística a ser utilizada.

Durante la planificación de los exámenes de la seguridad operacional, es necesario el desarrollo de las listas de verificación o material a ser utilizado para este fin, lo que contribuye para que el personal conozca a cabalidad todo lo que va a requerir y poder emitir el criterio correspondiente.

Para ejecutar los exámenes de la seguridad operacional y con la finalidad de alcanzar los objetivos de los mismos, el personal a cargo de llevar a cabo estos exámenes puede desarrollar listas de verificación con la finalidad de revisar los requerimientos correspondientes en temas específicos, tomando en cuenta la normativa vigente, normas y procedimientos internos.

Estas listas de verificación deben abordar todos los elementos requeridos para lograr identificar las deficiencias correspondientes, todo esto para asegurar la seguridad operacional en cuanto a la provisión de los servicios de tránsito aéreo.

Ejecución del examen de la seguridad operacional.
Antes de iniciar con la realización del examen de la seguridad operacional, se debe llevar a cabo una reunión de coordinación donde se debe socializar el alcance y área que se someterá al examen de la seguridad operacional, como también, se debe definir quien atenderá esta actividad. Por otra parte, se debe exponer el mecanismo a ser utilizado para cumplir con este objetivo.

Se debe tomar en cuenta que durante un examen de la seguridad operacional y ejecución de la lista de verificación, no se debe verificar el “paquete” de documentación, más al contrario, se debe verificar la aplicación y cumplimiento de los procedimientos y normativa vigente.

Lo que se pretende buscar, es que el ATSP sea coherente con lo que está escrito, que el personal sabe y comprende lo que hace en la provisión del servicio y en la aplicación de procedimientos, por lo tanto, no solamente se debe exigir pruebas documentales sino también, entrevistas, observación y visitas en sitio para poder identificar alguna deficiencia.

Resultados del examen de la seguridad operacional.
Después de haber aplicado la lista de verificación u otro mecanismo establecido por el ATSP, el personal a cargo de la aplicación de esta lista de verificación debe clasificar los hallazgos correspondientes dependiendo de la gravedad de los mismos, sin embargo, es necesario aclarar que todo este proceso no tiene el objetivo de desacreditar o demeritar funciones o elementos del ATSP, más al contrario, este tipo de clasificación debe ser utilizada para definir la solución de las deficiencias con la más óptima asignación de recursos.

Al momento de la elaboración del informe adecuado, se debe detallar todo el proceso realizado

justificando las deficiencias encontradas con la clasificación correspondiente, de la misma manera, se debe especificar las evidencias encontradas para aquellas preguntas que han sido catalogadas como válidas en cuanto al cumplimiento de lo requerido y verificado.

El ATSP puede elaborar una plantilla al procedimiento para la realización de exámenes de la seguridad operación, donde se especifique el contenido de este informe para la estandarización del mismo en la realización de diferentes exámenes de la seguridad operacional en las diferentes dependencias de control.

Medidas de mitigación o acciones correctivas.
El informe del examen de la seguridad operacional deberá redactarse de manera narrativa e incluir por lo menos los datos indicados a continuación respecto a cada observación:

- Una descripción de la deficiencia o aspectos problemáticos descubiertos.
- Recomendaciones para rectificar la situación
- La persona encargada de tomar las medidas correctivas
- Las fechas previstas para implantar las medidas correctivas necesarias.

Cuando el área correspondiente haya recibido el informe del examen de la seguridad operacional, es necesario que se desarrolle un plan de trabajo para abordar todas las deficiencias en el examen de la seguridad operacional estableciendo prioridades de acuerdo a la clasificación de los hallazgos y disponiendo los recursos necesarios para incrementar la seguridad operacional.

Actividades de seguimiento.
De acuerdo a los tiempos establecidos, se debe hacer el seguimiento correspondiente para la verificación de cumplimiento por parte del personal que realizo el examen de la seguridad operacional, esto con la finalidad de subsanar las deficiencias identificadas como también recolectar las evidencias de cumplimiento correspondiente.

Por lo tanto, todo el proceso de la realización de los exámenes de la seguridad operacional debe ser debidamente documentado y archivado para contar con evidencias de cumplimiento de este requisito que será verificado por los inspectores de la AAC en actividades de vigilancia o a requerimiento.

Programa de auditoria interna
Una auditoría es una revisión metódica y planificada para determinar cómo se llevan a cabo las actividades y si se llevan a cabo de acuerdo con los procedimientos publicados. La auditoría de seguridad operacional está estrechamente relacionada con los procesos de aseguramiento de la calidad y se considera una actividad de gestión de la seguridad operacional proactiva que proporciona los medios para identificar problemas potenciales antes de que tengan un impacto en la seguridad operacional. Las auditorías de seguridad operacional se centran en evaluar la efectividad de los SMS y los sistemas de apoyo del ATSP. Las auditorías de seguridad operacional son una de las herramientas que se pueden utilizar para evaluar la efectividad de los controles de riesgos de seguridad operacional implementados o para monitorear el cumplimiento de los reglamentos de seguridad operacional. Garantizar la independencia y la objetividad es un desafío para las auditorías de seguridad operacional. La independencia y la objetividad se pueden lograr mediante la participación de entidades externas o auditorías internas con protecciones establecidas a través de políticas, procedimientos, roles y protocolos de comunicación.

La auditoría se ha centrado tradicionalmente en el cumplimiento de las regulaciones y la conformidad con las políticas y los procedimientos. Las organizaciones reconocen ahora que es más valioso observar la eficacia de esas políticas y procedimientos; esto es particularmente importante para los sistemas de gestión de la seguridad operacional. La auditoría de seguridad operacional interna es una herramienta que se utiliza para asegurar el cumplimiento (la organización cumple con sus obligaciones) y para monitorear el rendimiento de la seguridad operacional.

Deben utilizarse auditorías de seguridad operacional para identificar que:

- el riesgo de seguridad operacional se está gestionando y los controles de riesgo son eficaces
- se cumplen los procedimientos del ATSP
- el SMS del ATSP tiene una estructura sólida y niveles adecuados de personal
- se alcanza el nivel requerido de competencia e instrucción del personal para operar equipos e

instalaciones, y para mantener sus niveles de rendimiento
- el rendimiento del equipo es adecuado para los niveles de seguridad operacional del servicio prestado
- existen arreglos efectivos para promover la seguridad operacional, monitorear el rendimiento de la seguridad operacional y procesar los problemas de seguridad operacional
- existen arreglos adecuados para manejar emergencias previsibles
- si es necesario, el área del ATSP que se audita identifica las medidas correctivas.

Establecimiento de un programa de auditoría.
Un programa de auditorías que cubra uno o dos años ayudará al ATSP a planificar sus actividades y recursos de auditoría. El cronograma deberá mostrar la fecha planificada de cada auditoría, una breve descripción del alcance y los nombres de los auditores. Se deberá considerar cómo y por quién se mantendrá este cronograma y cómo el personal relevante puede acceder a él. Los cambios en la programación y el alcance deben estar claramente justificados y documentados con autoridad para un acuerdo establecido en un nivel de alta gerencia apropiado.

Establecer el alcance y la frecuencia de la auditoría.
El alcance de la auditoría describe la amplitud de los servicios del ATSP que se cubrirán y depende del área de enfoque de la auditoría. La naturaleza y el alcance de las auditorías será un equilibrio entre la necesidad basada en el riesgo y la basada en el cumplimiento, impulsada principalmente por la importancia para la seguridad operacional de un área del ATSP, mientras se mantiene el cumplimiento operacional (es probable que una falla en el cumplimiento sea un riesgo para la seguridad operacional).

La frecuencia será impulsada en parte por los requisitos de cumplimiento de partes externas como reguladores y clientes, y en parte por el nivel de actividad y la experiencia del ATSP. Por ejemplo, una auditoría en un área operativa del ATSP puede ser necesaria solo una vez cada dos años, pero un área que tiene problemas conocidos o sospechados puede necesitar auditorías más frecuentes o adicionales. Estos deberán agregarse al programa y las razones deben registrarse.

El uso del riesgo de seguridad operacional como base para el alcance y la frecuencia de las auditorías requerirá que la organización considere al menos algunos o todos estos puntos:
- ¿Cuáles son los principales riesgos que gestiona el ATSP y dónde ocurren?
- ¿Cuántos controles de riesgo existen y qué tan efectivos son?
- ¿Qué está funcionando bien y por qué? ¿Ayudaría una auditoría a comprender las lecciones que podrían aplicarse a otras partes de la operación del ATSP?
- datos de seguridad operacional de las notificaciones y los resultados de investigaciones y auditorías previas: ¿se identificaron fallas de control que podrían ser aplicables a otras áreas?
- ¿Se están produciendo cambios que requieren un seguimiento más detenido para verificar que las medidas de control planificadas son eficaces?
- ¿Cómo realiza el seguimiento el ATSP con sus indicadores de rendimiento en seguridad operacional?

Establecer objetivos de la auditoria.
Los objetivos de la auditoría definen los logros tangibles que se esperan de cada auditoría. Es aconsejable establecer los objetivos detallados mucho antes de la auditoría para ayudar a los auditores a planificar y realizar la auditoría. Por ejemplo, para una auditoría dirigida a verificar la “el proceso de notificación de incidentes ATS”, un objetivo de la auditoría podría ser "determinar en qué momento se realiza el llenado del formulario posterior haber recibido la notificación de TCAS RA".

Descripción de la metodología de auditoría.
Es importante delinear las políticas, procesos y metodologías requeridas para realizar auditorías de seguridad operacional internas. La persona que gestiona el programa de auditoría debe seleccionar y determinar los métodos para realizar una auditoría de forma colectiva, según los objetivos, el alcance y los criterios de auditoría definidos.

Documentación de procesos.
Todos los procesos de auditoría deben estar claramente documentados para que sean fáciles de entender y, lo que es más importante, permitan que las auditorías se lleven a cabo de manera

estandarizada.

Realización de auditorías de seguridad operacional y seguimiento de resultados.
Una auditoría debe incluir los siguientes pasos:

a) Planificación de la auditoría

Una planificación cuidadosa ayuda al auditor a preparar herramientas apropiadas para el objetivo y alcance de la auditoría. Una herramienta es la lista de verificación de auditoría, que deberá utilizarse para identificar las funciones que se van a auditar y garantizar que no se pierda nada; podría incluir preguntas específicas para permitir al auditor determinar la efectividad de los procesos de calidad y seguridad operacional. Las listas de verificación nunca deberán usarse simplemente para mostrar el cumplimiento marcando casillas.

b) Realización de la auditoría

La auditoría se lleva a cabo para recopilar información a través de una combinación de revisión de documentos, entrevistas con el personal clave y personal del ATSP, y observaciones por parte del auditor o auditores. Los auditores deben:

- centrarse en cómo (y sí) se practican los procedimientos documentados, y si las prácticas y procedimientos actuales conducen a operaciones efectivas y seguras;
- utilizar preguntas abiertas, formuladas de manera neutral, y mantener un alto nivel de compromiso con el personal del servicio auditado;
- proporcionar un resumen inicial de los hallazgos u observaciones a los auditados al concluir la auditoría.

Redacción del informe de auditoría.
Es esencial que el contenido del informe de auditoría sea preciso, y que los hallazgos estén respaldados por pruebas sólidas que el lector pueda comprender. Los redactores de informes deberán asegurarse de:

- la consistencia de hallazgos, recomendaciones y observaciones;
- que las conclusiones están respaldadas con referencias;
- que los hallazgos, recomendaciones y observaciones se expresan de manera clara y concisa sin el uso de generalizaciones
- que los puntos de vista críticos no están dirigidos a personas o posiciones.

Difusión y seguimiento de los resultados de la auditoría.
El informe de auditoría debe presentarse formalmente a los auditados para que puedan abordar cualquier hallazgo. Es necesario realizar un seguimiento de las acciones para abordar los hallazgos de manera transparente y sistemática.

Selección e instrucción de auditores.
Los auditores deberán recibir instrucción formal para desarrollar competencia en habilidades y técnicas de auditoría, y se les deberá alentar, o incluso exigir, que obtengan calificaciones formales de auditor. También se esperaría de un auditor eficaz:

- actuar de forma estrictamente digna de confianza e imparcial
- revelar cualquier posible conflicto de intereses
- no aceptar regalos, etc.
- no revelar los hallazgos o cualquier otra información obtenida en el curso de la auditoría a ningún tercero a menos que esté autorizado para hacerlo.

La independencia operativa garantiza que los auditores no se encuentren en una posición en la que su objetividad pueda verse afectada por responsabilidades o lealtades conflictivas. Las organizaciones pequeñas pueden considerar contratar a un tercero para realizar auditorías; el tercero podría ser de un ATSP similar.

Revisión de gestión.
Como cualquier sistema de gestión empresarial (por ejemplo, financiero, de salud y seguridad operacional), para garantizar la adecuación y eficacia continúa del SMS, el Gerente Responsable deberá realizar revisiones periódicas de los procesos y procedimientos del SMS y evaluar el

rendimiento de seguridad operacional del ATSP. Hay muchas formas en que el Gerente Responsable puede revisar el SMS, como recibir y revisar un informe generado por el Responsable de seguridad operacional u otro personal, comunicación electrónica, como parte de una reunión regular de la gerencia o realizada una reunión separada. El ATSP necesita describir cómo se llevará a cabo el proceso de revisión por la dirección. Si es por reunión, entonces con qué frecuencia se reunirán, quiénes estarán en la reunión, qué se discutirá como una agenda permanente y cómo se documentarán las acciones acordadas y el seguimiento de su progreso.

Actividades de revisión por la dirección.
Es importante que la Gerente Responsable revise la eficacia del SMS, en ese sentido, los puntos a revisar por la gerencia son:

- examinar si el ATSP está logrando los objetivos de seguridad operacional;
- aprovechar la oportunidad para observar toda la información disponible sobre el rendimiento de la seguridad operacional para identificar tendencias generales;
- evaluar los SPI y SPT considerando las tendencias y, cuando los datos apropiados estén disponibles, comparar (punto de referencia) con otras proveedores similares, datos nacionales o globales;
- revisar el rendimiento de la auditoría; esto incluye auditorías internas y auditorías realizadas por otras organizaciones;
- monitorear los sucesos para detectar la repetición de sucesos de seguridad operacional, incluidos accidentes e incidentes ocurridos a consecuencia de la provisión de los servicios ATS, así como condiciones o actos inseguros;
- revisar los resultados de las evaluaciones realizadas, incluidas las evaluaciones de la cultura de seguridad y la eficacia del SMS
- revisar los resultados de las encuestas de seguridad operacional, incluidas las encuestas culturales que brindan comentarios útiles sobre la participación del personal con el SMS
- proporcionar una plataforma para que el ATSP aborde las lecciones aprendidas de los sistemas de notificación de seguridad operacional y las investigaciones de seguridad operacional; esto debería conducir a la implementación de mejoras de seguridad operacional.

Entradas para la revisión por el Gerente Responsable.
Las entradas para la revisión por el Gerente Responsable deberán considerar, entre otras cosas, información sobre:

- resultados de auditoría/revisión;
- resultados del logro de objetivos de seguridad operacional;
- estado y resultados de peligros y sucesos;
- estado y resultados de las acciones correctivas y preventivas;
- eficacia del programa de instrucción;
- acciones de seguimiento de revisiones de gestión anteriores;
- cambios que podrían afectar al SMS;
- recomendaciones de mejora.

Estos insumos pueden luego usarse para medir la efectividad general del SMS, y el equipo de revisión puede decidir sobre los cambios que se deben realizar para mejorar el SMS.

Resultados de la revisión por el Gerente Responsable.
Como resultados del proceso de revisión por el Gerente Responsable, debe haber evidencia de decisiones relacionadas con:

- actividad de mejora continua;
- el panorama actual de los riesgos de seguridad operacional;
- comunicaciones de seguridad operacional;
- actualizaciones de instrucción;
- revisiones de políticas y procedimientos.

Se requiere información documentada como evidencia de los resultados de las revisiones por Gerencia Responsable, y el formato de esta puede variar. Las actas de reuniones son el tipo más común, pero los registros electrónicos, cuadros estadísticos, presentaciones o fotografías de los resultados de las discusiones son tipos aceptables.

Es importante que la persona que redacta las actas no intente también presidir la reunión o dirigir las discusiones; necesitan poder transcribir con precisión suficiente información para evidenciar el proceso de decisión. La responsabilidad de implementar cada acción debe asignarse a una persona con la responsabilidad apropiada y los recursos apropiados asignados.

Frecuencia de las revisiones por la dirección.
Las revisiones del Gerente Responsable deben realizarse con la frecuencia necesaria para garantizar que la eficacia del sistema se pruebe verdaderamente. Esto debería reflejar la dimensión y la complejidad del ATSP, junto con la cantidad de información a revisar. Las entradas y resultados del proceso de revisión por el Gerente Responsable también deben ser relevantes a la dimensión y la complejidad del ATSP. La frecuencia y naturaleza de las revisiones también deberán tener en cuenta los diferentes niveles de seguimiento que se llevan a cabo, como las actividades de los grupos o comités de seguridad. La revisión no deberá ocurrir con tanta frecuencia que se vea envuelta en minucias que ocultarían las deficiencias en los SMS más grandes. Por otro lado, deberá realizarse con la suficiente frecuencia para evitar situaciones en las que las decisiones se tomen demasiado tarde para abordar las amenazas al SMS.

El ATSP deberá considerar lo siguiente al establecer la frecuencia de sus revisiones por la dirección:

- cambios anticipados o amenazas a las operaciones y SMS. Los nuevos sistemas requieren más atención y asignación de recursos para dar seguimiento y cerrar los puntos de acción.
- establecer una lista de elementos de seguridad operacional importantes que desencadenarían una revisión por la dirección entre las sesiones planificadas.

5.4. Componente 4 – Promoción de la seguridad operacional.

La promoción de la seguridad operacional comienza con la estrategia para desarrollar una cultura de seguridad operacional dentro del ATSP. La cultura de seguridad operacional permite una mejora continua en el rendimiento de la seguridad operacional.

Una estrategia de promoción de la seguridad operacional debe abordar la instrucción, educación y comunicación de información de seguridad operacional para apoyar la implementación y operación del SMS.

Instrucción y educación.

Comprensión.
La Educación es la formación práctica y metodológica que se le da a una persona en vías de desarrollo y crecimiento. Es un proceso mediante el cual al individuo se le suministran herramientas y conocimientos esenciales para ponerlos en práctica en la vida cotidiana. El aprendizaje de una persona comienza desde su infancia, al ingresar en institutos llamados escuelas o colegios en donde una persona previamente estudiada y educada implantará en el pequeño identidades, valores éticos y culturales para hacer una persona de bien en el futuro.

Cuando hablamos de instrucción nos referimos al proceso de adquisición de conocimientos que generalmente conduce al desarrollo de habilidades, destrezas y hábitos en quien los adquiere. Mediante la instrucción se capacita o adiestra para que el individuo esté en posibilidad de realizar un tipo de trabajo específico.

A veces nos referimos a instrucción y educación como sinónimos. No lo son. Educación es el desarrollo de sentimientos, convicciones, voluntad, carácter, en general, concienciación en valores y solidaridad. Un analfabeto se puede educar, mas no instruir. De la misma forma, un individuo muy instruido puede no ser educado ni estar en capacidad de educar.

El propósito de la instrucción es adquirir un nivel de competencia en las habilidades y competencias específicas.

El ATSP debería definir y mantener un programa de instrucción en seguridad operacional. La instrucción en seguridad operacional debe adaptarse a los empleados del ATSP, según sea apropiado para las competencias requeridas por cada función laboral. El ATSP debería identificar a la población

destinataria de la instrucción en seguridad operacional. Esto incluye a los empleados cuyas actividades pueden afectar la seguridad operacional del producto o servicio, además de los que están a cargo del SMS. La instrucción en seguridad operacional basada en roles debe garantizar que los empleados:

- Son competentes para desempeñar sus funciones y responsabilidades relevantes para la operación y rendimiento del SMS.
- Comprender cómo su actividad podría afectar la seguridad operacional.
- Conocer qué medios, herramientas y recursos están disponibles para la operación del SMS.

La competencia se define como: “Una capacidad que permite a una persona realizar varios procesos o tareas y lograr resultados. Es una combinación de conocimientos, habilidades y actitudes relevantes. Es la capacidad demostrada para aplicar conocimientos y habilidades”.

La competencia se manifiesta y se observa a través de comportamientos:

- Los **comportamientos observables** son comportamientos relacionados con el trabajo que pueden observarse y pueden no ser medibles.

  Esos comportamientos (observables) movilizan el conocimiento, las habilidades y las actitudes relevantes para llevar a cabo actividades o tareas en condiciones específicas.

- El **conocimiento** es información específica que se utiliza para permitir que una persona aplique habilidades y actitudes y recuerde hechos, identifique conceptos, aplique reglas, procedimientos o principios.

- La **habilidad** es la capacidad de realizar una actividad o acción.

- La **actitud** es un estado mental interno persistente o disposición que influye en la elección individual de una acción personal hacia algún objeto, persona o suceso que se pueda aprender.

Medios de cumplimiento.
El ATSP deberá definir un programa de instrucción en seguridad operacional para cumplir con los objetivos de la política de seguridad operacional.

Este programa debe cubrir, como mínimo, el alcance, el contenido, los métodos de entrega (por ejemplo, instrucción en el aula, aprendizaje virtual (E-learning), notificaciones, instrucción práctica en el puesto de trabajo) y la frecuencia de la instrucción que mejor satisfaga las necesidades del ATSP considerando el tamaño, el alcance requerido, competencias y complejidad del ATSP.

El programa de instrucción en seguridad operacional deberá revisarse periódicamente para garantizar que cumpla con los objetivos.

La instrucción debería ser específica para el SMS y las operaciones del ATSP y debería impartirse de acuerdo con las necesidades de competencia.

Como mínimo, la instrucción en seguridad operacional deberá proporcionar al personal los conocimientos necesarios para comunicar información que podría conducir a problemas de seguridad operacional y comprender su responsabilidad de notificar.

La instrucción de seguridad operacional deberá considerar:

a) instrucción para el Gerente Responsable, incluidas las responsabilidades de seguridad operacional, la supervisión y la gobernanza y su relación con la estrategia comercial del ATSP y otros sistemas de gestión;
b) instrucción para el personal clave y jefes sobre cómo liderar de manera efectiva el desarrollo, implementación y sostenimiento continuo del SMS;
c) competencia para el liderazgo organizacional y el personal clave de seguridad operacional en la aplicación de prácticas de gestión de riesgos;
d) Instrucción que proporciona competencia al personal superior del sistema de gestión de la seguridad operacional (responsable de seguridad operacional) en la gestión y administración del SMS y las prácticas de gestión de riesgos.

e) instrucción basada en competencias para todo el personal en la participación y el uso del SMS del ATSP que sea apropiado para sus deberes relacionados con la seguridad operacional.

En relación a la instrucción basada en competencias, esta es una instrucción y evaluación que se caracterizan por una orientación al rendimiento, énfasis en los estándares de rendimiento y su medición y el desarrollo de la instrucción para los estándares de rendimiento especificados.

La demostración de las competencias se puede evaluar utilizando los indicadores de comportamiento, los cuales deben cumplir con el nivel de rendimiento requerido, según lo establecido por la organización para su operación específica.

La instrucción basada en competencias tiene los siguientes beneficios:

- permite a las personas alcanzar su nivel más alto de capacidad operativa al tiempo que garantiza un nivel básico de competencia como estándar mínimo
- permite a las personas hacer frente a situaciones predecibles e imprevistas
- es relevante para el trabajo/rol y el contexto en el que se realizará el trabajo
- está orientado al aprendizaje en lugar de aprobar un examen.

Deben seguirse los siguientes principios de instrucción y evaluación basados en competencias:

- las competencias relevantes están claramente definidas para un rol particular dentro del SMS del ATSP.
- las competencias pueden ser capacitadas, observadas y evaluadas de manera consistente
- comprensión común de los requisitos de competencia
- el proveedor de instrucción establece criterios de rendimiento claros para evaluar la competencia
- la evidencia del rendimiento de la competencia es válida y confiable
- vínculo entre competencias e instrucción, requerido para el rendimiento y la evaluación
- evaluación basada en múltiples observaciones en múltiples contextos
- demostración de un desempeño integrado de todas las competencias requeridas

.

La siguiente tabla ayuda a mostrar la relación entre la competencia y el indicador de comportamiento.

Competencia	Descripción de la competencia	Indicador de comportamiento
Aplicación de los procedimientos de la coordinación de la planificación de respuestas ante emergencias (especifico al rol a cumplir)	Identifica y aplica procedimientos de acuerdo con el tipo de emergencia, utilizando los conocimientos adecuados.	Identifica la fuente de los pasos a seguir para brindar la asistencia a la aeronave en emergencia
		Identifica y sigue las instrucciones de manera oportuna (por ejemplo durante prácticas en simulador)
		Aplica el conocimiento procedimental relevante

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

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

La organización deberá mantener un registro de toda la instrucción en seguridad operacional proporcionada a cada sujeto individual del programa de instrucción. Dichos registros deben conservarse de acuerdo con la política de retención de datos de la organización y los requisitos

reglamentarios aplicables.

Desarrollar el contenido del programa de instrucción en seguridad operacional.
Es responsabilidad del Gerente Responsable asegurarse de que se asignen recursos suficientes y del Responsable de seguridad operacional garantizar que el programa desarrolle las competencias individuales requeridas del personal, de modo que el SMS se comprenda y aplique de manera efectiva en los diferentes niveles del ATSP, al tiempo que se construye una sólida cultura de seguridad operacional. Se pueden utilizar organizaciones de instrucción externas apropiadas, si es necesario, para proporcionar la instrucción necesaria para cumplir con determinadas responsabilidades del personal. Es responsabilidad del ATSP asegurarse de que cualquier instrucción externa sea adecuada a las necesidades de instrucción y los requisitos de competencia de su SMS.

Realización de un análisis de las necesidades de instrucción.
Se deberá realizar un análisis de las necesidades de instrucción para identificar el programa de instrucción apropiado para todo el personal, el alcance del programa de instrucción debe ser apropiado para el rol y la participación de cada individuo en el SMS del ATSP. Se puede realizar un análisis de las necesidades de instrucción mediante:

- analizar el trabajo:
  Iniciar por consultar la documentación específica que describe el trabajo, como la descripción del puesto. Identifique frases que especifiquen habilidades, procesos o áreas de conocimiento importantes requeridas.

- determinar las brechas de habilidades / conocimientos:
  Desarrollar una lista de áreas en las que se requeriría instrucción para mejorar la efectividad del trabajo en cuestión;

  Decidir si hay una brecha en las habilidades o conocimientos, o si se requiere alguna revisión para mejorar el conjunto de habilidades generales;

  Obtener retroalimentación de un grupo representativo de personas que realizan el trabajo sobre las áreas que consideran que deben abordarse.

- identificar soluciones de instrucción:
  Establecer la mejor manera de cerrar las brechas de habilidades/conocimientos identificados en el paso anterior. Las diferentes opciones pueden incluir cursos de instrucción realizados interna o externamente, aprendizaje autodirigido, instrucción individual o tutoría en el entorno laboral.

- evaluar el rendimiento después de la instrucción para determinar si aún existen brechas de rendimiento y si la solución de instrucción seleccionada era apropiada. Esto se puede lograr mediante:
  Pedir al personal y/o al responsable de ese personal que evalúen su efectividad en la tarea;

  Preguntar al personal si las brechas de rendimiento que fueron el motivo de la instrucción aún persisten;

  Evaluar al personal a medida que realiza tareas para determinar si todavía hay evidencia de deficiencia de habilidades o conocimientos.

Determinar los plazos del programa de instrucción en seguridad operacional.
Con respecto a los plazos del programa de instrucción, es necesario considerar, desarrollar y asignar los recursos necesarios tanto los requisitos de instrucción inicial como continuo.

Programa de instrucción de seguridad operacional.
Como mínimo, un programa de instrucción en seguridad operacional debe incluir las siguientes áreas de enfoque de alto nivel:

- políticas, logros y objetivos de seguridad operacional organizacionales
- roles y responsabilidades de seguridad operacional organizacional relacionados con la seguridad operacional
- fundamentos de SMS, incluida la relación con factores humanos

- principios de gestión de riesgos de seguridad operacional
- identificación de peligros y notificaciones de seguridad operacional
- comunicación de seguridad operacional.

El programa de instrucción deberá identificar el alcance y la profundidad del programa de instrucción para las diversas tareas y funciones relacionadas con la seguridad operacional de acuerdo con las necesidades y la complejidad del ATSP.

Programa de instrucción y documentación de cualificación.
Los requisitos de instrucción y calificación deben documentarse para cada dependencia en el ATSP. Se debe desarrollar un archivo de instrucción para todo el personal, incluido el Gerente Responsable, para identificar y registrar sus requisitos y logros de instrucción y competencia.

Quién necesita recibir instrucción en seguridad operacional.
Todo el personal debe participar en el programa de instrucción en seguridad operacional de la organización apropiado para sus responsabilidades de seguridad operacional. En particular, todo el personal operativo del ATSP, supervisores, jefes, personal clave y el Gerente Responsable deben estar capacitados y ser competentes para realizar sus funciones de SMS.

Material de orientación sobre instrucción y competencias.
El Responsable de seguridad operacional es la persona responsable del desarrollo, implementación, operación y mejora continua del SMS del ATSP. Deberán actuar como punto focal para la seguridad operacional en el ATSP.

Por lo general, el Responsable de seguridad operacional debe ser competente y responsable de lo siguiente:

- gestión del plan de implementación de SMS en nombre del Gerente Responsable;
- facilitar el proceso de gestión de riesgos (identificación del peligro, evaluación y control de riesgos);
- gestión de los procesos de rendimiento de seguridad operacional;
- monitorear las acciones correctivas y preventivas para asegurar su cumplimiento;
- mantener la documentación de seguridad operacional;
- garantizar que se proporcione la instrucción adecuada en gestión de la seguridad operacional;
- proporcionar asesoramiento independiente en materia de seguridad operacional;
- supervisar los procesos de gestión de la seguridad operacional;
- participación adecuada en las investigaciones de seguridad operacional;
- monitorear los problemas de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones del ATSP;
- coordinar y comunicarse (en nombre del Gerente Responsable) con la AAC según sea necesario sobre problemas relacionados con la seguridad operacional.

Además de lo anterior, la comprensión de la operación del ATSP y las tareas y sistemas críticos de seguridad operacional relacionados, y la competencia con respecto a los principios de gestión de la seguridad operacional, deberán tenerse en cuenta algunas habilidades/experiencia clave para complementar la experiencia profesional del Responsable de seguridad operacional:

- conocimiento profesional de las operaciones y el entorno específicos del ATSP;
- pensamiento analítico y habilidades para resolver problemas;
- habilidades de gestión de proyectos inter e intra-organizaciones;
- habilidades orientadas a las personas como objetividad, justicia, etc.;
- habilidades comunicativas, tanto escritas como orales.

La siguiente tabla describe un ejemplo de muestra de la instrucción en seguridad operacional para el puesto de Responsable de seguridad operacional. El programa de instrucción deberá tener en cuenta la complejidad del ATSP y el análisis de las necesidades de instrucción para el puesto.

EJEMPLO DEL CONTENIDO PARA LA INSTRUCCIÓN EN GESTIÓN DE SEGURIDAD OPERACIONAL PARA EL RESPONSABLE DE SEGURIDAD OPERACIONAL
Principios y prácticas de gestión de la seguridad operacional en el entorno de la aviación: • la necesidad de SMS • qué tiene de diferente los SMS • relación / integración con otros sistemas de gestión • principios y procesos clave los requisitos reglamentarios
SMS de la organización que incluye: • política, metas y objetivos de seguridad operacional • roles y responsabilidades de seguridad operacional • planificación de la coordinación de la planificación de respuestas ante emergencias • documentación • gestión de riesgos • garantía y medición de la seguridad operacional • notificaciones de seguridad operacional • comunicación e instrucción sobre seguridad operacional
Principios de gestión de riesgos de seguridad operacional • identificación de peligros, evaluación y control de riesgos. • Principios de investigación de seguridad operacional
Rendimiento humano • factores humanos • comprender el papel del ser humano en la seguridad operacional • comportamiento y rendimiento humanos • gestión de errores

Qué comunicar en todo el ATSP.

La siguiente información debe comunicarse regularmente al personal de manera sistemática y mensurable:

- compromiso de liderazgo con el SMS, sus objetivos y rendimiento de seguridad operacional
- información sobre riesgos de seguridad operacional; riesgos identificados, métodos de tratamiento, riesgos residuales, nuevos controles de riesgos de seguridad operacional y acciones correctivas, etc.
- peligros identificados y controles requeridos
- retroalimentación del personal sobre la presentación de notificaciones de seguridad operacional - el circuito de retroalimentación debe cerrarse
- tendencias y estadísticas de notificaciones de seguridad operacional
- difusión de información para fundamentar las decisiones de seguridad operacional
- cambios en el SMS
- cambios en los servicios prestados que pueden afectar la seguridad operacional o los procedimientos existentes
- resultados de las investigaciones de seguridad operacional, auditorías y acciones correctivas y preventivas asociadas
- lecciones aprendidas e información de seguridad operacional "bueno para saber".

Qué comunicar fuera del ATSP.
La siguiente información debe comunicarse según sea necesario:

- peligros potenciales, riesgos o incidentes que pueden afectar a otros
- lecciones aprendidas y soluciones a los peligros y riesgos identificados
- riesgos potenciales asociados con el cambio (por ejemplo, nueva infraestructura, cambios reglamentarios, etc.).

Métodos de comunicación.
La comunicación de seguridad operacional deberá entregarse por el método más apropiado según el rol del individuo y la necesidad de recibir información relacionada con la seguridad operacional. Esto se puede hacer a través de reuniones, hojas informativas de seguridad operacional, avisos, boletines, sesiones informativas o cursos de instrucción. Algunos paquetes de software de SMS tienen funciones de notificación por correo electrónico o aplicaciones de mensajería. Es importante utilizar más de un medio, asegurándose de que haya una combinación de comunicación activa (por ejemplo, la capacidad de interactuar y recibir comentarios) y comunicación pasiva. Algunos ejemplos son:

- Métodos activos de comunicación
  - reuniones periódicas relacionadas con la seguridad operacional
  - el Gerente Responsable transmite información estratégica, metas y objetivos de seguridad operacional (de arriba hacia abajo)
  - personal que informa a la dirección sobre problemas de seguridad operacional (de abajo hacia arriba). Por lo general, se trata de información más táctica sobre lo que está sucediendo en las áreas funcionales/departamentales.
  - reuniones informativas del equipo e iniciativas de "espectáculos itinerantes".

- Métodos pasivos de comunicación
  - la publicación de una revista u hoja informativa de seguridad operacional organizacional
  - presentación basada en la web
  - foros
  - correos electrónicos.

Los métodos de comunicación deben ser acordes con la dimensión y la complejidad del ATSP.

Promoción de seguridad operacional.
La promoción de la seguridad operacional respalda las metas y los objetivos de la comunicación de seguridad operacional. Está estrechamente relacionado con la instrucción y la difusión de información sobre seguridad operacional. Se refiere a aquellas actividades que el ATSP lleva a cabo para asegurar que el personal comprenda:

- por qué existen procedimientos de SMS
- qué significa la gestión de la seguridad operacional
- por qué se toman determinadas medidas de seguridad operacional, etc.

La promoción de la seguridad operacional proporciona un mecanismo a través del cual las lecciones de las investigaciones de seguridad operacional y otras actividades relacionadas con la seguridad operacional se ponen a disposición de todo el personal afectado.

Cómo promover la seguridad operacional de manera efectiva.
Las actividades de promoción de la seguridad operacional deben complementar las iniciativas de educación y comunicación. El programa de promoción de la seguridad operacional organizacional debe basarse en varios métodos de comunicación diferentes por razones de flexibilidad y costo. Los métodos típicos son:

- hablada: quizás el método más eficaz, especialmente si se complementa con una presentación visual.
- escrita: el método más popular debido a su rapidez y economía, el material impreso de promoción de la seguridad operacional también compite por la atención con cantidades considerables de otro material impreso.

- medios electrónicos: el uso de Internet ofrece un importante potencial de mejora en la promoción de la seguridad operacional. Esto podría incluir hojas informativas electrónicas, blogs, herramientas de retroalimentación como encuestas, etc.

Interfaces entre las organizaciones.

Principios de interfaz.
En el contexto de un SMS, la gestión de la interfaz debe abarcar los cuatro componentes (política y objetivos de seguridad operacional, SRM, SA y promoción de la seguridad operacional).

Las políticas y los objetivos de seguridad operacional pueden compartirse entre organizaciones interconectadas para garantizar enfoques de SMS consistentes.

Los riesgos de seguridad operacional en una organización pueden afectar a otras organizaciones a través de las posibles consecuencias de los riesgos o la gestión de su mitigación. Una buena práctica consiste en establecer un sistema de notificaciones sobre dichos riesgos entre las organizaciones interconectadas.

Los riesgos que se comparten entre las organizaciones interconectadas deben notificarse entre esas organizaciones y cada organización debe reconocerlos sobre la base de un esquema de evaluación de riesgos acordado. Para las organizaciones dentro de una empresa, el riesgo y el intercambio de información relacionada y las acciones comunes de mitigación pueden organizarse mediante una herramienta común de gestión de riesgos que también podría proporcionar el esquema de evaluación de riesgos acordado. Para las relaciones externas (por ejemplo, proveedores), los riesgos pueden mitigarse mediante prácticas de gestión, reconocimiento y presentación de informes acordados.

Los riesgos de seguridad operacional pueden resultar de interacciones entre organizaciones (por ejemplo, debido a brechas o superposición de interacciones) o falta de gestión de la interfaz (por ejemplo, ausencia de monitoreo).

Las actividades de aseguramiento de la seguridad operacional deberán centrarse primero en los intercambios de datos necesarios que están sujetos a requisitos reglamentarios. Estos intercambios generalmente se rigen por requisitos contractuales.

El nivel y los detalles de los intercambios de datos deben adaptarse y ser proporcionales a la complejidad y los riesgos de seguridad operacional de los productos, servicios y organizaciones de interfaz. También debe adaptarse a la madurez de cada organización en lo que respecta a la gestión de la seguridad operacional.

Los principios y prioridades de promoción de la seguridad operacional se pueden compartir entre las organizaciones interconectadas para garantizar enfoques de SMS consistentes (por ejemplo, compartir regularmente las políticas de seguridad operacional, los principales objetivos y riesgos de seguridad operacional, las mejores prácticas).

Cuando corresponda, los ATSP deberán definir cómo los servicios que trabajan bajo su propio sistema de gestión de calidad (QMS) contribuirán a las actividades de SMS. Las obligaciones contractuales deben establecerse y evaluarse para garantizar el pleno acuerdo de los otros servicios.

No se requiere que una organización justifique la identificación de peligros y decida acciones de control de riesgos más allá de sus obligaciones para evitar situaciones de interferencia.

La gestión de la interfaz entre organizaciones es relevante para cualquier sistema de gestión (por ejemplo, sistema de gestión de seguridad operacional, sistema de gestión de calidad, sistema de gestión ambiental, sistema de aseguramiento de diseño).

Documentación de interfaz.
Cuando sea relevante, la interfaz entre las organizaciones para la gestión de la seguridad operacional debe documentarse y mantenerse.

Esta documentación debe considerar los siguientes objetivos:

- Apoyar la comprensión de los límites de la organización y sus interacciones.
- Aclarar cómo interactúan las organizaciones (con o sin SMS implementado).
- Direccionar la gestión de problemas/elementos de seguridad operacional relevantes.

Ejemplos de documentación para las disposiciones de la interfaz SMS (tales disposiciones podrían ser objeto de documentos dedicados o parte de un conjunto de documentación más amplio):

- Manual de la organización.
- Contrato.
- Documento de interfaz de organización.
- Declaración de política general.
- Acuerdo operacional.
- Plan de aseguramiento de calidad.
- Procedimientos aplicables comunes cuando diferentes organizaciones se encuentran dentro de la misma empresa o grupo.

Esta documentación puede contener los siguientes elementos para los temas y actividades de interfaz:

- Organización y responsabilidades (por ejemplo, derechos y deberes de informar problemas, defectos o sucesos, responsabilidades y propiedad para la identificación de peligros y control de riesgos, identificación clara de los puntos focales interconectados).
- Descripciones de procesos y entregables (directa o indirectamente a través de referencias cruzadas a procedimientos).
- Criterios para informar problemas de seguridad operacional, constataciones de incumplimiento, no conformidades y sucesos. Estos criterios deben centrarse en la comunicación temprana de sucesos de seguridad operacional y posibles problemas de seguridad operacional (por ejemplo: cambios en el espacio aéreo, nuevos procedimientos, nueva servicios a proporcionarse)
- Medios acordados para la notificación oportuna de problemas de seguridad operacional entre organizaciones.
- Revisiones periódicas de la interfaz.

Enfoque de SMS corporativos.

Una organización puede optar por configurar un "SMS corporativo" cuando la empresa tiene más de un SMS (por ejemplo, SMS operador de aeródromo y SMS en un ATSP). Un SMS corporativo puede ayudar a simplificar la implementación de SMS al proporcionar un enfoque coherente sobre algunos o todos los cuatro componentes de SMS en las organizaciones. Un SMS corporativo podría garantizar:

- Las políticas y objetivos de seguridad operacional tienen una definición, implementación y mejora continua consistentes a través de las organizaciones.
- Los riesgos de seguridad operacional se gestionan de forma coherente en todas las organizaciones interconectadas (por ejemplo, definiendo una metodología común de riesgos de seguridad operacional, definiendo criterios de gestión de los principales riesgos de seguridad operacional).
- Las actividades de aseguramiento de seguridad operacional se gestionan de forma coherente (p. Ej., Seguimiento de tendencias, implementación de investigaciones sobre problemas sistémicos en todas las organizaciones, gestión de cambios).
- La promoción de la seguridad operacional define y asegura los principios, las prioridades, las lecciones aprendidas y las mejores prácticas compartidas entre las organizaciones (por ejemplo, los principales objetivos/riesgos de seguridad operacional) a través de sucesos corporativos y sesiones de sensibilización/instrucción.

Un manual de SMS corporativo podría describir la implementación de SMS de la organización general y común sobre los 4 componentes y 12 elementos del SMS.

Un SMS corporativo no es obligatorio y será necesario mostrar cómo cada una de las actividades del proveedor de servicios cumple con los requisitos de SMS. Es posible que las organizaciones tengan que rendir cuentas de la supervisión de las diferentes actividades de los proveedores de servicios a las diferentes autoridades supervisoras.

6. PROCESO DE IMPLEMENTACIÓN.

6.1. Planificación de la implementación.

La implementación del SMS implica cambios como la forma en que las organizaciones abordan y gestionan los riesgos, recopilan y analizan datos y establecen y miden el rendimiento de la seguridad operacional. En consecuencia, las organizaciones necesitarán algún tiempo para ajustar los procesos actuales, establecer otros nuevos cuando sea necesario y hacerlos efectivos.

El éxito de la implementación de la organización será determinado por AAC mediante el uso de una herramienta de evaluación del SMS. Esto también puede ayudar a las organizaciones a determinar cómo evaluar, desarrollar e implementar mejor los diversos elementos de un SMS eficaz que sea escalable.

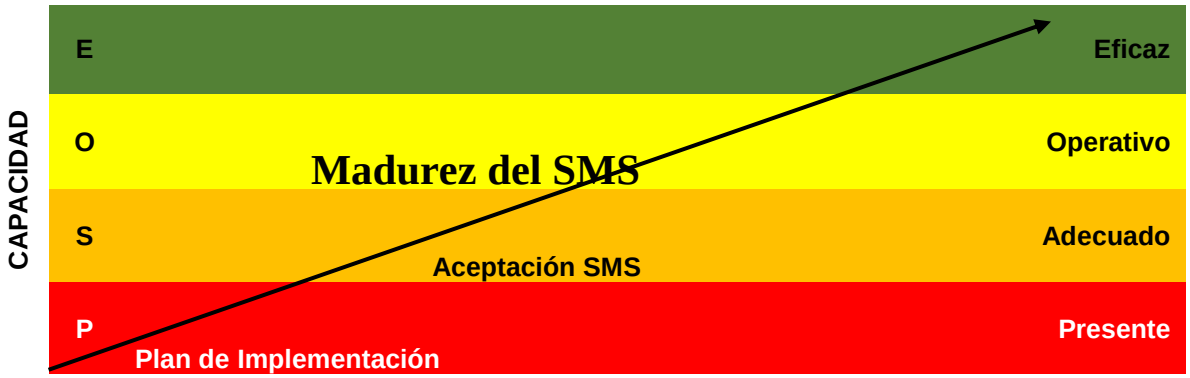
La herramienta ayuda a evaluar la madurez y eficacia del SMS del ATSP, la herramienta utiliza el concepto de diferentes niveles de rendimiento con respecto a la capacidad de gestión de la seguridad operacional de la organización. Estos se describen en la figura siguiente:

PRESENTE	Hay evidencia que el indicador pertinente esté documentado dentro de la documentación del SMS del ATSP.
ADECUADO	El indicador pertinente es adecuado en base al tamaño, naturaleza y complejidad del ATSP y el riesgo inherente asu actividad.
OPERATIVO	Hay evidencia que el indicador está siendo utilizado y se está generando un resultado
EFICAZ	Hay evidencia que el indicador pertinente está logrando el resultado deseado y tiene un impacto positivo en la seguridad operacional

La herramienta puede ayudar al ATSP a evaluar si los elementos requeridos de un SMS están "presentes y adecuados" durante la implementación y en una etapa posterior "operativa y eficaz". La herramienta se basa en una serie de indicadores para cada elemento de SMS.

6.2. El trayecto del SMS.

El ATSP elegible para utilizar las disposiciones de transición puede considerar escalonar las actividades de implementación durante un período de tiempo razonable para adaptarse a su capacidad para administrar el proceso de implementación. Los beneficios de una implementación por Etapas de un SMS incluyen:



- una serie de pasos manejables para que la organización los siga con expectativas claramente definidas para cada fase
- mejora continua a través de lecciones aprendidas
- la implementación efectiva de los elementos.

Dependiendo de la madurez original de la organización con respecto a la gestión de la seguridad

operacional (según los resultados del análisis de brechas), la implementación completa del SMS puede durar varios años. Los medios y herramientas para facilitar la mejora de una cultura de seguridad operacional tienen que utilizarse continuamente desde el principio del plan de implementación.

El Apéndice 2 “Ejemplo de método de evaluación de la madurez de SMS” propone algunas pautas para que una organización autoevalúe la madurez de su SMS a lo largo de su proceso de implementación.

6.3. Análisis de brechas.

El análisis de brechas sirve para comparar los procedimientos y procesos de gestión de la seguridad operacional existentes en el proveedor de servicios de tránsito aéreo, con los requisitos contenidos en la estructura del SMS.

El análisis de brechas facilita el desarrollo del plan de implantación del SMS, al identificar las brechas que deben ser satisfechas para lograr una implantación completa. Una vez que se ha completado y documentado este análisis, aquellos recursos y procesos que han sido identificados como faltantes o inadecuados, formarán la base del plan de implantación del SMS.

A continuación, se detalla una lista de verificación con preguntas para facilitar la evaluación sistemática y ordenada de los procesos y recursos existentes. Una vez completado el cuestionario, quedarán evidenciadas las mejoras y acciones requeridas.

El responsable de la implementación en conjunto con el equipo de implementación deberá evaluar las preguntas del GAP Analysis del SMS propuesto por la OACI (adjunto 5). Para cada pregunta se solicita que responda SI o NO dependiendo sea el caso, si la respuesta es SI, se deberá de describir la evidencia que respalda dicha respuesta, pero en el caso de que la respuesta sea negativa, el equipo encargado de la implementación deberá definir una medida correctiva para cada una de las preguntas con una respuesta negativa; estas medidas conformaran el Plan de Implementación del SMS, conforme se describe a continuación:

Una vez completado en análisis de brechas, debe ser documentado por el ATSP y enviado a la AAC para generar registros y evidencias del proceso de implementación del SMS dentro del ATSP.

6.4. Plan de implementación

Procesos de evaluación

Las organizaciones que aún no han implementado un SMS, y aquellas que realizan una solicitud inicial, deben presentar un plan de implementación de SMS a la AAC que describa cómo se implementará el sistema para la gestión de la seguridad operacional.

La AAC evaluará el plan y proporcionará retroalimentación a la organización. La AAC, si es aceptable, aprobará el plan de implementación de la organización.

Se deben considerar las siguientes tres acciones antes de desarrollar el plan de implementación:

1) Identifique al Gerente Responsable

   Sujeto a variaciones en cada organización, se espera que el Gerente Responsable tenga:
   - Plena autoridad para asuntos financieros y de recursos humanos.
   - Responsabilidad directa por la conducción de los asuntos de la organización.
   - Responsabilidad final por todos los asuntos de seguridad operacional.

2) Identifique la persona o el equipo de la organización responsable de desarrollar el plan de implementación.

3) Designe al Responsable de seguridad operacional. El Responsable de seguridad operacional deberá implementar el plan de implementación del SMS en nombre del Gerente Responsable además de sus funciones operativas

El desarrollo del plan de implementación del SMS podría considerarse como un proyecto podrían ayudar a la organización a enmarcar y ejecutar el plan de implementación de SMS.

Etapa 1 – Análisis de brechas
Esta Etapa es fundamental para definir un plan de implementación de SMS eficiente y eficaz.

Como primer paso de la Etapa 1, es necesario aclarar el perímetro del SMS (descripción del sistema). Además de la revisión de los requisitos de SMS aplicables a la organización en comparación con el sistema de gestión existente, el análisis de brechas ayudará a identificar lo que ya existe dentro de la organización y lo que falta.

La Etapa 1 debe considerarse completada cuando se logre el análisis de brechas.

A partir de los resultados del análisis de brechas y considerando lo que falta en su sistema de gestión para satisfacer las necesidades de SMS, la organización debe considerar pasar por todas o parte de las siguientes etapas.

Etapa 2 – Definición, planificación y preparación.
Esta Etapa debe considerarse completada cuando se cumplan los siguientes elementos:

- Objetivos de seguridad definidos y aprobados por el Gerente Responsable.
- Política de seguridad operacional firmada por el Gerente Responsable y comunicada dentro de la organización.
- Estructura de gobernanza de SMS implementada con responsabilidades de seguridad operacional establecidas.
- Personal que apoyará la implementación del plan de implementación de SMS identificado, designado y consciente de los conceptos básicos y objetivos de SMS.
- Plan de implementación de SMS aprobado.
- El plan de implementación de SMS deberá:
  - Abordar las brechas identificadas como resultado de la Etapa 1, definiendo acciones y responsabilidades.
  - Incluya cronogramas e hitos.
  - Abordar la coordinación con las organizaciones interconectadas
  - Ser aprobado por el Gerente Responsable.
  - Ser revisado periódicamente y actualizado, según sea necesario.

Etapa 3 – Desarrollo e implementación
Esta Etapa deberá considerarse completada cuando se logran todas las acciones definidas en el plan de implementación (Etapa 2) y se demuestra que el SMS implementado cumple con este estándar.

Como parte del despliegue, los siguientes temas deberán estar definidos, documentados y operativos. Se pueden considerar en una secuencia adaptada a las prioridades de la organización, tal como se define en el plan de implementación:

- Sistema de recolección de datos, comenzando con el mecanismo de notificación (incluyendo fuentes de datos, métodos y medios para recolectar y filtrar, etc.).
- Proceso de identificación de peligros.
- Procesos de mitigación y evaluación de riesgos de seguridad operacional:
  - La organización estará, al menos, preparada para realizar análisis de seguridad operacional basados en la información obtenida a través del sistema de notificación.
  - Esquema de la instrucción de la SRM.

- Aseguramiento de la seguridad operacional:
  - Control y medición del rendimiento en seguridad operacional.
  - Gestión de cambios.

- Promoción de la seguridad operacional:
  - Comunicación de seguridad operacional, teniendo en cuenta que el personal de alta y media dirección es el motor de un SMS eficaz.
  - Plan de sensibilización/instrucción para todo el personal, según sea apropiado.

- Documentación del SMS.
- Evaluación de la preparación del SMS:
  - El SMS implementado se evalúan contra el plan de implementación. Esta evaluación podría realizarse utilizando el método de evaluación propuesto en el Apéndice 2 “Ejemplo de método de evaluación de madurez de SMS”.
  - Según corresponda, se podría emitir una declaración de cumplimiento para respaldar la aceptación por parte de la AAC.

Etapa 4 – Mejora continua
Con la finalización de la Fase 3, la organización deberá tener todos los componentes/elementos de SMS requeridos operativos.

La implementación de iniciativas de mejora continua es clave para gestionar nuevos peligros o amenazas asociados a las continuas evoluciones del sistema de aviación global con el objetivo de mantener el más alto nivel de seguridad operacional de la aviación. Estas iniciativas deben estar sujetas a un plan de acción de mejora.

Contenido del plan
El plan de implementación describe cómo la organización tiene la intención de implementar procesos que cumplen con los requisitos de la RAB211. Por lo tanto, el plan de implementación deberá ser una estrategia para gestionar la implementación de SMS, incluyendo recursos adecuados y un cronograma realista. Como cualquier cambio comercial, la implementación de SMS requerirá cierto nivel de inversión para abordar la instrucción, los cambios de documentación, el tiempo de desarrollo y posiblemente las herramientas del sistema para administrar los flujos de datos y ayudar con el análisis. Los cambios que son necesarios para implementar el SMS deben gestionarse de forma estructurada para garantizar que existe una conciencia de los impactos y las posibles consecuencias, y que estos se gestionan de forma adecuada.

El plan de implementación no tiene por qué ser complejo. Sin embargo, debe haber suficientes detalles para garantizar que la organización haya identificado cómo cumplirá el objetivo general de implementar con éxito un SMS. Esto significa que cada elemento está presente y es adecuado en el contexto de las actividades que realiza la organización.

El plan de implementación debe desarrollarse en consulta con el Gerente Responsable y el personal clave del ATSP. La solicitud deberá incluir una declaración del Gerente Responsable de que el plan es apropiado, alcanzable y cuenta con los recursos adecuados, además de una fecha propuesta para la implementación.

El plan de implementación debe documentarse en un formato que sea apropiado para dimensión, el contenido y la complejidad, y debe abordar lo siguiente:
- las tareas identificadas durante el proceso de análisis de brechas, de acuerdo con los requisitos del tamaño de la organización y la complejidad de sus servicios;
- cronogramas e hitos para cada tarea o grupo de tareas desde la etapa de planificación, hasta la implementación completa de SMS;
- para un enfoque de implementación por fases o etapas, las tareas se ordenan en una progresión lógica de acuerdo con la asignación de fases de sus elementos relacionados;
- información sobre quién es responsable de completar la tarea o grupo de tareas identificado, incluida la gobernanza general del plan de implementación;
- un proceso identificado mediante el cual el estado y el rendimiento del plan de implementación del SMS se monitorea regularmente y se toman los pasos para mitigar el rendimiento deficiente;
- información que muestre cómo la coordinación de la integración de proveedores externos relacionados con la seguridad operacional sin un SMS, están dentro del alcance del SMS de la organización;
- requerimientos de recursos;
- gestión de riesgos asociados con la implementación de SMS.

Cualquier cambio material realizado por el ATSP a un plan de implementación aprobado debe documentarse y enviarse a la AAC para su aprobación. Un cambio material en este contexto es cualquier cambio que pueda afectar la capacidad de la organización para demostrar un rendimiento aceptable para la fecha de implementación y/o un cambio constante de las fechas de entrega de las tareas, como:

- cambios en quién es responsable de completar la tarea;
- una reducción significativa de los recursos disponibles;
- reprogramación debido a la subestimación de la complejidad de los cambios necesarios
- cambios en el alcance de la actividad operativa que se está realizando.

Guía de implementación

Los siguientes pasos proporcionan una guía para implementar un SMS.

PASO	DIRECTRICES
Paso 1: **Realizar un análisis de brechas**	**Un análisis de brechas se utiliza para identificar lo que el ATSP tiene implementado y lo que aún necesita. El contenido de esta circular de asesoramiento y los requisitos para un SMS proporcionan información que permitirá a una organización desarrollar una lista de lo que se necesita, lo que ya está en su lugar y lo que se requiere para llenar cualquier vacío.**
Paso 2: **Desarrollar un plande gestión**	**El Gerente Responsable deberá desarrollar un plan de gestión de SMS que podría incluir:** • **Logros relacionados con la seguridad operacional, objetivos y medidasde rendimiento** • **identificación de miembros del equipo de implementación y líneas dereporte** • **asignación provisional de recursos.** **Esto ayudará a determinar las prioridades del ATSP para la implementaciónde un SMS.**
Paso 3: **Desarrollar un plande implementación**	**El plan de implementación puede documentarse de diferentes formas, desde una simple hoja de cálculo hasta un software de proyecto especializado. Debe desarrollarse extrayendo la lista de tareas requeridas del análisis de brechas, ordenándolas en términos de la prioridad de implementación y enumerando los recursos requeridos y las personas responsables de completarlas. El plan de implementación debe incluir hitos y un cronograma consistente para cada una de las tareas que requerirán un monitoreo regular para ayudar a mantener el plan de implementación en marcha.** **Envíe el plan de implementación a la AAC para su aprobación.** **Esto puede incluir el formulario de la herramienta de evaluación del sistemade gestión de seguridad operacional de la AAC completo si se utiliza para elanálisis de brechas.**
Paso 4: **Asignación de rendición de cuentas y responsabilidades**	**Es esencial que los roles y responsabilidades del personal en la implementación de un SMS estén definidos, comunicados claramente y su participación asegurada. Las responsabilidades individuales recomendadas del Gerente Responsable, personal clave y personal individual deben incluirse en las descripciones de sus funciones.**

Paso 5: **Desarrollar políticas, procesos / Procedimientos y otra documentación.**	**Es esencial garantizar que exista un SMS integrado, bien entendido y bien comunicado.** **Se requiere una declaración de política de seguridad operacional diseñada por la alta dirección y respaldada por el Gerente Responsable que describa su compromiso con la seguridad operacional.** **El manual de gestión de la seguridad operacional (MSMS) debe cubrir los procesos, acciones y flujos de trabajo involucrados.**
Paso 6: **Establecer el kit de herramientas de SMS**	**Un conjunto de herramientas contiene las acciones, los procesos y lasherramientas de apoyo que son el corazón de un SMS.** **Puede incluir cualquiera o todo de lo siguiente:** • **procesos de identificación de peligros, incluidos los resultados de lasinvestigaciones de seguridad operacional** • **procesos de evaluación de riesgos y plantillas de apoyo** • **procesos internos de notificación de seguridad operacional (incluida una base de datos que una organización puede utilizar para capturar notificaciones).** • **procedimientos de investigación de seguridad operacional interna** • **un sistema de auditoría interna** • **procesos de comunicación de seguridad operacional, como reuniones del SRC, y cómo se escala y difunde la información relacionada con laseguridad operacional.** • **programa de instrucción en seguridad operacional.**
Paso 7: **Implementar un programa de instrucción en SMS**	**Una vez que los planes, las políticas, los procedimientos y el conjunto de herramientas están en su lugar, la justificación para implementar un SMS debe comunicarse a todo el personal. Esto se puede hacer a través de un programa de instrucción estructurado que puede incluir una presentación para todo el personal, un paquete basado en la web o una serie de boletines informativos o correos electrónicos. Considerar el nivel de instrucción requerido por aquellos con responsabilidades de seguridad operacional (por ejemplo, los ejecutivos responsables, el responsable de seguridad operacional, los certificadores de conformidad de mantenimiento y el personal operativo.**
Paso 8: **Aceptación del SMS – Fecha de implementación**	**Para la aceptación del SMS, la AAC realizará una inspección in situ para verificar la madurez del SMS en un nivel ADECUADO antes de la aceptación del mismo.** **Esto debe incluir un formulario de herramienta de evaluación de SMS completo.**
Paso 9: **Vigilar y revisar**	**Una vez que se han implementado los componentes de un sistema de gestión de la seguridad operacional, es importante asegurarse de que realmente estén funcionando. Las medidas de rendimiento descritas originalmente en el plan de gestión se pueden utilizar para rastrear el éxito del SMS.** **La forma de rastrearlos podría ser a través de una reunión del SRC o a través de una revisión periódica de la gestión del SMS.**

6.5. Aceptación del SMS: fecha de implementación.

Generalidades.

Los procesos de aceptación del SMS de la AAC actuales se utilizarán para la evaluación del desarrollo de SMS de una organización. Consistirá en una evaluación del MSMS y la documentación de apoyo,

seguida de una inspección y demostración.

Evaluación y revisión.
Como parte del proceso de evaluación, se revisará el manual y la documentación de respaldo para confirmar que la organización ha desarrollado e implementado su SMS. Los solicitantes deben presentar documentación que demuestre que han abordado todos los elementos del SMS.

Esto se logra mejor utilizando la herramienta de evaluación del sistema de gestión de seguridad operacional que la AAC utilizará para ayudar a evaluar la capacidad del SMS de la organización. Los procesos y procedimientos de SMS pueden documentarse en un manual de la organización o incorporarse en otro manual.

Los cambios organizacionales, como el nombramiento de un Responsable de seguridad operacional (la persona responsable de facilitar y gestionar el SMS de la organización) también deberán enviarse al mismo tiempo. Los cambios del personal clave del ATSP asociada con la implementación de SMS estarán sujetos al proceso normal de evaluación de alto nivel de la AAC.

Cuando corresponda, la integración de los procesos de gestión de la seguridad operacional con los procesos de gestión de la calidad deberá estar claramente establecida y documentada.

Inspección y demostración.
Después de la evaluación de la documentación, la AAC llevará a cabo una inspección en el sitio para garantizar que las políticas, procesos, procedimientos y sistemas documentados estén presentes y sean adecuados, y para validar cualquier observación de la revisión de la documentación. Cuando sea posible, la AAC puede requerir que la organización demuestre, en la medida de lo posible, rendimiento real del SMS.

Una vez que la AAC haya evaluado que la organización ha logrado satisfactoriamente su plan de implementación y que la capacidad y el rendimiento del SMS están en una madurez de 'presente' y 'adecuado', proporcionará una confirmación en la forma y manera establecida por la AAC de la aceptación del SMS. Esto incluirá una aceptación del MSMS.

Monitoreo continuo.
El SMS de una organización estará sujeto a la vigilancia de rutina de la AAC (inspección y monitoreo) para verificar que la capacidad y el rendimiento del SMS están madurando hacia "operativo" y "eficaz".

Las actividades de vigilancia de la seguridad operacional de la AAC se basan en los riesgos de seguridad operacional identificados a través del análisis. Las decisiones e intervenciones reglamentarias se basan en la evaluación del rendimiento de seguridad operacional de la organización. El monitoreo continuo se utiliza para obtener garantía de la capacidad de gestión de la seguridad operacional de la organización y su capacidad para cumplir con sus objetivos de rendimiento de seguridad operacional.

Vigilancia.
Para las organizaciones que tienen un SMS aceptado, la AAC evaluará el SMS de acuerdo al plan de vigilancia establecido. En esa etapa, el nivel de madurez debería haber progresado desde el nivel “presente y adecuado” a “operativo” y en desarrollo hacia eficaz. Se recomienda que las organizaciones utilicen la herramienta de evaluación de SMS para evaluar y demostrar la progresión en su madurez y cualquier cambio introducido como parte de las actividades de mejora continua.

6.6. Madurez del SMS

¿Cómo va el SMS?
En realidad, la implementación del SMS es el nuevo negocio y debería haber pocas cosas "habituales" al respecto, aparte de que el ATSP aplica rutinariamente la gestión de riesgos de seguridad operacional a las decisiones diarias y está activamente intranquila: ¿qué podría salir mal todavía?

Habrá oportunidades para que la organización se detenga y reflexione sobre lo que está funcionando, lo que podría funcionar mejor y lo que no funcionó como se esperaba; sucesos como:

- Cambio significativo: ¿se logró la gestión del proceso de cambio?
- Alto riesgo de seguridad operacional identificado: ¿identificación proactiva o reactiva?
- Revisión del SMS: ¿los objetivos y las medidas le brindan la información para respaldar la toma de decisiones?

Intentar concentrarse en lo que está funcionando bien para aprovechar la oportunidad de compartir y aplicar esos procesos y prácticas en toda la organización y, cuando sea posible, incluso en los terceros relacionados.

¿Cómo sé que el sistema está madurando?
Una forma es examinar críticamente cada componente (o elemento) como un proceso para ver si está operando según lo previsto, luego buscar resultados para ver si es efectivo. Utilizar la herramienta de evaluación de SMS para ayudarlo y actualizarla para cualquier cambio. Por ejemplo:

Proceso	Etapa de implementación		Mayor capacidad / Madurez	
	Presente	Adecuado	Operativo	Eficaz
Gestión del cambio	El proceso está establecido y documentado	Existen desencadenantes para utilizar el proceso de gestión de cambio. El proceso considera a las partes interesadas internas / externas	El proceso se está utilizando y se establecen controles de riesgo antes de que se produzca el cambio	El proceso se utiliza para todos los cambios que pueda afectar la seguridad operacional. Iniciado de manera planificada, oportuna y consistente.
Nombramiento de personal clave / comunicación de seguridad operacional	La organización ha establecido comités de seguridad operacional	El alcance de los comités de seguridad operacional incluye riesgos de seguridad operacional y problemas de cumplimiento. La asistencia del comité de seguridad operacional de más alto nivel incluye menos el Gerente Responsable y el personal clave del ATSP.	Muestra de actas, reuniones en curso, asistencia, discusiones, acciones identificadas. Se está monitoreando la efectividad del SMS, incluidos los recursos suficientes, las acciones tomadas y se han establecido las medidas apropiadas.	

7. **APENDICES:**

Apéndice 1 – Mejores prácticas para la gestión de riesgos de seguridad operacional (SRM)

Propósito
El propósito de este apéndice es introducir algunas de las mejores prácticas para la gestión de riesgos de seguridad operacional.

- Ejemplos de técnicas de evaluación de riesgos (fuente ISO 31010):
  - Lluvia de ideas.
  - Lista de verificación.
  - Análisis de causa raíz.
  - Análisis de modos y efectos de falla (FMEA).
  - Análisis del árbol de fallas.
  - Árbol de decisiones.
  - Análisis de Bow tie.
  - Simulación de Monte Carlo,
  - Matriz de consecuencias / probabilidades.

Alcance de la gestión de riesgos de la seguridad operacional (SRM)
SRM debe cubrir las siguientes áreas:

- Descripción del sistema: para establecer el marco para la identificación de peligros.

- Identificación de peligros: para identificar peligros de acuerdo con un método.

- Identificación de riesgos de seguridad operacional: para identificar los riesgos de seguridad operacional asociados con los peligros identificados.

- Análisis de riesgos de seguridad operacional: para determinar la gravedad y la probabilidad de un riesgo asociado con los peligros identificados.

- Evaluación de riesgos de seguridad operacional: a partir de los resultados del análisis de riesgos, para determinar si un riesgo es inaceptable según los criterios definidos.

- Control de riesgos de seguridad operacional: para eliminar, reducir o mitigar un riesgo de seguridad operacional mediante acciones que se definirán cuando el riesgo es inaceptable.

  Ejemplos de situaciones en las que la SRM debería ser aplicada por diferentes tipos de organizaciones:

- Organizaciones que no tienen una aprobación o certificado.

- Las organizaciones no aprobadas deberían aplicar la gestión de riesgos de seguridad operacional a lo siguiente:
  - Implementación de nuevos sistemas.
  - Revisión significativa de sistemas existentes.
  - Desarrollo de procedimientos operativos.
  - Identificación de peligros o controles de riesgo ineficaces a través de los procesos de garantía de seguridad operacional.

Mejores prácticas para la identificación de peligros
La identificación de peligros permite identificar “problemas de seguridad operacional” o “amenazas” (a los que se hace referencia como peligros) que requieren la aplicación de la SRM y SA. Esto permite al ATSP asignar recursos de gestión de la seguridad operacional a fuentes de riesgo de seguridad operacional potencial significativo y evitar dedicar recursos a riesgos más bajos o insignificantes.

N°	Mejores prácticas para la identificación de peligros
1	Evitar tratar de identificar todos los peligros concebibles o teóricamente posibles. Esto no es posible ni deseable. Se requiere juicio para determinar el nivel adecuado de detalle en la identificación de peligros. Debe ejercerse la debida diligencia para determinar los peligros importantes y razonablemente previsibles relacionados con las operaciones de la organización.
2	Centrarse en las áreas con mayor potencial para introducir peligros que puedan conducir a riesgos de seguridad operacional inaceptables, por ejemplo: ➢ escenarios de accidentes (por ejemplo, de investigaciones) ➢ Factores humanos y organizacionales (por ejemplo, actividad que puede conducir a riesgos inaceptables y afectar la seguridad operacional de los servicios que realiza el ATSP) ➢ Cambios en las decisiones y procesos del negocio (por ejemplo, cambios significativos en los principios de un procesador en la estructura de la organización o ambos). ➢ Interfaz con otras organizaciones (por ejemplo, subcontratistas). ➢ Novedad, criticidad o complejidad o ambas cosas en el servicio que brinda el ATSP (por ejemplo, inspección de la estructura compuesta).
3	Identificar el peligro a partir de la revisión/análisis de los datos de seguridad operacional disponibles, por ejemplo: ➢ Notificaciones/publicaciones de seguridad operacional (por ejemplo, informes de la OACI, AAC, explotadores, otras organizaciones). ➢ Informes de auditoría. ➢ Estudios de seguridad operacional. ➢ Investigaciones ➢ Análisis de seguridad operacional en el marco de las iniciativas de mejora de la seguridad operacional.
4	No mezclar los peligros con factores desencadenantes/contribuyentes para mantener un número razonable de peligros confirmados necesarios para ser considerados para la evaluación de riesgos basada en la complejidad de la organización.
5	Agrupar los peligros en categorías, por ejemplo: **Peligros sistémicos:** ➢ Organizacionales: gestión, recursos, documentación, procedimientos. ➢ Humano: limitaciones de la persona que en el sistema tiene el potencial de causar daño, fatiga, estrés. **Peligros operacionales:** ➢ Técnico: diseño. ➢ Funcionamiento del producto. **Peligros para el medio ambiente:** ➢ Regulación, finanzas y presupuesto, instalaciones, cambio climático.
6	No mezclar el peligro con sus consecuencias previsibles. Un peligro no está sujeto a la clasificación de gravedad o probabilidad, pero su riesgo de seguridad operacional asociado sí lo está.
7	Considerar que, dependiendo de su naturaleza, categorización y escenario de identificación: ➢ No todos los peligros identificados deben resultar en acción por el SMS (p.ej. análisis de riesgos de seguridad operacional y acciones de control de riesgos). ➢ Varios peligros pueden resultar en acciones combinadas de SMS
8	Considerar que varios peligros ya están sujetos a una evaluación sistemática del riesgo y la mitigación del riesgo en el marco de la provisión de los servicios ATS y que pueden no necesitar más actividades de SMS.
9	Considere la posibilidad de identificar los peligros de manera incremental desde la implementación inicial de SMS hasta cuando el SMS este totalmente operativo.
10	Considere revisar los peligros en un ciclo cerrado de mejora continua.

Evaluación y control de riesgos de seguridad operacional

El riesgo de seguridad operacional debe identificarse utilizando los métodos, técnicas y/o herramientas más apropiadas.

.

Cuando se identifica, el riesgo de seguridad operacional debe analizarse para determinar su gravedad y probabilidad. El análisis cualitativo y el juicio técnico son aceptables cuando no hay suficientes datos cuantitativos disponibles.

La evaluación de riesgos de seguridad operacional utiliza los resultados del análisis de riesgos para determinar la aceptabilidad del riesgo de acuerdo con criterios definidos. Cuando un riesgo de seguridad operacional es inaceptable, se deben definir e implementar acciones de control de riesgos de seguridad operacional.

N°	Mejores prácticas para la evaluación y control de riesgos de seguridad operacional
1	El análisis y la evaluación de riesgos solo deben llevarse a cabo para peligros confirmados que necesitan más acciones de SMS.
2	El riesgo inaceptable debe estar sujeto a acciones de control de riesgo para eliminar, reducir o mitigar el riesgo.
3	Las acciones de control de riesgos deben monitorearse con retroalimentación al menos de lo siguiente: ➢ Gerentes operativos relevantes impactados por los riesgos de seguridad operacional. ➢ Personal de gestión de seguridad operacional relevante para monitorear la efectividad del control de riesgos.
4	El análisis de riesgos en términos de gravedad y probabilidad debe revisarse si se ha detectado un control de riesgos ineficaz.
5	La evaluación de riesgos debe revisarse periódicamente para garantizar que las acciones de control de riesgos identificadas sigan siendo adecuadas.
6	Las acciones de control de riesgos podrían ser una combinación de acciones a corto plazo y acciones a largo plazo: ➢ Es posible que las acciones de control de riesgos de seguridad operacional a largo plazo no se conozcan hasta o solo se puedan determinar cuándo se implemente el control de riesgos a corto plazo. ➢ Una acción intermedia de control de riesgos de seguridad puede resultar útil antes de que ocurra un riesgo más grave.
7	Los criterios de aceptabilidad del riesgo de seguridad operacional deben revisarse en función de: ➢ Retroalimentación de la determinación del control de riesgos. ➢ Medición y seguimiento del rendimiento en seguridad operacional.
8	Deben registrarse las pruebas y la justificación de las decisiones sobre la evaluación de riesgos de seguridad operacional (nivel de riesgo) y los controles (acciones).

Apéndice 2 – Ejemplo de método de evaluación de madurez de SMS

Antecedentes y objetivo
Este apéndice proporciona orientación y propone un método para la evaluación de la madurez del SMS durante la implementación inicial y la mejora continua.

La organización debe utilizarlo como una autoevaluación, pero las autoridades de aviación también podrían considerarlo para evaluar la madurez del SMS de la organización.

Nota. Dentro de este método, la columna "Qué buscar (ejemplos de evidencia)" es una descripción simplificada de los medios de cumplimiento / evidencia con los requisitos de SMS. El texto básico y otros apéndices de esta circular de asesoramiento siguen siendo la base para la evaluación de la madurez de los SMS.

Esta guía:
- Se basa en un conjunto de criterios y evidencias para ayudar a determinar la madurez general de un SMS con respecto a los 12 elementos del marco de SMS según se captura en este estándar y como resultado de lo establecido en el RAB211.
- Considera el tránsito de mejora de la madurez de SMS desde Presente (P), Adecuado (S) hasta ser Operativo (O) y el Eficaz (E).

Definiciones
Niveles de madurez. Los niveles de madurez se pueden definir de la siguiente manera:

- Nivel Presente (P): Hay evidencia de que el elemento está definido y documentado.
- Nivel Adecuado (S): Es apropiado al tamaño, naturaleza y complejidad del ATSP y el riesgo inherente a su actividad.
- Nivel Operativo (O): Hay evidencia de que el elemento se implementa con resultados / entregables.
- Nivel Eficaz (E): Existe evidencia de que el ítem está logrando el resultado deseado y tiene un impacto positivo en la seguridad operacional.

Evidencia. Documentación, notificaciones, registros de entrevistas y discusiones. Si bien la finalización del nivel de madurez "Presente y Adecuado" se basa en la documentación de procedimiento disponible, la finalización de los niveles de madurez "Operativo" y "Eficaz" se basa en la aplicación consistente de procesos documentados para producir y evaluar hechos, cifras y registros.

Utilizando el método
Este método se puede utilizar por primera vez para completar el análisis de brechas. Este análisis de brechas y el plan de implementación resultante son los principales insumos para la (s) próxima (s) evaluación (es) de madurez del SMS.

El método puede usarse tal cual o puede ser personalizado por cada organización dependiendo de su dimensión, complejidad, estructura y actividades.

Para cada elemento de SMS, se enumera una serie de "criterios de cumplimiento y rendimiento" seguidos de evidencia (es decir, "qué buscar"). Cada criterio debe revisarse para determinar si se encuentra en el nivel de madurez Presente, Adecuado, Operativo o Eficaz, de modo que se pueda evaluar la madurez general del elemento SMS, teniendo en cuenta los demás elementos interrelacionados (por ejemplo, “La política de seguridad operacional debe ser comunicada, con visible respaldo, en toda la organización”). Este requisito puede declararse a nivel operativo bajo las condiciones de que se nombre a un Gerente Responsable y se le informe sobre los SMS y se defina y promueva la política de seguridad operacional. Estos aspectos están sujetos a otros elementos dentro de esta herramienta de evaluación (como 1.2 “Responsabilidades de seguridad operacional, 4.2 “Comunicación de seguridad operacional”).

Una vez que se han evaluado todos los criterios para cada elemento de SMS, se puede registrar un juicio en el bloque de "comentarios", con respecto al nivel general de madurez de dicho elemento de SMS.

Alcanzar un nivel de madurez para el SMS general no significa que cada elemento de SMS esté en el mismo

nivel de madurez (por ejemplo, algunos elementos de SMS pueden estar en el nivel "Presente", otros en nivel “Adecuado”, otros en el nivel "Operativo" y algunos en el nivel " Nivel Eficaz”. En este estado, la madurez general del SMS se puede considerar en el nivel “Operativo”). Una persona que utilice este método debe estar familiarizada con lo siguiente:

- Sistemas de gestión de la seguridad operacional basados en el marco de SMS de la OACI.
- Principios y técnicas de evaluación del sistema de gestión.
- Principios de garantía de seguridad operacional y gestión de riesgos de seguridad operacional.

Apéndice 3 – Guía del contenido del Manual SMS

Antecedentes y objetivo
Este apéndice proporciona orientación y un resumen del contenido del manual SMS.

Un Manual SMS es parte fundamental de la documentación SMS que debe tener disponible cualquier Proveedor de Servicios de Tránsito Aéreo y está basada en el Anexo 19 de la OACI Gestión de la Seguridad Operacional y en el Doc 9859 de la OACI Manual de Gestión de la Seguridad Operacional (SMM).

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

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

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

El Manual SMS puede ser un documento independiente o puede integrarse con otros documentos organizacionales (o documentación) del proveedor de servicios. En el caso de que la información de los procesos de la organización SMS ya se encuentre detallada en documentos existentes la referencia cruzada apropiada para tales documentos podría ser suficiente, sin embargo, Es recomendable que el Manual SMS haga referencia a la documentación sobre la preparación, recopilación y mantenimiento de registros operacionales que acreditan la implantación y operación efectiva del SMS.

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

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

Este Manual, así como cualquier documento existente SMS debe mantenerse al día. Como parte del proceso de actualización, debe tenerse presente que antes de realizar modificaciones significativas en el Manual SMS, es necesario la coordinación con la AAC ya que este es un manual debe contar con la aceptación de la Autoridad como evidencia de aceptación del SMS propuesto por la organización.

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

a) La política y los objetivos de seguridad operacional;
b) Las referencias a cualquier requerimiento SMS regulatorio aplicable;
c) Una descripción del sistema;

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

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

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

a) Compromiso de la dirección;
b) Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional;
c) Designación del personal clave de seguridad operacional;
d) Coordinación de la planificación de respuestas ante emergencias; y
e) Documentación SMS.

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

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

Como parte del compromiso se deberá establecer un procedimiento explicando los procesos a seguir para presentar los informes en materia de seguridad. Asimismo, se deberá indicar claramente qué tipos de comportamientos son inaceptables en lo que respecta a las actividades que realiza el proveedor de servicios y también deberá incluir las circunstancias en las que no se podrán aplicar medidas disciplinarias apuntando a una cultura justa y de protección de los empleados.

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

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

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

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

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

Nota. A los efectos de esta CA, el concepto de “obligación de rendición de cuentas” se refiere a una “obligación” que no puede delegarse, y “responsabilidades” se refiere a las funciones y actividades que pueden delegarse.

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

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

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

a) Revise los objetivos de seguridad operacional;
b) Supervise los rendimientos de seguridad operacional y los logros en los objetivos de seguridad operacional establecidos;
c) Tome decisiones de seguridad operacional a tiempo;
d) Asigne los recursos apropiados;
e) Pedir cuentas a los respectivos jefes por sus responsabilidades por seguridad operacional, rendimiento y fechas de implementación; y
f) Ser visualizado por todo el personal como un ejecutivo a cargo y comprometido con la seguridad operacional.

El Director Ejecutivo no está generalmente implicado en las actividades diarias de la organización o los problemas que a diario se enfrentan en el trabajo y por lo tanto se debe asegurar que existe una estructura organizacional adecuada para administrar y operar el SMS. La responsabilidad de la gestión de la seguridad operacional a menudo se delega en el equipo de alta gerencia y otro personal clave de seguridad operacional. Sin embargo, aunque puede delegarse la responsabilidad de la operación diaria del servicio SMS, el Director Ejecutivo no puede delegar la rendición de cuentas para el SMS ni puede delegar las decisiones sobre los riesgos de seguridad operacional. Por ejemplo, no se puede delegar la rendición de cuentas de seguridad operacional siguientes:

a) Garantizar que las políticas de la seguridad operacional sean apropiadas y eficientemente comunicadas;
b) Garantizar recursos necesarios (financieros, personal, capacitación, compras); y
c) Garantizar los límites de riesgo de seguridad operacional aceptables y los recursos para los controles necesarios.

El Director Ejecutivo debe ser responsable de:

a) Proveer suficiente financiamiento y recursos humanos para la apropiada implantación de un eficiente y eficaz SMS;
b) Promover una cultura de seguridad operacional positiva;
c) Establecer y promover una política de seguridad operacional;
d) Establecer los objetivos de seguridad operacional de la organización;
e) Garantizar que el SMS es apropiadamente implantado y está de acuerdo con los requerimientos y

necesidades; y
f) Supervisar la mejora continua del SMS.

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

a) Resolución sobre asuntos de seguridad operacional; y
b) Operaciones bajo certificado, autorización o aprobación de la organización, incluyendo la cancelación de operaciones o actividades.

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

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

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

El proveedor de servicios debe procurar evitar conflictos de intereses entre las responsabilidades de seguridad de los miembros del personal y otras responsabilidades de su organización. Deben asignarse las obligaciones de rendir cuentas SMS y responsabilidades, de forma de reducir al mínimo cualquier superposición o vacíos.

Rendición de cuentas y responsabilidades en relación a organizaciones externas.

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

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

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

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

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

Algunas de las interfaces internas pueden parecer, a primera vista, que no están muy relacionadas con la seguridad operacional, al menos directamente, sin embargo algunas decisiones de áreas como la de marketing, finanzas, jurídica o de recursos humanos, por nombrar algunas, pueden impactar internamente la seguridad operacional sobre inversiones, recursos humanos o con acuerdos o contratos con otras organizaciones que no necesariamente aplican procesos de seguridad operacional en sus actividades, procesos o en sus productos.

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

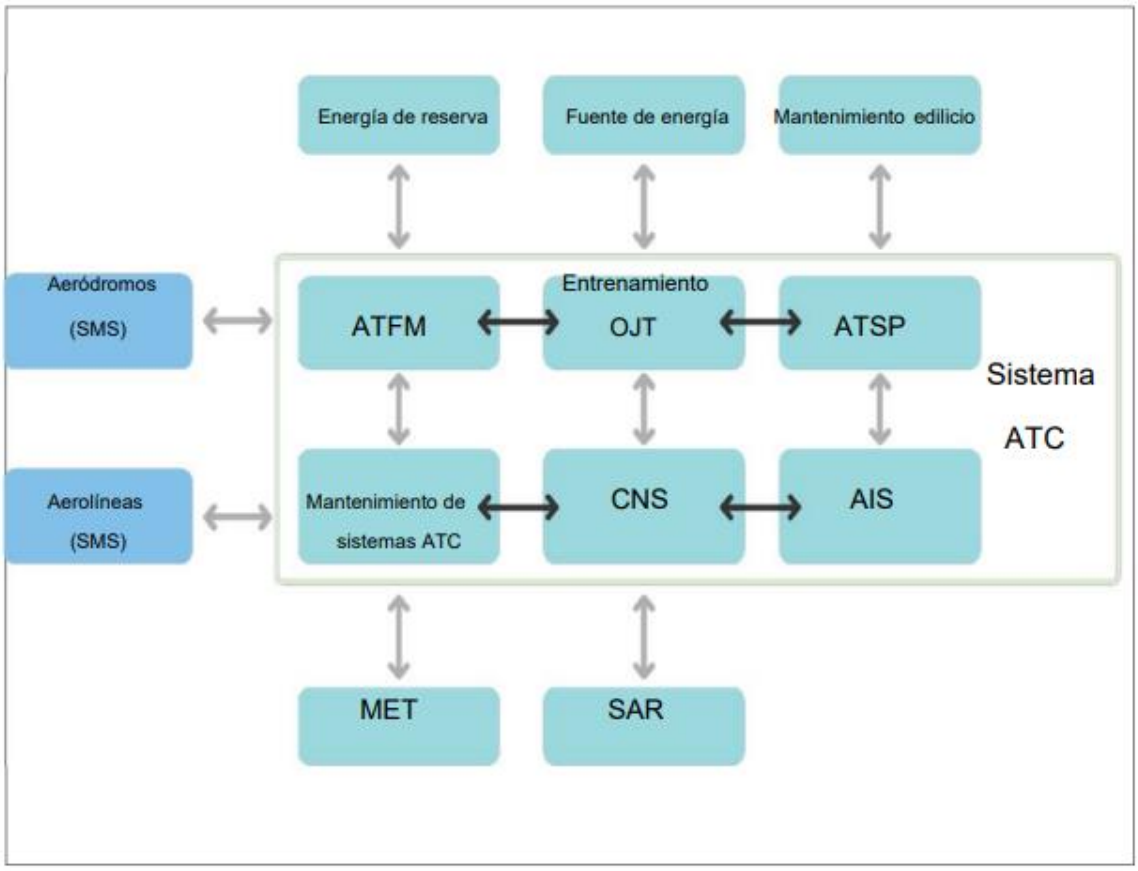


Figura 1: Ejemplo de las interfaces SMS del Proveedor de Servicios de Tránsito Aéreo

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

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

a) Qué se provee;
b) Por qué es necesario;
c) ¿Tiene un SMS u otro Sistema de gestión implantado la organización proveedora?; y
d) La interface contempla la compartición de datos de seguridad operacional/información.

El proveedor del servicio al analizar las interfaces con las otras organizaciones o sistemas debe identificar

cualquier peligro relacionado con las mismas y llevar la gestión para la identificación de peligros y evaluación de riesgo de la seguridad operacional.

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

Es necesario detallar las estructuras organizativas, los procesos y los acuerdos que sean importantes para las funciones de gestión de seguridad operacional. Puede ser que, al describir el sistema, la organización identifique la necesidad de desarrollar políticas, procesos y/o procedimientos para establecer requisitos adicionales para mejorar la gestión de la seguridad operacional, asimismo, cuando una organización elige hacer un cambio significativo o sustancial en los procesos identificados en la descripción del sistema, los cambios pueden potencialmente afectar a su línea de base de evaluación de riesgos de seguridad operacional. Por lo tanto, la descripción del sistema también debe ser revisada como parte de la gestión cuando se desarrollan procesos de cambio.

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

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

Personal clave de seguridad operacional

La asignación de personal competente para desempeñarse como Gerente de Seguridad Operacional es esencial para un SMS efectivamente implementado y en funcionamiento. El Gerente de Seguridad Operacional puede ser identificado por diversos títulos dependiendo de la normativa en cada Estado.

La persona encargada de la función de Gerente de Seguridad Operacional es responsable ante el Director Ejecutivo por el rendimiento de los SMS y por la prestación de servicios de seguridad operacional a las otras unidades de la organización.

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

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

En la mayoría de las organizaciones, una persona es nombrada como Gerente de Seguridad Operacional. Dependiendo del tamaño, naturaleza y complejidad de la organización, el rol del Gerente de Seguridad Operacional puede ser una función exclusiva o se puede combinar con otras funciones. En alguna

organización esta función es asignada a un grupo de personas.

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

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

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

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

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

Puede que por su tamaño o complejidad la organización requiera personal adicional para apoyar al Gerente de Seguridad Operacional sobre todo para las tareas de una pronta recolección de datos, análisis o la rápida y apropiada distribución dentro de la organización de la información de seguridad operacional relacionada con la valoración del riesgo y su control que deben ser hechos.

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

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

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

a) Realizando el control del rendimiento de la seguridad operacional dentro de sus áreas funcionales de la organización y asegurar que las actividades apropiadas de SRM se llevan a cabo;
b) Revisando los datos de seguridad operacional disponibles e identificando la implementación de estrategias de control de riesgos de seguridad operacional y asegurando se proporcione retroalimentación al empleado;

c) Evaluando el impacto en la seguridad operacional relacionados con la introducción de cambios organizativos o de nuevas tecnologías;
d) Coordinando la implementación de las acciones relacionadas con controles de riesgo de seguridad operacional y asegurar que se adopten medidas rápidamente; y
e) Revisando la eficacia de los controles específicos de riesgo de seguridad operacional.

Plan para la coordinación de las emergencias

Por definición, una emergencia es una situación repentina, imprevista o un suceso que requieren una acción inmediata. La coordinación de planificación de respuesta a emergencias se refiere a la planificación de actividades que se desarrollan dentro de un período limitado de tiempo durante una situación de emergencia operacional no planificado. La coordinación de planificación de respuesta de emergencia se aplica sólo a aquellos proveedores de servicio que deben establecer y mantener un ERP (“Emergency Response Plan”).

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

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

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

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

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

Nota. Debido a que la mayoría de las situaciones de emergencia requiere una acción coordinada entre las diferentes organizaciones, posiblemente con otros proveedores de servicios y con otras organizaciones externas tales como los servicios de emergencias no relacionadas con la aviación el ERP debe ser fácilmente accesible al personal clave apropiado, así como a las organizaciones externas.

Gestión de riesgos de la seguridad operacional

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

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

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

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

Procesos y procedimientos para la identificación de peligros

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

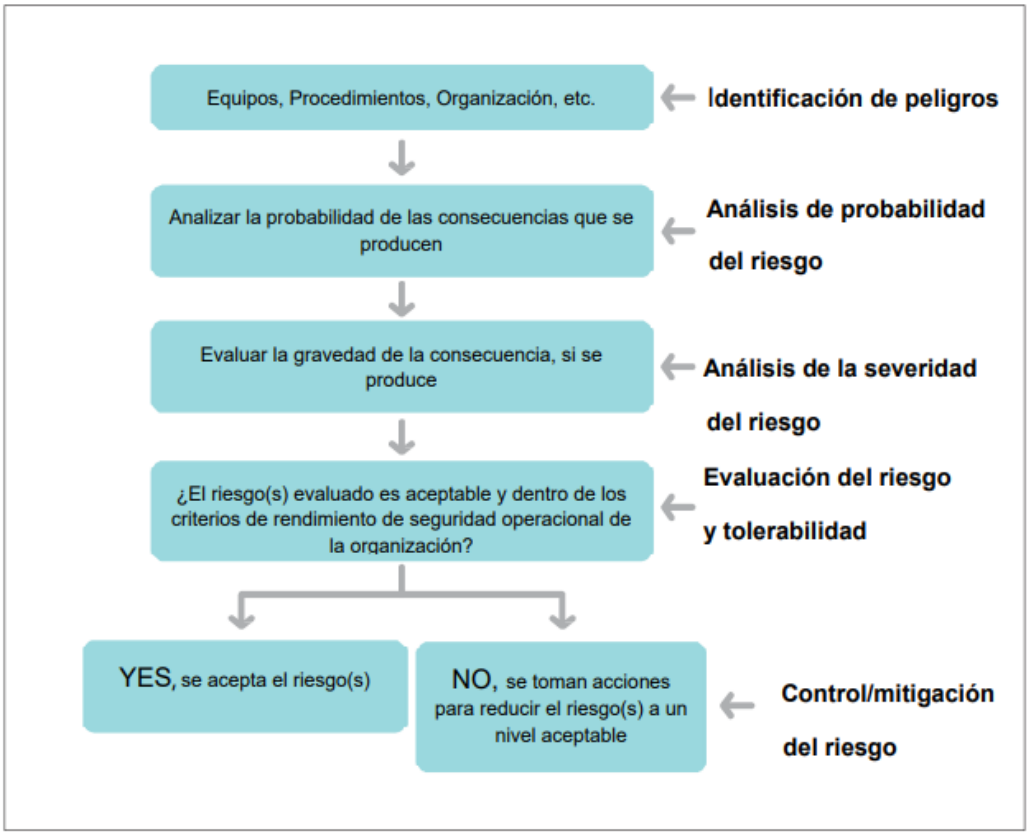
Como se puede apreciar, aunque la norma requiere que un proceso se ponga en marcha para identificar los peligros, no especifica lo que debería ser un proceso. Por lo tanto, los proveedores de servicios deben diseñar su propia metodología para la identificación de los peligros. Las dos metodologías utilizadas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

Este proceso formal debe considerar los equipos, instalaciones y sistemas. Cualquier riesgo relacionado con la seguridad operacional que se pueda identificar y controlar será un aporte muy beneficioso para la seguridad operacional. También es importante considerar los peligros que puedan existir como resultado de las interfases SMS con organizaciones externas.

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

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

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



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

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

Algunos ejemplos de fuentes externas para la identificación de peligros pueden incluir los reportes de accidentes/incidentes incluso de otros Estados, auditorías USOAP, inspecciones AAC e informes de Asociaciones de la Industria entre otras.

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

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

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

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

Cualquier persona que realiza una notificación sobre seguridad operacional debe recibir la retroalimentación respectiva sobre qué decisiones o acciones se tomaron. Esta retroalimentación sirve para demostrar que dichos informes se consideran seriamente y ayuda a promover una cultura de seguridad operacional positiva y animar a futuros informes. Es importante que se documenten los peligros identificados, una vez que se identifican los peligros, sus consecuencias (es decir, cualquier suceso específico o resultado) deben ser determinadas.

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

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

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

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

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

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

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

Una investigación de seguridad operacional del proveedor de servicio es iniciada generalmente por una notificación (informe) a través del sistema de notificación de la seguridad operacional. No todos los sucesos o peligros pueden o deben ser investigados; la decisión de llevar a cabo una investigación y su profundidad dependerá de las consecuencias reales o potenciales de riesgo del peligro o del suceso. Un escrutinio preliminar de los sucesos y peligros considerados es necesario para determinar el alto o menor riesgo potencial. La prioridad la debe tener el alto riesgo potencial. Para investigar ayuda tener estructurado y definido un enfoque para la toma de decisiones. Qué investigar y cuál será el alcance de la investigación.

Este enfoque estructurado puede considerar:

a) La severidad o gravedad potencial de los resultados;
b) Requisitos reglamentarios o de organización para llevar a cabo una investigación;
c) Se puede mejorar la seguridad operacional;
d) Oportunidad para que se puedan tomar medidas de seguridad operacional;
e) Riesgos asociados si no se efectúa la investigación;
f) Contribución a los programas de seguridad operacional específicos;
g) Identificar tendencias;
h) Beneficios para el entrenamiento; y
i) Disponibilidad de recursos.

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

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

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

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

a) Establecer un cronograma (líneas de tiempo) de sucesos clave, incluyendo las acciones de las personas involucradas;
b) Revisión de las políticas y procedimientos relacionados con las actividades;
c) Revisión de toda decisión tomada en relación con el suceso;

d) Identificación de los controles de riesgo que eran aplicados y que debería haber prevenido la ocurrencia del suceso; y
e) Revisión de datos de seguridad operacional para cualquier suceso anterior o similar.

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

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

Valoración y mitigación del riesgo operacional (SRM)
El proveedor de servicios debe desarrollar un modelo de evaluación de riesgos de seguridad y procedimientos que permitirán un enfoque coherente y sistemático para la evaluación de riesgos de seguridad. Esto debe incluir un método que le ayudará a determinar qué riesgos son aceptables o inaceptables y priorizar acciones.

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

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

El proceso de evaluación de riesgos de seguridad debe utilizar todos los datos y la información de seguridad operacional que está disponible. Una vez que se han evaluado los riesgos de seguridad, el proveedor de servicios participará en un proceso de toma de decisiones basada en datos para determinar qué controles de riesgos de seguridad son necesarios. Las evaluaciones de riesgos de seguridad operacional a veces tienen que usar información cualitativa (juicio experto) en lugar de datos cuantitativos debido a falta de datos. La utilización de la matriz de riesgos de seguridad operacional permite al usuario expresar el riesgo de seguridad asociado con los riesgos identificados en un formato cuantitativo. Esto permite la comparación de la magnitud directa entre los riesgos de seguridad identificados. Un criterio de evaluación de riesgo de seguridad cualitativa como "probable" o "improbable" se puede asignar a cada riesgo de seguridad identificado donde la información cuantitativa no está disponible.

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

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

a) Evaluar y controlar el riesgo más alto de seguridad operacional;
b) Asignar recursos a los más altos riesgos de seguridad operacional;
c) Mantener la mejora y la eficiencia de la seguridad operacional;
d) Alcanzar los objetivos de seguridad operacional establecidos y acordados y los objetivos de rendimiento de seguridad operacional (SPTs); y
e) Satisfacer los requisitos de las regulaciones del estado en materia de control de riesgos de seguridad operacional.

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

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

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

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

Esta documentación SRM se convierte en una fuente organizacional histórica de conocimiento de seguridad operacional que puede usarse como referencia en la toma de decisiones y para el intercambio de información sobre seguridad operacional. Asimismo, esta documentación es un material importante para los análisis de tendencia, entrenamiento y comunicación además de constituir una valiosa información para la auditoría interna al evaluar si los controles de riesgo de la seguridad operacional y las acciones implantadas han sido efectivos.

Aseguramiento de la seguridad operacional

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

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

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

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

Auditorías internas

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

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

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

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

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

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

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

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

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

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

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

a) Objetivos de seguridad operacional, que se deben establecer primero para reflejar los logros estratégicos o los resultados deseados relacionados con preocupaciones de seguridad específicas del contexto operacional de la organización;
b) Indicadores de rendimiento de seguridad operacional (SPIs), que son parámetros tácticos relacionadas con los objetivos de seguridad y, por lo tanto, son la referencia para la recolección de datos; y
c) objetivos de rendimiento de seguridad operacional (SPTs), que también son parámetros tácticos utilizados para supervisar el progreso hacia el logro de los objetivos de seguridad.

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

a) Definir qué es lo que la organización espera alcanzar.
b) Debe ser una declaración de un resultado deseado.
c) Los objetivos de seguridad operacional deben ser declaraciones cortas y de alto nivel sobre las

prioridades de seguridad operacional y deben reflejar la política de seguridad operacional de la organización.

d) Los objetivos de seguridad operacional deben abordar los riesgos más significativos de la organización.

Indicadores de rendimiento de seguridad operacional (SPIs)

Al establecer los SPIs los proveedores de servicio deben considerar:

a) Medir las cosas correctas: Determinar los mejores SPIs que mostrarán que la organización está en camino para alcanzar sus objetivos de seguridad operacional. También se debe considerar cuáles son los mayores problemas de seguridad operacional y los riesgos que enfrenta la organización e identificar los SPI que mostrarán que se realiza un control efectivo de estos.
b) Disponibilidad de datos: ¿Hay datos disponibles que se alinean con lo que la organización desea medir? Si no hay, puede ser necesario establecer fuentes de recolección de datos adicionales. Para las organizaciones pequeñas con una cantidad limitada de datos, la puesta en común de los conjuntos de datos también puede ayudar a identificar las tendencias. Esto se puede apoyar por asociaciones de la industria que pueden recopilar datos de seguridad de múltiples organizaciones.
c) Fiabilidad de los datos: los datos pueden ser poco fiables debido a su subjetividad o porque está incompleto.
d) SPIs comunes de la industria: puede ser útil acordar SPIs comunes con organizaciones similares para que puedan hacer comparaciones entre organizaciones. Las asociaciones de industria o regulador pueden activarlos.
e) Indicadores establecidos dentro del Programa Estatal de Seguridad Operacional.

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

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

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

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

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

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

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

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

sector de servicio considerado.

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

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

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

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

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

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

a) Cuán crítico es el impacto del cambio en las actividades de su organización, y el impacto en otras organizaciones del sistema aeronáutico en su conjunto.
b) Es importante que expertos clave de la comunidad aeronáutica estén involucrados en las actividades de gestión del cambio desde un primer momento. Esto puede incluir a individuos de organizaciones externas.
c) Disponibilidad de información y datos de rendimiento de la seguridad operacional. Es necesario conocer qué datos e información está disponible y si se puede utilizar como información sobre la situación y maximizar el análisis previo al cambio planificado.

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

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

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

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

El proceso de gestión del cambio debe considerar lo siguiente:

a) Comprender y definir el cambio. Esto debe incluir una descripción del cambio y por qué se está implementando;
b) Comprender y definir quién y qué afectará; estos pueden ser individuos dentro de la organización, otros departamentos o personas externas o de organizaciones. Los equipos, sistemas y procesos también pueden ser afectados. Puede ser necesaria una revisión de la descripción del sistema y las interfases de las organizaciones. Esta es una oportunidad para determinar quién debe participar en el cambio. Los cambios pueden afectar los controles de riesgo establecidos, y por lo tanto, el cambio podría aumentar los riesgos en áreas que no son inmediatamente evidentes;
c) Identificar los peligros relacionados con el cambio y llevar a cabo una evaluación de riesgo de seguridad; esto debe identificar cualquier peligro directamente relacionado con el cambio, pero nuevamente también debe revisarse el impacto en los riesgos y controles de riesgo de seguridad que pueden ser afectados por el cambio. Este paso debe utilizar procesos SRM de la organización existente;
d) Desarrollar un plan de acción; esto debe definir lo que debe hacerse, por quién y cuándo. Debe haber un plan claro que describe cómo se implementará el cambio y quién será responsable de las acciones y la secuenciación y la programación de cada tarea;
e) El Ejecutivo Responsable de liderar la implantación del cambio debe firmar el cambio; para confirmar que el cambio no afecta la seguridad operacional; y
f) Plan de aseguramiento; se trata de determinar qué medidas de seguimiento son necesarias. Considerar cómo será comunicado el cambio y si son necesarias otras actividades adicionales (por ejemplo, auditorías) durante o después del cambio. Cualquier suposición realizada debe ser probada.

Mejora continua del SMS

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

a) Evaluación proactiva del día a día las operaciones, instalaciones, equipos, documentación y procedimientos a través de auditorías de seguridad operacional y encuestas;
b) Evaluación del rendimiento individual para verificar el cumplimiento de sus responsabilidades de seguridad operacional;
c) Evaluaciones reactivas para comprobar la eficacia del sistema de control y mitigación de riesgo, por ejemplo: incidentes, accidentes e investigaciones;
d) Seguimiento de los cambios organizativos para asegurar que son eficaces; y
e) Revisión periódica del funcionamiento de la seguridad y planes de acción de seguridad de la organización.

Promoción de la seguridad operacional

Instrucción y educación

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

El Gerente de Seguridad Operacional es el responsable de asegurar que existe un programa de formación de seguridad adecuada implantado. El programa de capacitación debe incluir requerimientos de entrenamiento inicial y recurrente para mantener las competencias.

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

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

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

a) Formación específica en concientizar nuevos ejecutivos responsables y titulares de puestos que deben rendir cuentas y responsabilidades SMS;
b) Importancia del cumplimiento de los requisitos de seguridad operacional a nivel nacional y organizacional;
c) Compromiso de gestión;
d) Asignación de recursos;
e) Promoción de la política de seguridad operacional y los SMS;
f) Promoción de una cultura de seguridad operacional positiva;
g) Comunicación interdepartamental de seguridad operacional efectiva;
h) Objetivo de seguridad operacional, SPTs y niveles de alerta; y
i) Política disciplinaria.

Comunicación de la seguridad operacional

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

a) Garantizar que el personal es plenamente consciente del SMS; esta es una buena forma de promover la política y los objetivos de seguridad operacional de la organización.
b) Transmitir información crítica para la seguridad operacional; la información crítica para la seguridad operacional es información específica relacionada con problemas y riesgos de seguridad operacional que podrían exponer a la organización a ese tipo de riesgo. Podría tratarse de información recopilada de fuentes internas o externas como enseñanzas obtenidas o relacionadas con controles de riesgos de seguridad operacional. El proveedor de servicios determina el tipo de información que se considera crítica para la seguridad operacional, así como la oportunidad de comunicarla.
c) Crear conciencia sobre nuevos controles de riesgos de seguridad operacional y medidas correctivas; los riesgos de seguridad operacional que enfrenta el proveedor de servicios cambiarán con el tiempo, y si se trata de un nuevo riesgo de seguridad operacional que ha sido identificado o de cambios en los controles de riesgos de seguridad operacional dichos cambios deberán comunicarse al personal apropiado.
d) Proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados; cuando se actualizan los procedimientos de seguridad operacional es importante que las personas apropiadas tengan conocimientos de dichos cambios.
e) Promover una cultura de seguridad operacional positiva y alentar al personal a identificar y notificar peligros; la comunicación de seguridad operacional es en ambos sentidos. Es importante que todo el personal comunique los problemas de seguridad operacional a la organización a través del sistema de notificaciones de seguridad operacional.
f) Proporcionar comentarios e información; proporcionar comentarios al personal que presenta notificaciones de seguridad operacional respecto de las medidas que se han adoptado para abordar las preocupaciones identificadas.

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

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

Apéndice 4 – Indicadores de rendimiento en materia de seguridad operacional (SPI) del SMS

1. En este apéndice se exponen algunos ejemplos de indicadores de seguridad operacional que podrían ser utilizados por el ATSP, de la misma manera, los SPI deben aportar y estar en concordancia con los indicadores y metas del SSP del Estado.

2. Por este motivo el ATSP deben desarrollar los SPI del SMS con el asesoramiento de la AAC. Sus SPI propuestos deberán ser coherentes con los indicadores de seguridad operacional de SSP del Estado; por lo tanto, se debe obtener un acuerdo/aceptación necesaria de la AAC.

N°	INDICADOR	METRICA
1	Perdida de Separación IFR – IFR	➢ Cantidad de sucesos ➢ Tasa (número de ocurrencias por 100.000 vuelos IFR); ➢ Tasa (número de ocurrencias por millón de horas de vuelo IFR); ➢ Tasa (menos de 2/3 de la separación lograda) (número de ocurrencias con menos de 2/3 de separación lograda por cada 100.000 vuelos IFR); ➢ Tasa (menos de 2/3 de la separación lograda) (número de ocurrencias con menos de 2/3 de separación alcanzada por cada millón de horas de vuelo IFR);
2	LHD en espacio aéreo RVSM	➢ Cantidad de eventos
3	Eventos TCAS (con o sin pérdida de separación)	➢ Cantidad de eventos
4	Aproximaciones frustradas	➢ Aproximaciones fallidas = (número de aproximaciones fallidas / número total de aproximaciones) x 100
5	Excursiones de pista	➢ Cantidad de eventos
6	Incursiones de pista	➢ % de las incursiones de pista en las que no es necesario maniobra evasiva ➢ % de las incursiones de pista en las que haya requerido maniobra evasiva

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

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
CONFORMIDAD	Monitoreo de auditorías/cumplimiento internas: todos los incumplimientos	Reducción del % de los incumplimientos analizados por su importancia para la seguridad operacional en comparación con los del año anterior.
	Monitoreo de auditorías/cumplimiento internas: incumplimientos importantes	Reducción del % de incumplimientos significativos en comparación con el número total de incumplimientos significativos del año anterior. Reducción del % de incumplimientos repetidos dentro del ciclo de planificación de auditorías del año anterior.
	Monitoreo de auditorías / cumplimiento internas: la capacidad de respuesta a las	Reducción en un % del tiempo de espera promedio para completar las

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

		notificante dentro de los 10 días hábiles, en comparación con las del año anterior. Incremento en % de las notificaciones seguidas de una revisión independiente de la seguridad operacional, en comparación con las del año anterior.
	Identificación de los peligros	Reducción del % del número de escenarios de accidentes/incidentes graves analizados para apoyar la Gestión de Riesgos de Seguridad operacional (SRM) en relación al año anterior. Número de nuevos peligros identificados a través del sistema de notificación interno al año y la tendencia por cada 10 peligros identificados. Reducción de un % de los incumplimientos de las auditorías externas relacionados con peligros que no habían sido percibidos por el personal / gestión previamente en comparación con el año anterior. Incremento del % del número de notificaciones de seguridad operacional recibidas del personal al año y la tendencia en relación al año anterior.
	Controles de riesgo	Número de nuevos controles de riesgo validados por año en los últimos dos años. Incremento en un % del presupuesto total asignado a nuevos controles de riesgo en relación al año anterior.
	Gestión y desarrollo de las competencias de recursos humanos	Incremento en un % de la plantilla para la que se ha establecido una evaluación de competencias en los últimos dos años. Incremento en un % de personal que ha tenido instrucción en gestión de la seguridad operacional en los últimos dos años (instrucción continua). Incremento en un % la frecuencia de revisión de los perfiles de competencias en los últimos dos años. Incremento en un % la frecuencia de revisión del alcance, contenido y calidad de los programas de

		instrucción en comparación con el año anterior. Número de cambios realizados en los programas de instrucción a raíz de la retroalimentación del personal al año en relación a las 10 últimas revisiones efectuadas. Numero de cambios realizados en los programas de instrucción a raíz del análisis de las notificaciones de seguridad operacional internas por año en relación a los 10 últimos cambios.
	Gestión del cambio	Número de cambios organizacionales en los que se ha realizado una evaluación formal de riesgos de seguridad operacional al mes / trimestre / año y la tendencia en relación a los 10 últimos cambios. Número de cambios en los procedimientos para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al mes/trimestre/año y la tendencia en relación a los 10 últimos cambios. Número de cambios técnicos (por ejemplo: nuevos equipos, nuevas instalaciones, nuevo hardware) para los que se ha realizado una evaluación formal de riesgos de seguridad operacional al mes/trimestre/año y tendencia en relación a los 10 últimos cambios. Número de controles de riesgo implementados por los cambios al mes/trimestre/año y tendencia en relación a los 10 últimos cambios. % de cambios (organizacionales / procedimientos / técnicos, etc.) que han sido objeto de evaluación de riesgos en relación a los 10 últimos cambios.
	Gestión de contratistas	Incremento del % de contratistas cuyo rendimiento en materia de seguridad operacional se ha evaluado en relación a la cantidad de contratistas que se tuvo el año anterior. Reducción del % de la frecuencia con la que se determina el rendimiento en materia de seguridad operacional de los contratistas en relación a la del año anterior.

		Reducción en un % del tiempo de demora para impartir instrucción de los contratistas en seguridad operacional en relación al año anterior. Incremento de un % de los contratistas que han implementado procedimientos de control de la instrucción en temas de seguridad operacional en relación al año anterior. Incremento en un % de los contratistas que tienen establecido un sistema de información (o seguimiento) sobre cuestiones de seguridad operacional con sus clientes en relación al año anterior. Número de notificaciones de seguridad operacional recibidas de los contratistas por año y tendencia en relación a la cantidad de contratistas que tiene el ATSP. Número de acciones de seguridad operacional iniciadas debido a la evaluación del rendimiento en materia de seguridad operacional o de las notificaciones de seguridad operacional recibidas al año y tendencia en relación a la cantidad de contratistas que tiene el ATSP.
	Plan de coordinaciónde respuestas ante emergencia	Número de simulacros de emergencia cumplidos por año en relación a la cantidad planificada. Frecuencia de la revisión del plan de coordinación de respuestas ante emergencias en relación a la cantidad simulacros de respuesta ante emergencias realizadas. Número de cursos de instrucción en planes de coordinación de respuestas ante emergencias realizados por mes / trimestre / año en relación a los cursos programados. % de personal que recibe instrucción en el plan de coordinación de respuestas ante emergencias dentro de un cuarto de año en relación al total del personal del ATSP. Número de reuniones con los socios principales y contratistas para coordinar el plan de coordinación de

		respuestas ante emergencias al mes / trimestre / año en relación a todas las reuniones planificadas al año.
	Promoción de la seguridad operacional	Número de comunicaciones de seguridad operacional publicadas Número de cursos realizados Número de sesiones informativas de seguridad operacional realizadas (por mes / trimestre / año)
	Cultura de la seguridad operacional	Incremento en un % del grado en que el personal considera la seguridad operacional como un valor que guía su trabajo diario, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el ATSP (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un % del grado en que el personal considera que la seguridad operacional es muy valorada por sus gestores, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el ATSP (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un % del grado en que se aplican los principios de actuación humana, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el ATSP (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un % del grado en que toma iniciativa el personal para mejorar las prácticas organizacionales o notificar u problema a la gestión, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el ATSP (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un % del grado en el que el comportamiento consciente de la seguridad operacional es apoyado, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el ATSP (por ejemplo: en una

		escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un % del grado en el que el personal y la gestión son conscientes de los riesgos de sus operaciones y lo que implican para ellos mismos y para los demás, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el ATSP (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior.

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

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

La fórmula siguiente permitirá calcular la desviación estándar (σ), considerando que “X” es el valor de cada punto de datos; “N” es el número de puntos de datos y “μ” es el valor promedio de todos los puntos de datos.

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

Con este método de visualización, alerta y control, es factible establecer los objetivos que se representan en un porcentaje (por ejemplo, un 5%) sobre el promedio del año anterior.

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

Los objetivos de rendimiento de seguridad operacional se determinan durante la fase de planificación. Se establecen de manera que definen el logro del nivel aceptable de seguridad operacional para la organización. Una meta de rendimiento de seguridad operacional se puede expresar en términos absolutos o relativos

El ATSP deberá considerar estos factores al establecer sus objetivos de rendimiento de seguridad operacional:

- Los objetivos deberán soportar el objetivo de seguridad operacional primario y los ALOSP de la AAC;
- La selección y priorización de objetivos deben basarse en el riesgo de la seguridad operacional;
- La fijación de objetivos deberá tomar en cuenta desarrollos nuevos o previstos, tanto internos como externos, que pueden afectar al ATSP, con el fin de medir la respuesta de la organización a esos cambios:
- Los objetivos deberán ser realistas, y tener en cuenta el rendimiento anterior de la organización para determinar la magnitud de los cambios necesarios;
- La fijación de objetivos debe incluir la evaluación comparativa (benchmarking) contra las organizaciones de buena performance (nacional e internacional);
- La terminación del objetivo período/fecha deberá tener en cuenta el riesgo para la seguridad operacional. Por ejemplo, las áreas críticas para la seguridad operacional deben tener controles de progreso o hitos de desarrollo más frecuente;

- Deberá asegurarse de que ningún riesgo está por encima del máximo aceptable y se esfuerzan por conducir el riesgo 'tan bajo como sea razonablemente posible "

Apéndice 5 - Lista de verificación de análisis de brechas de SMS y plan de implementación

No.	*Aspecto a analizar o pregunta a responder*	*Referencia de la 4ª edición de SMM*	*Respuesta*	*Estado de la aplicación*
1.1-1	¿Existe una política de seguridad?	9.3.1	☐ Sí ☐ No ☐ Parcial	
1.1-2	¿Refleja la política de seguridad el compromiso de la alta dirección con respecto a la gestión de la seguridad?	9.3.1 9.3.2 9.3.3	☐ Sí ☐ No ☐ Parcial	
1.1-3	¿Es la política de seguridad adecuada al tamaño, naturaleza y complejidad de la organización?	9.3.1 9.3.4.3	☐ Sí ☐ No ☐ Parcial	
1.1-4	¿Es la política de seguridad pertinente para la seguridad aérea?		☐ Sí ☐ No ☐ Parcial	
1.1-5	¿La política de seguridad está firmada por el ejecutivo responsable?	9.3.4.1	☐ Sí ☐ No ☐ Parcial	
1.1-6	¿Se comunica la política de seguridad, con respaldo visible, a toda la [Organización]?	9.3.4.2	☐ Sí ☐ No ☐ Parcial	
1.1-7	¿Se revisa periódicamente la política de seguridad para asegurarse de que sigue siendo pertinente y apropiada para la [Organización]?	9.3.4.6	☐ Sí ☐ No ☐ Parcial	
1.1-8	¿Existen objetivos de seguridad relevantes?	9.3.4.7	☐ Sí ☐ No ☐ Parcial	
1.1-9	¿Se revisan periódicamente los objetivos de seguridad para garantizar que se mantengan actualizados?	9.3.4.8	☐ Sí ☐ No ☐ Parcial	
1.2-1	¿Ha identificado [la Organización] a un ejecutivo responsable que, independientemente de otras funciones, tenga la responsabilidad última, en nombre de la [Organización], de la aplicación y el mantenimiento de un SGS eficaz?	9.3.5.3 9.3.5.4	☐ Sí ☐ No ☐ Parcial	
1.2-2	¿Tiene el ejecutivo responsable el control total de los recursos financieros y humanos necesarios para las operaciones autorizadas a realizar bajo el certificado de operaciones?	9.3.5.1	☐ Sí ☐ No ☐ Parcial	
1.2-3	¿Tiene el Ejecutivo Responsable la autoridad final sobre todas las actividades de aviación de su organización?	9.3.5.1 9.3.5.8 b)	☐ Sí ☐ No ☐ Parcial	
1.2-4	¿Ha identificado y documentado [la Organización] las responsabilidades de seguridad de la gerencia y del personal operativo, con respecto al SMS?	9.3.5.11 9.3.5.12	☐ Sí ☐ No ☐ Parcial	
1.2-5	¿Existe un comité de seguridad o una junta de revisión con el propósito de revisar el desempeño de los SMS y la seguridad?	9.3.6.7 9.3.6.8	☐ Sí ☐ No ☐ Parcial	
1.2-6	¿El comité de seguridad está presidido por el ejecutivo responsable o por un adjunto debidamente asignado,	9.3.6.8	☐ Sí ☐ No	

No.	*Aspecto a analizar o pregunta a responder*	*Referencia de la 4ª edición de SMM*	*Respuesta*	*Estado de la aplicación*
	debidamente justificado en el manual de SMS?		☐ Parcial	
1.2-7	¿El comité de seguridad incluye a los jefes operativos o departamentales relevantes, según corresponda?	9.3.6.8	☐ Sí ☐ No ☐ Parcial	
1.2-8	¿Existen grupos de acción de seguridad que trabajen en conjunto con el comité de seguridad (especialmente para organizaciones grandes/complejas)?	9.3.6.9	☐ Sí ☐ No ☐ Parcial	
1.3-1	¿Ha designado [Organización] a una persona cualificada para gestionar y supervisar el funcionamiento diario del SMS?	9.3.6.1	☐ Sí ☐ No ☐ Parcial	
1.3-2	¿La persona cualificada tiene acceso directo o reporta al ejecutivo responsable en relación con la implementación y el funcionamiento del SMS?	9.3.6.1	☐ Sí ☐ No ☐ Parcial	
1.3-3	¿El gerente responsable de administrar el SMS tiene otras responsabilidades que puedan entrar en conflicto o perjudicar su papel como administrador de SMS?	9.3.6.3	☐ Sí ☐ No ☐ Parcial	
1.4-1	En caso de tener que establecer un plan de respuesta a emergencias (PRV), ¿coordina [la Organización] su ERP con las entidades externas pertinentes con las que debe interactuar durante el suministro de sus productos y servicios?	9.3.7.2	☐ Sí ☐ No ☐ Parcial	
1.4-2	¿Aborda el ERP las emergencias previsibles identificadas a través del SMS e incluye acciones, procesos y controles de mitigación para gestionar eficazmente las emergencias relacionadas con la aviación, cuando corresponda?	9.7.3.1	☐ Sí ☐ No ☐ Parcial	
1.4.3	¿Ejercer la coordinación del ERP como parte de las pruebas periódicas de su ERP, cuando corresponda?	9.7.3.3	☐ Sí ☐ No ☐ Parcial	
1.5-1	¿Existe un resumen o documento de exposición de SMS de alto nivel que sea aprobado por el gerente responsable y aceptado por la CAA? [5.3.36 a 5.3.38]	9.3.6.2 e) 9.3.8.2	☐ Sí ☐ No ☐ Parcial	
1.5-2	¿La documentación de SMS aborda el SMS de la organización y sus componentes y elementos asociados?	9.3.8.1 9.3.8.3	☐ Sí ☐ No ☐ Parcial	
1.5-3	¿Está el marco de SGS de [Organización] alineado con el marco regulatorio de SMS?	9.3.8.3 b)	☐ Sí ☐ No ☐ Parcial	
1.5-4	¿Mantiene [Organización] un registro de la documentación de respaldo pertinente para la implementación y operación del SMS?	9.3.8.4	☐ Sí ☐ No ☐ Parcial	
1.5-5	¿Tiene [Organización] un plan de implementación de SMS para establecer su proceso de implementación de SMS, incluidas tareas específicas y sus hitos de implementación relevantes?	9.7.7.1 9.7.7.2	☐ Sí ☐ No ☐ Parcial	
1.5-6	¿El plan de implementación de SMS aborda la coordinación entre el SMS del proveedor de servicios y el SMS de organizaciones externas, cuando corresponda?	9.7.7.3	☐ Sí ☐ No ☐ Parcial	

No.	*Aspecto a analizar o pregunta a responder*	*Referencia de la 4ª edición de SMM*	*Respuesta*	*Estado de la aplicación*
1.5-7	¿Se elabora el plan de implementación del SMS en consulta con el ejecutivo responsable y otros altos directivos?	9.7.7.3	☐ Sí ☐ No ☐ Parcial	
1.5-8	¿Se supervisa periódicamente el plan de implementación del SMS y se actualiza según sea necesario?	9.7.7.4	☐ Sí ☐ No ☐ Parcial	
2.1-1	¿Existe un proceso oficial para determinar todos los posibles peligros que podrían afectar a la seguridad de la aviación en todas las esferas de operaciones y actividades, teniendo en cuenta las interfaces tanto internas como externas a [la Organización]?	2.5.2 9.4.4	☐ Sí ☐ No ☐ Parcial	
2.1-2	¿La identificación de peligros se basa en una combinación de métodos reactivos y proactivos que utilizan fuentes internas y externas utilizadas para el peligro?	9.4.4.1 9.4.4.2 9.4.4.13 9.4.5	☐ Sí ☐ No ☐ Parcial	
2.1-3	¿Se utiliza un sistema de informes de seguridad obligatorio?	9.4.4.3	☐ Sí ☐ No ☐ Parcial	
2.1-4	¿Existe un sistema de denuncia voluntaria con protecciones adecuadas para alentar a las personas a presentar información adicional que no esté sujeta a un sistema de denuncia obligatorio?	9.4.4.4	☐ Sí ☐ No ☐ Parcial	
2.1-5	¿Se alienta al personal de todos los niveles y de todas las disciplinas a identificar y notificar los peligros y otras cuestiones de seguridad a través de los sistemas de informes de seguridad dentro de [Organización]?	9.4.4.6	☐ Sí ☐ No ☐ Parcial	
2.1-6	¿La investigación de seguridad de los proveedores de servicios forma parte de su SMS para apoyar la identificación de peligros?	9.4.5	☐ Sí ☐ No ☐ Parcial	
2.1-7	¿Se documentan los peligros identificados y sus posibles consecuencias para su uso en los procesos de evaluación de riesgos de seguridad?	9.4.4.11	☐ Sí ☐ No ☐ Parcial	
2.2-1	¿Ha desarrollado [Organización] un modelo de evaluación de riesgos para la seguridad operacional y procedimientos para la evaluación de los riesgos de seguridad asociados con los peligros identificados?	2.5.3 2.5.4 2.5.5 2.5.6 9.4.6.1	☐ Sí ☐ No ☐ Parcial	
2.2-2	¿El proceso de evaluación de riesgos de seguridad utiliza los datos de seguridad y la información de seguridad que están disponibles para el análisis y la evaluación de los riesgos de seguridad asociados con los peligros identificados?	9.4.6.4 9.4.6.5	☐ Sí ☐ No ☐ Parcial	
2.2-3	¿Tiene [Organización] un proceso para priorizar sus evaluaciones de riesgos de seguridad?	9.4.6.6 9.4.6.7	☐ Sí ☐ No ☐ Parcial	
2.2-4	¿Tiene [Organización] procedimientos para implementar controles de riesgos de seguridad adecuados?	2.5.7 2.5.9 9.4.6.8	☐ Sí ☐ No ☐ Parcial	
2.2-5	¿Existen medios para supervisar y validar la eficacia del control de riesgos de seguridad implementado en	2.5.7.5	☐ Sí ☐ No	

No.	*Aspecto a analizar o pregunta a responder*	*Referencia de la 4ª edición de SMM*	*Respuesta*	*Estado de la aplicación*
	condiciones operativas?	9.4.6.9	☐ Parcial	
2.2-6	¿Están documentadas las actividades de gestión de riesgos de seguridad y sus resultados?	2.5.8 9.4.6.10	☐ Sí ☐ No ☐ Parcial	
3.1-1	¿Se han establecido medios para supervisar y verificar el rendimiento de la organización en materia de seguridad, auditorías internas y el establecimiento y seguimiento de indicadores de rendimiento en materia de seguridad?	9.5.1 9.5.2 9.5.3 9.5.4	☐ Sí ☐ No ☐ Parcial	
3.1-2	¿Existe un proceso establecido para la gestión del rendimiento en materia de seguridad?	4.1.1 4.1.2 4.1.3 9.5.4.11	☐ Sí ☐ No ☐ Parcial	
3.1-3	¿Existen indicadores de desempeño de seguridad establecidos para medir y monitorear el desempeño de seguridad de la organización y el desempeño de su SMS?	4.3.1 4.3.2 9.5.4.13	☐ Sí ☐ No ☐ Parcial	
3.1-4	¿Son los indicadores de rendimiento de seguridad relevantes para los objetivos de seguridad de la organización?	4.3.2.5 9.5.4.14 a) 9.5.4.17	☐ Sí ☐ No ☐ Parcial	
3.1-5	¿Incluyen los indicadores de rendimiento en materia de seguridad un seguimiento cuantitativo de los resultados de seguridad de altas consecuencias (por ejemplo, tasas de accidentes e incidentes graves), los eventos de menor consecuencia (por ejemplo, tasa de incumplimiento, desviaciones) y el rendimiento de los procesos (por ejemplo, formación, mejoras del sistema y procesamiento de informes)?	9.5.4.12	☐ Sí ☐ No ☐ Parcial	
3.1-6	¿Existe un uso adecuado de los correspondientes objetivos de rendimiento en materia de seguridad operacional para trabajar junto con los indicadores de rendimiento en materia de seguridad?	4.3.3 4.3.5 9.5.4.15 9.5.4.18	☐ Sí ☐ No ☐ Parcial	
3.1-7	¿Se elaboran los indicadores de rendimiento en materia de seguridad operacional y sus objetivos asociados en materia de rendimiento operacional en consulta con la autoridad de aviación civil y están sujetos al acuerdo de ésta?	8.4.7.14 8.4.7.15 9.5.4.20	☐ Sí ☐ No ☐ Parcial	
3.1-8	¿Existe un procedimiento para tomar medidas correctivas o de seguimiento sobre la base de los resultados de los SPI monitoreados y medidos?	4.4.7	☐ Sí ☐ No ☐ Parcial	
3.1-9	¿Se revisan periódicamente los objetivos de seguridad, los indicadores de rendimiento en materia de seguridad y los objetivos de rendimiento en materia de seguridad asociados a ellos?	4.4.4 4.5	☐ Sí ☐ No ☐ Parcial	
3.2-1	Al enfrentar cambios, ¿identifica [la Organización] los peligros y evalúa y controla los riesgos asociados utilizando sus procedimientos existentes de identificación de peligros o de gestión de riesgos de seguridad?	9.5.5.2	☐ Sí ☐ No ☐ Parcial	
3.2-2	¿Revisa [la Organización] periódicamente la descripción de su sistema para determinar si sigue siendo válido, ya que podría experimentar cambios regulares o incluso	9.5.5.1 9.5.5.4	☐ Sí ☐ No ☐ Parcial	

No.	*Aspecto a analizar o pregunta a responder*	*Referencia de la 4ª edición de SMM*	*Respuesta*	*Estado de la aplicación*
	continuos, grandes o pequeños?			
3.2-3	¿Ha definido [Organización] el desencadenante de su proceso formal de gestión del cambio?	9.5.5.5	☐ Sí ☐ No ☐ Parcial	
3.2-4	¿Existe un proceso desarrollado para la gestión del cambio para identificar y gestionar los riesgos de seguridad que pueden surgir de los cambios que podrían afectar al nivel de riesgo de seguridad de la organización?	9.5.5.3 9.5.5.7	☐ Sí ☐ No ☐ Parcial	
3.3-1	¿Existe un procedimiento para la auditoría/evaluación interna periódica de la eficacia de los SMS del proveedor de servicios, utilizando una variedad de métodos para determinar su efectividad?	9.5.6.1 9.5.6.2 9.5.6.3	☐ Sí ☐ No ☐ Parcial	
3.3-2	¿La función de auditoría interna del proveedor de servicios incluye la evaluación de todas las funciones de gestión de la seguridad en toda su organización?	9.5.6.2	☐ Sí ☐ No ☐ Parcial	
4.1-1	¿Existe un programa para impartir formación/familiarización con el SMS al personal que participa en la aplicación o el funcionamiento del SMS?	9.6.4.1 al 9.6.4.9	☐ Sí ☐ No ☐ Parcial	
4.1-2	¿Ha recibido el ejecutivo responsable una familiarización, sesión informativa o formación adecuada por SMS?	9.6.4.1 al 9.6.4.9	☐ Sí ☐ No ☐ Parcial	
4.1-3	¿El personal involucrado en la mitigación de riesgos recibe la capacitación o familiarización adecuada en la gestión de riesgos?	9.6.4.1 al 9.6.4.9	☐ Sí ☐ No ☐ Parcial	
4.1-4	¿Hay evidencia de esfuerzos de educación o concientización de SMS en toda la organización?	9.6.4.1 al 9.6.4.9	☐ Sí ☐ No ☐ Parcial	
4.2-1	¿Participa [Organización] en el intercambio de información de seguridad con proveedores u organizaciones externas de productos y servicios de la industria pertinentes, incluidas las organizaciones reguladoras de la aviación pertinentes?	9.6.5.1 a 9.6.5.4	☐ Sí ☐ No ☐ Parcial	
4.2-2	¿Existe evidencia de una publicación, circular o canal de seguridad (SMS) para comunicar asuntos de seguridad (SMS) a los empleados?	9.6.5.1 a 9.6.5.4	☐ Sí ☐ No ☐ Parcial	
4.2-3	¿Es accesible o difundido el manual de SMS de [Organización] y el material de orientación relacionado a todo el personal pertinente?	9.6.5.1 a 9.6.5.4	☐ Sí ☐ No ☐ Parcial	

Los ítems catalogados como NO o PARCIAL formarán parte de los requerimientos del Plan de Implementación del SMS.

8. CONTACTO PARA MAYOR INFORMACION:

Cualquier consulta técnica adicional sobre esta Circular de Asesoramiento, favor dirigirla a la oficina de Estándares de Vuelo (EDV):

Av. Arce 2631, Edificio Multicine, Piso 9
Tel. (591-2) 2444450
E-correo: ca.edv@dgac.gob.bo