CIRCULAR DE ASESORAMIENTO

CA	**:**	**CA-PEL-141-001**
FECHA	**:**	**15/07/2020**
REVISIÓN	**:**	**1**
EMITIDA POR	**:**	**DGAC**

ASUNTO: ESTABLECIMIENTO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN CENTROS DE INSTRUCCIÓN DE AERONÁUTICA CIVIL (RAB 141) TIPO 2 Y 3

1. PROPÓSITO

Esta circular de asesoramiento (CA) provee información de orientación para establecer, implementar y mantener un sistema de gestión de la seguridad operacional (SMS), así como establecer los métodos aceptables de cumplimiento (MAC) para los requisitos descritos en la Sección 141.275 y el Apéndice 10 de la RAB 141.

2. APLICABILIDAD

Esta circular de asesoramiento es aplicable al postulante o titular de un certificado de aprobación de centro de instrucción de aeronáutica civil (CCIAC), conforme a los requisitos de la RAB 141, con la categoría de Tipo 2 o Tipo 3, es decir aquellos que realizan actividades de instrucción en vuelo, que están expuestos a riesgos de seguridad operacional relacionados con la operación de las aeronaves y su finalidad es proporcionar una guía y lineamientos de como cumplir de manera aceptable a la AAC los requisitos establecidos en la RAB 141.

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

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

El uso de los términos “CIAC” y “organización” se utilizan indistintamente a lo largo de todo el documento.

3. SECCIONES DE LA RAB 141 RELACIONADAS CON EL SMS

a) Sección 141.275 - Sistema de gestión de seguridad operacional (SMS).

b) Apéndice 10 - Marco para el sistema de gestión de la seguridad operacional (SMS).

4. DOCUMENTOS RELACIONADOS

a) Anexo 19 - Gestión de la seguridad operacional, Enmienda 1

b) Doc. 9859 - Manual de gestión de la seguridad operacional, Cuarta edición.

5. DEFINICIONES Y ABREVIATURAS

5.1 Definiciones

a) **Cultura de seguridad operacional.**- Actitudes, creencias, percepciones y valores que las personas, empleados, comparten en relación con la seguridad operacional en una organización; es la forma en que se comportan las personas en relación con la seguridad operacional

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

Nota.- *Dichos datos de seguridad operacional se recopilan a través de actividades preventivas o reactivas, relacionadas con la seguridad operacional, incluyendo entre otros las siguientes:*

- *Investigación de accidentes o incidentes.*
- *Notificaciones de seguridad operacional.*
- *Notificaciones sobre el mantenimiento de la aeronavegabilidad.*
- *Supervisión de la eficiencia operacional*
- *Inspecciones, auditorias, constataciones, o*
- *Estudios y exámenes de seguridad operacional.*

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

d) **Desencadenantes (triggers)**.- Nivel establecido, valor de criterios, de un indicador de rendimiento de seguridad operacional, que sirve para iniciar una acción necesaria (ejemplo una evaluación, un ajuste o acción correctiva).

e) **Eficacia de la seguridad operacional.-** Resultados de seguridad de un CIAC definidos por sus objetivos de seguridad y por sus indicadores de rendimiento en materia de seguridad operacional.

f) **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.

Nota.- *En el caso de este procedimiento se le denominará gerente responsable tal como lo indica la RAB 141. El CIAC puede utilizar cualquier otra denominación en su estructura organizacional siempre que sus funciones y responsabilidades estén alineadas con lo indicado en la RAB 141.*

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

h) **Indicadores de rendimiento de seguridad operacional.-** Parámetro basado en datos, que se utiliza para monitorear y evaluar el rendimiento en materia de seguridad operacional.

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

j) **Investigación sobre seguridad operacional**.- Proceso que se lleva a cabo con el propósito de prevenir accidentes y que comprende la reunión y el análisis de información, la obtención de conclusiones, incluida la determinación de las causas y/o factores contribuyentes y, cuando proceda la formulación de recomendaciones sobre seguridad operacional.

k) **Investigador.-** Persona responsable en razón de sus calificaciones, de la organización, realización y control de una investigación.

Nota.- *Nada de lo mencionado en la definición, trata de impedir que las funciones de un investigador se asignen a una comisión o a otro órgano*

l) **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 peligros identificados o en las estrategias de control de los riesgos, son evaluados apropiadamente antes de ser implementados.

m) **Mitigación de riesgos.-** Proceso de incorporación de defensas o controles preventivos para reducir la gravedad y/o la probabilidad de las consecuencias proyectadas con relación a un peligro.

n) **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.

o) **Objetivos sobre seguridad operacional**.- Breve declaración de alto nivel sobre el logro que se desea alcanzar en materia de seguridad operacional, o el resultado deseado a ser realizado por el SSP o los proveedores de servicio del SMS.

p) **Meta de rendimiento de la seguridad operacional**.- Meta planificada por el Estado o proveedor de servicios, para un indicador de desempeño de seguridad operacional sobre un período dado que se alinea con los objetivos de seguridad operacional.

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

r) **Programa estatal de Seguridad Operacional (SSP).-** Conjunto integrado de reglamentos y actividades dirigidas con la finalidad de incrementar la seguridad operacional.

s) **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.

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

u) **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.

v) **Sistema.-** Estructura organizada y con un propósito que consiste en elementos y componentes interrelacionados e interdependientes, políticas, procedimientos y prácticas relacionadas, creados para llevar a cabo una actividad específica o resolver problemas.

w) **Sistema de gestión de la seguridad operacional (SMS).-** Enfoque sistemático para la gestión de la seguridad operacional, que incluye las estructuras orgánicas, la obligación de rendición de cuentas, las políticas y los procedimientos necesarios.

5.2 Abreviaturas

a) AAC Autoridad de Aviación Civil.
b) ALoSP Nivel aceptable de rendimiento de seguridad operacional.
c) CIAC Centro de instrucción de aeronáutica civil.
d) CCIAC Certificado de centro de instrucción de aeronáutica civil.
e) CP Puesto de comando.
f) CVR Registrador de la voz en el puesto de pilotaje.
g) DGAC Dirección General de Aeronáutica Civil.
h) EC Control de intensificación.
i) EF Factor de intensificación.
j) EMC Centro de control de la emergencia.

k) ERP Plan de respuesta ante emergencias.

l) FDR Registrador de datos de vuelo.

m) H Peligro.

n) HIRM Identificación de peligros y mitigación de los riesgos.

o) MIP Manual de instrucción y procedimientos.

p) MOR Informe obligatorio de sucesos.

q) OACI Organización de Aviación Civil Internacional.

r) OSHE Seguridad ocupacional, salud y medio ambiente.

s) PC Control preventivo.

t) QA Garantía de calidad.

u) QMS Sistema de gestión de calidad.

v) RM Medida de recuperación.

w) SAG Grupo de acción de seguridad operacional.

x) SAR Búsqueda y rescate.

y) SDCPS Sistemas de recopilación y procesamiento de datos de seguridad operacional.

z) SMM Manual de gestión de la seguridad operacional.

aa) SMS Sistema de gestión de la seguridad operacional.

bb) SMSM Manual de sistemas de gestión de la seguridad operacional.

cc) SPI Indicadores de rendimiento en materia de seguridad operacional.

dd) SPT Metas de rendimiento de seguridad operacional.

ee) SRB Junta de revisión de seguridad operacional.

ff) SRM Gestión de riesgos de la seguridad operacional.

gg) SSP Programa estatal de seguridad operacional.

hh) TNA Análisis de necesidades de capacitación.

ii) UC Consecuencia final.

jj) UE Evento inseguro.

6. INTRODUCCIÓN AL SISTEMA DE GESTIÓN DE SEGURIDAD OPERACIONAL

6.1 El propósito del SMS es proporcionar a los CIAC un enfoque sistémico para gestionar la seguridad operacional y, por lo tanto, garantizar la operación segura de las aeronaves durante el proceso de instrucción en vuelo.

6.2 Este sistema está diseñado para mejorar continuamente la seguridad de las operaciones aéreas mediante la identificación de peligros, la recolección de datos y el análisis de la información de seguridad, así como la evaluación continua de los riesgos de la seguridad operacional. El SMS busca proactivamente mitigar los riesgos antes de que se produzcan accidentes e incidentes de aviación.

6.3 Asimismo, permite al centro de instrucción gestionar en forma efectiva sus actividades, el rendimiento de la seguridad y los recursos, al tiempo que obtiene una mayor comprensión de su contribución a la seguridad de la aviación.

6.4 El primer paso para definir el alcance y la aplicabilidad de un SMS es una revisión a la descripción de los elementos del SMS y su interfaz con los sistemas y procedimientos a ser establecidos por el CIAC, así como el contexto de la operación de instrucción de vuelo a ser realizada.

6.5 El desarrollo y la planificación de la implementación del sistema que llevará a cabo el CIAC deberá incluir las interfaces del SMS dentro de la organización, así como las interfaces pertinentes con organizaciones externas que pudieran afectar su sistema de gestión. Un resumen de la descripción del sistema, las responsabilidades, la estructura, la cadena de mando y la comunicación debe incluirse en la documentación del SMS.

6.6 Asimismo, el CIAC al momento de definir el alcance del SMS, debe considerar que éste sea directamente proporcional al tamaño de la organización y a la complejidad de sus operaciones.

6.7 Resulta útil para una buena comprensión del SMS, considerar como complemento de la descripción básica del sistema y sus procedimientos, un diagrama del CIAC, con sus respectivas referencias cruzadas de cada uno de los elementos que establece la Sección 141.275 de la RAB.

7. Cultura de seguridad operacional

7.1 La Sección 141.275 (a) establece que todo CIAC debe orientarse a desarrollar una cultura de seguridad operacional que incluya el conocimiento del SMS a nivel de toda su organización.

7.2 Una cultura de seguridad es la consecuencia natural de contar con personas que participan en el sistema de aviación. La cultura de seguridad operacional ha sido definida "*cómo la forma en que se comportan las personas en relación con la seguridad y el riesgo cuando nadie está mirando*". Es una expresión de cómo la seguridad es percibida, valorada y priorizada por la alta dirección y los empleados de una organización y que refleja en qué medida las personas y los grupos:

a) Son conscientes de los riesgos y peligros conocidos que enfrenta la organización y sus actividades;

b) orientan su comportamiento en forma continua a preservar y mejorar la seguridad;

c) pueden acceder a los recursos requeridos para realizar operaciones seguras;

d) están dispuestos y son capaces de adaptarse para enfrentar problemas de seguridad;

e) están dispuestos a comunicar los problemas de seguridad; y

f) evaluar sistemáticamente los comportamientos relacionados con la seguridad en toda la organización.

7.3 Es por ello, que el Anexo 19 y la RAB 141 requiere que las organizaciones sujetas al cumplimiento del SMS promuevan una cultura de seguridad positiva, con el objetivo de fomentar la implementación efectiva de la gestión de la seguridad a través del SMS.

7.4 Para lograr una cultura de seguridad positiva, el CIAC deberá asegurarse que ésta tiene las siguientes características:

a) El personal directivo y empleados, individual y colectivamente, quieren tomar decisiones y adoptar las acciones que promuevan la seguridad;

b) los individuos y los grupos evalúan continuamente sus comportamientos y procesos y reciben favorablemente las críticas de otros que buscan oportunidades para cambiar y mejorar a medida que cambia su entorno;

c) la alta dirección y el personal comparten una conciencia común de los peligros y riesgos que enfrenta la organización y sus actividades, así como la necesidad de gestionar los riesgos;

d) el personal actúa y toma decisiones de acuerdo con la creencia común de que la seguridad es parte de la forma en que llevan a cabo sus actividades;

e) el personal valora estar informado e informar a otros sobre cuestiones de seguridad;

f) el personal confía a sus colegas y jefes información sobre sus experiencias y el reporte de errores para mejorar la forma de hacer las cosas en el futuro.

7.5 Es importante para implementar un SMS en forma eficaz, que el CIAC pueda monitorear y evaluar el comportamiento de la cultura de seguridad operacional, para:

a) comprender cómo se siente la gente con respecto a la organización y qué tan importante se percibe la seguridad;

b) identificar sus fortalezas y debilidades;

c) identificar las diferencias entre varios grupos (subculturas) dentro de una organización;

d) examinar los cambios a lo largo del tiempo (por ejemplo, en respuesta a cambios organizativos significativos, como un accidente, un cambio en la alta dirección o una modificación respecto a acuerdos laborales.

7.6 Existen varias herramientas que se utilizan para evaluar la madurez de la cultura de seguridad operacional en un CIAC, las cuales se pueden aplicar en forma combinada tales como:

a) cuestionarios;

b) entrevistas y focus groups;

c) observaciones; y

d) revisión de documentos.

7.7 La evaluación de la madurez de la cultura de seguridad operacional puede proporcionar una visión valiosa, dado que la administración puede tomar acciones para fomentar los comportamientos deseados en cuanto a la cultura de seguridad. Sin embargo, puede existir un grado de subjetividad con tales evaluaciones y reflejar los puntos de vista y percepciones de las personas involucradas en un momento particular solamente. Además, puede tener consecuencias imprevistas al alentar inadvertidamente al CIAC a esforzarse por lograr un puntaje “correcto”, en lugar de trabajar juntos para comprender y mejorar la cultura de seguridad.

8. SMS PROPORCIONAL AL TAMAÑO Y COMPLEJIDAD DEL CIAC

8.1 Con la finalidad de orientar a los CIAC respecto a lo indicado en la Sección 141.275 (e), que establece que el SMS debe ser directamente proporcional al tamaño del CIAC y la complejidad de sus servicios, se ha considerado clasificar a los centros de instrucción en tres categorías: pequeño, mediano y grande, considerando diversos criterios para su clasificación.

8.2 Es importante indicar, que ello no significa que deje de cumplir requisitos o que omita algunos elementos de componentes del SMS, sino que podría presentar algunos métodos de cumplimiento no complejos a consideración de la AAC al momento de evaluar su establecimiento en el manual correspondiente y su plan de implantación.

8.3 Asimismo, para contar con un adecuado entendimiento de lo que significan estos términos en el contexto del SMS, se detallan las siguientes definiciones:

a) Tamaño.- Magnitud o dimensión del CIAC, en la cual debería considerarse la cantidad de alumnos en instrucción de vuelo, el número de aeronaves y el número de satélites con los que cuenta.

b) Complejidad.- Estaría referenciada a las habilitaciones con que cuenta para el desarrollo de los cursos y la variedad de aeronaves destinadas a la instrucción.

8.4 Para una mejor visualización de esta clasificación, se detalla a continuación una tabla de orientación de criterios para un centro pequeño, mediano y grande, a fin de proporcionar un concepto de escalabilidad. En la práctica puede variar según el tamaño de la organización y además, porque el SMS debe ser adecuado a las circunstancias y operaciones de la organización.

8.5 Se debe tener en cuenta que si un CIAC parece pertenecer a una categoría para un criterio (por ejemplo, cantidad de alumnos en instrucción en vuelo y una segunda categoría para otro (por ejemplo, variedad de aeronaves), se recomienda seleccionar la más alta de las categorías para su clasificación.

8.6 Por ejemplo, un CIAC pequeño con dos aeronaves monomotores y que solo está autorizado para la formación de pilotos privados con un número de 16 alumnos no tendría inconveniente en implementar los requisitos señalados en los 4 componentes y 12 elementos del SMS, pero en algunos casos a un nivel más simple, como por ejemplo en lo que se refiere a la estructura organizacional podría aceptarse que el gerente responsable, sea igualmente el gerente del SMS y del sistema de calidad, siempre que él pueda demostrar a la AAC con evidencia que cuenta con las calificaciones correspondientes para tal función.

Tabla 1. Categorización de los CIAC

Reglamento	Clasificación	Criterios	Categorización de los CIAC		
			Pequeño	Mediano	Grande
RAB 141 Centros de instrucción de aeronáutica civil CIAC Tipo 2 y Tipo 3	Tamaño	Alumnos en instrucción en vuelo	Hasta 20	21 a 40	41 o más
		Número de aeronaves	Hasta 2	3 a 8	9 o más
		Número de satélites	0	1	2 o más
	Complejidad de operaciones	Número de habilitaciones	Piloto privado	Piloto privado Piloto comercial IFR	Piloto privado Piloto Comercial IFR Hab. multimotor Hab. instructor de vuelo
		Variedad de flota	1	2	3 o más

9. ESTRUCTURA DEL SMS

9.1 De acuerdo a lo señalado en el Apéndice 2 del Anexo 19 – Gestión de la seguridad operacional y lo establecido en la Sección 141.275 (f) de la RAB 141, la estructura del SMS está compuesta por cuatro (4) componentes y doce (12) elementos que se describen a continuación:

Tabla 2. Componentes y elementos del SMS

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

9.2 El postulante a un certificado de aprobación de centro de instrucción de aeronáutica civil Tipo 2 y Tipo 3, conforme a la Sección 141.275 (d), deberá establecer y desarrollar a través de procedimientos documentados el cumplimiento de cada uno de los requisitos del SMS en su organización, en un manual que forme parte integrante del MIP o en un documento independiente, que contengan todos los elementos que se detallan en la estructura del SMS, para que a partir de la fecha que haya recibido el certificado de aprobación por parte de la AAC, pueda iniciar su implementación en un plazo máximo de tres (3) años.

9.3 Los requisitos de cada componente y elemento de la estructura del SMS, se describen en los numerales siguientes.

10. Componente 1: Política y objetivos de seguridad operacional

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

El compromiso de la administración y su liderazgo en seguridad operacional es clave para la implementación de un SMS eficaz y se afirma a través de la política de seguridad operacional y el establecimiento de objetivos de seguridad operacional. Este compromiso se demuestra a través de la toma de decisiones gerenciales y la asignación de recursos, siendo estas decisiones y acciones siempre coherentes con la política y los objetivos de seguridad operacional a fin de cultivar una cultura de seguridad operacional positiva.

La política de seguridad operacional deberá ser desarrollada y respaldada por la alta dirección y debe ser firmada por el gerente responsable. El personal clave de la seguridad operacional y, cuando corresponda, los órganos de representación del personal (foros de empleados, sindicatos) deberían ser consultados al desarrollar la política y los objetivos de

seguridad operacional para promover un sentido de responsabilidad compartida.

10.1 Compromiso de la administración

Política de seguridad operacional

10.1.1 La política de seguridad operacional deberá ser endosada (firmada) visiblemente por el gerente responsable del CIAC. El "endoso visible" se refiere a que el apoyo activo de la administración a la política de seguridad operacional pueda ser visto por toda la organización. Esto puede hacerse a través de cualquier medio de comunicación (página intranet de la organización, avisos, documentos de acceso a todo el personal de la organización, entre otros) y alineando cada una de sus actividades con la política de seguridad operacional.

10.1.2 Es responsabilidad de la gerencia comunicar la política de seguridad operacional en toda la organización para garantizar que todo el personal comprenda y trabaje de acuerdo con la política establecida.

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

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

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

c) cumplir con todos los requisitos reglamentarios aplicables;

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

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

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

10.1.4 La política de seguridad operacional también deberá hacer referencia al sistema de notificaciones de seguridad operacional para alentar la comunicación de problemas de seguridad operacional e informar al personal sobre la política disciplinaria aplicada en caso de eventos o problemas de seguridad operacional que se informan.

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

10.1.6 Una política sobre la protección de los datos y la información de seguridad operacional, así como de las notificaciones, puede tener un efecto positivo en la cultura de reporte. El CIAC debería permitir el anonimato de las personas que notifican algún problema de seguridad operacional de forma voluntaria, para que pueda llevarse a cabo análisis de seguridad operacional significativos sin tener que involucrar al personal.

10.1.7 En la **Apéndice 1** se muestra un ejemplo de una declaración de política de seguridad operacional.

Objetivos de seguridad operacional

10.1.8 Teniendo en cuenta su política de seguridad operacional, el CIAC también deberá establecer objetivos de seguridad operacional para definir lo que pretende lograr con respecto a los resultados de seguridad operacional.

10.1.9 Los objetivos de seguridad operacional deberán ser declaraciones breves y de alto nivel de las prioridades de seguridad operacional de la organización y deben abordar sus riesgos de seguridad operacional más significativos. Estos objetivos pueden incluirse en la política de seguridad operacional (o documentarse por separado) y definen lo que la

organización pretende lograr en términos de gestión de seguridad operacional.

10.1.10 Los indicadores de rendimiento de seguridad operacional (SPI) y las metas de rendimiento de seguridad operacional (SPT) son necesarios para monitorear el logro de estos objetivos y se detallan en el Componente 3 del SMS.

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

10.1.12 *El compromiso de la administración será aceptable para la AAC si se han observado los siguientes criterios:*

- *Se ha desarrollado la política de seguridad operacional que contiene lo indicado en el Numeral 10.1.3 precedente y está firmada por el gerente responsable del CIAC.*
- *La alta dirección respalda abiertamente esta política, por ejemplo, con asignación de una partida presupuestaria adecuada para las actividades relacionadas con el SMS.*
- *La política hace referencia al sistema establecido para las notificaciones de seguridad operacional, la política disciplinaria para fomentar su notificación y la protección de los datos e información de seguridad operacional.*
- *La política es comunicada en toda la organización.*
- *El CIAC ha establecido en el manual los objetivos de seguridad operacional para definir lo que pretende lograr con respecto a los resultados de seguridad operacional.*
- *Se promueve y mantiene una cultura de seguridad operacional.*
- *Está previsto y documentada la revisión periódica de la política y objetivos de seguridad operacional.*

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

Designación del gerente responsable

10.2.1 El gerente responsable es la persona que tiene la máxima autoridad sobre la operación segura del CIAC. El gerente responsable es quien establece y promueve la política y los objetivos de seguridad operacional como un valor central de la organización, por ello es importante que la persona seleccionada esté ubicada en el nivel más alto de la organización, asegurando de esa forma que pueda tomar en forma correcta las decisiones estratégicas de seguridad operacional.

10.2.2 Según la envergadura, estructura y complejidad de la organización, el gerente responsable puede ser:

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

b) el presidente del directorio;

c) un socio principal; o

d) el propietario.

10.2.3 El gerente responsable debe:

a) tener la autoridad para tomar decisiones en nombre de la organización;

b) tener el control de los recursos, tanto financieros como humanos; y

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

10.2.4 Asimismo, el gerente responsable debe definir las responsabilidades específicas de

seguridad operacional del personal directivo del CIAC y su rol en relación con el SMS debe reflejar cómo pueden contribuir a una cultura de seguridad operacional positiva.

10.2.5 Las responsabilidades de seguridad operacional, la rendición de cuentas y la autoridad en relación a éstas, deben documentarse y comunicarse en toda la organización. Las responsabilidades de seguridad operacional de los directivos del CIAC deben incluir la asignación de los recursos humanos, técnicos, financieros u otros necesarios para el desempeño efectivo y eficiente del SMS.

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

10.2.6 En el caso en que un SMS se aplica a varias organizaciones diferentes, que son parte de la misma entidad legal o razón social, debería haber un solo gerente responsable. Cuando esto no sea posible, se deben identificar a los gerentes o ejecutivos individuales responsables para la aprobación de cada organización, definiendo las líneas claras de responsabilidad y la forma cómo se coordinarán sus rendiciones de cuentas de seguridad operacional.

10.2.7 Una de las maneras más efectivas en que el gerente responsable puede involucrarse en forma visible, es liderando regularmente reuniones ejecutivas de seguridad operacional, dado que su participación activa en estas reuniones le permite:

a) revisar los objetivos de seguridad operacional;

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

c) tomar decisiones de seguridad operacional oportunas;

d) asignar recursos apropiados;

e) mantener la rendición de cuentas de los gerentes respecto a sus responsabilidades, rendimiento y plazos de implementación de seguridad operacional; y

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

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

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

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

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

10.2.9 Es apropiado que el gerente responsable tenga las siguientes responsabilidades de seguridad operacional:

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

b) promover una cultura de seguridad operacional positiva;

c) establecer y promover la política de seguridad operacional;

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

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

f) ver a la mejora continua de los SMS.

10.2.10 La autoridad del gerente responsable incluyen, pero no se limitan a tener la autoridad final:

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

b) sobre operaciones de instrucción de vuelo que han sido autorizadas al CIAC, incluida la autoridad para detener la operación o actividad.

10.2.11 Deberá estar claramente definida dentro del CIAC la autoridad para tomar decisiones con respecto a la tolerabilidad del riesgo de seguridad operacional. Esto incluye quién puede tomar decisiones sobre la aceptabilidad de los riesgos, así como la autoridad para acordar que se puede implementar un cambio. La autoridad puede asignarse a una persona, un puesto de gestión o un comité.

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

Rendición de cuentas y responsabilidades

10.2.13 La obligación de rendición de cuentas y las responsabilidades del personal, tanto el directivo como el personal involucrado en la seguridad operacional, deben estar definidas claramente para garantizar la operación segura de la instrucción en vuelo. Las responsabilidades en seguridad operacional deben centrarse en la contribución del personal al rendimiento de la seguridad operacional de la organización (resultados). La gestión de la seguridad operacional es una función clave, dado que el gerente responsable del CIAC tiene un alto grado de involucramiento en el funcionamiento del SMS.

10.2.14 La obligación de rendición de cuentas, las responsabilidades y autoridades deben estar definidas en el manual del SMS del CIAC y deben ser comunicada a toda la organización. Asimismo, estas obligaciones y responsabilidades deben estar establecidas en la descripción de funciones del personal.

10.2.15 Las líneas de responsabilidad de seguridad operacional en toda la organización y la forma de cómo se definen dependerán del tamaño y la complejidad de la organización, así como los métodos de comunicación preferidos. Típicamente, las responsabilidades de seguridad y las obligaciones de rendición de cuentas se reflejan en el organigrama, los documentos que definen las responsabilidades del área y las descripciones de funciones o roles del personal de la organización.

10.2.16 El CIAC debe tratar de evitar conflictos de intereses entre las responsabilidades de seguridad operacional de los miembros del personal y sus otras responsabilidades organizativas.

Rendición de cuentas y responsabilidades con respecto a las organizaciones externas

10.2.17 El CIAC es responsable del rendimiento de seguridad operacional de las organizaciones externas donde exista una interfaz del SMS. El CIAC 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 CIAC, cuando sea el caso, interactúen con los sistemas de seguridad operacional de cualquier organización externa que contribuya a la entrega segura de sus productos o servicios.

10.2.18 La obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional será aceptable para la AAC si se han observado los siguientes criterios:

- *El gerente responsable está plenamente identificado y ha sido designado observando las orientaciones 10.2.1 y 10.2.3. s*
- *Las obligaciones en materia de seguridad operacional, así como las líneas de obligación de rendición de cuentas sobre la seguridad operacional, para toda la organización, incluidos la de la administración superior, el encargado del SMS y los directivos o responsables de las áreas del CIAC están claramente definidas, documentadas y disponibles.*
- *Los niveles de atribución para la toma de decisiones sobre la tolerabilidad de los riesgos de seguridad operacional están claramente definidas, documentadas y disponibles.*
- *La autoridad y responsabilidades del ejecutivo responsable incluyen al menos aquellas señaladas en 10.2.8 y 10.2.9*
- *Existe una declaración expresa de que las responsabilidades del gerente responsable en materia de seguridad operacional no pueden delegarse.*
- *Los puestos, las responsabilidades y las autoridades relacionadas con la seguridad operacional han sido definidas, publicadas y comunicadas a toda la organización.*
- *Existe una declaración expresa de que el CIAC es responsable del rendimiento en materia de seguridad operacional de los productos o servicios que proporcionan las organizaciones externas.*
- *Se han establecido y publicado los procedimientos del CIAC que garantizan el cumplimiento de 10.2.17 con relación a organizaciones externas.*
- *Todos los puntos anteriores están documentados en el manual de SMS del CIAC.*

10.3 Nombramiento del personal clave de *seguridad operacional*

Designación del gerente de seguridad operacional

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

Nota.- *Si bien en la RAB 141 se denomina a esta persona gerente del SMS, puede el CIAC denominarlo de forma distinta como por ejemplo jefe del SMS, responsable del SMS o encargado conforme a su estructura organizacional; sin embargo, debe garantizar que cuenta con las funciones y responsabilidades que le asigna la RAB 141 en el Apéndice 10 y lo indicado en esta circular.*

10.3.2 El gerente del SMS asesora al gerente responsable y a los ejecutivos (jefes de instrucción, por ejemplo) en asuntos de administración de seguridad, y es responsable de coordinar y comunicar los asuntos de seguridad operacional dentro de la organización, así como con los miembros externos de la comunidad aeronáutica. Las funciones del gerente del SMS 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 capacitación de seguridad 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 de la organización dirigidas a la entrega de productos y servicios; y

i) coordinar y comunicar a la AAC del Estado y otras autoridades estatales (en nombre del gerente responsable), los problemas relacionados con la seguridad operacional.

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

10.3.3 En la mayoría de las organizaciones, se designa a una persona del staff como el gerente del SMS. Dependiendo del tamaño, naturaleza y complejidad del CIAC, la función de gerente del SMS puede ser una función exclusiva o puede combinarse con otras funciones. Además, algunas organizaciones pueden necesitar asignar el rol a un grupo de personas. El CIAC debe asegurarse de que la opción elegida no genere ningún conflicto de intereses. Siempre que sea posible, el gerente del SMS no deberá involucrarse directamente en la entrega del producto o servicio, pero deberá tener un conocimiento práctico de estos. Asimismo, es conveniente evitar posibles conflictos de interés con otras tareas y funciones, los cuales podrían incluir:

a) competencia por el financiamiento (por ejemplo, el gerente financiero es el gerente 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.

10.3.4 En los casos en que la función se asigna a un grupo de personas (por ejemplo, cuando los CIAC extienden sus SMS a través de múltiples actividades) una de las personas debe ser designada como gerente de SMS "principal" para mantener una línea directa con el gerente responsable.

10.3.5 Las competencias para un gerente de SMS deben incluir, entre otras, las siguientes:

a) experiencia en gestión de seguridad operacional / calidad;

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

c) antecedentes técnicos para comprender los sistemas que respaldan las operaciones o producto / servicio provisto;

d) habilidades interpersonales;

e) habilidades analíticas y de resolución de problemas;

f) habilidades de gestión de proyectos;

g) habilidades de comunicación oral y escrita; y

h) una comprensión de los factores humanos.

***Nota**.- Los requisitos del perfil y competencia del gerente de seguridad operacional del CIAC deben estar incluidos en el manual del SMS.*

10.3.6 Dependiendo del tamaño, naturaleza y complejidad del CIAC, personal adicional puede apoyar al gerente del SMS, quienes en conjunto son responsables de garantizar la recopilación y el análisis oportuno de los datos de seguridad operacional y la distribución apropiada dentro de la organización de la información de seguridad operacional relacionada, de manera que se puedan tomar decisiones y controles de riesgos de seguridad operacional, según sea necesario.

Conformación de la junta de revisión de seguridad operacional (SRB) y del grupo de acción de seguridad operacional (SAG), cuando corresponda

10.3.7 Además, una función del gerente del SMS es evaluar la efectividad de cualquier estrategia de mitigación de riesgos utilizada para lograr los objetivos de seguridad operacional de la organización. Esto se puede hacer a través del comité de seguridad de más alto nivel, como una junta de revisión de seguridad operacional (SRB, por sus siglas en inglés). El SRB es estratégico y se ocupa de cuestiones de alto nivel relacionadas con las políticas, la asignación de recursos y el monitoreo del rendimiento organizacional. La SRB deberá incluir al gerente responsable y a la alta gerencia para monitorear:

a) efectividad del SMS;

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

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

d) la efectividad de los procesos de gestión de seguridad operacional de la organización que soportan:

   i. la prioridad declarada por la organización en cuanto a la gestión de la seguridad operacional; y

   ii. la promoción de la seguridad operacional en toda la organización.

***Nota**.- Este SRB debería ser establecido en CIACs grandes y en medianos, si así lo considera la organización de acuerdo a su tamaño y complejidad de su operación.*

10.3.8 Una vez que el comité de seguridad operacional de más alto nivel haya desarrollado una dirección estratégica, la implementación de las estrategias de seguridad operacional debería coordinarse en toda la organización. Esto se puede lograr creando un grupo de acción de seguridad operacional (SAG) que esté más centrado en las operaciones. El SAG normalmente están compuestos por gerentes y personal de primera línea y está usualmente presidido por el gerente del SMS. El SAG es una entidad táctica que se ocupan de cuestiones de implementación específicas según la dirección del SRB. El SAG:

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

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

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

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

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

***Nota**: Este SAG debería ser establecido en centros de instrucción grandes y medianos según lo considere la organización por el tamaño y complejidad de sus operaciones.*

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

- *El CIAC ha definido los requisitos y ha designado un gerente de seguridad operacional que tendrá la responsabilidad de la implementación y el mantenimiento de un SMS eficaz debidamente calificado según la orientación de 10.3.5.*
- *En el manual del SMS se describen las funciones del gerente de seguridad operacional que incluyen como mínimo los criterios de 10.3.2.*

- *Se han establecido y documentado en el manual del SMS la junta de revisión de seguridad operacional (SRB) y el grupo de seguridad operacional (SAG), cuando sea aplicable por su tamaño y complejidad, incluyendo la descripción de sus funciones, sus miembros, la frecuencia y circunstancias de sus reuniones, según la orientación de 10.3.7 y 10.3.8.*

10.4 Coordinación del plan de respuesta ante emergencia

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

10.4.2 Por definición, una emergencia es una situación repentina y no planificada o un evento que requiere una acción inmediata. La coordinación de la planificación de respuesta ante emergencias se refiere a la planificación de actividades que tienen lugar dentro de un período de tiempo limitado durante una situación de emergencia operacional de aviación no planificada.

10.4.3 Un plan de respuesta ante emergencia (ERP) es un componente integral del proceso de gestión de riesgos de seguridad operacional (SRM) de un centro de instrucción para abordar emergencias, crisis o eventos relacionados en donde la organización tenga que participar.

10.4.4 El objetivo general del ERP es la continuación segura de las operaciones y el retorno a las operaciones normales tan pronto como sea posible. Esto debería garantizar una transición ordenada y eficiente de las operaciones normales a las de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de autoridad. Incluye el período de tiempo requerido para restablecer las operaciones "normales" después de la emergencia.

10.4.5 El ERP identifica las acciones que deberá realizar el personal responsable durante una emergencia. La mayoría de las emergencias requerirán una acción coordinada entre diferentes organizaciones, posiblemente con otros proveedores de servicios y con otras organizaciones externas, como los servicios de emergencia no relacionados con la aviación. El ERP deberá ser fácilmente accesible para el personal clave apropiado, así como para las organizaciones externas coordinadoras.

10.4.6 La coordinación de la planificación de respuesta ante emergencias se aplica solo a los proveedores de servicios requeridos a establecer y mantener un ERP como es el caso de los aeropuertos y explotadores aéreos. Sin embargo, dada la naturaleza de la operación realizada por los centros de instrucción de aeronáutica civil que llevan a cabo instrucción de vuelo, es aplicable contar con un ERP para establecer los procedimientos con el detalle de las funciones y responsabilidades que deberán cumplirse en caso de un accidente o incidente grave en las actividades de instrucción que involucra a alumnos e instructores.

10.4.7 En el **Apéndice 2** se presenta el contenido de un plan de respuesta ante emergencias (ERP).

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

- *El CIAC ha desarrollado y documentado un plan de respuesta ante emergencias, con los elementos establecidos en el Apéndice 2 de esta circular.*

- *El plan de respuesta ante emergencias forma parte del manual del SMS o ha sido desarrollada en un documento independiente y referenciado en el manual del SMS.*

10.5 Documentación del SMS

10.5.1 La documentación de SMS debe incluir en primer lugar un "manual de SMS" que constituye un documento de alto nivel, que describe las políticas, procesos y procedimientos de SMS para facilitar la administración interna, la comunicación y el mantenimiento del SMS de la organización.

10.5.2 El postulante a un certificado de aprobación de centro de instrucción de aeronáutica civil conforme a la RAB 141 tipo 2 y Tipo 3, deberá al momento de presentar la solicitud formal del proceso de certificación, presentar este manual, estableciendo la forma como el centro al inicio de sus operaciones cumplirá con cada uno de los componentes y elementos señalados en el marco del SMS que figura en el Apéndice 10 de la RAB 141.

10.5.3 En ese sentido, este manual que puede formar parte del MIP o ser desarrollado en forma independiente, tiene por objetivo ayudar al personal a comprender cómo funciona el SMS de la organización y cómo se cumplirán los objetivos y la política de seguridad operacional, incluyendo una descripción del sistema del SMS y su interrelación con las distintas políticas, procesos, procedimientos y prácticas de la organización para el cumplimiento de la política y objetivos de seguridad operacional.

10.5.4 Es necesario que este manual aborde las actividades diarias de gestión de la seguridad operacional de forma clara y precisa, para que sea fácilmente comprendido por el personal de toda la organización.

10.5.5 Este manual también sirve como una herramienta de comunicación de seguridad operacional primaria entre el CIAC y las partes interesadas clave en seguridad operacional (por ejemplo, la AAC con el propósito de la aceptación reglamentaria, la evaluación y el seguimiento posterior del SMS).

10.5.6 El manual del SMS debe incluir una descripción detallada de las políticas, procesos y procedimientos del CIAC, que incluyan como mínimo:

a) La política y objetivos de seguridad de seguridad operacional;

b) La referencia a cualquier requisito de SMS reglamentario aplicable;

c) La descripción del sistema;

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

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

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

g) los procedimientos de investigación de seguridad operacional;

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

i) los procesos y procedimientos de capacitación y comunicación de SMS;

j) los procesos y procedimientos de comunicación de seguridad operacional;

k) los procedimientos de auditoría interna;

l) los procedimientos de gestión del cambio;

m) los procedimientos de gestión de documentación de SMS; y

n) la coordinación de la planificación de respuesta ante emergencias.

10.5.7 En el **Apéndice 3** se presenta un modelo de estructura para el desarrollo de un manual de SMS.

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

a) los registros de peligros y notificaciones de peligros / seguridad operacional;

b) los SPI y gráficos relacionados;

c) los registros de evaluaciones de riesgos de seguridad operacional completados;

d) la revisión interna del SMS o registros de auditoría;

e) los registros de auditorías internas;

f) los registros de SMS / registros de capacitación de seguridad operacional;

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

h) el plan de implementación de SMS (durante la implementación inicial); y

i) los análisis de brechas para apoyar el plan de implementación que establece la RAB 141.275 (d).

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

- *El CIAC ha desarrollado un manual del SMS de acuerdo con 10.5.6.*
- *El CIAC mantiene un sistema de registros adecuado, de acuerdo con 10.5.8.*
- *El CIAC ha desarrollado un plan de implementación para poner en práctica los procesos y procedimientos descritos en el manual del SMS.*

11. Componente 2: Gestión de riesgos de seguridad operacional

Los CIAC deberán asegurarse de que se encuentran administrando sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de la seguridad operacional (SRM, sus siglas en inglés) que incluye la identificación de peligros, la evaluación de riesgos y la mitigación de riesgos de seguridad operacional.

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

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

Figura 1 – Identificación de peligros y proceso de gestión de riesgos

11.1 Identificación de peligros

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

Metodologías para identificación de peligros

11.1.2 Existen dos metodologías para la identificación de peligros:

a) *Reactiva*. Esta metodología implica el análisis de resultados o eventos pasados. Los peligros son identificados a través de la investigación de sucesos de seguridad operacional. Los incidentes y accidentes son una indicación de las deficiencias del sistema y, por lo tanto, se pueden usar para determinar qué peligro(s) contribuyeron al evento.

b) *Proactiva*. Esta metodología involucra la recolección de datos de seguridad de eventos o procesos de menor consecuencia o rendimiento, analizando la información de seguridad operacional o la frecuencia de ocurrencia para determinar si existe un peligro que podría provocar un accidente o incidente. La información de seguridad operacional para la identificación proactiva de peligros proviene principalmente de programas de análisis de datos de vuelo (FDA), sistemas de informes de seguridad y del aseguramiento de la seguridad.

11.1.3 Los peligros también pueden identificarse a través del análisis de datos de seguridad operacional que identifican tendencias adversas y hace predicciones sobre peligros emergentes, etc.

Fuentes para identificación de peligros

11.1.4 Existe una variedad de fuentes de datos de identificación de peligros que pueden ser internos o externos a la organización. Entre los ejemplos de fuentes de datos de identificación de peligros internos se incluyen:

a) Sistemas de notificación de seguridad operacional voluntarios y obligatorios: Esto proporciona a todos, incluido el personal de organizaciones externas, la oportunidad de informar los peligros y otros problemas de seguridad a la organización.

b) Auditorías: estos pueden usarse para identificar peligros en la tarea o proceso que se audita. Estos también deberían coordinarse con los cambios organizacionales para identificar los peligros relacionados con la implementación del cambio.

c) Retroalimentación de la capacitación: la capacitación que es interactiva (bidireccional) puede facilitar la identificación de nuevos peligros por parte de los participantes.

d) Investigaciones de seguridad operacional del CIAC: peligros identificados en la investigación de seguridad operacional interna e informes de seguimiento de accidentes / incidentes.

e) Reportes de aseguramiento de calidad.

f) Análisis de tendencia de SPIs.

g) Registros de evaluación de riesgos.

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

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

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

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

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

Sistema de notificación de seguridad operacional

11.1.6 La notificación precisa y oportuna de información relevante relacionada con peligros, incidentes o accidentes es una actividad fundamental de la gestión de la seguridad operacional. Los datos usados para respaldar los análisis de seguridad operacional se informan usando múltiples fuentes. Una de las mejores fuentes de datos es la notificación directa del personal de primera línea, ya que estos observan los peligros como parte de sus actividades diarias.

11.1.7 Los peligros encontrados durante las operaciones reales deberán ser documentados en un registro de peligros y capturados para su análisis. El registro de peligros es una parte vital de la documentación del SMS. Un lugar de trabajo donde se haya capacitado y se aliente constantemente al personal a informar sus errores y experiencias es un requisito previo para lograr una notificación de seguridad operacional eficaz.

11.1.8 Es importante que los CIAC brinden las protecciones adecuadas para alentar a las personas a informar lo que ven o experimentan. 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.

11.1.9 Los sistemas de notificación voluntarios de seguridad operacional deberán ser confidenciales, lo que requiere que toda la información de identificación del notificador sea conocida solo por el custodio para permitir el seguimiento de las acciones. El rol del custodio debe mantenerse, por lo general restringido al responsable de seguridad operacional y al personal involucrado en la investigación de seguridad operacional.

11.1.10 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 pueden estar sin identificar y archivar una vez que se toman las medidas de seguimiento necesarias. Las notificaciones sin identificación pueden respaldar futuros análisis de tendencias para rastrear la efectividad de la mitigación de riesgos e identificar los peligros emergentes.

11.1.11 Se alienta al personal en todos los niveles y en todas las disciplinas a identificar e informar 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.

11.1.12 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 de 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 la presentación de informes futuros.

11.1.13 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.

11.1.14 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 CIAC 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 encaja limpiamente 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.

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

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

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

Investigación de peligros

11.1.18 La identificación del peligro debe ser una actividad continua en el CIAC. Algunas condiciones pueden merecer una investigación más detallada, por ejemplo:

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

b) cambios significativos en la organización o sus actividades.

Investigación de seguridad operacional

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

11.1.20 Las investigaciones de seguridad operacional de los CIAC son conducidas por la organización como parte de su SMS para respaldar los procesos de identificación de peligros y evaluación de riesgos. Hay muchos sucesos de seguridad operacional que quedan fuera del Anexo 13 que podrían proporcionar una valiosa fuente de identificación de peligros o identificar debilidades en los controles de riesgos. Estos problemas pueden ser revelados y remediados por una investigación de seguridad operacional dirigida por el proveedor del servicio.

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

11.1.22 Las investigaciones de los CIAC sobre sucesos y peligros de seguridad operacional son una actividad esencial del proceso general de gestión de riesgos. Los beneficios de llevar a cabo una investigación de seguridad operacional incluyen:

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

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

c) identificar peligros y realizar evaluaciones de riesgos;

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

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

Desencadenantes de la investigación

11.1.23 Una investigación de seguridad operacional de un CIAC, generalmente se desencadena por una notificación (informe) enviado a través del sistema de notificaciones de seguridad operacional, el cual describe el proceso de decisión de la investigación de seguridad operacional y la distinción entre cuándo se debe realizar una investigación de seguridad del CIAC y cuándo se debe iniciar una investigación conforme a las disposiciones del Anexo 13.

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

a) La gravedad potencial del resultado;

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

c) valor de seguridad operacional que se obtendrá;

d) oportunidad para tomar medidas de seguridad operacional;

e) riesgos asociados con no investigar;

f) contribución a programas de seguridad operacional específicos;

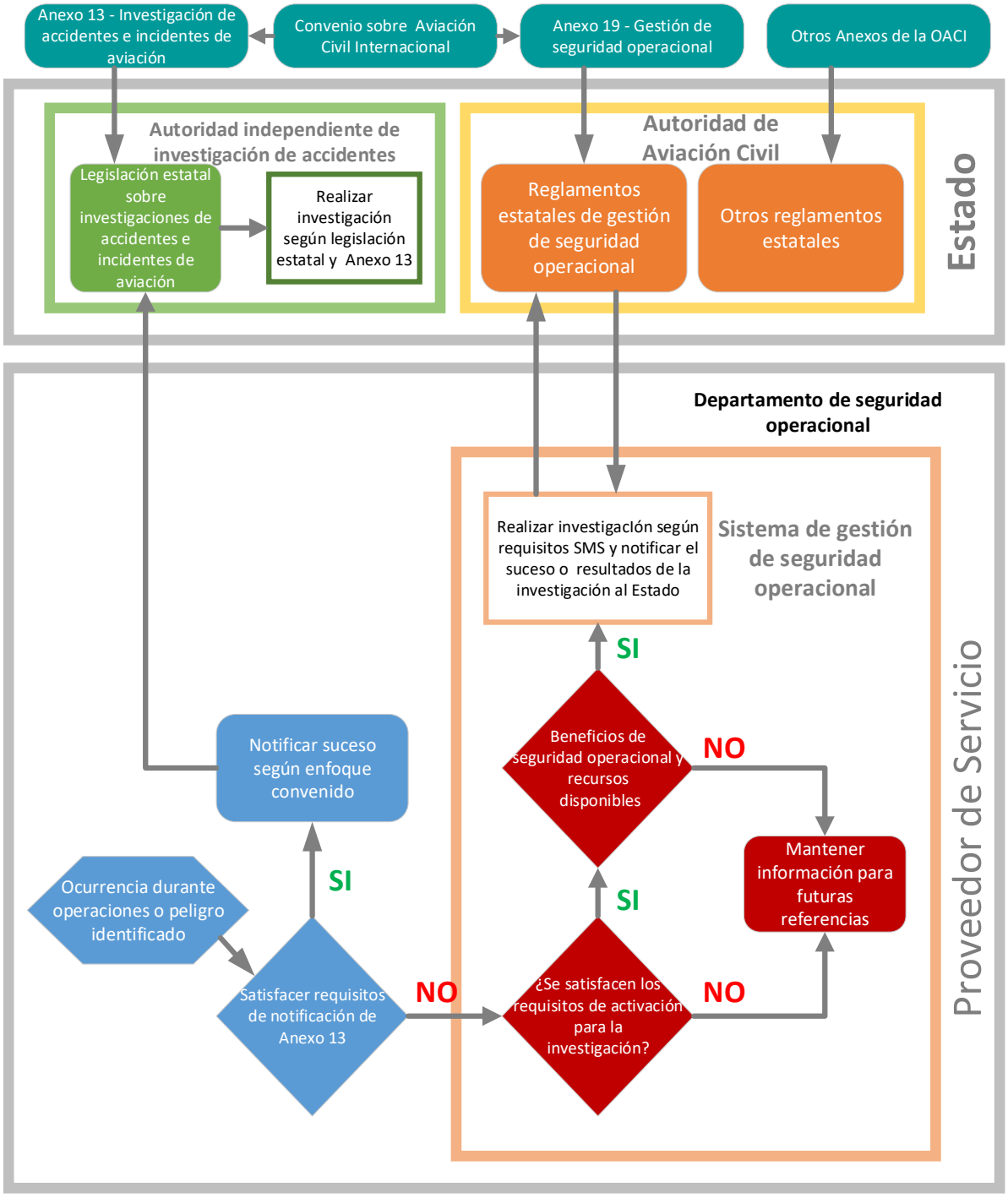
g) tendencias identificadas;

h) beneficio de la capacitación; y

i) disponibilidad de los recursos.

11.1.25 La **Figura 2** describe como sería el proceso de decisión de investigación de seguridad operacional.

Figura 2. Proceso de decisión de investigación de seguridad operacional



Asignación del investigador

11.1.26 Si va a comenzar una investigación, la primera acción será designar un investigador o,

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

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

El proceso de investigación

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

a) Establecer cronogramas de eventos clave y las acciones de las personas involucradas;

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

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

d) identificar cualquier control de riesgo existente que debería haber evitado que ocurriera el evento; y

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

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

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

11.1.31 En el **Apéndice 4** de esta circular se describe el ejemplo de un sistema de notificación voluntaria, incluyendo un modelo de formulario de reporte voluntario.

11.1.32 En conclusión, la Identificación de peligros será aceptable para la AAC si se han observado los siguientes criterios:

- *El CIAC ha definido de manera clara y detallada en su manual del SMS las metodologías, medios y procedimientos que garanticen la identificación de los peligros asociados a sus productos o servicios de aviación.*
- *Las fuentes para la identificación de peligros del CIAC pueden ser internas o externas a la organización.*
- *El CIAC ha establecido y documentado un sistema de notificación voluntaria y obligatoria, incluyendo las situaciones que requieren ser reportadas en cada uno de estos sistemas, los procedimientos de notificación, los formularios, y la garantía de protección de la información, e incentiva al personal en la cultura de notificación de peligros de la seguridad operacional.*
- *Existe un método adecuado para la documentación y registro de los peligros identificados.*
- *El CIAC ha establecido un sistema para la investigación de seguridad operacional.*

11.2 Evaluación y mitigación de riesgos de seguridad operacional

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

11.2.2 Para ello, necesita desarrollar un modelo y procedimientos de evaluación de riesgos de seguridad operacional que permitan un enfoque sistemático y consistente para la evaluación de los riesgos de seguridad operacional. Esto debería incluir un método que ayudará a determinar qué riesgos de seguridad operacional son aceptables o inaceptables y a priorizar acciones

11.2.3 Es posible que las herramientas de la SRM utilizadas necesiten ser revisadas y personalizadas periódicamente para garantizar que sean adecuadas para el entorno operativo del CIAC. La organización puede encontrar enfoques más sofisticados que reflejen mejor las necesidades de su operación a medida que los SMS crezcan. El CIAC y la AAC deberían acordar una metodología.

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

11.2.5 El proceso de evaluación de riesgos de seguridad operacional deberá usar los datos y la información de seguridad operacional disponible. Una vez que se han evaluado los riesgos de seguridad operacional, la organización participará en un proceso de toma de decisiones basado en datos para determinar qué controles de riesgos de seguridad operacional se necesitan.

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

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

11.2.8 La decisión del CIAC es priorizar sus evaluaciones de riesgos de seguridad operacional y adoptar controles de riesgos de seguridad operacional. Como guía, el centro de instrucción deberá declarar en el proceso de priorización como:

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

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

c) mantiene o mejora efectivamente la seguridad operacional;

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

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

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

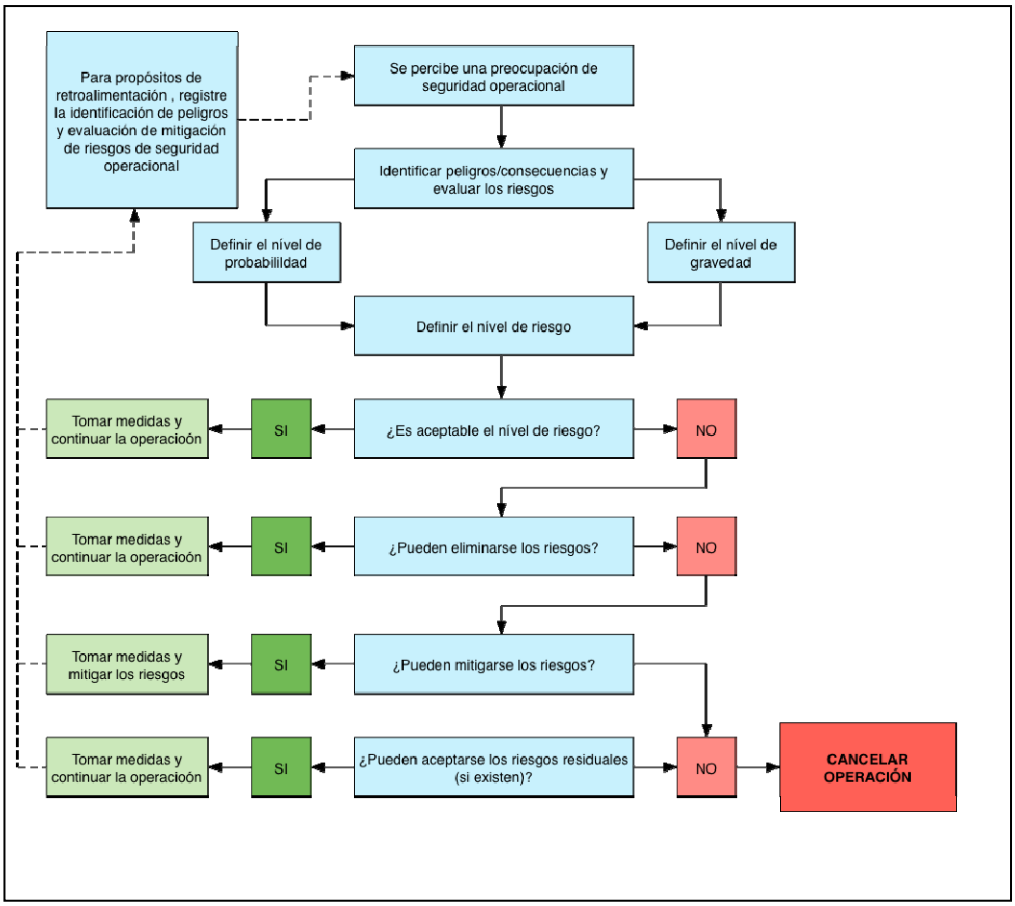
11.2.10 Una vez que se haya acordado e implementado el control de riesgos de seguridad operacional, se debe monitorear el rendimiento de seguridad operacional para asegurar la efectividad del control de riesgos de seguridad operacional. Esto es necesario para verificar la integridad, eficiencia y eficacia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

11.2.11 Los resultados de la SRM deben documentarse. Esto deberá incluir el peligro y las consecuencias, la evaluación de riesgos de seguridad operacional y cualquier acción de control de riesgos de seguridad operacional que se tome. Estos a menudo se capturan en un registro para que puedan ser rastreados y monitoreados. Esta documentación de la SRM se convierte en una fuente histórica de conocimiento de seguridad organizacional que puede usarse como referencia al tomar decisiones de seguridad operacional y para el intercambio de información de seguridad operacional. Este conocimiento de seguridad operacional proporciona material para análisis de tendencias de seguridad operacional, y entrenamiento y comunicación de seguridad operacional. También es útil para las auditorías internas evaluar si los controles y acciones de riesgos de seguridad se han implementado y son efectivos.

11.2.12 La **Figura 3** presenta el proceso de gestión de riesgos de seguridad operacional por completo. El proceso comienza con la identificación de los peligros y sus posibles consecuencias. Los riesgos de seguridad operacional se evalúan en términos de probabilidad y gravedad, para definir el nivel de riesgos de seguridad operacional (índice de riesgo de seguridad operacional).

11.2.13 Si los riesgos de seguridad operacional evaluados se consideran tolerables, se debe tomar una medida adecuada y la operación puede continuar. La identificación de peligros completada y el proceso de evaluación y mitigación de riesgos de seguridad operacional se documentan y aprueba como corresponda y forma parte del sistema de gestión de información de seguridad operacional. Luego de identificar los peligros, se deben determinar sus consecuencias (es decir, cualquier evento o resultado específico) se deben determinar.

Figura 3 - Proceso de gestión de riesgos de la seguridad operacional



11.2.14 En muchos casos será necesario priorizar los peligros de acuerdo con la gravedad/probabilidad de sus consecuencias proyectadas. Esto facilita la priorización de las estrategias de mitigación de riesgos, tanto como para usar recursos limitados de la forma más eficaz. La **Figura 4** presenta un ejemplo de un procedimiento de priorización de peligros.

Figura 4 – Ejemplo de un procedimiento de priorización de peligros

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

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

c) concluir que la priorización del peligro es:

<table><tr><th>Consecuencia proyectada</th><th>Nivel de peligro</th></tr><tr><td>Accidente
Incidente grave
Incidente</td><td>Nivel 1
Nivel 2
Nivel 3</td></tr></table></td><td>a) proyectar el número de índice de riesgo (según la matriz de gravedad y probabilidad pertinente) de la peor consecuencia posible del peligro (véase la Figura 7 de esta circular);

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

c) concluir que la priorización del peligro es:

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

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

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

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

b) la probabilidad que sucederá.

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

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

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

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

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

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

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

11.2.18 La **Figura 5** presenta una tabla de probabilidad de riesgo de seguridad operacional típica, en este caso, una tabla de cinco puntos. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un evento o una condición inseguros, la descripción de cada categoría y una asignación de valor a cada categoría.

Figura 5 – Tabla de probabilidad de riesgo de seguridad operacional

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

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

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

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

11.2.20 La evaluación de gravedad debe considerar todas las posibles consecuencias relacionadas con una condición o un objeto inseguros, considerando la peor situación predecible. La **Figura 6** presenta una tabla de gravedad de riesgo de seguridad operacional típico. Incluye cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada categoría. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla solo es un ejemplo.

Figura 6 – Tabla de gravedad de riesgo de seguridad operacional

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

11.2.21 El proceso de evaluación de la probabilidad y gravedad del riesgo de seguridad operacional puede usarse para derivar un índice de riesgo de seguridad operacional. El índice que se crea mediante la metodología descrita anteriormente consta de un identificador alfanumérico, que indica los resultados combinados de las evaluaciones de probabilidad y gravedad. Las combinaciones de gravedad / probabilidad respectiva se presentan en la matriz de evaluación del riesgo de seguridad operacional en la **Figura 7**.

Figura 7 – Ejemplo de una matriz de evaluación (índice) de riesgos de seguridad operacional.

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

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

11.2.23 El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a una matriz de tolerabilidad del riesgo de seguridad operacional (véase la Figura 8) que describe los criterios de tolerabilidad para una organización en particular. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B cae en la categoría “inaceptable bajo las circunstancias existentes”. En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por tanto, la organización debe:

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

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

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

11.2.24 La pirámide invertida en la **Figura 8** refleja un esfuerzo constante para impulsar el índice de riesgo hacia el vértice inferior de la parte inferior de la pirámide. La **Figura 9** proporciona un ejemplo de una matriz de tolerabilidad de riesgo de seguridad operacional alternativa.

Figura 8 – Matriz de tolerabilidad del riesgo de seguridad operacional

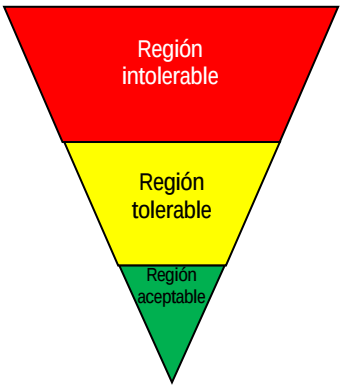
Descripción de la tolerabilidad	Índice de riesgo evaluado	Criterios sugeridos
	5A, 5B, 5C, 4A, 4B, 3A	Inaceptable según las circunstancias existentes
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Aceptable según la mitigación de riesgos. Puede necesitar una decisión de gestión.
	3E, 2D, 2E, 1B, 1C,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

Figura 9 – Matriz de tolerabilidad del riesgo de seguridad operacional alternativa

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

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

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

Estrategias de mitigación de riesgos de seguridad operacional

11.2.27 Las mitigaciones de riesgos de seguridad operacional son acciones que a menudo generan cambios en los procedimientos operativos, equipos o infraestructura de la organización. Estas estrategias se dividen en tres categorías:

a) ***Evitar*.** La operación o actividad se cancela o evita debido a que el riesgo de seguridad excede el beneficio de continuar la actividad, eliminando así el riesgo de seguridad por completo.

b) ***Reducir*.** La frecuencia de la operación o actividad se reduce, o se toma una acción para reducir la magnitud de las consecuencias del riesgo de seguridad.

c) ***Segregar*.** Se toman medidas para aislar los efectos de las consecuencias del riesgo de seguridad o se construyen varias capas de defensas para protegerse de ellas.

11.2.28 La consideración de los factores humanos es una parte integral de la identificación de mitigaciones efectivas, porque el personal es llamado a aplicar o contribuir a la mitigación o a las acciones correctivas. Por ejemplo, las mitigaciones pueden incluir la utilización de procesos o procedimientos que sin el aporte de quienes los utilizarán en situaciones del día a día, estos podrían no ser adecuados para su propósito y resultar en consecuencias no deseadas. Además, las limitaciones de rendimiento del factor humano deben considerarse como parte de cualquier mitigación de los riesgos de seguridad, estableciendo estrategias de captura de errores para abordar la variabilidad del desempeño humano.

11.2.29 Las alternativas de mitigación para cada riesgo deben ser evaluadas desde las siguientes perspectivas:

a) ***Eficacia*.** El grado hasta donde las alternativas reducen o eliminan los riesgos de seguridad operacional. La eficacia puede determinarse en términos de defensas técnicas, de capacitación y reglamentarias que pueden reducir o eliminar los riesgos de seguridad operacional.

b) ***Costo/beneficio*.** El grado hasta donde los beneficios percibidos de la mitigación exceden los costos.

c) ***Practicidad*.** El grado hasta donde la mitigación puede ser implementada y que tan adecuada es en términos de disponibilidad de tecnología, recursos financieros y administrativos, legislación y reglamentos, voluntad política, etc.

d) ***Aceptabilidad*.** El grado hasta donde la alternativa es coherente con los paradigmas del accionista.

e) ***Ejecutabilidad*.** El grado hasta donde el cumplimiento de nuevas reglas, reglamentos o procedimientos de operación pueden supervisarse.

f) ***Durabilidad*.** El grado hasta donde la mitigación será sostenible y eficaz.

g) ***Riesgos de seguridad operacional residual*.** El grado de los riesgos de seguridad operacional que sigue siendo secundario a la implementación de la mitigación inicial y que podría necesitar medidas de control de riesgos adicionales.

h) ***Consecuencias no deseadas*.** La introducción de nuevos peligros y riesgos de seguridad operacional relacionados que estén asociados con la implementación de cualquier alternativa de mitigación.

i) ***Tiempo*.** Tiempo requerido para la implementación de la alternativa de mitigación de riesgo.

11.2.30 Luego de aprobar e implementar la mitigación, cualquier impacto asociado con el rendimiento en materia de seguridad operacional proporciona retroalimentación para el proceso de aseguramiento de la seguridad operacional del CIAC. Esto es necesario para garantizar la integridad, eficiencia y eficacia de las defensas según las nuevas condiciones operacionales.

11.2.31 Cada ejercicio de mitigación de riesgos se documentará de manera progresiva. Esto puede lograrse al usar una variedad de aplicaciones, desde hojas de cálculo o tablas básicas

hasta software personalizado de mitigación de riesgos comercial. Los documentos de mitigación de riesgos completos deben recibir la aprobación del nivel correspondiente de la administración.

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

- *El CIAC ha establecido y documentado en su manual del SMS un proceso de evaluación y mitigación de los riesgos que garantice el análisis, la evaluación y el control de los riesgos de seguridad operacional asociados a los peligros identificados.*
- *El proceso de evaluación y mitigación de los riesgos incluye los procedimientos para:*
  - *la priorización de los peligros;*
  - *la evaluación del nivel de riesgos asociados a los peligros identificados en términos de probabilidad y gravedad;*
  - *la determinación de la tolerabilidad del riesgo;*
  - *la definición de las medidas adecuadas y las estrategias de mitigación de riesgos; y*
  - *alguna forma de retroalimentación.*
- *Existe un método y procedimientos adecuados para la documentación y archivo de la identificación de peligros y la evaluación y mitigación de los riesgos, de acuerdo con 11.2.10 y 11.2.31.*
- *El CIAC ha desarrollado tablas de probabilidad y gravedad para identificar los valores y definiciones respectivas, de acuerdo con 11.2.18 y 11.2.20.*
- *El CIAC ha desarrollado una matriz de evaluación del riesgo de seguridad operacional de acuerdo con 1a.2.21.*
- *El CIAC ha desarrollado una matriz de tolerabilidad de riesgo de acuerdo con 11.2.22 y 11.2.23 y 11.2.24.*
- *El CIAC ha establecido las estrategias para la mitigación de riesgos y la metodología para su selección de acuerdo con 11.2.27 y 11.2.29.*

12. Componente 3: Aseguramiento de la seguridad operacional

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

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

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

La gestión de la seguridad no es una actividad de "hacer una vez y olvidar". Requiere atención constante, y mejora del SMS para lograr un sistema maduro y una organización resistente. La mejora continua del SMS requiere un enfoque de proceso: la identificación de entradas relevantes para medir la efectividad del SMS, analizando y determinando las implicaciones de estos insumos, y generando posteriormente salidas que mejoran su efectividad

y su impacto en la seguridad operacional. Es decir, una vez que la organización ha evaluado su desempeño de la seguridad operacional, necesita actuar en esa información para mejorar los SMS.

12.1 Observación y medición del rendimiento en materia de seguridad operacional

12.1.1 Para verificar el rendimiento de seguridad operacional y validar la efectividad de los controles de riesgos de seguridad operacional, se requiere el uso de una combinación de auditorías internas y el establecimiento y monitoreo de SPI.

12.1.2 Evaluar la efectividad de los controles de riesgos de seguridad operacional es importante ya que su aplicación no siempre logra los resultados previstos. Esto ayudará a identificar si se seleccionó el control de riesgos de seguridad operacional adecuado y puede dar como resultado la aplicación de una estrategia de control de riesgos de seguridad operacional diferente.

Auditoría interna

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

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

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

a) cumplimiento con los reglamentos;

b) cumplimiento de políticas, procesos y procedimientos;

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

d) la efectividad de las acciones correctivas; y

e) la efectividad del SMS.

12.1.6 Algunas organizaciones no pueden garantizar la independencia apropiada de una auditoría interna, en tales casos, el CIAC debe considerar contratar auditores externos (por ejemplo, auditores independientes o auditores de otra organización).

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

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

a) Determinación del cumplimiento

   1) ¿Existe el proceso o procedimiento requerido?

   2) ¿Está documentado el proceso o procedimiento (entradas, actividades, interfaces y

resultados definidos)?

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

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

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

6) ¿Se están produciendo los resultados definidos?

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

b) Evaluación de la efectividad

1) ¿Los usuarios entienden el proceso o procedimiento?

2) ¿Se está logrando el propósito del proceso o procedimiento de manera consistente?

3) ¿Son los resultados del proceso o procedimiento lo que el "cliente" solicitó?

4) ¿El proceso o procedimiento se revisa regularmente?

5) ¿Se realiza una evaluación de riesgos de seguridad operacional cuando hay cambios en el proceso o procedimiento?

6) ¿Las mejoras al proceso o al procedimiento dieron como resultado los beneficios esperados?

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

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

12.1.11 Un ejemplo de reporte de acción correctiva y preventiva como resultado de una auditoría se incluye en el **Apéndice 5** de esta circular.

Monitoreo del rendimiento de la seguridad operacional

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

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

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

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

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

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

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

b) eventos de alta probabilidad / baja gravedad (por ejemplo, eventos operativos sin incidentes, informes de no conformidad, desviaciones, etc.): y

c) rendimiento del proceso (por ejemplo, capacitación, mejoras del sistema y procesamiento de informes).

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

12.1.16 Al establecer SPI, el CIAC debe establecer:

a) **Medición de las cosas correctas**: determine los mejores SPI que mostrarán que la organización está en camino de lograr sus objetivos de seguridad operacional. También considere cuáles son los mayores problemas y riesgos de seguridad operacional que enfrentan la organización, e identifique los SPI que mostrarán un control efectivo de estos.

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

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

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

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

12.1.18 En el **Apéndice 6** se brinda información para el desarrollo de indicadores y metas de rendimiento de seguridad operacional y en los **Apéndice 7 y 7A** ejemplos de indicadores y formulario de indicador.

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

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

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

Ejemplos de formularios de notificación de eventos en vuelo, en mantenimiento y de acción de seguimiento del evento, se detallan en los **Apéndices 8, 9 y 10** de esta circular.

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

d) **Las auditorías de seguridad operacional** se centran en evaluar la integridad de los SMS y los sistemas de soporte del proveedor del servicio. Las auditorías de seguridad operacional también se pueden usar para evaluar la efectividad de los controles de riesgo de seguridad operacional instalados o para monitorear el cumplimiento de los requisitos 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 vigentes: políticas, procedimientos, roles, protocolos de comunicación.

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

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

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

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

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

12.1.23 El Estado puede tener procesos específicos para la aceptación de SPI y SPT que necesitarán seguirse. Por lo tanto, durante el desarrollo de SPI y SPT, el proveedor del servicio deberá consultar con la autoridad reguladora de la organización o cualquier información relacionada que el Estado haya publicado.

12.1.24 También existen otras actividades que contribuyen a la observación y medición del rendimiento en materia de seguridad, como:

a) La encuesta sobre las percepciones de seguridad del personal dentro de la organización (por ejemplo, una encuesta de cultura de seguridad);

b) la captura sistemática de datos para ayudar a contextualizar estadísticas (por ejemplo, número de ocurrencias por mes, número de informes de defectos por mes, etc.);

c) la comunicación de resultados a todo el personal;

d) desarrollar métodos para rastrear cómo funciona el sistema de gestión de seguridad. (por ejemplo, cuadro de mando integral);

e) establecimiento de reuniones periódicas para revisar el desempeño en seguridad.

12.1.25 La observación y medición del rendimiento en materia de seguridad operacional será aceptable para la AAC si se han observado que el CIAC ha considerado los siguientes criterios:

a) Procedimientos para la realización de auditorías internas e identificación de áreas para una mejora potencial de la efectividad del SMS.

b) Procedimientos para la implementación y monitoreo efectivo de todos los controles de riesgo de seguridad operacional.

c) Procedimientos para evaluar el cumplimiento y la efectividad de la seguridad operacional.

d) Métodos para el monitoreo del progreso en el cierre de incumplimientos previamente identificados, mediante el análisis de la causa raíz e implementación de planes de acción correctivos y preventivos.

e) Procedimientos para establecer los SPI para medir el rendimiento de seguridad operacional de la organización;

f) Que los SPI establecidos consideren lo señalado en el 12.1.16.

g) Monitorear el rendimiento de SPI y SPT establecidos para identificar cambios o distorsiones en el rendimiento de seguridad operacional.

12.2 Gestión del cambio

12.2.1 El CIAC 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 que ofrece, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios.

12.2.2 Los centros de instrucción experimentan cambios debido a una serie de factores que incluyen, entre otros:

a) Expansión organizacional o contracción;

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

c) cambios en el entorno operativo del centro;

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

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

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

12.2.4 El proceso de gestión de cambio de la organización deberá tener en cuenta las siguientes consideraciones:

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

b) Disponibilidad de expertos en la materia. Es importante que los miembros clave de la comunidad aeronáutica participen en las actividades de gestión del cambio. Esto puede incluir individuos de organizaciones externas.

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

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

12.2.6 El CIAC debe definir el desencadenante para el proceso de cambio formal. Los cambios que probablemente desencadenarán la gestión formal del cambio incluyen:

a) La incorporación de nueva tecnología o equipos;

b) cambios en el entorno operacional;

c) cambios del personal clave;

d) cambios significativos en los niveles de empleo;

e) cambios en los requisitos regulatorios de seguridad operacional;

f) reestructuración significativa de la organización; y

g) cambios físicos (nueva instalación o sede de operaciones, cambios en el diseño del aeródromo utilizado para la instrucción de vuelo, etc.

12.2.7 El CIAC también debe considerar el impacto del cambio en el personal. Esto podría afectar la forma como el cambio es aceptado por los afectados. La comunicación temprana y el compromiso de la alta dirección normalmente mejoran la forma en que el cambio es percibido e implementado.

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

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

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

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

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

12.2.9 El ejemplo de formulario para la evaluación de gestión de cambio se detalla en el **Apéndice 11** de esta circular.

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

- *El CIAC ha desarrollado y publicado en su manual del SMS un proceso para identificar los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus productos o servicios de aviación, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios.*
- *Mantener un proceso que identifique los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus productos o servicios de aviación que ofrece, con la identificación de peligros y riesgos de seguridad operacional evaluados y controlados.*
- *El proceso de gestión de cambio de la organización ha tomado en cuenta consideraciones de criticidad, disponibilidad de expertos en la materia y disponibilidad de datos e información sobre el rendimiento de seguridad operacional.*
- *Que el sistema de gestión de cambios sea revisado regularmente.*
- *Definir el desencadenante para el proceso de cambio formal.*
- *Considerar el efecto del cambio en el personal de la organización.*

12.3 Mejora continua del SMS

12.3.1 El Anexo 19 sobre la gestión de la seguridad operacional, Apéndice 2, Numeral 3.3 requiere que: *"El proveedor de servicios observará y evaluará sus procesos SMS para mantener y mejorar continuamente la eficacia".* El mantenimiento y la mejora continua de la efectividad del SMS del CIAC se respaldan en actividades de seguridad operacional que incluyen la verificación y el seguimiento de las acciones y los procesos de auditoría interna. Se deberá reconocer que mantener y mejorar continuamente el SMS es un viaje continuo ya que la organización y el entorno operativo cambiarán constantemente.

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

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

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

b) Evaluaciones, incluyendo evaluaciones de la cultura de seguridad operacional y efectividad de SMS.

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

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

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

f) Evaluación de SPIs y SPTs, posiblemente como parte de la revisión de la administración, como se consideran las tendencias y, cuando los datos apropiados están disponibles, se pueden comparar con otros proveedores de servicios o datos estatales o globales.

g) Abordar las lecciones aprendidas, desde los sistemas de informes de seguridad operacional y las investigaciones de seguridad operacional del proveedor del servicio. Esto deberá conducir a la implementación de mejoras de seguridad operacional.

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

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

- *El CIAC ha establecido las políticas, características, frecuencia y procedimientos (incluidas las ayudas de trabajo) relacionados con las auditorías internas y auditorías externas de su SMS.*
- *Las auditorías internas incluyen la evaluación de todas las funciones de gestión de la seguridad operacional en toda la organización.*
- *Que se hayan establecido e implementado los métodos para determinar la efectividad del SMS, considerando los criterios señalados en 12.3.3.*
- *Las políticas y procedimientos relacionados con las auditorías externas incluyen los criterios de selección de las organizaciones auditoras, y el compromiso y procedimientos para el tratamiento de los hallazgos y no conformidades*

13. Componente 4: Promoción de la seguridad operacional

Este último componente del SMS está orientado a promover una cultura de seguridad positiva y ayuda a alcanzar los objetivos de seguridad operacional del CIAC a través de la combinación de competencia técnica que se mejora continuamente a través de capacitación y educación, comunicaciones efectivas y compartición de información. La alta dirección del CIAC proporciona el liderazgo para promover la cultura de seguridad en toda la organización.

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

La organización debe establecer e implementar procesos y procedimientos que faciliten la comunicación bidireccional efectiva en todos los niveles de la organización. Esto debería incluir una clara dirección estratégica desde la parte superior de la organización y la habilitación de una comunicación "ascendente" que aliente comentarios abiertos y constructivos de todo el personal.

13.1 Instrucción y educación

13.1.1 El Anexo 19 requiere que "*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"*. También requiere que *"El alcance del programa de instrucción en seguridad operacional sea apropiado para el tipo de participación que cada persona tenga en el SMS*".

13.1.2 Para garantizar que el personal sea competente para realizar sus tareas relacionadas con la seguridad, deben recibir capacitación en el SMS de su organización para comprender los

objetivos de seguridad de la organización y adquirir las habilidades y conocimiento para ayudar a alcanzarlos. La formación en seguridad es la base para el desarrollo y mantenimiento de la cultura de seguridad de una organización.

13.1.3 El responsable de seguridad operacional debe garantizar que exista un programa de capacitación de seguridad operacional adecuado. Esto incluye proporcionar la información de seguridad operacional relevante a los problemas de seguridad operacional específicos registrados por la organización.

13.1.4 El personal capacitado y competente para realizar sus tareas de SMS, independientemente de su nivel en la organización, es una indicación del compromiso de la administración con un SMS efectivo. El programa de capacitación debe incluir requisitos de capacitación inicial y periódica para mantener las competencias. La instrucción inicial debe considerar, como mínimo, lo siguiente:

a) Políticas de seguridad operacional organizacional y objetivos de seguridad operacional;

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

c) principios básicos de la SRM;

d) sistemas de notificaciones de seguridad operacional;

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

f) factores humanos.

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

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

13.1.7 Los requisitos de capacitación deben documentarse para cada área de actividad. Se debe desarrollar un archivo de capacitación para cada empleado, incluida la administración.

13.1.8 Deberá haber capacitación de seguridad específica para el gerente responsable y los altos directivos que incluya los siguientes temas:

g) capacitación específica de sensibilización respecto a sus rendiciones de cuentas; las responsabilidades de SMS y su relación con la estrategia comercial general de la organización;

h) compromiso de gestión;

i) asignación de recursos;

j) promoción de la política de seguridad operacional y del SMS;

k) promoción de una cultura de seguridad operacional positiva;

l) comunicación efectiva de seguridad operacional a nivel de toda la organización;

m) objetivos de seguridad operacional, SPT y niveles de alerta; y

n) política disciplinaria.

Análisis de necesidades de capacitación

13.1.9 Para la mayoría de las organizaciones, un *análisis formal de las necesidades de capacitación* (TNA) es necesario para garantizar que haya una comprensión clara de la operación, las obligaciones de seguridad operacional del personal y la capacitación disponible.

13.1.10 Una TNA típica normalmente comenzará realizando un análisis de personal objetivo, que generalmente incluye los siguientes pasos:

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

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

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

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

13.1.11 También es importante identificar el método apropiado para la entrega de la instrucción. El objetivo principal es que, al finalizar la capacitación, el personal sea competente para realizar sus tareas de SMS. Los instructores competentes suelen ser la consideración más importante, su compromiso, sus habilidades de enseñanza y su experiencia en administración de seguridad operacional tendrán un impacto significativo en la efectividad de la capacitación entregada. El programa de capacitación en seguridad operacional también deberá especificar las responsabilidades para el desarrollo del contenido y la programación de la capacitación, así como los registros de los archivos de capacitación y competencia.

13.1.12 La organización debe determinar quién deberá ser capacitado y a qué profundidad y esto dependerá de su participación en el SMS. La mayoría de las personas que trabajan en la organización tienen alguna relación directa o indirecta con la seguridad operacional de la aviación y, por lo tanto, tienen algunos deberes de SMS. Esto se aplica al personal directamente involucrado en la entrega de los productos y servicios y al personal involucrado en los comités de seguridad operacional de la organización. Además, algunos miembros del personal administrativo y de apoyo aún tienen algunas responsabilidades limitadas de SMS, ya que su trabajo puede tener un impacto indirecto en la seguridad operacional de la aviación y aún necesitaría algo de capacitación de SMS.

13.1.13 La organización deberá identificar las responsabilidades de SMS del personal y esto se deberá usar para determinar el alcance del programa de capacitación de seguridad operacional y garantizar que cada individuo reciba capacitación alineada con su participación en el SMS. El programa de capacitación en seguridad operacional deberá especificar el contenido de la capacitación en seguridad operacional para el personal de apoyo, el personal operativo, los gerentes y supervisores, los gerentes principales y el ejecutivo responsable.

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

- *El CIAC ha establecido dentro de su programa de instrucción, la instrucción inicial y periódica del SMS para todas las personas involucradas en actividades de seguridad operacional que garantice el nivel de competencia de su personal. El programa establece que la instrucción de SMS debe ser recibida al menos por:*
  - *Director o el gerente responsable;*
  - *gerente del SMS;*

- *jefe de instructores y los instructores;*
- *alumnos*

- *El gerente del SMS garantizará que exista un programa de capacitación de seguridad operacional adecuado.*
- *La instrucción inicial y la periódica debe incluir lo indicado 13.1.4, 13.1.5 y 3.1.8;*
- *El programa de capacitación deberá adaptarse a las necesidades del rol del individuo dentro del SMS.*
- *Está claramente establecida la responsabilidad por el desarrollo de los contenidos de los cursos, la programación y el mantenimiento de los registros de capacitación.*
- *La capacitación del gerente responsable y altos directivos ha sido especialmente diseñada para ser una sesión de alto nivel, que asegure la comprensión sus responsabilidades con relación al SMS, así como la descripción general del SMS y su relación con la estrategia comercial de la organización.*
- *Se documentarán y archivarán los requisitos de capacitación para cada empleado.*

13.2 Comunicación de seguridad operacional

13.2.1 El CIAC debería comunicar los objetivos y procedimientos del SMS de la organización a todo el personal apropiado. Asimismo, debería existir una estrategia de comunicación que permita que la comunicación de seguridad operacional se brinde por el método más apropiado en función al rol del individuo y la necesidad de recibir información relacionada con la seguridad operacional. Esto puede hacerse a través de boletines de seguridad operacional, avisos, boletines, informes o cursos de capacitación. El responsable de seguridad operacional también deberá asegurarse de que las lecciones aprendidas de las investigaciones y los historiales o experiencias, tanto internamente como de otras organizaciones, se distribuyan ampliamente. Por lo tanto, la comunicación de seguridad operacional tiene como objetivo:

a) Asegurarse de que el personal tenga pleno conocimiento del SMS, esta es una buena forma de promover la política y los objetivos de seguridad operacional de la organización;

b) transmitir información crítica para la seguridad operacional, la información crítica de seguridad operacional es información específica relacionada con problemas de seguridad operacional y riesgos de seguridad operacional que podrían exponer a la organización a riesgos de seguridad operacional. Esto podría ser a partir de la información de seguridad operacional recopilada de fuentes internas o externas, como las lecciones aprendidas o relacionadas con los controles de riesgos de seguridad operacional. El centro de instrucción determina qué información se considera de seguridad operacional crítica y la oportunidad de su comunicación;

c) crear conciencia sobre nuevos controles de riesgos de seguridad operacional y acciones correctivas, los riesgos de seguridad operacional que enfrenta el centro de instrucción cambiará con el tiempo y si se trata de un nuevo riesgo de seguridad operacional identificado o cambios en los controles de riesgos de seguridad operacional, estos cambios deberán comunicarse al personal apropiado;

d) proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados, cuando se actualizan los procedimientos de seguridad operacional, es importante que las personas adecuadas conozcan estos cambios;

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

f) proporcionar retroalimentación al personal que presente informes de seguridad operacional sobre qué acciones se han tomado para abordar cualquier problema identificado.

13.2.2 El CIAC debería considerar si alguna de la información de seguridad operacional

enumerada anteriormente necesita ser comunicada a organizaciones externas.

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

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

a) La difusión del manual del SMS;

b) los procesos y procedimientos de seguridad operacional;

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

i) sitios web o correo electrónico.

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

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

- *El CIAC ha establecido un método oficial de comunicación sobre seguridad operacional que cumpla con los objetivos señalados en 13.2.1.*
- *Se han desarrollado y documentado procedimientos para la comunicación regular de información sobre tendencias de rendimiento en materia de seguridad operacional y temas de seguridad relevantes, incluyendo la responsabilidad por la preparación y publicación de esta información.*
- *Se han determinado los medios apropiados para distribuir la información del punto anterior, de tal forma de garantizar su amplia distribución.*
- *Se asegurará que el personal de la organización tenga pleno conocimiento del SMS.*
- *Concientizar sobre nuevos controles de riesgos de seguridad operacional y acciones correctivas.*
- *Proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados.*
- *Promover cultura de seguridad operacional positiva y alentar al personal a identificar e informar los peligros.*
- *Proporcionar retroalimentación al personal que presente informes de seguridad operacional.*

14. Ejemplos de métodos aceptables de cumplimiento de los requisitos del SMS en base al tamaño y complejidad del CIAC 141

Para una mejor orientación de cumplimiento de los requisitos de cada uno de los elementos de la estructura del SMS, se establece en el **Apéndice 12** ejemplos de diferencias y similitudes que pudieran ser aceptables por la AAC, basados en el tamaño y complejidad de la organización, conforme a la clasificación establecida en la **Tabla 1** de esta circular.

15. PLANIFICACIÓN DE LA IMPLEMENTACIÓN DEL SMS

15.1 Descripción del sistema

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

15.1.2 Debido a que cada centro de instrucción es único, no existe un método "único para todos" para la implementación de SMS. Se espera que cada centro implemente un SMS que funcione para su situación particular. Cada centro deberá definir por sí mismo cómo pretende cumplir los requisitos fundamentales.

15.1.3 Para lograr ello, es importante que cada CIAC prepare una descripción del sistema que identifique sus estructuras organizacionales, procesos y acuerdos comerciales que considere importantes para las funciones de gestión de seguridad operacional. Con base en la descripción del sistema, la organización deberá identificar o desarrollar políticas, procesos y procedimientos que establezcan sus propios requisitos de administración de seguridad operacional.

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

15.2 Gestión de interfaz

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

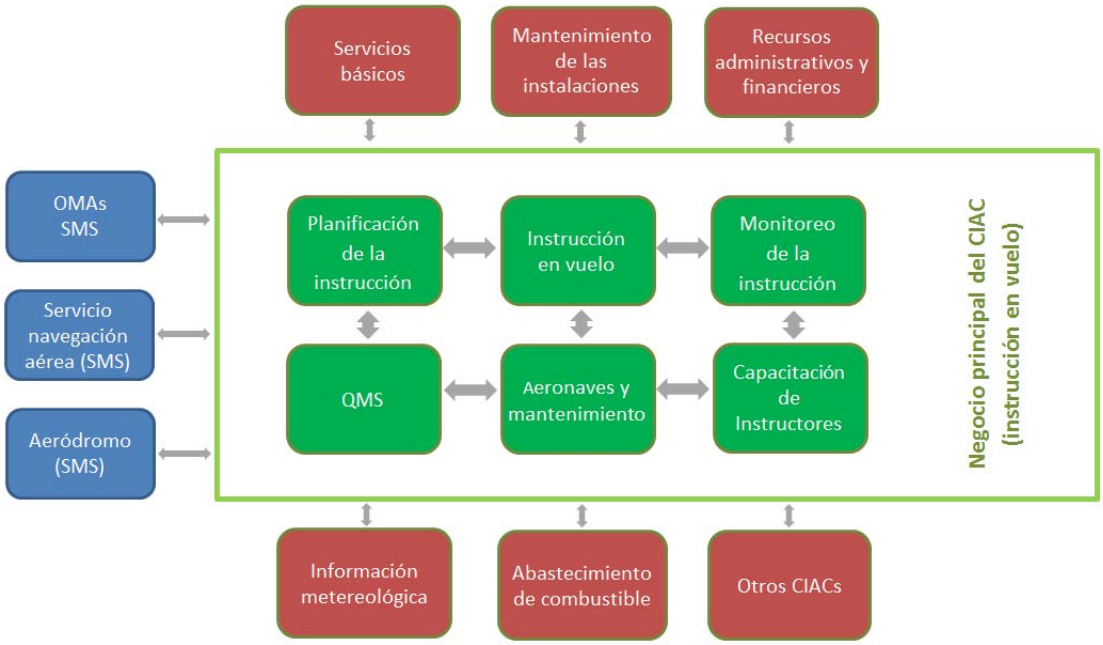
15.3 Identificación de las interfaces de SMS

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

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

15.3.3 La **Figura 10** es un ejemplo de cómo un CIAC podría mapear las diferentes organizaciones con las que interactúa para identificar cualquier interfaz de SMS. El objetivo de esta revisión es producir una lista completa de todas las interfaces. El motivo de este ejercicio es que puede haber interfaces de SMS de las que una organización no está necesariamente al tanto. Puede haber interfaces donde no hay un acuerdo formal. En este caso, la fuente de alimentación o el mantenimiento del edificio son buenos ejemplos.

Figura 10. Ejemplo de las interfaces del SMS de un CIAC



15.3.4 Una vez que se han identificado las interfaces del SMS, el CIAC deberá considerar su criticidad relativa. Esto permite al CIAC priorizar la gestión de las interfaces más críticas y sus posibles riesgos de seguridad operacional. Los aspectos a considerar son:

a) qué se está proporcionando;

b) por qué es necesario;

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

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

Evaluar el impacto de seguridad operacional de las interfaces

15.3.5 El CIAC deberá entonces identificar cualquier peligro relacionado con las interfaces y llevar a cabo una evaluación de riesgos de seguridad operacional utilizando sus procesos existentes de identificación de peligros y evaluación de riesgos de seguridad operacional.

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

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

Gestionar y monitorear interfaces

15.3.8 El CIAC deberá entonces identificar cualquier peligro relacionado con las interfaces y llevar a cabo una evaluación de riesgos de seguridad operacional utilizando sus procesos existentes de identificación de peligros y evaluación de riesgos de seguridad operacional.

15.3.9 Los desafíos asociados con la capacidad del CIAC para administrar los riesgos de seguridad de la interfaz incluyen:

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

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

c) recursos insuficientes o experiencia técnica disponible para administrar y monitorear la interfaz; y

d) número y ubicación de las interfaces.

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

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

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

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

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

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

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

15.4 Escalabilidad del SMS

15.4.1 El SMS del CIAC, incluyendo las políticas, procesos y procedimientos, deben reflejar el tamaño y la complejidad de la organización y sus actividades. Debe considerar:

a) la estructura organizacional y la disponibilidad de recursos;

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

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

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

Consideraciones de riesgo de seguridad operacional

15.4.3 Independientemente del tamaño del CIAC, la escalabilidad también debe ser una función del riesgo inherente de seguridad operacional de sus actividades. Incluso las organizaciones pequeñas pueden participar en actividades que pueden implicar riesgos significativos para la seguridad operacional de la aviación. Por lo tanto, la capacidad de gestión de seguridad operacional debe ser acorde con el riesgo de seguridad operacional que se gestionará.

Datos de información de seguridad operacional y su análisis

15.4.4 Para organizaciones pequeñas, el bajo volumen de datos puede significar que es más difícil identificar tendencias o cambios en el rendimiento de seguridad operacional. Esto puede requerir reuniones para plantear y discutir problemas de seguridad operacional con la

experiencia adecuada. Esto puede ser más cualitativo que cuantitativo, pero ayudará a identificar los peligros y riesgos para el CIAC.

15.4.5 Puede ser útil colaborar con otros proveedores de servicios o asociaciones de la industria, ya que estos pueden tener datos que el propio CIAC no tiene. Por ejemplo, los proveedores de servicios más pequeños pueden intercambiar con organizaciones / operaciones similares para compartir información de riesgos de seguridad operacional e identificar tendencias de rendimiento de seguridad operacional. Los CIAC deberán analizar y procesar adecuadamente sus datos internos, a pesar de que pueden ser limitados.

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

15.5 Integración de sistemas de gestión

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

15.5.2 Un sistema típico de gestión integrado puede incluir, por ejemplo:

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

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

c) sistema de gestión ambiental (EMS);

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

e) sistema de gestión financiera (FMS);

f) sistema de gestión de la documentación (DMS); y

g) gestión del riesgo de fatiga (FRMS)

15.5.3 Una CIAC podría escoger integrar estos sistemas de gestión basados en sus requisitos únicos. Los procesos de gestión de riesgos y los procesos de auditoría interna son características esenciales de la mayoría de estos sistemas de gestión. Deberá reconocerse que los riesgos y controles de riesgo desarrollados en cualquiera de estos sistemas podrían tener un impacto en otros sistemas. Además, pueden existir otros sistemas operativos asociados a las actividades empresariales que también pueden integrarse, como la gestión de proveedores, la gestión de instalaciones, etc.

15.5.4 Un CIAC podría también considerar la aplicación del SMS a otras áreas que no tienen un requisito reglamentario actual para un SMS. Alternativamente, puede haber situaciones en las que se prefiera un SMS individual para cada tipo de actividad de aviación. Las organizaciones 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

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

a) Reducción de la duplicidad y superposición de procesos y recursos;

b) reducción de las responsabilidades y relaciones potencialmente conflictivas;

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

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

15.5.6 Los posibles desafíos de la integración del sistema de gestión son:

a) Los sistemas existentes pueden tener diferentes administradores funcionales que resistan la integración que 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 por separado.

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

15.6 Integración de SMS y QMS

15.6.1 Los CIAC 141 Tipo 2 y Tipo 3 tienen tanto sistema de gestión de la seguridad operacional (SMS) y sistema de gestión de calidad (QMS). Algunas veces se integran en un único sistema de gestión. El QMS generalmente se define como la estructura organizacional y las responsabilidades asociadas, recursos, procesos y procedimientos necesarios para establecer y promover un sistema de aseguramiento y mejora continua de la calidad al entregar un producto o servicio.

15.6.2 Ambos sistemas son complementarios, el SMS se centra en la gestión de los riesgos y el rendimiento de la seguridad operacional mientras que el QMS se centra en el cumplimiento de las normas y requisitos prescriptivos para cumplir con las expectativas del cliente y las obligaciones contractuales. Los objetivos de un SMS son identificar los peligros, evaluar el riesgo de seguridad operacional asociado e implementar controles efectivos de riesgos de seguridad operacional. En contraste, el QMS se enfoca en la entrega consistente de productos y servicios que cumplen con las especificaciones relevantes. No obstante, tanto el SMS como el QMS, tienen aspectos comunes y también diferencias que se especifican a continuación:

Tabla 3. Aspectos comunes entre SMS y QMS

Aspectos comunes entre SMS y QMS
1. Deberán planificarse y gestionarse.
2. Involucrar todas las funciones organizacionales relacionadas con la entrega de productos y servicios de aviación.
3. Identificar procesos y procedimientos ineficaces.
4. Esforzarse por mejorar continuamente.
5. Tienen el mismo objetivo de proporcionar productos y servicios seguros y confiables a los clientes.

Tabla 4. Diferencias entre el SMS y QMS

El SMS se centra en:	El QMS se centra en:
1. Identificación de los peligros relacionados con la seguridad operacional que enfrenta la organización.	1. Cumplimiento de los reglamentos y requisitos.
2. Evaluación del riesgo asociado.	2. Consistencia en la entrega de productos y servicios.
3. Implementación de controles de riesgo efectivos para mitigar los riesgos de seguridad operacional.	3. Cumplimiento con los estándares de rendimiento especificados.
4. Medición del rendimiento de seguridad operacional.	4. Entrega de productos y servicios que sean "adecuados para el propósito" y libres de defectos o errores
5. Mantenimiento de una asignación de recursos apropiada para cumplir con los requisitos de rendimiento de seguridad operacional.	

15.6.3 El monitoreo del cumplimiento de los reglamentos es necesario para asegurar que los controles de riesgo aplicados en forma de reglamentos sean efectivamente implementados y monitoreados por el CIAC. Las causas y factores contribuyentes de cualquier incumplimiento, deberán también ser analizados y tratados.

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

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

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

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

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

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

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

15.7 Análisis de brechas (GAP) e implementación del SMS

15.7.1 Antes de implementar un SMS, el CIAC deberá llevar a cabo un análisis de brechas. Este análisis de brechas tiene dos objetivos:

a) Para el postulante al certificado de aprobación de un CIAC 141 Tipo 2 y Tipo 3, el análisis de brechas constituye una guía para desarrollar los procesos y procedimientos requeridos por la Sección 141.275 y el Apéndice 10 de la RAB 141 para el establecimiento del SMS, determinando aquellos elementos que aún no puede cumplir en desarrollar o implantar hasta que haya recibido el CCIAC e inicie sus operaciones, los cuales deberán ser considerados en un plan de implantación hasta en tres años, con una secuencia lógica de actividades anuales hasta lograr una eficaz implantación de todos los

elementos de los componentes del SMS.

b) Para un CIAC 141 Tipo 2 y Tipo 3 certificado que se encuentra en proceso de implementación del SMS, el análisis de brechas le permitirá realizar una verificación de las actividades e inclusive procedimientos que aún no ha desarrollado adecuadamente, para sincerar o adecuar el plan de implementación con el objetivo de culminar en el plazo que la AAC considere aceptable la total implementación del SMS, conforme a su tamaño y complejidad, que en este caso no podrá ser de tres años, sino el tiempo que determine la AAC.

c) Para ambos casos en el **Apéndice 13** se proporciona una herramienta para la evaluación del SMS, en la cual se puede determinar el nivel que tiene el centro de instrucción con respecto al establecimiento, implementación y mantenimiento del SMS, con los siguientes criterios:

Para el postulante a un certificación de CIAC 141 Tipo 2 y Tipo 3	Se verificará que en el manual del SMS y documentos complementarios, los requisitos estén Presentes (P) y Adecuados (S) y en base a ello, el CIAC podrá realizar un plan de implementación que ejecutará una vez inicie sus actividades a fin de poner el SMS operativo.
Para un centro de instrucción certificado Tipo 2 y Tipo 3.	Se verificará que los requisitos y procedimientos del manual y documentos complementarios se encuentren operativos (O) y, asimismo, podrá realizar un plan de implementación de aquellos que aún no están operativos, para luego poder proceder a las actividades que garanticen su eficacia (E).

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

a) requisitos regulatorios, de clientes y reglamentarios;

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

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

d) la disponibilidad de recursos y presupuestos;

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

f) la cultura de seguridad operacional existente.

15.7.3 El plan de implementación del SMS deberá ser desarrollado en consulta con el ejecutivo responsable y otros altos directivos. El plan de implementación de SMS debe incluir quién es responsable de las acciones junto con los plazos. El plan deberá abordar la coordinación con organizaciones externas o contratistas, donde sea aplicable.

15.7.4 El plan de implementación de SMS puede documentarse en diferentes formas, que van desde una simple hoja de cálculo hasta un software especializado de gestión de proyectos. El plan deberá ser monitoreado regularmente y actualizado según sea necesario. También deberá aclarar cuándo un elemento específico puede considerarse implementado con éxito (Ver **Apéndice 14**).

16. PROCEDIMIENTO DE ACEPTACIÓN PROVISIONAL DEL SMS

El proceso de aceptación provisional del SMS forma parte integral del proceso de certificación del CIAC 141 Tipo 2 y Tipo 3. La aceptación del SMS es un requisito previo al otorgamiento del certificado y las ESIN, dado que los procedimientos del SMS deben ser aplicados desde el primer día de operaciones. A continuación, se describen las acciones que debe llevar a cabo el CIAC, durante el proceso de certificación para obtener la aceptación provisional del manual del SMS.

16.1 Fase I – Pre-solicitud

16.1.1 La AAC facilitará al solicitante de un CCIAC una copia de esta circular de asesoramiento durante la Fase I del proceso de certificación. Es muy importante que esté familiarizado con su contenido antes de la reunión de pre-solicitud de tal manera de tener listas todas sus preguntas e inquietudes con relación a la implementación del SMS que necesita aclarar con la AAC. Al culminar la Fase I el solicitante debe comprender a cabalidad el contenido de esa circular, así como ser capaz de interpretar correctamente cada uno de sus Adjuntos

16.1.2 En la reunión de pre-solicitud y durante las reuniones sucesivas que podrían requerirse antes de pasar a la Fase II, la AAC y el solicitante acordarán el alcance del SMS en función del tipo y complejidad de las operaciones propuestas. Este es el primer paso para la planificación adecuada del SMS y el desarrollo del manual del SMS que presentarán en la Fase II – Solicitud formal. Sólo una vez que el inspector está satisfecho con el grado de comprensión que el solicitante demuestra sobre el alcance de los requisitos del SMS, se deberá proceder a pasar a la siguiente fase.

16.1.3 Para facilitar el trabajo del solicitante y para una mayor transparencia, es recomendable facilitar al solicitante el acceso a este procedimiento de aceptación junto con el paquete de certificación.

16.2 Fase II – Solicitud formal

16.2.1 Durante la Fase II y con anterioridad a la presentación de la carta de solicitud formal, el CIAC deberá desarrollar los procesos y procedimientos para cumplir con cada uno de los elementos que conforman los componentes del SMS señalados en la Sección 141.275 y el Apéndice 10 de la RAB 141, así como el plan implementación correspondiente para los tres (3) años de plazo que tienen establecido en la RAB 141 como máximo.

16.2.2 El análisis de brechas también debe ser presentado por el postulante a la certificación, como evidencia de la verificación de cada elemento y la referencia cruzada con el manual del SMS u otro documento complementario.

16.2.3 El manual del SMS y el plan de implementación deberán ser presentados a la AAC junto con la carta de solicitud formal y el resto de los documentos del CIAC. Una vez que se ha presentado la carta de solicitud formal, la AAC llevará adelante una revisión superficial del manual del SMS para verificar que se han cumplido todos los aspectos formales, y notificará la admisión o rechazo del documento. La AAC tiene un plazo de cinco (5) días para pronunciarse con relación al documento. Esta eventual admisión no implica de ninguna manera la aceptación del SMS del CIAC ni de su manual, sólo indica que aparentemente está completo y que puede iniciarse su revisión en detalle como parte de la Fase III del proceso de certificación.

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

16.3 Fase III – Evaluación de la documentación

16.3.1 Una vez que el documento ha sido admitido como parte de la solitud formal, a la AAC le corresponde revisar el manual del SMS y el plan de implementación en detalle. Durante esta fase, es muy importante que el CIAC mantenga una comunicación fluida con la AAC para poder resolver oportunamente cualquier observación que surja durante la revisión del manual y el resto de los documentos.

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

16.3.3 Una vez que el CIAC haya subsanado todas las observaciones de la AAC con relación al manual el SMS y el plan de implementación, le corresponde a la AAC aceptar dichos documentos como parte del MIP del CIAC.

16.3.4 Durante esta etapa la AAC revisará el contenido del curso de SMS del CIAC como parte de su programa de instrucción y le otorgará, si corresponde, la aprobación inicial para que el CIAC proceda a impartir esta capacitación.

16.3.5 En función de la disponibilidad de recursos, los inspectores de la AAC deberán maximizar sus esfuerzos para verificar las primeras sesiones de instrucción del SMS al personal del solicitante, para comprobar que se están impartiendo en armonía con el programa aprobado.

16.3.6 En resumen, en la Fase III corresponde al inspector de la AAC revisar y aceptar en forma provisional el manual del SMS y el plan de implementación, y aprobar inicialmente el programa de instrucción del SMS como parte del programa de instrucción del personal del CIAC.

16.4 Fase IV – Inspección y demostración

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

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

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

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

16.5 Fase V – Aceptación provisional

16.5.1 La aceptación provisional del SMS por parte de la AAC es un requisito previo a la emisión del certificado y las especificaciones de instrucción (ESIN) del CIAC.

16.5.2 A partir del primer día de operaciones, el CIAC implementará su SMS, poniendo en

funcionamiento todos los procesos y procedimientos establecidos y aceptados por la AAC durante el proceso de certificación.

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

———————

Apéndice 1

Ejemplo de declaración de política de seguridad operacional del CIAC

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

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

Nuestro compromiso es para:

- *Respaldar* la gestión de la seguridad operacional mediante la disposición de los recursos correspondientes que generarán una cultura institucional que fomenta prácticas seguras, alienta una notificación y comunicación eficaces de la seguridad operacional y gestiona activamente la seguridad operacional con la misma atención a los resultados como la atención a los resultados de otros sistemas de gestión de la organización;
- *garantizar que la gestión de la seguridad operacional sea una de las responsabilidades principales de todos los funcionarios y empleados;*
- *definir claramente, para todo el personal, funcionarios y empleados por igual, sus responsabilidades para la entrega del rendimiento en materia de seguridad operacional de la organización y el rendimiento de nuestro sistema de gestión de la seguridad operacional;*
- *establecer y operar los procesos de identificación de peligros y gestión de riesgos, incluido un sistema de notificación de peligros, para eliminar o mitigar los riesgos de seguridad operacional de las consecuencias de peligros que se generen de nuestras operaciones o actividades, para alcanzar una mejora continua en nuestro rendimiento en materia de seguridad operacional;*
- *garantizar que no se tome ninguna medida en contra de ningún empleado que divulgue una preocupación de seguridad operacional mediante el sistema de notificación de peligros, a menos que dicha divulgación indique, más allá de cualquier duda razonable, una negligencia grave o una despreocupación deliberada o consciente de los reglamentos y procedimientos;*
- *cumplir con y, cuando sea posible, superar los requisitos y las normas reglamentarias y legislativas;*
- *garantizar que estén disponibles suficientes recursos humanos cualificados y capacitados para implementar las estrategias y los procesos de seguridad operacional;*
- *garantizar que todo el personal disponga de información y capacitación adecuadas y correspondientes de la seguridad operacional de la aviación, sea competente en asuntos de seguridad operacional y tengan asignadas solo tareas proporcionales a sus habilidades;*
- *establecer y medir nuestro rendimiento en materia de seguridad operacional en contraste con indicadores de rendimiento en materia de seguridad operacional realistas y objetivos de rendimiento en materia de seguridad operacional;*
- *mejorar continuamente nuestro rendimiento en materia de seguridad operacional mediante un control y una medición continuos, revisión y ajuste regulares de los objetivos y las metas de seguridad operacional y el logro diligente de estos; y*
- *garantizar que se implementen los sistemas y servicios suministrados de forma externa para respaldar nuestras operaciones y que cumplan nuestras normas de rendimiento en materia de seguridad operacional."*

_____

(Firma y nombre)

Gerente responsable

Ejemplo de declaración de política de seguridad operacional de un CIAC pequeño

"La seguridad operacional es importante para nosotros, esto nos ayudará a continuar con nuestro propósito de incursionar en esta actividad de la aviación como CIAC.

Nuestro objetivo de seguridad operacional es simplemente evitar que ocurran accidentes de aviación durante nuestras operaciones aéreas.

Nos comprometemos a cumplir con las normas reglamentarias y superarlas cuando sea necesario.

Garantizar que la gestión de seguridad operacional sea una de las responsabilidades principales de todos los funcionarios y empleados.

Garantizar que estén disponibles recursos para implementar las estrategias y los procesos de la seguridad operacional.

Establecer y poner en marcha los procesos de identificación de peligros, así como promover una cultura hacia todo el personal para la aplicación del sistema de notificación de peligros, y que no se tome ninguna represalia o medida en contra de la o las personas que informen de alguna situación que afecte a la seguridad operacional.

Esto ayudará a nuestra organización a desarrollar y mejorar nuestro rendimiento en materia de seguridad operacional, la cual es nuestra gran responsabilidad."

_____
(Firma y nombre)
Gerente responsable

Nota.- *Este es un ejemplo de declaración de política de seguridad operacional para una CIAC pequeño, la misma que no necesariamente deberá reflejar este contenido.*

Apéndice 2

Planificación de la respuesta ante emergencias (ERP)

La respuesta exitosa ante una emergencia, empieza con una efectiva planificación. Un ERP establece las bases para un manejo sistemático y ordenado de los asuntos de la organización luego de un evento significativo no planificado, en el peor de los casos, un accidente mayor.

El propósito de ERP consiste en asegurar:

a) Delegación de autoridad en caso de emergencia.
b) Asignación de responsabilidades en caso de emergencia.
c) Documentación de los procesos y procedimientos de emergencia.
d) Coordinación de los esfuerzos de emergencia de forma interna y con partes externas.
e) Continuación segura de las operaciones esenciales, mientras se maneja la crisis.
f) Identificación proactiva de todos los posibles eventos/ escenarios de emergencia y sus respectivas medidas de mitigación.

Para ser eficaz, un ERP debe:

a) Ser apropiado para el tamaño, naturaleza y complejidad de la organización.
b) Estar fácilmente accesible a todo el personal relevante y en otras organizaciones si fuera necesario.
c) Incluir listas de verificación y procedimientos relevantes a situaciones de emergencia específicas.
d) Contar con listas de referencia rápida con la información de contacto del personal clave.
e) Ser validado periódicamente a través de ejercicios/simulacros.
f) Ser periódicamente revisado y actualizado ante cambios en la organización que afectan al ERP.

Contenido del ERP

Un ERP debería estar organizado y documentado en un formato de manual. Éste debería definir los roles, responsabilidades y acciones del personal y otras organizaciones involucrados en la respuesta a una emergencia. El ERP debería tomar en cuenta las siguientes consideraciones:

a) **Políticas gobernantes.** El ERP debería brindar orientación para la respuesta ante una emergencia, como las leyes aplicables, reglamentos para las investigaciones, acuerdos con las autoridades locales políticas de la compañía y prioridades.

b) **Organización**. El ERP debería definir:

1. Designar quien estará a cargo de la respuesta y quienes estarán asignados a los equipos correspondientes.
2. Definir los roles y las responsabilidades para el personal asignado a los equipos de respuesta.
3. Establecer claramente las líneas de autoridad y comunicación.
4. Definir el establecimiento del centro de control de la emergencia (EMC).
5. Establecer los procedimientos para recibir y gestionar una gran cantidad de solicitudes de información, especialmente durante los primeros días después de la emergencia. Designar el vocero oficial para las relaciones con la prensa.
6. Definir los recursos que estarán disponibles, incluyendo los responsables con acceso a los recursos económicos necesarios para hacer frente a las primeras actividades relacionadas con la respuesta.
7. Designar al representante de la empresa para participar y colaborar con las investigaciones oficiales de la AAC y otras autoridades cuando corresponda.
8. Definir un plan de llamadas para el personal clave.

Puede utilizarse un organigrama para mostrar las distintas relaciones funcionales y canales de comunicación.

c) **Notificaciones.** El ERP debe especificar quienes deben ser notificados en caso de una emergencia, quien estará a cargo de las notificaciones externas y los medios que se utilizarán para estas comunicaciones. Las siguientes notificaciones deberían ser tomadas en cuenta:

1. La dirección.
2. Autoridades del Estado (AAC, Junta de Investigaciones, SAR, etc).
3. Servicios locales de respuesta ante emergencias (autoridades aeródromo, policía, instituciones médicas, bomberos, etc.)
4. Familiares de las víctimas.
5. Personal de la compañía.
6. Los medios de comunicación
7. Área legal, contabilidad, aseguradores, etc.

d) **Respuesta inicial.** Dependiendo de las circunstancias, un equipo de respuesta inicial puede ser enviado al lugar de la emergencia para apoyar a los servicios locales y para velar los intereses de la organización. Los factores que deben considerarse por este equipo incluyen:

1. ¿Quién liderar el equipo de respuesta inicial?
2. ¿Quiénes deben conformar el equipo de respuesta inicial?
3. ¿Quién debe hablar a nombre del CIAC en el lugar del accidente?
4. ¿Qué cosas especiales podrían necesitarse (equipo especial, documentos, credenciales, transporte, alojamiento, etc.)?

e) **Ayuda adicional.** Aquellos empleados con la instrucción apropiada y con experiencia pueden brindar ayuda muy útil durante la preparación, evaluación, ensayos y actualización del ERP. Sus conocimientos pueden resultar útiles en la planificación y ejecución de tareas tales como:

1. Actuar como pasajeros o clientes durante los ejercicios/simulacros.
2. Abordar a los supervivientes o partes externas.
3. Hablar con el familiar más cercano, las autoridades, etc.

f) **Centro de control de la emergencia.** El EMC puede instalarse en el aeródromo o centro de operaciones del CIAC, una vez que los criterios de activación se han cumplido. Adicionalmente, un puesto de comando (CP) puede establecerse cerca del lugar del accidente. El ERP debe contemplar cómo se cumplirán los siguientes requisitos:

1. Personal (tal vez por 24 horas al día, los 7 días de la semana, durante el período de respuesta inicial);
2. equipo de comunicaciones (Teléfono, fax, internet, etc.);
3. requisitos de documentación, mantenimiento de los registros de las actividades de emergencia;
4. incautar los registros empresariales relacionados;
5. mobiliario y material de oficina requerido tanto en el EMC como en el CP;
6. documentos de referencia (como listas de verificación y procedimientos de respuesta ante emergencias, manuales de la empresa, planes de emergencia del aeródromo y listas telefónicas).

g) **Registros.** Adicionalmente a la necesidad de la compañía de mantener registros de los eventos y actividades relacionados con la emergencia, La organización también deberá preparar información y registros que serán requeridos por la AAC y por el equipo de la investigación oficial del Estado. El ERP debería incluir la preparación de la siguiente documentación para ser facilitada a las autoridades:

1. Todos los registros pertinentes acerca del producto o servicio de interés;

2. listas de puntos de contacto y cualquier personal asociado con el suceso;
3. notas de cualquier entrevista (o declaración) con alguien asociado con el evento;
4. cualquier evidencia fotográfica o de otro tipo.

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

1. Asignar un representante de alto nivel al lugar del accidente si:
   a. El accidente ocurre en la base del CIAC.
   b. El accidente ocurre lejos de la base del CIAC.
2. gestión de las víctimas supervivientes;
3. las necesidades de los familiares de las víctimas;
4. preservación de los restos de la aeronave y de cualquier otro tipo de evidencia.
5. manejo de los restos de las víctimas y de sus efectos personales.
6. preservación de la evidencia;
7. disposición de ayuda (según sea necesario) a las autoridades de la investigación;
8. retiro y eliminación de los restos de la aeronave; etc.

i) **Medios de prensa.** La manera en que la organización responda frente a los medios puede afectar qué tan bien se recupera del evento. Es muy importante una dirección clara en este aspecto. Por ejemplo:

1. ¿qué información está protegida por un estatuto, como declaraciones de testigos, etc.?
2. ¿quién puede hablar en nombre del CIAC en la sede de operaciones y en el sitio del accidente?
3. declaraciones preparadas para obtener una respuesta inmediata a las consultas de los medios de comunicación
4. ¿Qué información pueda ser divulgada y cuál debe ser evitada?
5. la sincronización y el contenido de la declaración inicial de la compañía.
6. Las disposiciones relativas a las actualizaciones periódicas para los medios.

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

k) **Ayuda para la familia.** El ERP también debe incluir orientación sobre la relación y la asistencia a las familias de las víctimas. Esta guía debería incluir al menos los siguientes elementos:

1. Requisitos del Estado para la disposición de servicios de ayuda.
2. Arreglos de viaje y alojamiento, para visitar el lugar del accidente.
3. Designación de coordinadores y puntos de contacto definidos para proveer información sobre las víctimas.
4. Brindar información actualizada.

La Circular 285 de la OACI - Orientación para la asistencia de las víctimas de accidentes aéreos y sus familiares, provee información adicional sobre este tema.

l) **Revisión post-accidente.** El ERP debe contener los procedimientos para asegurarse que, después de la emergencia, el personal clave brinde un aleccionamiento post-emergencia y se registren todas las lecciones aprendidas que pudieran resultar en enmiendas al ERP y otros documentos asociados.

Listas de verificación

Cualquier persona involucrada en la respuesta inicial a un accidente o emergencia enfrentará algún grado de desorientación. Es por ello que todo el proceso de respuesta debe estar apoyado y basado en el uso de listas de verificación. Estas listas pueden formar parte integral del manual de operaciones de la compañía o del ERP. Para ser efectivas, las listas de verificación, de forma regular deben:

1. Ser revisadas y actualizadas (tipo de cambio, lista de números telefónicos, etc.)
2. Ser validadas mediante ejercicios o simulacros.

Instrucción y simulacros

El ERP es una declaración de intenciones escritas en papel. Es de esperar que la mayor parte del contenido de un ERP nunca tenga que ser utilizado en condiciones reales, sin embargo, se requiere capacitación para asegurarse que estas intenciones puedan ser convertidas en capacidades reales. Debido a que la retención de la instrucción no es absoluta, es aconsejable realizar ejercicios y simulacros de manera periódica. Algunas partes del ERP como el plan de llamadas y el plan de comunicaciones, pueden ser ensayadas desde el “escritorio”. Sin embargo, otros aspectos como los relacionados a las actividades en el lugar del accidente, deben ser simulados periódicamente en escenarios lo más reales posibles. Estos ejercicios tienen la ventaja de identificar las deficiencias del ERP y corregirlos antes de que sean utilizados en una emergencia real. Para determinados proveedores de servicios como los aeropuertos, la realización de simulacros a escala real de manera regular puede ser obligatoria y exigida por los reglamentos del Estado.

———————

Apéndice 3

Estructura del manual de SMS

1. Generalidades

Este apéndice sirve como una guía para el CIAC 141 al momento de desarrollar el manual del sistema de gestión de la seguridad operacional (SMSM). Dependiendo de la decisión del CIAC y el alcance de sus operaciones, el manual del SMS puede ser desarrollado con un solo documento independiente, o puede ser integrado en el manual de instrucción y procedimientos (MIP) existente, como un volumen, capítulo o sección nueva.

Si bien el formato sugerido por este apéndice para la elaboración del SMSM no es de adopción obligatoria y la estructura final dependerá de cada CIAC, se alienta a todos los centros y Estados del SRVSOP a regirse lo más estrictamente posible a estas disposiciones para alcanzar los mayores niveles de armonización.

Un SMSM sirve como un medio para comunicar el marco del SMS tanto dentro de la organización como hacia las organizaciones y organismos externos pertinentes. Normalmente el SMSM está sujeto a la **aceptación** de la AAC como una evidencia aceptable de cumplimiento de los requisitos del SMS propuesto por la organización.

Es importante distinguir entre el manual del SMS (SMSM) y la documentación del SMS. Los documentos o documentación, también mencionada como la biblioteca del SMS se refiere a la información sobre seguridad operacional, así como los documentos generados durante la implementación y operación del SMS son las evidencias de la creación y funcionamiento del SMS de una organización.

2. Estructura

Para un mejor ordenamiento se recomienda la siguiente estructura para el SMSM, en ella se ha incorporado las referencias de los numerales de esta circular de asesoramiento que deberán ser revisados para su desarrollo:

Carátula
Registro de actualizaciones
Índice general
Listado de páginas efectivas
Registro de modificaciones

1. Generalidades

- 1.1 Objetivo del manual
- 1.2 Estructura del manual
- 1.3 Control, actualización y distribución del manual (procedimiento)
- 1.4 Documentos asociados al manual
- 1.5 Definiciones
- 1.6 Abreviaturas

2. Sistema de gestión de seguridad operacional (SMS)

- 2.1 Sistema de gestión de seguridad operacional del CIAC (*nombre*)
- 2.2 Alcance del SMS
- 2.3 Componentes del SMS
- 2.4 Tratamiento de la documentación y control de registros del SMS.

3. Políticas y objetivos de seguridad operacional

3.1 Política de seguridad operacional (Ver 10.1.1 al 10.1.7)

3.2 Objetivos de seguridad operacional (Ver 10.1.8 al 10.1.11)

3.3 Estructura organizacional del SMS en el CIAC (nombre)

3.4 Funciones, responsabilidades y atribuciones del gerente responsable respecto al SMS (Ver 10.2.1 al 10.2.14)

3.5 Funciones, responsabilidades y atribuciones del gerente del SMS (Ver 10.3)

3.6 Funciones y conformación de la junta de revisión de seguridad operacional (SRB) (Ver 10.3.7).

3.7 Funciones y conformación del grupo de acción de seguridad operacional (SAG) (Ver 10.3.8, si corresponde).

3.8 Coordinación del plan de respuesta ante emergencia (Ver 10.4 y Apéndice 2).

3.9 Documentación del SMS (Ver 10.5).

4. Gestión del riesgo de seguridad operacional

4.1 Medios y procedimientos para la identificación de peligros (Ver 11.1.1 a 11.1.3).

4.2 Sistema de notificación e investigación de seguridad operacional. (Ver 11.1.4 a 11.29).

4.3 Análisis y evaluación de riesgos

4.3.1 Matriz de riesgos y procedimientos (Ver 11.2.1 al 11.2.26)

4.3.2 Estrategias de mitigación de riesgos y metodología para su selección (Ver 11.2.27 al 11.2.31)

4.3.3 Tratamiento de riesgo residual (Ver 11.2.29).

5. Aseguramiento de la seguridad operacional

5.1 Observación y medición del rendimiento de seguridad operacional

5.1.1 Indicadores y metas de seguridad operacional del CIAC (Ver 12.1.12 al 12.1.4 – Apéndices 6 y 7).

5.1.2 Auditorías internas y externas de seguridad operacional (Ver 12.1.3 al 12.1.11)

5.2 Gestión del cambio (Ver 12.2)

5.3 Mejora continua del SMS (Ver 12.3)

6. Promoción de la seguridad operacional

6.1 Instrucción y educación

5.1.3 Programa de instrucción inicial y periódico del SMS (Ver 13.1.1 al 13.1.8)

5.1.4 Análisis de necesidades de capacitación (Ver 13.1.9 al 13.1.13).

6.2 Comunicación de la seguridad operacional (Ver 13.2)

Apéndices (Pueden ser utilizados para describir procedimientos e incluir formularios)

_____

Apéndice 4

Sistemas de notificación voluntaria y confidencial

Un sistema de notificación voluntaria y confidencial de un CIAC 141 debe definir como mínimo:

a) El objetivo del sistema de notificación;
b) el alcance de los sectores/áreas involucrados en el sistema;
c) quiénes pueden hacer un informe voluntario;
d) cuándo debe hacerse dicho informe;
e) cómo se procesan los informes;
f) cómo contactar al gerente del sistema;

Objetivo del sistema

Un sistema de informes voluntario y confidencial debe estar bien definido y no servir a otros propósitos más que a la identificación de peligros. Durante el establecimiento del sistema, el CIAC debe decidir si integra este sistema al programa OSHE (en caso que exista) y si esto es aceptable tanto para la AAC como para la autoridad encargada del OSHE. En caso que ambos sistemas de informes sean independientes, los formularios, alcance y otros elementos de cada sistema deben estar claramente definidos para evitar confundir a quien reporta.

A continuación se incluye un ejemplo de definición del objetivo de un sistema de informes voluntario y confidencial:

El objetivo principal del sistema de informes voluntario y confidencial de (nombre de la organización), es la mejora de la seguridad operacional de las actividades aéreas de nuestro centro de instrucción, a través de la recolección de informes sobre deficiencias reales o potenciales que regularmente no son reportados por otros medios. Estos informes pueden incluir ocurrencias, peligros, amenazas, o cualquier otra situación relevante para la seguridad de nuestras operaciones. Este sistema no elimina la necesidad de reportar formalmente los accidentes o incidentes de acuerdo con los procedimientos nuestra compañía, así como los informes obligatorios contenidos en los reglamentos o aquellos determinados por la AAC.

El (nombre del sistema) es un sistema de informes de peligros y ocurrencias, voluntario, confidencial, no-punitivo, administrado por (nombre de la oficina o departamento). Provee un canal directo para el reporte voluntario de ocurrencias y peligros que ponen en riesgo la seguridad de nuestras operaciones, y al mismo tiempo protege la identidad de la persona que realiza el reporte.

Alcance del sistema

Debe describirse de manera clara las áreas cubiertas por el sistema de informes voluntario y confidencial. Un ejemplo común incluiría:

- instrucción en vuelo;
- vuelo solo del alumno piloto;
- instrucción en vuelo IFR;
- mantenimiento de la aeronave;
- fallas de equipos;
- registros técnicos;
- maniobras inseguras;
- Etc.

¿Quiénes deben reportar?

Si bien muchos de estos sistemas se encuentran abiertos a todo el personal de la empresa, desde el punto de vista de la seguridad operacional este tipo de sistemas busca la participación activa de aquellos miembros involucrados directamente con las actividades clave de la organización. A continuación, se incluye un ejemplo que identifica a quienes está dirigido este tipo de sistemas:

Si usted pertenece a cualquiera de los siguientes departamentos/grupos, puede contribuir al mejoramiento de la seguridad de nuestras operaciones a través del (nombre del sistema) reportando cualquier ocurrencia, peligro o amenaza que afecte o pueda afectar la seguridad de nuestras operaciones.

- *Instructores de vuelo*
- *examinadores de vuelo;*
- *alumnos;*
- *personal del aeródromo*
- *personal ATS;*
- *personal de mantenimiento;*
- *y otros vinculados a la operación.*

¿Cuándo debe hacerse un informe?

Existen diversas formas para advertir la presencia de situaciones de peligro, sin embargo los canales de notificación tradicionales tienen algunas limitaciones y no funcionan de la manera en que fueron concebidos.

Es importante que el CIAC maneje con máxima responsabilidad y cuidado sus sistemas de informes voluntario y confidencial para asegurarse que goza de la confianza de los usuarios. Un ejemplo sobre cuando usar este tipo de sistemas para reportar una condición de peligro se encuentra a continuación:

Usted debe hacer un informe cuando:

- *Desea que otros aprendan y se beneficien con el conocimiento de un incidente, ocurrencia o situación peligrosa pero al mismo tiempo desea proteger su identidad.*
- *No existen otros canales o procedimientos adecuados para la notificación.*
- *Ha probado con otros procedimientos o canales de notificación sin conseguir que el problema sea adecuadamente atendido.*

¿Cómo se procesa un reporte?

Para garantizar la confianza de los usuarios en el sistema, es fundamental que su funcionamiento sea transparente. Esto evitará susceptibilidades sobre la forma en la que se manejan los informes. A continuación, se cita un ejemplo de cómo divulgar el tratamiento de los informes dentro la organización:

El (nombre del sistema) presta especial atención a la necesidad de proteger la identidad de quienes presentan un reporte al momento de procesar la información. Cada reporte será leído y validado por el administrador del sistema. El administrador puede tratar de ponerse en contacto con el autor del reporte para asegurarse que comprende la naturaleza y las circunstancias del peligro reportado o para obtener información adicional o clarificación.

Una vez que el administrador está satisfecho y la información obtenida es completa y coherente, se eliminará toda la información sobre la identidad del quien realizó el reporte y la información será ingresada en la base de datos del (nombre del sistema). En caso que se necesite la participación de terceros, ésta se realizará después de que la información sobre la identidad ha sido eliminada.

Una vez que se ha reunido toda la información sobre el evento, el formulario original será devuelto al autor del reporte como constancia de su procesamiento. Este proceso no debería demorar más de 10 días. En caso que el administrador del (nombre del sistema) esté ausente por un largo periodo, un administrador alterno debería asegurarse que se cumplen los procedimientos y plazos establecidos.

Difusión de la información sobre seguridad operacional con la comunidad aérea

Algunos informes (sin ninguna información sobre la identidad del autor) así como partes de un reporte o resúmenes pueden ser distribuidos dentro y fuera de la compañía con fines exclusivamente de prevención. Esto permite al personal de la empresa así como a los terceros interesados, revisar y adecuar sus operaciones para mejorar los niveles de seguridad operacional.

Si el contenido de un reporte sugiere o indica la existencia de un peligro o condición que representa una amenaza inminente a la seguridad operacional, éste será manejado y procesado con prioridad (previa eliminación de la información sobre la identidad del autor), y derivado a los niveles o autoridades relevantes para la toma de acciones correctivas inmediatas.

¿Cómo contactar al responsable del sistema?

Parte de la transparencia del sistema, depende de la disponibilidad de sus administradores para resolver cualquier inquietud o ampliar información con respecto al sistema de informes. Los administradores deben estar disponibles al universo de potenciales autores de informes para fortalecer la transparencia y la confianza en el sistema. A continuación, se cita un ejemplo de invitación a contactarse con los administradores:

Usted es bienvenido a contactar al (nombre del sistema) para solucionar cualquier inquietud sobre el (nombre del sistema) o para solicitar una reunión informativa con el administrador antes de realizar un reporte. El gerente y el gerente suplente pueden ser contactados de lunes a viernes en horarios de oficina en la siguiente información de contacto:

Ejemplo de formulario de reportes voluntarios

Un modelo de formulario para notificaciones voluntarias de seguridad operacional que puede utilizar un CIAC 141 Tipo 2 y 3, se indica a continuación.

Modelo de formulario de reporte voluntario de seguridad operacional

DGAC DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL	**REPORTE VOLUNTARIO DE SEGURIDAD OPERACIONAL**	**CÓDIGO**	**VIGENCIA**
		F-	**XX/XX/XXXX**
			REVISIÓN
			0

El único objetivo de la información reportada en este formulario es mejorar la seguridad operacional. No está obligado a dar su identidad ni posición en la organización. Sin embargo, si usted desea hacerlo, estos datos no se darán a conocer sin su aprobación.

1. Fecha: (opcional) **2. Lugar:** (opcional)	**3. Tipo de operación:** ☐ Instrucción en vuelo ☐ Vuelo solo ☐ Vuelo de travesía	**4. Condiciones de vuelo** ☐ Vuelo VFR ☐ Vuelo IFR ☐ Día ☐ Noche	**5. Aeronave** (Matrícula y modelo)

6. Descripción del evento

Explicar cómo ocurrió el evento, por qué ocurrió y por qué no resultó en un accidente.

7. ¿Cuáles son sus sugerencias para prevenir que este evento vuelva a ocurrir o para prevenir que este evento pueda resultar en un accidente?

PARA SER LLENADO POR EL GERENTE DEL SMS DEL CIAC:

8. Análisis adicional y curso de acción dispuesto.

Validado por: (nombre, cargo y firma)	Fecha:

9. Procesado por el Grupo de Acción (o gerente del SMS) Fecha:

Responsable:	Abierto en: (Día/mes/año)	Cerrado en: (Día/mes/año)

Nota.- *Dependiendo del tamaño y complejidad de la organización este formulario puede variar incorporando otros ítems.*

Apéndice 5

Ejemplo de reporte de acción correctiva y preventiva

<table>
<tr><td colspan="2">LOGOTIPO</td><td colspan="2">REPORTE DE ACCIÓN CORRECTIVA Y PREVENTIVA</td><td>CÓDIGO
F-</td><td>VIGENCIA
XX/XX/XXXX
REVISIÓN
0</td></tr>
<tr><td rowspan="4">Paso 1: Identificación</td><td colspan="2">☐ ACCIÓN CORRECTIVA</td><td colspan="3">☐ ACCIÓN PREVENTIVA</td></tr>
<tr><td>Organización/Área/ Departamento</td><td colspan="4"></td></tr>
<tr><td>Descripción del evento o no-conformidad</td><td colspan="4"></td></tr>
<tr><td>Auditor / Revisor</td><td>Auditor</td><td>Firma</td><td colspan="2">Fecha: Día/mes/año</td></tr>
<tr><td rowspan="3">Paso 2: Análisis de causas y acción</td><td>Causa(s) raíz</td><td colspan="4"></td></tr>
<tr><td>Propuesta de acción correctiva / preventiva a ser tomada incluyendo la persona responsable y la fecha tope</td><td>Qué</td><td>Quién</td><td colspan="2">Para cuándo</td></tr>
<tr><td>Aceptado por</td><td>Nombre</td><td>Firma</td><td colspan="2">Fecha: Día/mes/año</td></tr>
<tr><td rowspan="5">Paso 3: Verificación y evaluación</td><td>Fecha actual de la(s) acción(es) tomada(s)</td><td colspan="4"></td></tr>
<tr><td>Comentarios</td><td colspan="4"></td></tr>
<tr><td>¿Requiere acción adicional?</td><td colspan="2">☐ Sí</td><td colspan="2">☐ No</td></tr>
<tr><td>Aceptación de cierre</td><td>Auditor / revisor</td><td>Firma</td><td colspan="2">Fecha: Día/mes/año</td></tr>
</table>

Nota.- *Dependiendo del tamaño y complejidad de la organización este formulario puede variar incorporando otros ítems.*

Apéndice 6

Indicadores y metas de rendimiento de seguridad operacional

1. Tipos de indicadores de seguridad operacional

1.1 Las dos categorías más comunes utilizadas para clasificar los SPI son los de resultados (lagging indicator) y los avanzados (leading inicators). Los SPI de resultados miden eventos que ya han ocurrido. También se los conoce como "SPI basados en resultados" y normalmente (pero no siempre) son los resultados negativos que la organización intenta evitar.

1.2 Los SPI avanzados miden procesos y entradas que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como "SPI de actividad o proceso", ya que monitorean y miden las condiciones que tienen el potencial de convertirse o contribuir a un resultado específico.

1.3 Los SPI de resultados ayudan a la organización a comprender lo que sucedió en el pasado y son útiles para las tendencias a largo plazo. Se pueden usar como indicadores de alto nivel o como una indicación de tipos o lugares específicos de ocurrencia, como "tipos de accidentes por tipo de aeronave" o "tipos de incidentes específicos por región". Debido a que los SPI de resultados miden los resultados de seguridad operacional, pueden medir la efectividad de las medidas de mitigación de seguridad operacional.

1.4 Los SPI de resultados son efectivos para validar el rendimiento general de seguridad operacional del sistema. Por ejemplo, monitorear el "número de colisiones de rampa por cantidad de movimientos entre vehículos luego de un rediseño de marcas de rampa" proporciona una medida de la efectividad de las nuevas marcas (suponiendo que nada más haya cambiado). La reducción en colisiones valida una mejora en el rendimiento de seguridad operacional general del sistema de rampa; la cual puede ser atribuible al cambio en cuestión

1.5 Las tendencias en los SPI de resultados pueden analizarse para determinar las condiciones existentes en el sistema que deberán abordarse. Utilizando el ejemplo anterior, una tendencia creciente en colisiones de rampa por número de movimientos pudo haber sido lo que llevó a la identificación de marcas de rampa por debajo del estándar como una mitigación.

1.6 Los SPIs de resultados se dividen en dos grupos:

a) **Baja probabilidad / Alta gravedad**: resultados tales como accidentes o incidentes graves. La baja frecuencia de resultados de alta gravedad significa que la agregación de datos (a nivel de segmento industrial o nivel regional) puede resultar en análisis más significativos. Un ejemplo de este tipo de SPI de resultados sería "daños a la aeronave y / o al motor debido al impacto con aves".

b) **Alta probabilidad / Baja gravedad**: resultados que no necesariamente se manifiestan en un accidente o incidente grave, a veces también se los denomina indicadores precursores. Los SPIs para resultados de alta probabilidad / baja gravedad se usa principalmente para monitorear problemas de seguridad operacional específicos y medir la efectividad de las mitigaciones de riesgos de seguridad operacional existentes. Un ejemplo de este tipo de SPI precursor sería "detecciones de aves en el radar", que indica el nivel de actividad de las aves en lugar de la cantidad de impactos con ave actual.

1.7 Las medidas de seguridad operacional de la aviación históricamente han estado sesgadas hacia los SPI que reflejan resultados de "baja probabilidad / alta gravedad". Esto es comprensible ya que los accidentes e incidentes graves son eventos de alto perfil y son fáciles de contar. Sin embargo, desde una perspectiva de la gestión del rendimiento de seguridad operacional, existen inconvenientes en una dependencia excesiva de accidentes e incidentes graves como un indicador confiable del rendimiento de seguridad operacional. Por ejemplo, los accidentes e incidentes serios son poco frecuentes (puede haber un solo accidente en un año, o ninguno) lo que dificulta la

realización de análisis estadísticos para identificar tendencias. Esto no necesariamente indica que el sistema es seguro. Una consecuencia de confiar en este tipo de datos es un falso sentido de confianza potencial de que el desempeño de seguridad operacional de una organización o sistema es efectivo, cuando de hecho puede estar peligrosamente cerca de un accidente.

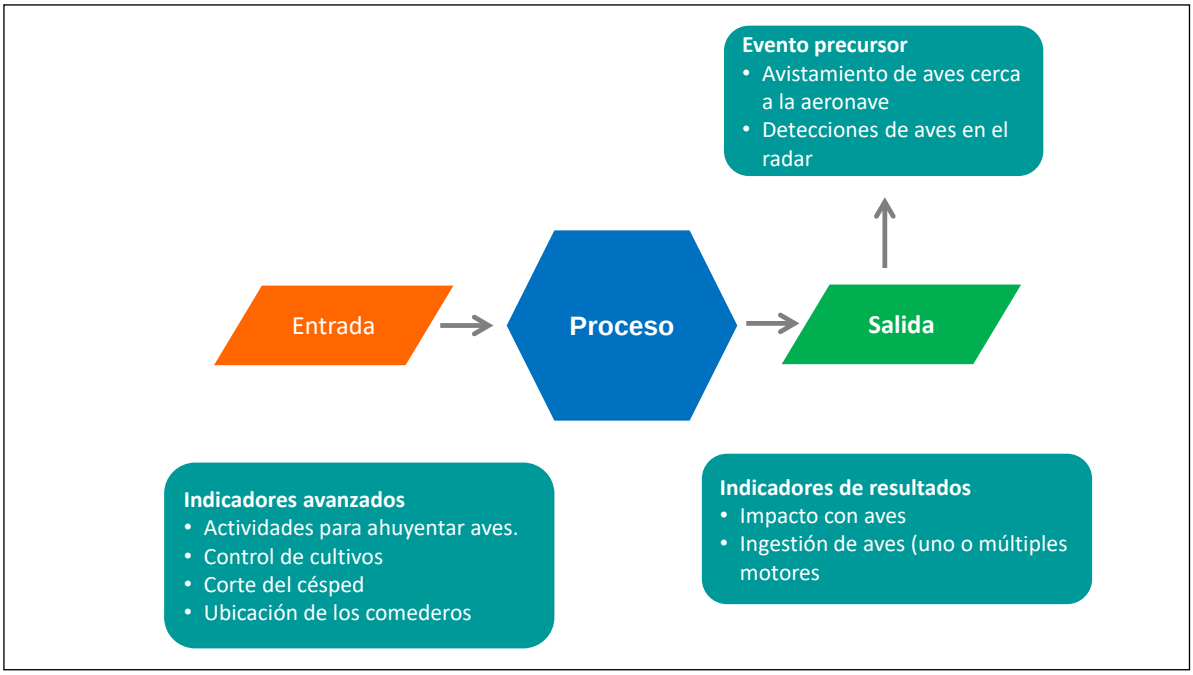
1.8 Los indicadores avanzados son medidas que se centran en los procesos y entradas que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como "SPIs de actividad o proceso", ya que monitorean y miden las condiciones que tienen el potencial de convertirse o contribuir a un resultado específico.

1.9 Los ejemplos de SPI avanzados que impulsan el desarrollo de capacidades organizativas para la gestión proactiva del rendimiento de seguridad operacional incluyen cosas tales como "porcentaje del personal que ha completado con éxito el entrenamiento de seguridad operacional a tiempo" o "frecuencia de actividades de amedrentamiento de pájaros".

1.10 Los SPI avanzados también pueden informar a la organización sobre cómo su operación se enfrenta al cambio, incluidos los cambios en su entorno operativo. La atención se centrará en anticipar debilidades y vulnerabilidades como resultado del cambio o la supervisión del rendimiento después de un cambio. Un ejemplo de SPI para monitorear un cambio en las operaciones sería "porcentaje de áreas que han implementado el procedimiento X".

1.11 Para una indicación más precisa y útil del rendimiento de seguridad operacional, los SPI de resultados, que miden tanto el evento de "alta gravedad / baja probabilidad" y el evento de "alta probabilidad / baja gravedad " se deberán combinar con los SPI avanzados. La **Figura 6.1** ilustra el concepto de indicadores avanzados y de resultados que proporciona una imagen más completa y realista del rendimiento de seguridad operacional de la organización.

Figura 6-1: Etapas del concepto de indicador avanzado versus indicador de resultados



Seleccionando y definiendo SPIs

1.12 Los SPI son los parámetros que proporcionan a la organización una visión de su rendimiento de seguridad operacional:

- dónde ha estado;
- donde está ahora; y
- hacia dónde se dirige, en relación con la seguridad operacional.

1.13 Esta imagen actúa como una base sólida y defendible sobre la cual se toman decisiones de seguridad operacional basadas en datos de la organización. Estas decisiones, a su vez, afectan positivamente el rendimiento de seguridad operacional de la organización. Por lo tanto, la identificación de los SPI debe ser realista, relevante y estar vinculada a los objetivos de seguridad operacional, independientemente de su simplicidad o complejidad.

1.14 Es probable que la selección inicial de SPI se limite al monitoreo y medición de parámetros que representan eventos o procesos que son fáciles y / o convenientes de capturar (datos de seguridad operacional que pueden estar fácilmente disponibles). Idealmente, los SPI deberían enfocarse en parámetros que son indicadores importantes del rendimiento de seguridad operacional, en lugar de en aquellos que son fáciles de alcanzar.

1.15 Los SPIs deberán ser:

a) relacionados con el objetivo de seguridad operacional que pretenden indicar;

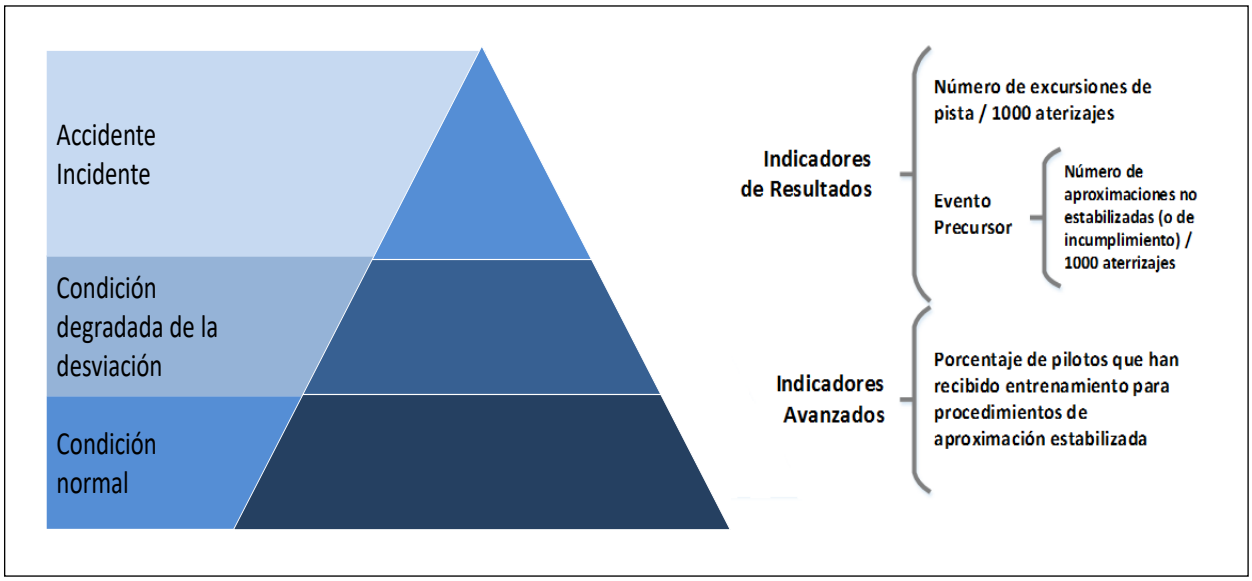
b) seleccionado o desarrollado en base a los datos disponibles y la medición confiable;

c) apropiadamente específico y cuantificable; y

d) realista, teniendo en cuenta las posibilidades y limitaciones de la organización.

1.16 Generalmente, se requiere una combinación de SPIs para proporcionar una indicación clara del rendimiento de seguridad operacional. Debería existir un vínculo claro entre los SPIs de resultados y avanzados. Lo ideal es definir los SPI de resultados antes de determinar los SPI avanzados. La definición de un SPI precursor vinculado a un evento o condición más grave (el SPI de resultado) asegura que existe una clara correlación entre los dos. Todos los SPI, de resultados y avanzados, son igualmente válidos y valiosos. Un ejemplo de estos enlaces se ilustra en la **Figura 6-2**.

Figura 6-2: Ejemplos de enlaces entre indicadores de resultados y avanzados



1.17 Es importante seleccionar SPI que se relacionen con los objetivos de seguridad operacional de la organización. Tener SPI que estén bien definidos y alineados, facilitará la identificación de los SPTs, lo que mostrará el progreso hacia el logro de los objetivos de seguridad operacional. Esto le permite a la organización asignar recursos con el

mayor efecto de seguridad operacional al saber exactamente qué se requiere, y cuándo y cómo actuar para lograr el rendimiento de seguridad planeado.

Definiendo SPIs

1.18 El contenido de cada SPI debe incluir:

a) una descripción de lo que mide el SPI;

b) el propósito del SPI (qué se pretende gestionar y a quién se destina informar);

c) las unidades de medida y cualquier requisito para su cálculo;

d) quién es responsable de recopilar, validar, controlar, informar y actuar sobre el SPI (pueden ser personal de diferentes partes de la organización);

e) dónde o cómo deben recopilarse los datos; y

f) la frecuencia de los informes, la recopilación, el seguimiento y el análisis de los datos de SPI.

SPIs y notificaciones de seguridad operacional

1.19 Los cambios en las prácticas operativas pueden llevar a una notificación insuficiente hasta que su impacto sea totalmente aceptado por los posibles notificadores. Esto se conoce como "sesgo de notificación". Los cambios en las disposiciones relacionadas con la protección de la información de seguridad y las fuentes relacionadas también podrían conducir a un exceso de informes. En ambos casos, el sesgo de notificación puede distorsionar la intención y la precisión de los datos utilizados para el SPI. Empleado juiciosamente, las notificaciones de seguridad operacional aún pueden proporcionar datos valiosos para la gestión del rendimiento de seguridad operacional.

2. Establecer metas de rendimiento de la seguridad operacional

2.1 Las metas de rendimiento de seguridad operacional (SPT) definen los logros deseados de gestión del rendimiento de seguridad operacional a corto y mediano plazo. Actúan como "hitos" que brindan la confianza de que la organización está encaminada a lograr sus objetivos de seguridad operacional y proporcionan una forma medible de verificar la efectividad de las actividades de gestión del rendimiento de seguridad operacional.

2.2 La configuración de SPT deberá tener en cuenta factores como el nivel de riesgo de seguridad operacional prevaleciente, la tolerabilidad de los riesgos de seguridad operacional, así como las expectativas con respecto a la seguridad operacional del sector de la aviación en particular. La configuración de los SPT debe determinarse después de considerar qué se puede lograr de forma realista para el sector de aviación asociado y el rendimiento reciente de un SPI particular, donde se dispone de datos de tendencias históricas.

2.3 Si la combinación de objetivos de seguridad, SPIs y SPTs que trabajan en conjunto son **SMART (Específico, medible, alcanzable, realista**, **y tiempo**) le permite a la organización demostrar de manera más efectiva su rendimiento de seguridad operacional.

2.4 Existen múltiples enfoques para alcanzar los objetivos de la gestión del rendimiento de la seguridad operacional, especialmente el establecimiento de SPTs. Un enfoque implica el establecimiento de objetivos generales de seguridad operacional de alto nivel con SPIs alineados y luego la identificación de niveles razonables de mejoras después de que se haya establecido un rendimiento de seguridad operacional básico.

2.5 Estos niveles de mejoras pueden basarse en metas específicas (por ejemplo, disminución porcentual) o el logro de una tendencia positiva. Otro enfoque que se puede usar cuando los objetivos de seguridad son SMART es hacer que los objetivos de seguridad actúen como hitos para lograr los objetivos de seguridad operacional. Cualquiera de estos enfoques es válido y puede haber otros que una organización encuentre efectivos para demostrar su rendimiento de seguridad operacional. Se pueden

usar diferentes enfoques en combinación según corresponda a las circunstancias específicas.

Establecer metas con objetivos de seguridad de alto nivel

2.6 Se establecen metas con la alta dirección que acuerda objetivos de seguridad operacional de alto nivel. Luego, la organización identifica los SPIs apropiados que mostrarán mejoras en el rendimiento de seguridad operacional hacia los objetivos de seguridad operacional acordados.

2.7 Los SPIs se medirán utilizando fuentes de datos existentes, pero también pueden requerir la recopilación de datos adicionales. La organización luego comienza a reunir, analizar y presentar los SPIs. Las tendencias comenzarán a surgir, lo que proporcionará una visión general de los resultados de seguridad operacional de la organización y si se dirige hacia o lejos de sus objetivos de seguridad operacional. En este punto, la organización puede identificar SPT razonables y alcanzables para cada SPI.

Establecer metas con objetivos de seguridad SMART

2.8 Los objetivos de seguridad operacional pueden ser difíciles de comunicar y pueden parecer difíciles de lograr. Al dividirlos en objetivos de seguridad concretos más pequeños, el proceso de entrega es más fácil de administrar. De esta forma, los objetivos forman un vínculo crucial entre la estrategia y las operaciones cotidianas.

2.9 Las organizaciones deben identificar las áreas clave que impulsan el rendimiento de seguridad operacional y establecer una forma de medirlas. Una vez que una organización tiene una idea de cuál es su nivel actual de rendimiento al establecer el rendimiento de seguridad operacional básico, puede comenzar a establecer SPT para darles a todos en el Estado una idea clara de lo que deberían aspirar a lograr. La organización también puede usar la evaluación comparativa para ayudar a establecer objetivos de rendimiento. Esto implica usar información de rendimiento de organizaciones similares que ya han estado midiendo su rendimiento para tener una idea de cómo les está yendo a otros en la comunidad.

2.10 A continuación, se ilustra un ejemplo de la relación entre los objetivos de seguridad, SPI y SPT. En este ejemplo, la organización registró 100 excursiones de pista por millón de movimientos en 2018. Se ha determinado que esto es demasiado, y se ha establecido un objetivo para reducir el número de excursiones en la pista en un 50% para 2022.

2.11 Se han definido acciones específicas y cronogramas asociados para cumplir estas metas. Para monitorear, medir e informar su progreso, la organización ha elegido "excursiones RWY por millón de movimientos por año" como el SPI. La organización es consciente de que el progreso será más inmediato y eficaz si se establecen objetivos específicos que se alinean con el objetivo de seguridad. Por lo tanto, han establecido un objetivo de seguridad operacional que equivale a una reducción promedio de 12,5 por año durante el período del informe (cuatro años). Como se muestra en la representación gráfica, se espera que el progreso sea mayor en los primeros años y menor en los años posteriores. Esto está representado por la proyección curva hacia su objetivo. En el ejemplo:

a) el **objetivo de seguridad operacional** SMART es “reducción del 50 por ciento en la tasa de excursiones en RWY para 2022”;

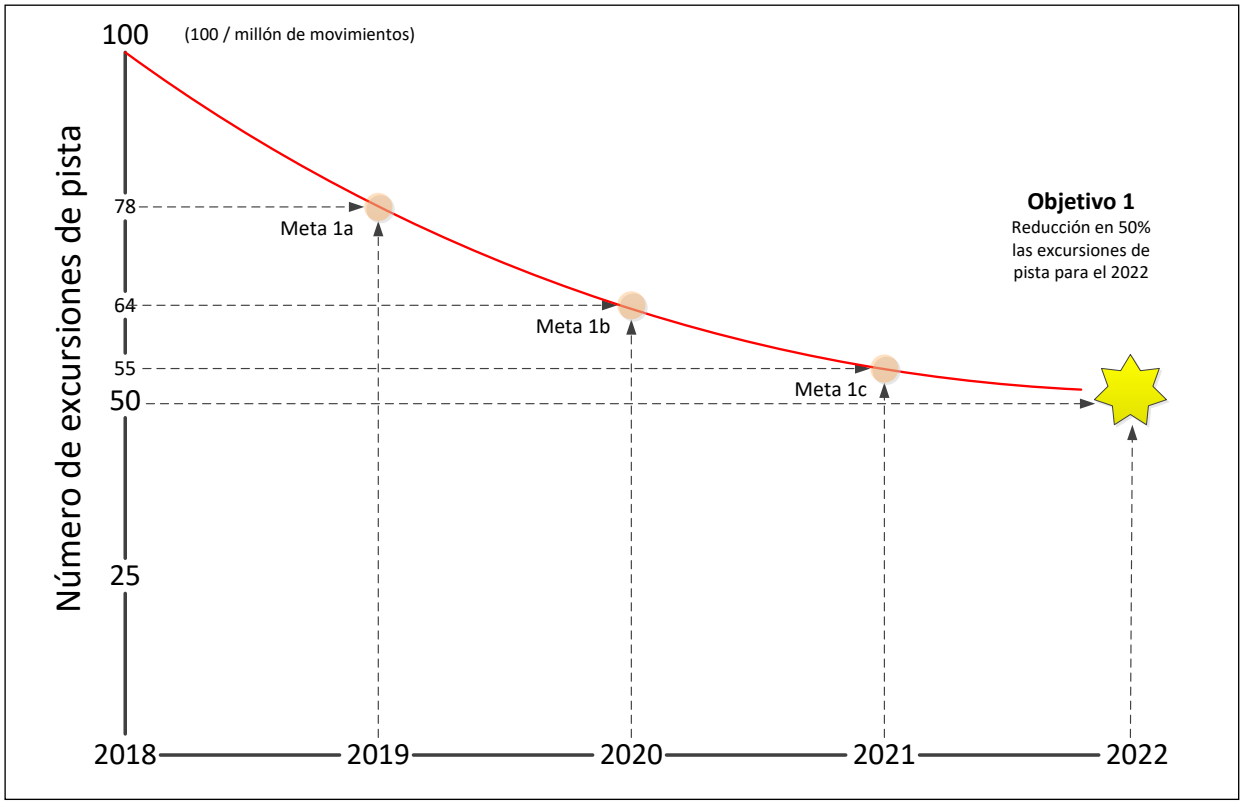
b) el **indicador de rendimiento de seguridad operacional** seleccionado es el “número de excursiones en la pista por millón de movimientos por año”; y

c) las **metas de seguridad operacional** relacionados con este objetivo representan hitos para alcanzar el Objetivo de Seguridad Operacional SMART y equivalen a una reducción de ~ 12% cada año hasta 2022;

- SPT 1a es “menos de 78 excursiones en la pista por millón de movimientos en 2019”;

- SPT 1b es “menos de 64 excursiones por pista por millón de movimiento en 2020”;
- SPT 1c es “menos de 55 excursiones en la pista por millón de movimiento en 2021”.

Figura 6-3: Ejemplo SPT con objetivos de seguridad operacional SMART



Consideraciones adicionales para la selección de SPIs y SPTs

2.12 A Al seleccionar SPIs y SPTs, también debe tenerse en cuenta lo siguiente:

a) **Gestión de la carga de trabajo**. La creación de una cantidad factible de SPI puede ayudar al personal a administrar su carga de trabajo de monitoreo e informes. Lo mismo ocurre con la complejidad de SPI o la disponibilidad de los datos necesarios. Es mejor acordar lo qué es factible y luego priorizar la selección de SPI sobre esta base. Si un SPI ya no está informando el rendimiento de seguridad operacional, o se le ha dado una prioridad más baja, considere descontinuar a favor de un indicador de mayor prioridad o más útil.

b) **Difusión óptima de SPIs**. Una combinación de SPIs que abarquen las áreas de enfoque ayudará a obtener una visión general del rendimiento de seguridad operacional de la organización y permitirá la toma de decisiones basadas en datos.

c) **Claridad de los SPIs**. Al seleccionar un SPI, debe quedar claro qué se está midiendo y con qué frecuencia. Los SPIs con definiciones claras ayudan a comprender los resultados, evitan las interpretaciones erróneas y permiten comparaciones significativas a lo largo del tiempo.

d) **Fomentar el comportamiento deseado**. Los SPTs pueden cambiar comportamientos y contribuir a los resultados deseados. Esto es especialmente relevante si el logro del objetivo está vinculado a las recompensas organizacionales; como la gestión de la remuneración. Los SPTs deberán fomentar positivamente

conductas organizacionales e individuales que den lugar deliberadamente a decisiones defendibles y a la mejora del rendimiento de la seguridad operacional. Es igualmente importante considerar los posibles comportamientos no deseados al seleccionar SPIs y SPTs.

e) **Elegir mediciones importantes**. Es imperativo que se seleccionen SPIs útiles, no solo aquellos que son fáciles de medir. Depende de la organización decidir cuáles son los parámetros de seguridad operacional más útiles; aquellos que guían a la organización hacia decisiones de seguridad operacional mejoradas, rendimiento de seguridad operacional y alcanzar sus objetivos de seguridad operacional.

f) **Alcanzar metas de rendimiento de seguridad operacional**. Esta es una consideración particularmente importante, y está vinculada a los comportamientos de seguridad deseados. Alcanzar los SPT acordados no siempre es indicativo de la mejora del rendimiento de seguridad operacional. La organización deberá distinguir entre el solo cumplimiento de los SPTs y la mejora real y demostrable del rendimiento de la seguridad operacional de la organización. Es imperativo que la organización considere el contexto dentro del cual se logró el objetivo, en lugar de mirar un SPT de forma aislada. El reconocimiento de una mejora general en el rendimiento de la seguridad operacional, en lugar de un logro SPT aislado, fomentará los comportamientos organizacionales deseables y alentará el intercambio de información de seguridad operacional que se encuentra en el núcleo de SRM y el aseguramiento de la seguridad operacional. Esto también podría mejorar la relación entre el Estado y el proveedor del servicio y su disposición a compartir datos e ideas de seguridad operacional.

Advertencias sobre el establecimiento de SPTs

2.13 No siempre es necesario o apropiado definir SPTs ya que puede haber algunos SPIs que es mejor monitorear las tendencias en lugar de determinar una meta. Los informes de seguridad operacional son un ejemplo en el que tener una meta puede desalentar a las personas a no informar (si la meta no va a exceder un número) o informar asuntos triviales para alcanzar una meta (si la meta es alcanzar un cierto número).

2.14 También puede haber SPIs que es mejor definir una dirección de viaje para mejorar el rendimiento de seguridad operacional continuo de la meta (es decir, para reducir la cantidad de eventos) en lugar de definir una meta absoluta, ya que pueden ser difíciles de determinar. Lo siguiente también se debe considerar al decidir los SPTs apropiados:

a) **Impulsar conductas indeseables**, si los gerentes u organizaciones están demasiado enfocados en el logro de los números como un indicador de éxito, es posible que no logren la mejora prevista en el rendimiento de seguridad operacional;

b) **Metas operacionales**, centrarse demasiado en alcanzar las metas operacionales (como Reducción de componentes por problemas de seguridad operacional luego de un trabajo de mantenimiento, reducción de costos indirectos, etc.) sin un equilibrio de metas de rendimiento de seguridad operacional puede llevar a 'alcanzar los objetivos operacionales' sin mejorar necesariamente el rendimiento de seguridad operacional;

c) **Enfocarse en la cantidad en lugar de en la calidad**; esto puede alentar a las personas o departamentos a alcanzar la meta, pero al hacerlo, entregar un producto o servicio deficiente;

d) **Límite de la innovación**; aunque no es la intención, una vez que se alcanza la meta, esto puede llevar a una relajación y no se necesitan más mejoras y la complacencia puede establecerse.

e) **Conflicto organizacional**; las metas pueden crear conflictos entre departamentos y organizaciones cuando discuten sobre quién es responsable en lugar de centrarse en intentar trabajar juntos.

2.15 Obtener la medición correcta del rendimiento de seguridad operacional implica decidir cómo medir mejor el logro de los objetivos de seguridad operacional. Esto variará de Estado a Estado y de organización a organización. Las organizaciones deberán tomarse

el tiempo para desarrollar su conocimiento estratégico de qué es lo que impulsa la mejora de la seguridad operacional para sus objetivos de seguridad operacional.

2.16 Los SPIs y SPTs se pueden usar de diferentes formas para demostrar el rendimiento de seguridad operacional. Es crucial que las organizaciones personalicen, seleccionen y apliquen diversas herramientas y enfoques de medición según sus circunstancias específicas y la naturaleza de lo que se está midiendo. Por ejemplo, en algunos casos, las organizaciones podrían adoptar SPIs que tengan SPTs asociados específicos. En otra situación, puede ser preferible enfocarse en lograr una tendencia positiva en los SPIs, sin valores objetivos específicos. El paquete de métricas de rendimiento seleccionadas usualmente empleará una combinación de estos enfoques.

3. Monitoreo del rendimiento de la seguridad operacional

3.1 Una vez que una organización ha identificado los objetivos en función de los SPI que creen que entregarán el resultado planificado, deben asegurarse de que los interesados cumplan asignando una responsabilidad clara para la entrega. La definición de los SPT respalda el logro del ALoSP para el Estado mediante la asignación de una rendición de cuentas clara.

3.2 Se deberán establecerse mecanismos para monitorear y medir el rendimiento de seguridad operacional de la organización a fin de identificar qué cambios pueden ser necesarios si el progreso realizado no es el esperado y reforzar el compromiso de la organización para cumplir con los objetivos de seguridad operacional.

Línea base del rendimiento de seguridad operacional

3.3 Comprender cómo la organización planea avanzar hacia sus objetivos de seguridad operacional requiere que sepan dónde están, en relación con la seguridad operacional. Una vez que la estructura de rendimiento de seguridad operacional de la organización (objetivos de seguridad operacional, indicadores, metas, factores desencadenantes) se ha establecido y está funcionando, es posible conocer su rendimiento de seguridad operacional de línea de base a través de un período de monitoreo.

3.4 El rendimiento de seguridad operacional básico es el rendimiento de seguridad operacional al comienzo del proceso de medición del rendimiento de seguridad operacional. El punto de referencia desde el cual se puede medir el progreso. El caso del ejemplo utilizado en la **Figura 6-3**, el rendimiento de seguridad operacional de línea base, para ese objetivo de seguridad operacional particular fue "100 excursiones de pista por millón de movimientos durante el año (2018)". A partir de esta base sólida, se pueden registrar indicaciones y metas precisas y significativas.

Refinamiento de SPIs y SPTs

3.5 Los SPI y los SPT asociados deberán revisarse para determinar si proporcionan la información necesaria para seguir el progreso hacia los objetivos de seguridad operacional y para garantizar que las metas sean realistas y alcanzables.

3.6 La gestión del rendimiento de seguridad operacional es una actividad continua. Los riesgos de seguridad operacional y o disponibilidad de los datos cambian con el tiempo. Los SPI iniciales pueden desarrollarse utilizando recursos limitados de información de seguridad. Más tarde, se podrán establecer más canales de información, habrá más datos de seguridad operacional disponibles y las capacidades de análisis de seguridad operacional de las organizaciones probablemente maduren.

3.7 Puede ser apropiado para las organizaciones desarrollar SPI simples (más amplios) inicialmente. A medida que recopilan más datos y la capacidad de gestión de seguridad operacional, pueden considerar refinar el alcance de SPI y SPT para alinearse mejor con los objetivos de seguridad operacional deseados. Las organizaciones pequeñas no complejas pueden elegir refinar sus SPI y SPT y/o seleccionar indicadores genéricos (pero específicos) que se aplican a la mayoría de los sistemas de aviación. Algunos ejemplos de indicadores genéricos serían:

a) eventos que incluyen daños estructurales a los equipos;

b) eventos que indican las circunstancias en las que casi se produjo un accidente;

c) eventos en los que el personal operativo o los miembros de la comunidad aeronáutica resultaron heridos de muerte o gravedad;

d) eventos en los que el personal operativo quedó incapacitado o limitado para realizar sus tareas de manera segura;

e) tasa de informes de ocurrencia voluntaria; y

f) índice de informes de ocurrencia obligatoria.

3.8 Las organizaciones más grandes y complejas pueden optar por instituir un rango más amplio y más profundo de SPI y SPT e integrar indicadores genéricos como los enumerados anteriormente con los específicos de la actividad.

3.9 Un aeropuerto grande, por ejemplo, que preste servicios a las principales líneas aéreas y se encuentre bajo un espacio aéreo complejo, podría considerar combinar algunos de los SPI genéricos con SPI de mayor alcance que representen aspectos específicos de su operación. El monitoreo de estos puede requerir un mayor esfuerzo, pero probablemente produzca resultados de seguridad operacional superiores.

3.10 Existe una clara correlación entre la complejidad relativa de los SPI y los SPT, y la escala y complejidad de las operaciones del Estado o de los proveedores de servicios. Esta complejidad relativa debe reflejarse en el indicador y el conjunto de objetivos. Los responsables de establecer la gestión del rendimiento de seguridad deberían ser conscientes de esto.

3.11 El conjunto de SPI y SPT seleccionados por una organización debe **revisarse periódicamente** para garantizar su continuidad significativa como indicadores del rendimiento de seguridad operacional de la organización. Algunos motivos para continuar, interrumpir o cambiar SPI y SPT incluyen:

a) Los SPI que continuamente reportan el mismo valor (por ejemplo, cero por ciento o 100 por ciento); es poco probable que estos SPI proporcionen información significativa para la toma de decisiones de la alta gerencia;

b) los SPI que tienen similares comportamientos y, como tal, se considera que general duplicidad;

c) el SPT para un SPI implementado para medir la introducción de un programa o mejora específica de una meta que ha sido cumplida;

d) otro problema de seguridad operacional que se convierte en una prioridad más alta para monitorear y medir;

e) obtener una mejor comprensión de un problema de seguridad operacional particular al reducir los detalles de un SPI (es decir, reducir el "ruido" para aclarar la "señal"); y

f) los objetivos de seguridad han cambiado y, como consecuencia, los SPI requieren actualización para seguir siendo relevantes.

Factores desencadenantes

3.12 Una breve perspectiva de las nociones de factores desencadenantes es relevante para ayudar en su eventual rol dentro del contexto de la gestión del desempeño de seguridad por parte de una organización.

3.13 Un factor desencadenante es un nivel establecido o un valor de criterio que sirve para activar (iniciar) una evaluación, decisión, ajuste o acción correctiva relacionada con el indicador en particular. Un método para establecer criterios factores desencadenantes fuera de los límites para los SPTs es el uso del principio de **desviación estándar de la población** (STDEVP – Population Standard Desviation Principle).

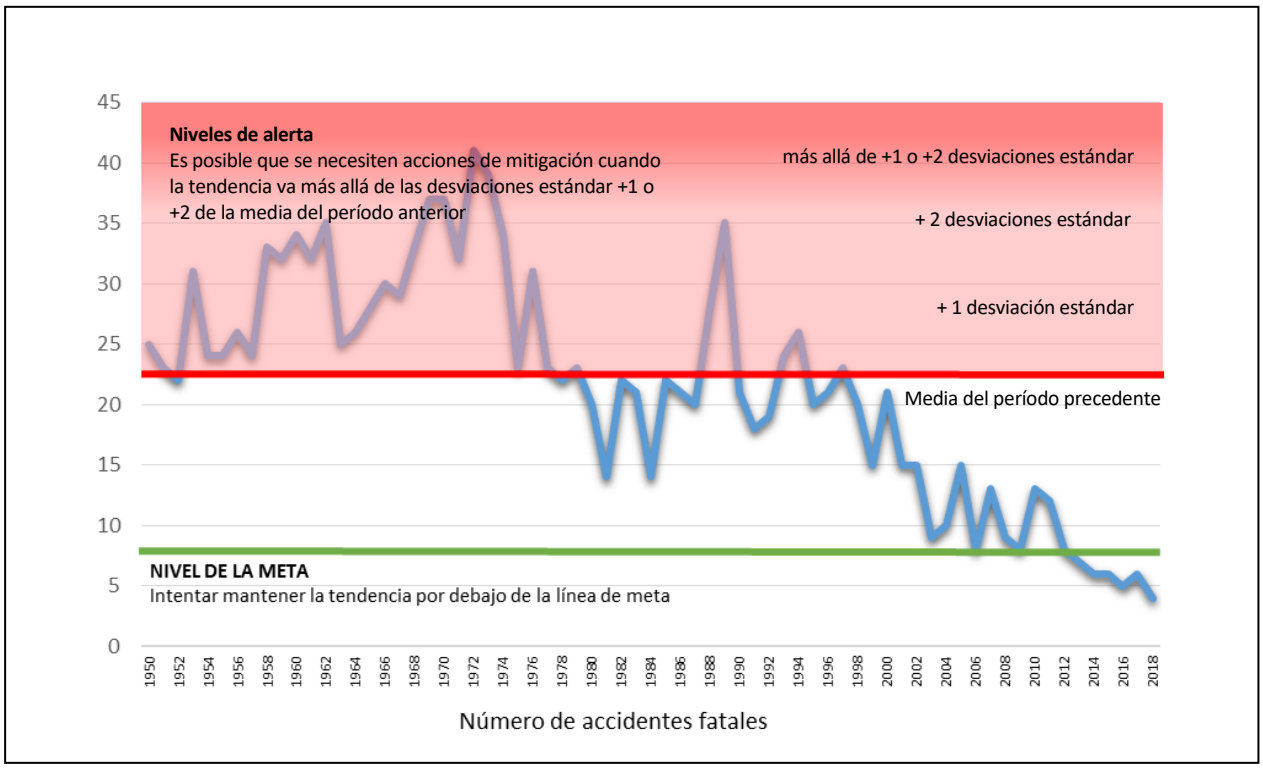
3.14 Este método deriva el valor de desviación estándar (SD) basado en los puntos de datos históricos anteriores de un indicador de seguridad operacional dado. El valor de SD más

el valor promedio (media) del conjunto de datos históricos forma el valor del factor desencadenante básico para el siguiente período de monitoreo. El principio de la SD (una función estadística básica) es establecer los criterios del nivel del factor desencadenante basado en función del rendimiento histórico real del indicador dado (conjunto de datos), incluida su volatilidad (fluctuaciones del punto de datos).

3.15 Un conjunto de datos históricos más volátiles generalmente dará como resultado un valor de nivel de factor desencadenante más alto (más generoso) para el próximo período de monitoreo. Los factores desencadenantes proporcionan advertencias tempranas que permiten a los responsables de la toma de decisiones tomar decisiones de seguridad informadas y, por lo tanto, mejorar el rendimiento de la seguridad operacional.

3.16 Un ejemplo de niveles de factores desencadenante basados en desviaciones estándar se proporciona en la **Figura 6-4** a continuación. En este ejemplo, las decisiones basadas en datos y las medidas de mitigación de la seguridad operacional pueden necesitar tomarse cuando la tendencia va más allá de + 1SD o + 2SD de la media del período anterior. A menudo, los niveles de factores de activación (en este caso + 1SD, + 2SD o más allá de + 2SD) se alinearán con los niveles de gestión de decisiones y la urgencia de la acción.

Figura 6-4: Ejemplo de representación de niveles de factores desencadenantes de seguridad operacional



3.17 Una vez que se han definido los SPT y los factores desencadenantes (si se utiliza), se puede rastrear su SPI asociado para conocer su estado de rendimiento respectivo. Un resumen consolidado del total de SPT y resultados de rendimiento de factores desencadenantes del paquete de SPI completados podría también ser compilado y/o agregado para un periodo de monitoreo establecido. Se pueden asignar valores cualitativos (satisfactorio/insatisfactorio) para cada SPT alcanzado y cada factor desencadenante no violado. Alternativamente, los valores numéricos (puntos) se pueden usar para proporcionar una medida cuantitativa del rendimiento general del paquete de SPI.

3.18 Es importante tener en cuenta que los valores de factores desencadenantes sirven para activar (iniciar) una evaluación, decisión, ajuste o acción correctiva relacionada con el indicador en particular. Un factor desencadenante de SPI no es necesariamente catastrófica o una indicación de falla. Es simplemente una señal de que la actividad se ha movido más allá del límite predeterminado. El factor desencadenante tiene el objetivo de atraer la atención de los que toman las decisiones que ahora están en condiciones de tomar medidas correctivas, o no, según las circunstancias.

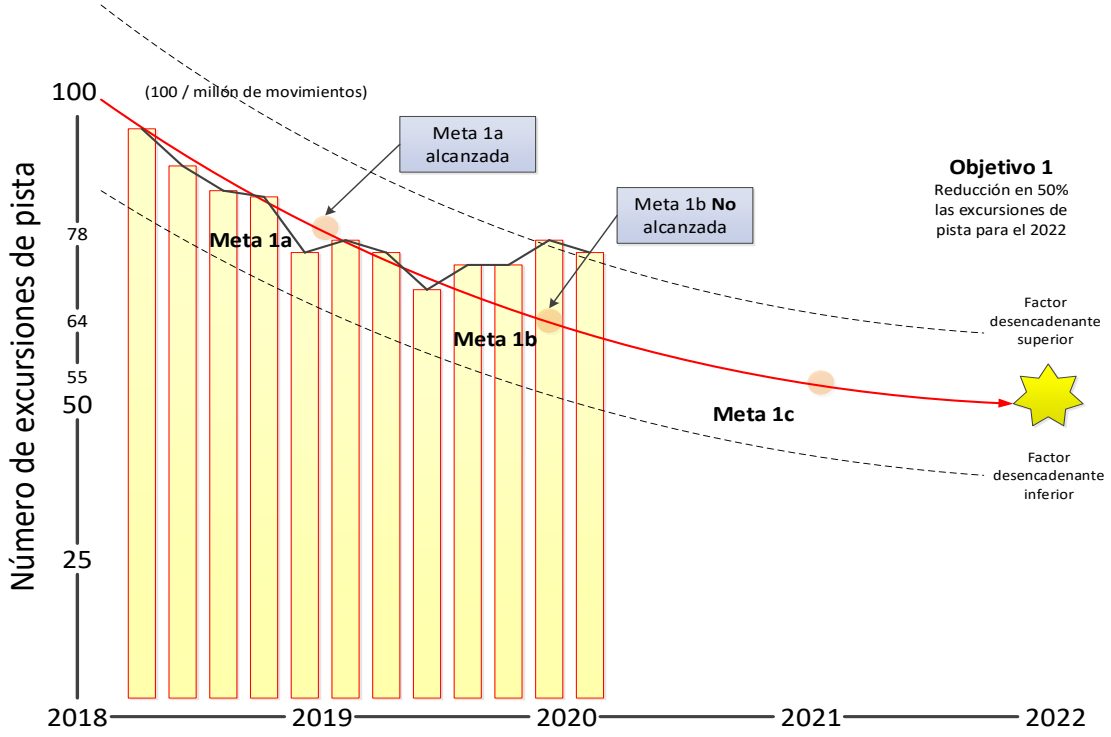
Advertencia sobre los factores desencadenantes

3.19 Existen desafíos que definen niveles de activación confiables. Los factores desencadenantes y sus niveles asociados funcionan mejor cuando hay amplios datos de seguridad operacional y capacidades de administración de datos de seguridad operacional. Esto puede imponer una carga de trabajo adicional en la organización. La noción del factor desencadenante se diseñó y se adaptó mejor a la gestión de riesgos de seguridad operacional (SRM) de sistemas puramente técnicos, por ejemplo: control del motor de la aeronave del CIAC.

3.20 En el caso referido, grandes cantidades de datos cuantitativos se prestan a factores desencadenantes precisos y a definiciones de niveles de factores desencadenantes. La noción de factores desencadenantes es posiblemente menos relevante para la SRM de los sistemas socio-técnicos. Los sistemas socio-técnicos son sistemas en los que las personas interactúan activamente con los procesos y las tecnologías para lograr la entrega del servicio del sistema o los objetivos de producción. El SMS es un sistema socio-técnico. Los factores desencadenantes menos confiables y significativos utilizados en los sistemas socio-técnicos se deben a las limitaciones de las medidas confiables cuando los humanos están involucrados.

3.21 Por lo tanto, se necesita un enfoque más flexible para que los factores desencadenantes sean significativos. No se requiere que las organizaciones de mantenimiento definan niveles de factores desencadenantes para cada SPI. Sin embargo, existen beneficios para las organizaciones donde sus datos para un SPI son muy específicos, hay suficientes puntos de datos y los datos son suficientemente confiables.

Figura 6-5: Ejemplo de configuración de factores desencadenantes de seguridad operacional



3.22 La ilustración anterior es una extensión del ejemplo anterior, "reducción del 50 por ciento en las excursiones en la pista para 2022". En este escenario, ahora es el año 2020. La organización ha estado recolectando datos de seguridad operacional (SPI - 'N° excursiones en la pista / millón de movimiento en el año') y trabajando con las partes interesadas para reducir las instancias. El SPT para 2019 (<78 excursiones en la pista / millón de movimiento en el año) se logró. Sin embargo, el SPI indica que no solo no se logró el SPT para 2020 (<64 excursiones de pista / millón de movimiento en el año), el número de excursiones ha excedido el factor desencadenante en 2 períodos de informe consecutivos. Los responsables de la toma de decisiones han sido alertados sobre el deterioro en el rendimiento de seguridad operacional y están en buena posición para tomar decisiones basadas en los datos para tomar medidas adicionales. Sus decisiones basadas en datos tendrán como objetivo volver a colocar el rendimiento de seguridad operacional dentro de la zona aceptable y en camino de alcanzar su objetivo de seguridad operacional.

Identificación de acciones requeridas

3.23 Podría decirse que el resultado más importante de establecer una estructura de gestión del rendimiento de seguridad operacional es la presentación de información a los responsables de la toma de decisiones de la organización para que ellos puedan tomar decisiones basadas en datos e información de seguridad operacional actuales y confiables. El propósito siempre debe ser tomar decisiones de acuerdo con la política de seguridad operacional y hacia los objetivos de seguridad operacional.

3.24 En relación con la gestión del rendimiento de seguridad operacional, la toma de decisiones impulsada por datos, es sobre tomar decisiones efectivas y bien informadas basadas en los resultados de SPI monitoreados y medidos u otros informes y análisis de datos de seguridad operacional e información de seguridad operacional. El uso de datos de seguridad operacional válidos y relevantes combinados con información que proporciona contexto respalda a la organización en la toma de decisiones que se alinean con sus objetivos y metas de seguridad operacional.

3.25 La información contextual también puede incluir otras prioridades de las partes interesadas, deficiencias conocidas en los datos y otros datos complementarios para evaluar los pros, los contras, las oportunidades, las limitaciones y los riesgos asociados con la decisión. Tener la información fácilmente disponible y fácil de interpretar, ayuda a mitigar el sesgo, la influencia y el error humano en el proceso de toma de decisiones.

3.26 La toma de decisiones impulsada por los datos también respalda la evaluación de decisiones tomadas en el pasado para respaldar cualquier realineación con los objetivos de seguridad operacional. En el capítulo 6 se proporciona más orientación sobre la toma de decisiones basada en datos.

4. Actualización de los objetivos de seguridad operacional

La gestión del rendimiento de seguridad operacional no está destinada a ser "establecida y olvidada". La gestión del rendimiento de seguridad operacional es dinámica y central para el funcionamiento de cada organización de mantenimiento. La revisión y actualización de la estructura de gestión del rendimiento de seguridad operacional es deseable:

a) Rutinariamente, de acuerdo con el ciclo periódico establecido y acordado por el comité de seguridad de alto nivel;

b) basado en las aportaciones de los análisis de seguridad operacional; y

c) en respuesta a cambios importantes en la operación, riesgos principales o medio-ambiente.

Apéndice 7

Ejemplos de indicadores de rendimiento en materia de seguridad operacional

Tabla 1: Ejemplos de indicadores de seguridad operacional (SPI)

Los ejemplos de los SPI de un SMS se encuentran al lado derecho de la Tabla 1. En esta tabla se presentan los criterios para determinar los objetivos y las alertas para cada indicador. Los indicadores de eficacia de la seguridad operacional del SSP se presentan en el lado izquierdo para ilustrar la correlación necesaria entre el SMS y el SSP. Los SPI del SMS deben ser desarrollados por los CIAC 141 en coordinación con la AAC. Los SPI propuestos deberían ser coherentes con los indicadores de seguridad del SSP establecidos por la AAC, por tanto es necesaria la coordinación y el acuerdo entre los CIAC y los funcionarios responsables de la AAC.

Tabla 2: Ejemplo de cuadro de indicador de rendimiento en materia de seguridad operacional del SMS

Este es un ejemplo de un cuadro de SPI de resultado. Es un ejemplo de la tasa de incidentes reportables/obligatorios de un CIAC. El cuadro de la izquierda representa el rendimiento del año anterior, mientras que el cuadro de la derecha representa la información actualizada del presente año. La determinación de las alertas está basada en criterios de métricas estándar de desviación. La fórmula de Excel es: *"=STDEVP*". Para los propósitos de cálculo manual, la fórmula de desviación estándar es:

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

Donde "X" es el valor de cada dato; "N" es el número de datos y "μ" es el valor promedio de todos los datos.

El nivel de alerta corresponde a una mejora deseada en porcentaje (en este caso 5%) con relación al promedio de datos del año anterior. Este cuadro es generado por la hoja de datos que se muestra en la Tabla 2.

Tabla 3: Hoja de datos para el cuadro de ejemplo de SPI

Esta hoja de datos se utiliza para generar el cuadro de indicadores de eficacia de seguridad operacional de la Tabla 1. El mismo procedimiento puede ser utilizado para generar cualquier otro indicador de eficacia con los datos apropiados y con la modificación correspondiente del descriptor.

Tabla 4: Ejemplo de resumen de indicadores del SMS

Este es un resumen de todos los indicadores de eficacia de la seguridad operacional del CIAC, con sus respectivas metas y niveles de alerta. Este tipo de resumen puede ser útil al final de cada periodo de revisión para brindar una visión general de la eficacia del SMS. Si se desea un resumen más cuantitativo, se puede asignar una puntuación a cada Si/No en cada meta y alerta. Por ejemplo:

Indicadores de resultado de baja probabilidad / alta gravedad:
- Nivel de alerta no violado (Si=4, No=0)
- Objetivo alcanzado (Si=3, No=0)

Indicadores de resultados de alta probabilidad / baja gravedad
- Nivel de alerta no violado (Si=2, No=0)
- Objetivos alcanzada (Si=1, No=0)

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

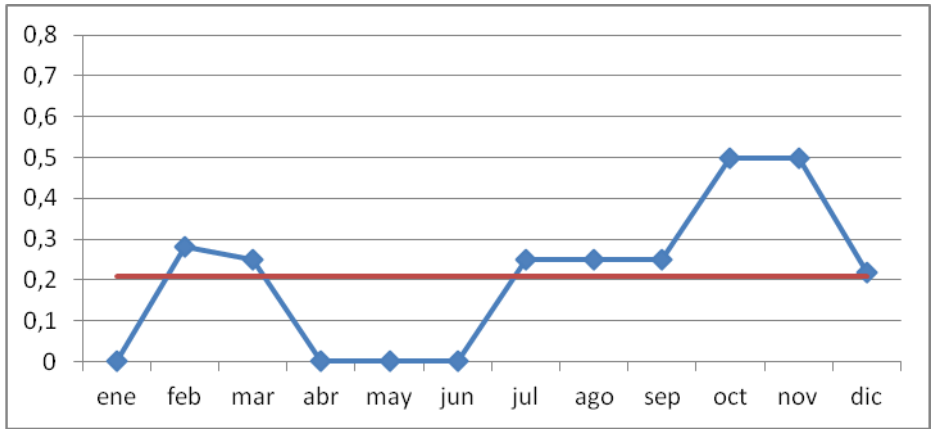
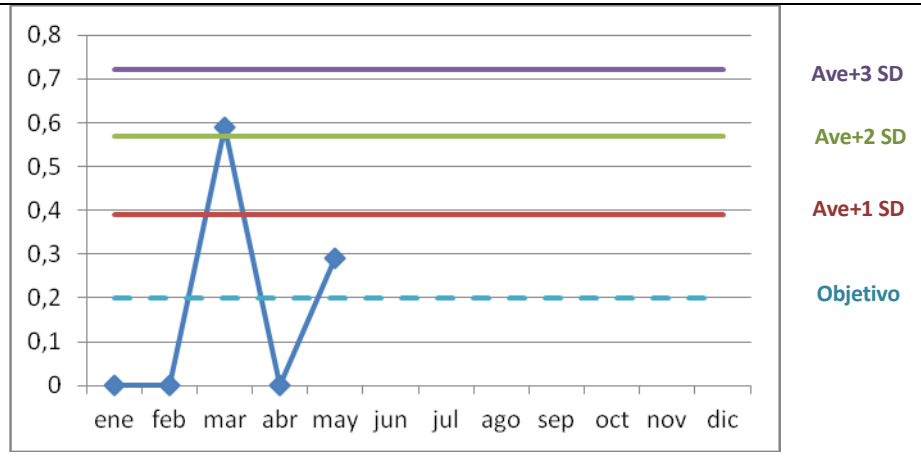
Tabla 5: Ejemplos de indicadores de cuestiones sistémicas

En esta tabla se describen una serie de ejemplos que pueden ser utilizados por el CIAC para el desarrollo de sus propios indicadores de rendimiento de seguridad operacional. Es importante, que antes de utilizarlos se realice un análisis para determinar si el indicador es aplicable a las operaciones del CIAC, teniendo en cuenta la madurez del SMS de la organización y las características que podría mejorar o que requieran mayor atención.

Tabla 7-1: Ejemplos de indicadores de rendimiento en materia de seguridad operacional

Indicadores de seguridad operacional del SSP (Estado)						Indicadores de rendimiento en materia de seguridad operacional del SMS (CIAC 141)					
Indicadores de resultados (Baja probabilidad / Alta gravedad)			Indicadores de resultados (Alta probabilidad /Baja gravedad)			Indicadores de resultados (Baja probabilidad / Alta gravedad)			Indicadores de bajo impacto (Alta probabilidad / Baja gravedad)		
Indicador de seguridad operacional	Criterios del nivel de alerta	Criterios del nivel de objetivos	Indicador de seguridad operacional	Criterios del nivel de alerta	Criterios del nivel de objetivos	Indicador de seguridad operacional	Criterios del nivel de alerta	Criterios del nivel de objetivos	Indicador de seguridad operacional	Criterios del nivel de alerta	Criterios del nivel de objetivos
Tasa mensual de accidentes / incidentes serios de todos los CIAC 141 (ej.: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de resultados de la vigilancia anual LEI% o tasa de hallazgos (hallazgos por auditoría)	Por definir	Por definir	Tasa mensual de incidentes serios por aeronave (ej: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa mensual de incidentes combinada de todas las flotas (ej: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.
Tasa trimestral de incidentes relacionados con paradas de motor en vuelo (engine IFSD) (ej.: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de resultados de la inspección anual LEI% o tasa de hallazgos (hallazgos por auditoría)	Por definir	Por definir	Tasa mensual de incidentes serios del total de aeronaves (ej: por/1000HV)	Ave + 1/2/3 SD. (ajustado cada año o cada dos años)	___% (ej. 5%) de mejora entre la tasa media anual.	Tasa de hallazgos o LEI% de la auditoría interna anual de SMS/QMS (ej: hallazgos por auditoría)	Por definir	Por definir

Tabla 7-2: Ejemplos de indicadores de rendimiento en materia de seguridad operacional

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>A) Ajuste del nivel de alerta:

El nivel de alerta para un nuevo período de control (año actual) está basado en la eficacia del año anterior (o del período de control anterior), en sus datos desviación estándar promedio % (Average % Standard Desviation). Las 3 líneas de alerta son: Ave+1sD, Ave+2SD y Ave+3SD</td>
<td>C) Ajuste de los objetivos

El ajuste de los objetivos puede ser menos estructurado que el ajuste de los niveles de alerta – Por ejemplo: el objetivo para la tasa promedio (Avg rate) para el nuevo período de control (presente año) será de 5% más bajo (mejor) que el valor promedio del periodo pasado.</td>
</tr>
<tr>
<td rowspan="2">B) Disparador de alerta

Una alerta (tendencia anormal/inaceptable) se activa cuando CUALQUIERA de las siguientes condiciones se cumplen para el período actual de control (año presente):
- Cualquier dato se encuentra por encima de la línea 3 SD
- 2 datos consecutivos se encuentran por encima de la línea 2 SD
- 3 datos consecutivos se encuentran por encima de la línea 1 SD

Cuando una alerta se activa (situación de alto riesgo potencial o fuera de control), deben tomarse acciones de seguimiento como análisis más profundos para identificar la causa raíz del cambio en la tasa, así como las acciones necesarias para controlar la tendencia.</td>
<td>D) Logro de los objetivos

Si al final del año actual la tasa promedio (Average) para todo el año es menor al 5% o menor que el valor del período anterior, puede considerarse que se ha cumplido el objetivo.</td>
</tr>
<tr>
<td>E) Niveles de alerta y objetivos: Período de validez

Los objetivos y los niveles de alerta deben ser revisados y ajustados para cada nuevo período de control como corresponda, basado en la tasa promedio del período anterior.</td>
</tr>
</table>

Tabla 7-3: Ejemplos de indicadores de rendimiento en materia de seguridad operacional

Ejemplo de indicador de seguridad operacional de resultados baja probabilidad / alta gravedad (Con el criterio de ajuste de objetivos y alertas)

Año anterior				
Mes	CIAC 141 Total HV	Número de incidentes MOR reportables	Tasa de inc.*	Ave
Ene	3,992	-	0.00	0.21
Feb	3,727	1.00	0.27	0.21
Mar	3,900	1.00	0.26	0.21
Abr	3,870	-	0.00	0.21
May	3,976	-	0.00	0.21
Jun	3,809	-	0.00	0.21
Jul	3,870	1.00	0.26	0.21
Ago	3,904	1.00	0.26	0.21
Sep	3,864	1.00	0.26	0.21
Oct	3,973	2.00	0.50	0.21
Nov	3,955	2.00	0.51	0.21
Dic	3,369	1.00	0.23	0.21
		Ave	**0.21**	
		SD	**0.18**	

*Cálculo de la tasa (por 1000 HV)

Presente año							
Mes	CIAC 141 Total HV	Número de incidentes MOR reportables	Tasa de inc.*	Ave+1SD Año anterior	Ave+2SD Año anterior	Ave+3SD Año anterior	Objetivo promedio año actual
Dic	3,396	1.00	0.23	0.39	0.57	0.76	0.21
Ene	4,090	0.00	0.00	0.39	0.57	0.76	0.20
Feb	3,316	0.00	0.00	0.39	0.57	0.76	0.20
Mar	3,482	2.00	0.57	0.39	0.57	0.76	0.20
Abr	3,549	0.00	0.00	0.39	0.57	0.76	0.20
May	3,633	1.00	0.28	0.39	0.57	0.76	0.20
Jun				0.39	0.57	0.76	0.20
Jul				0.39	0.57	0.76	0.20
Ago				0.39	0.57	0.76	0.20
Sep				0.39	0.57	0.76	0.20
Oct				0.39	0.57	0.76	0.20
Nov				0.39	0.57	0.76	0.20
Dic				0.39	0.57	0.76	0.20
		Ave					
		SD					

*Cálculo de la tasa (por 1000 HV)

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

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

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

Tabla 7-4: Ejemplo de medición de la eficacia de la seguridad operacional

Indicadores de resultados (baja probabilidad / alta gravedad)					
Descripción del SPI		Criterio/Nivel de alerta del SPI	Nivel de alerta violado (Si/No)	Criterio/Objetivo SPI	Objetivo logrado /Si/no)
1	Tasa de incidentes serios de la flota monomotor (por/1000 HV)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)	Si	5% de mejora en la tasa promedio con relación al año anterior	No
2	Tasa de incidentes “Paradas de motor en vuelo” (por/1000 HV)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)	Si	3% de mejora en la tasa promedio con relación al año anterior	Si
3	ETC				

Indicadores de resultados (alta probabilidad / baja gravedad)					
Descripción del SPI		Criterio/Nivel de alerta del SPI	Nivel de alerta violado (Si/No)	Criterio/Objetivo del SPI	Objetivo alcanzado (Si/no)
1	Tasa combinada de incidentes de aviones mono/multimo-tor (por/1000 HV)	Ave+1/2/3 SD. (Ajustado anualmente o cada dos años)	Si	5% de mejora en la tasa promedio con relación al año anterior	No
2	LEI% o tasa de hallazgos de la auditoría interna anual QMS (hallazgos por auditoría)	>25% LEI promedio; O cualquier hallazgo de nivel 1; O >5 hallazgos de nivel 2 por auditoría	Si	5% de mejora en la tasa promedio con relación al año anterior	Si
3	Tasa de informes voluntarios de peligros (ej: por/1000 HV)	TBD		TBD	
4	ETC.				

Tabla 7-5: Ejemplo de indicadores de cuestiones sistémicas

Área	Enfoque de 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 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.
	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

Área	Enfoque de medición	Métrica
		– 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 de años 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

Área	Enfoque de medición	Métrica
		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 formación en gestión de la seguridad operacional en los últimos dos años (instrucción continua). – Incremento en un ____% la frecuencia de revisión de los perfiles de competencias en los últimos dos años. – Incremento en un ____% la frecuencia de revisión del alcance, contenido y calidad de los programas de formación en comparación con el año anterior. – Número de cambios realizados en los programas de capacitación a raíz de la retroalimentación del personal al año en relación a las 10 últimas revisiones efectuadas. – Numero de cambios realizados en los programas de formación a raíz del análisis de las notificaciones de seguridad operacional internas por año en relación a los 10 últimos cambios.
	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

Área	Enfoque de medición	Métrica
		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/técnico, etc.) que han sido objeto de evaluación de riesgos en relación a los 10 últimos cambios.
	Planificación de respuesta ante emergencia	– Número de simulacros de emergencia cumplidos por año en relación a la cantidad planificada. – Frecuencia de la revisión del ERP en relación a la cantidad simulacros de ERP realizadas. – Número de cursos de formación en ERP realizados por mes / trimestre / año en relación a los cursos programados. – % de personal formado en el ERP dentro de un cuarto de año en relación al total del personal del CIAC. – Número de reuniones con los socios principales y contratistas para coordinar el ERP al mes / trimestre / año en relación a todas las reuniones planificadas al año.
	Promoción de la seguridad operacional	– Incremento en un ____% del grado en que el personal considera la seguridad operacional como un valor que guía su trabajo diario, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en el CIAC (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 CIAC (por ejemplo: en una escala de 1

Área	Enfoque de medición	Métrica
		= 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 CIAC (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 toma iniciativas 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 CIAC (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 CIAC (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 CIAC (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior.

Apéndice 7A
Ejemplo de formulario de indicador

LOGOTIPO	FORMULARIO DE INDICADOR	CÓDIGO	VIGENCIA
		F-	XX/XX/XXXX
			REVISIÓN
			0

Parte A: Identificación del indicador

1. Indicador
Ingrese el nombre del indicador.

2. Descripción
Ingrese una breve descripción del indicador.

3. Objetivo estratégico
Indique el objetivo estratégico al cual está relacionado el indicador.

Parte B: Especificaciones del indicador

4. Proyecto o programa:
Si corresponde, identificar el proyecto o programa específico al cual está relacionado el indicador.

5. Tipo de indicador
El indicador es: ☐ relacionado a la actividad (predictivo o leading) o ☐ relacionado con el resultado (reactivo o lagging)

6. Fundamento
Explicar cómo el indicador está relacionado al objetivo estratégico señalado en el ítem 3 y los soportes de su medición.

7. Limitaciones
Describa el alcance de la variable o categoría que mide el indicador.

8. Definición de términos técnicos o específicos
Si corresponde, proporcione una definición de los términos técnicos o específicos.

9. Método de cálculo/fórmula
Si corresponde, proporcione la fórmula de cálculo específica.

Parte C: Datos

En la siguiente tabla, proporcione información sobre los datos que respaldan la medición del indicador:

10. Conjunto(s) de datos	11. Disponibilidad	12. Nivel de desagregación	13. Proveedor	14. Custodio

Parte D: Detalles del contacto para seguimiento

Completado por:	**Correo electrónico:**	**Fecha de finalización:**
Ingrese su nombre.	*Ingrese su correo electrónico.*	*Ingrese la fecha.*

Parte E: Para uso de la sección o responsable de análisis integrado

Número de indicador	**Clasificación de nivel**
Dejar en blanco.	*Dejar en blanco.*

(Orientación para completar este formulario está en la siguiente página)

Orientación para completar el formulario

1. **Indicador:** Nombre asignado al indicador. El indicador debe apoyar el logro de una meta / objetivo, realizar un resultado deseado o evitar un resultado peligroso / no deseado. Los siguientes criterios deben ser considerados al definir un indicador:

   - Simple: El indicador medirá una variable claramente definida que los interesados comprendan;
   - Específico: El indicador debe incluir una sola métrica precisa;
   - Medible: El indicador debe incluir una métrica clara y específica que se pueda medir;
   - Relevante: El indicador debe ser relevante para el objetivo de la organización o el resultado / actividad que se está midiendo;
   - Tiempo: El indicador se definirá dentro de un período de tiempo específico.

2. **Descripción:** Una breve pero clara explicación del indicador, la métrica relacionada y lo que medirá; por ejemplo, el número de, porcentaje de, promedio de o tasa de algo.

3. **Objetivo del CIAC:** El objetivo estratégico del CIAC al cual se relaciona el indicador.

4. **Proyecto o programa**: Si corresponde, el proyecto o programa al cual está relacionado el indicador. Ejemplo: PBN, RPAS, etc.

5. **Tipo de indicador:** Puede tener uno de los siguientes tipos. El indicador puede estar relacionado con la actividad (o leading), es decir, medir los eventos y actividades actuales o futuras e informar sobre el desempeño de la organización, por ejemplo, los resultados de auditoria o inspección, realización de tareas o proyectos. El otro tipo, es cuando el indicador puede estar relacionado con el resultado (o lagging), es decir, medir eventos pasados e identificar las condiciones dentro de un sistema después de que hayan ocurrido eventos.

6. **Justificación:** Una explicación de cómo el indicador se conecta con el objetivo estratégico identificado por el centro de instrucción y lo que apoya la medición y el monitoreo del indicador.

7. **Limitaciones:** El alcance o el alcance de la variable o categoría que mide el indicador. Por ejemplo, las tasas de accidentes pueden limitarse a una categoría de aeronave específica o el cumplimiento puede aplicarse a cierto tipo o conjunto de estándares.

8. **Definición de términos técnicos o específicos**: Si corresponde, una definición de cualquier terminología técnica, específica o relacionada con el proyecto, utilizada para nombrar o definir el indicador que puede no ser ampliamente conocido o entendido.

9. **Método o fórmula de cálculo:** Si corresponde, la fórmula específica o técnica disponible para el cálculo del valor del indicador.

10. **Conjunto (s) de datos:** Los datos que se necesitan para medir el indicador.

11. **Disponibilidad de datos:** Los conjuntos de datos enumerados pueden tener diferentes niveles de disponibilidad, variando de 0 para datos no disponibles a 5 para datos completamente disponibles.

12. **Nivel de desagregación de datos**: El nivel más bajo en el que se pueden desglosar los datos a un nivel más detallado. Por ejemplo, los datos pueden estar disponibles a nivel mundial, regional o nacional. En ese caso, el nivel de desagregación son los datos nacionales.

13. **Proveedor de datos:** El proveedor de los datos o la fuente de donde provienen los datos. Es mejor indicar una base de datos o un programa en lugar de una persona o una sola tarea/proyecto de donde provienen los datos.

14. **Custodio:** La organización que administra o controla los datos; será útil referirse a un programa específico (en lugar de a una persona).

Apéndice 8

Ejemplo de formulario de reporte de ocurrencia en vuelo (obligatorio)

<table>
<tr><td>LOGOTIPO</td><td colspan="3">REPORTE DE EVENTO EN VUELO</td><td>CÓDIGO
F-</td><td>VIGENCIA
XX/XX/XXXX
REVISIÓN
0</td></tr>
<tr><td>Clasificación:</td><td colspan="3">☐ Técnica</td><td colspan="2">☐ Operacional</td></tr>
<tr><td colspan="6">Identificación de la aeronave</td></tr>
<tr><td>Aeronave</td><td>Modelo</td><td colspan="2">Matrícula</td><td colspan="2">Horas de vuelo</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="6">Circunstancias</td></tr>
<tr><td>Fecha:</td><td colspan="3">Lugar:</td><td colspan="2">Observaciones:</td></tr>
<tr><td colspan="6">Seleccionar la categoría apropiada</td></tr>
<tr><td colspan="3">Fase de vuelo:</td><td>Condiciones de vuelo:</td><td colspan="2">Misión:</td></tr>
<tr><td colspan="3">□ Carreteo
□ Inspección pre-vuelo
□ Abastecimiento combustible
□ Puesta en marcha
□ Rodaje
□ Despegue
□ Subida < 500ft
□ Subida > 500ft
□ Travesía
□ Maniobra
□ Descenso
□ Aproximación
□ Aterrizaje
□ Parada de motor
□ Inspección post-vuelo</td><td>□ VFR
□ IFR
□ Día
□ Noche</td><td colspan="2">□ Instrucción
□ Vuelo solo
□ Pre-chequeo</td></tr>
<tr><td colspan="6">Documentos utilizados</td></tr>
<tr><td colspan="3">Referencia del manual de vuelo:</td><td colspan="3">Revisión:</td></tr>
<tr><td colspan="6">Condiciones de vuelo</td></tr>
<tr><td colspan="6">Condiciones meteorológicas:</td></tr>
</table>

<table>
<tr><th colspan="2">Descripción de la ocurrencia</th></tr>
<tr><td colspan="2">Explicar cómo ocurrió el evento, por qué ocurrió y por qué no resultó en un accidente:</td></tr>
<tr><td>Acciones de alumno en instrucción o de instructor para gestionar el evento.</td><td></td></tr>
<tr><td>Propuestas para prevenir que el evento vuelva a ocurrir o para evitar que tal evento resulte en un accidente.</td><td></td></tr>
<tr><th colspan="2">Retroalimentación al reportante</th></tr>
<tr><td colspan="2"></td></tr>
<tr><th colspan="2">Firmas</th></tr>
<tr><td>Reportante: (nombre y firma)</td><td>Responsable del SMS: (nombre y firma)</td></tr>
</table>

Nota.- *Dependiendo del tamaño y complejidad de la organización este formulario puede variar incorporando otros ítems.*

Apéndice 9
Ejemplo de formulario de reporte de evento de mantenimiento

LOGOTIPO	REPORTE DE EVENTO DE MANTENIMIENTO	CÓDIGO	VIGENCIA
		F-	XX/XX/XXXX
			REVISIÓN
			0

Identificación de la aeronave			
Tipo de aeronave	**Modelo**	**Matrícula**	**Horas de vuelo**

Circunstancias		
Fecha:	Lugar:	Fase de mantenimiento:

Seleccionar la categoría correspondiente

Fase de mantenimiento:

□ Mantenimiento programado
□ Mantenimiento no programado
□ Reparación
□ Inspección post-vuelo
□ Remolque
□ Abastecimiento de combustible
□ Inspección pre-vuelo

Condiciones de mantenimiento

Seleccionar el área relevante (Capítulo ATA)

□ 21	Sistema de aire acondicionado	□ 52	Puertas y cubiertas de protección
□ 22	Automatic pilot	□ 53	Fuselaje
□ 23	Sistema de comunicación	□ 55	Estabilizador
□ 24	Sistema eléctrico	□ 56	Parabrisas y ventanas
□ 25	Equipamiento, mobiliario	□ 62	Motor principal
□ 26	Sistema de protección de incendio	□ 67	Controles de vuelo
□ 28	Sistema de combustible	□ 71	Planta motriz
□ 29	Sistema hidraúlico	□ 72	Turbina motor
□ 30	Protección contra lluvia y hielo	□ 73	Sistema de combustible del motor
□ 31	Sistema de grabación e información		
□ 32	Tren de aterrizaje	□ 74	Sistema de ignición
□ 33	Luces/lámparas	□ 76	Control de motor
□ 34	Sistema de navegación/datos de vuelo	□ 77	Indicadores de motor
		□ 79	Sistema de lubricación del motor
□ 36	Sistema neumático	□ 80	Sistema de arranque del motor
□ 39	Equipamiento y panel eléctrico/electrónico	□ 81	Turbo cargado
		□ 82	Inyección de agua
□ 45	Sistema de centralización de mantenimiento	□ 83	Caja de accesorios
		□ 85	Equipamiento opcional
□ 46	Sistema de integración de pantallas	□ 88	Arnés eléctrico.
□ 49	Sistema externo de generación de Energía		

<table>
<tr><td rowspan="2">Ensamblaje(s) o componente(s) relevantes</td><td>Descripción N° Parte</td><td>Tipo de operación</td><td colspan="3">Documentación de mantenimiento utilizada</td></tr>
<tr><td></td><td></td><td>Tipo Ref:</td><td>Rev. Nro:</td><td>Versión:</td></tr>
<tr><td colspan="6">Descripción de la ocurrencia</td></tr>
<tr><td colspan="6">Explicar cómo sucedió el evento, por qué ocurrió y por qué no resultó en un accidente:</td></tr>
<tr><td>Acciones tomadas por el staff de mantenimiento (u otra parte que maneja el evento).</td><td colspan="5"></td></tr>
<tr><td>Propuestas de prevención para que el evento no vuelva a ocurrir o para evitar que tal evento resulte en un accidente.</td><td colspan="5"></td></tr>
<tr><td colspan="6">Retroalimentación al reportante</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">Firmas</td></tr>
<tr><td colspan="3">Reportante: (nombre y firma)</td><td colspan="3">Gerente del SMS: (nombre y firma)</td></tr>
</table>

Nota. - *Dependiendo del tamaño y complejidad de la organización este formulario puede variar incorporando otros ítems.*

Apéndice 10

Modelo de formulario de acción de seguimiento de evento

<table>
<tr><td rowspan="2">LOGOTIPO</td><td colspan="3" rowspan="2">FORMULARIO DE ACCIÓN DE SEGUIMIENTO AL EVENTO</td><td>CÓDIGO</td><td>VIGENCIA</td></tr>
<tr><td rowspan="2">F-</td><td>XX/XX/XXXX</td></tr>
<tr><td></td><td>REVISIÓN</td></tr>
<tr><td>Reporte de evento en vuelo No.:</td><td></td><td>Reporte de evento de mantenimiento No.:</td><td></td><td>Reporte voluntario No.:</td><td>0</td></tr>
<tr><td colspan="6">1. Análisis preliminar</td></tr>
<tr><td colspan="3">Realizado por:</td><td colspan="3">Fecha: Día/mes/año</td></tr>
<tr><td colspan="6">a) Evento (Resumen de los hechos):</td></tr>
<tr><td colspan="6">b) Razones por las cuales ocurrió el evento – Barreras de seguridad que fallaron o quedaron inoperativas</td></tr>
<tr><td colspan="6">c) Razones por las cuales no resultó en un accidente – Barreras de seguridad que estuvieron operativas:</td></tr>
<tr><td colspan="6">Clasificación del evento utilizando la matriz de riesgo (marcar con X)</td></tr>
<tr><td colspan="2">Aceptable</td><td colspan="2">Tolerable</td><td colspan="2">Inaceptable</td></tr>
<tr><td colspan="6">2. Análisis adicional por la junta de revisión de seguridad operacional o el grupo de acción de seguridad operacional (Si el riesgo no es aceptable)</td></tr>
<tr><td colspan="6"></td></tr>
</table>

Validado por:	**Fecha:**

3. Acciones correctivas

No.	Acción	Responsable	Inicio	Cierre	Comentarios

4. Cierre del evento

Retroalimentación transmitida al personal interesado:

Gerente del SMS:	Firma:	Fecha: Día/mes/año

Nota. - *Dependiendo del tamaño y complejidad de la organización este formulario puede variar incorporando otros ítems.*

Apéndice 11

Ejemplo de formulario para la gestión del cambio

LOGOTIPO	FORMULARIO PARA LA GESTIÓN DE CAMBIOS	CÓDIGO	VIGENCIA
		F-	XX/XX/XXXX
			REVISIÓN
			0

1. ¿Cuál es el cambio?

(Describir el cambio y especificar si es permanente o temporal)

2. ¿Quién?

(Describir quién es el responsable o responsables de implementar el cambio)

3. Describir los componentes principales del cambio

(Esto le ayudará a identificar el riesgo principal de cada componente que se completará en la Sección 7)

4. ¿A quiénes afecta el cambio?

(Considerar que individuos, departamentos y organizaciones son afectados por el cambio)

5. ¿Cuál es el impacto del cambio?

(Considerar porque el cambio ha tenido lugar, el impacto en la organización y en sus procesos y procedimientos)

6. ¿Qué acción de seguimiento es necesaria? (aseguramiento)

(Considerar como el cambio será comunicado y si se necesitan actividades adicionales, tales como auditorías durante el cambio y después que se haya producido el cambio)

7. Problemas de seguridad y evaluación del riesgo

¿Cuál es el problema (peligro)	¿Qué podría suceder como resultado? (consecuencia)	¿Qué tan malo será? (gravedad)	¿Qué tan probable es que ocurra? (probabilidad)	Nivel de riesgo	¿Qué acción(es) serán tomadas? (mitigación)	Acción por quién y cuando
1.						
2.						
3.						
4.						

El cambio es aceptado para implementación: **Sí** ☐ **No** ☐

Firma de la persona autorizada	**Nombre:** **Fecha:**

Nota.- Dependiendo del tamaño y complejidad de la organización este formulario puede variar incorporando otros ítems.

Apéndice 12

Orientaciones de cumplimiento de requisitos del SMS en base al tamaño y complejidad del CIAC

1. De acuerdo a la Sección 14 de esta circular, se detalla a continuación algunos ejemplos respecto a diferencias y similitudes que pueden ser aceptables por la AAC para el cumplimiento de los requisitos del SMS (componentes y elementos), conforme a la categorización de los CIAC que se detalla en la **Tabla 1** de esta circular.

2. Los siguientes ejemplos no abarcan todos los requisitos que debe cumplir el CIAC, dado que las orientaciones para su cumplimiento se detallan con mayor amplitud en el cuerpo de esta circular.

Tabla 12.1. Ejemplos de cumplimiento de los requisitos de políticas y objetivos de seguridad operacional

<table>
<tr><th colspan="4">1. Políticas y objetivos de seguridad operacional</th></tr>
<tr><th rowspan="2">Elementos</th><th colspan="3">Tamaño de la organización</th></tr>
<tr><th>Pequeña</th><th>Mediana</th><th>Grande</th></tr>
<tr><td rowspan="3">Compromiso de la administración</td><td colspan="3">La política de seguridad operacional debe estar documentada, firmada por el gerente responsable y comunicada a toda la organización.</td></tr>
<tr><td colspan="3">Objetivos y metas de seguridad operacional documentados.</td></tr>
<tr><td>Métodos formales o informales para revisar regularmente los objetivos desarrollados.</td><td>Métodos formales para revisar los objetivos desarrollados.</td><td>Métricas para el cumplimiento de los objetivos desarrollados y revisados por la alta dirección.</td></tr>
<tr><td rowspan="3">Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional</td><td colspan="3">Gerente responsable con atribuciones establecidas para toma de decisiones, control de recursos y adopción de medidas adecuadas para resolución de problemas y riesgos de seguridad operacional.</td></tr>
<tr><td colspan="3">Definidas y documentadas las obligaciones de rendición de cuentas y responsabilidades.</td></tr>
<tr><td>N/A</td><td colspan="2">Métodos formales para medir si el personal ha cumplido con sus obligaciones de rendición de cuentas y responsabilidades (Ejm. KPIs).</td></tr>
<tr><td>Nombramiento de personal clave de seguridad operacional</td><td>Podría aceptarse que el gerente responsable, sea también el gerente del SMS, siempre que pueda demostrar a la AAC que reúne las calificaciones para ello.</td><td>Designación de gerente del SMS y de la junta de revisión de seguridad operacional (SRB)</td><td>Designación de gerente del SMS, de la junta de revisión de seguridad operacional (SRB) y del grupo de acción de seguridad operacional (SAG) en apoyo al gerente del SMS cuando corresponda.</td></tr>
</table>

1. Políticas y objetivos de seguridad operacional			
Elementos	**Tamaño de la organización**		
	Pequeña	**Mediana**	**Grande**
Coordinación de plan de respuesta ante emergencias	Guía de referencia rápida describiendo el plan de respuesta de emergencia básico y lista de personal u organizaciones involucradas.	Guía de referencia rápida con el resumen de los detalles críticos.	
	N/A	Manual detallado del plan de respuesta a la ante emergencias incluyendo las referencias de todo el personal del CIAC y organizaciones externas involucradas.	
	Ejercicios en mesa, donde el personal clave se reúne y avanza a través de un escenario, sin previo aviso a los involucrados.	Programar simulacros del plan de respuesta a emergencias y documentar ejercicios.	
Documentación del SMS	Manual del SMS que establezca las políticas y procedimientos para implementar los componentes y elementos del SMS.		
	Políticas y procedimientos formales de control de documentos implementados.		
	Persona designada para coordinar todas las actualizaciones y distribución de los documentos del SMS.	Equipo de personas designadas para coordinar todas las actualizaciones y distribución de los documentos del SMS.	

Tabla 12.2. Ejemplos de cumplimiento de los requisitos de gestión de riesgos de la seguridad operacional

2. Gestión de riesgos de la seguridad operacional			
Elementos	**Tamaño de la organización**		
	Pequeña	**Mediana**	**Grande**
Identificación de peligros	El CIAC definirá y mantendrá un proceso formal que garantice la identificación de los peligros asociados a sus productos y servicios.		
	Métodos informales o formales para identificar y registrar peligros (Ejm. registro simple de peligros o riesgos).	Métodos y herramientas formales para identificar peligros, como un registro de peligros que se mantiene regularmente.	
	Sistema formal y a disposición del personal para reportar ocurrencias, riesgos y problemas de seguridad.		
	Al menos un canal para la presentación de notificaciones (por ejemplo: en papel, electrónico o ambos).		

<table>
<tr><th colspan="4">2. Gestión de riesgos de la seguridad operacional</th></tr>
<tr><th rowspan="2">Elementos</th><th colspan="3">Tamaño de la organización</th></tr>
<tr><th>Pequeña</th><th>Mediana</th><th>Grande</th></tr>
<tr><td rowspan="4"></td><td colspan="3">Confidencialidad aplicable a las notificaciones de seguridad operacional.</td></tr>
<tr><td>Capacidad para proporcionar retroalimentación a los que notifican (aunque de manera informal).</td><td colspan="2">Procesos formales para proporcionar retroalimentación al personal que emite notificaciones.</td></tr>
<tr><td>Hoja en Excel de registro de notificaciones y resultado de evaluación.</td><td>Implementación y mantenimiento de una base de datos de notificaciones de seguridad operacional con la capacidad para revisar notificaciones individuales</td><td>Implementación y mantenimiento de una base de datos de notificaciones de seguridad operacional con la capacidad para revisar notificaciones individuales, proporcionando datos de tendencias, con apoyo de investigaciones de seguridad operacional y auditorías.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="2">Evaluación y mitigación de riesgos de seguridad operacional</td><td colspan="3">El CIAC definirá y mantendrá un proceso que garantice el análisis, la evaluación y el control de los riesgos de seguridad operacional asociados a los peligros identificados.</td></tr>
<tr><td colspan="2">Todo el personal responsable de la instrucción de vuelo capacitado en cómo llevar a cabo una evaluación del riesgo.</td><td>Capacitación sobre los principios y procesos de gestión de riesgos provistos a nivel de toda la organización</td></tr>
</table>

Tabla 12.3. Ejemplos de cumplimiento de los requisitos de aseguramiento de la seguridad operacional

<table>
<tr><th colspan="4">3. Aseguramiento de la seguridad operacional</th></tr>
<tr><th rowspan="2">Elementos</th><th colspan="3">Tamaño de la organización</th></tr>
<tr><th>Pequeña</th><th>Mediana</th><th>Grande</th></tr>
<tr><td rowspan="4">Observación y medición del rendimiento en materia de seguridad</td><td colspan="3">El CIAC deberá contar con Indicadores de rendimiento de seguridad operacional, los cuales serán monitoreados y rastreados regularmente para su logro.</td></tr>
<tr><td>N/A</td><td>El CIAC utilizará metodologías de análisis consistentes.</td><td>El CIAC utilizará metodologías formales y avanzadas de análisis de datos de seguridad operacional.</td></tr>
<tr><td colspan="3">El CIAC debe desarrollar un enfoque de auditoría basado en riesgos.</td></tr>
<tr><td>Personal capaz de llevar a cabo auditorías de seguridad operacional en forma regular (o por personal externo).</td><td>Auditoría de seguridad operacional llevada a cabo por el gerente del SMS delegado.</td><td>Personal especializado para realizar auditorías de seguridad (Este personal puede ser el gerente de sistemas de seguridad, el personal de gestión de calidad, etc.).</td></tr>
<tr><td>Gestión del cambio</td><td>El CIAC evaluará los riesgos respecto a los cambios significativos de la organización, por ejemplo un nuevo aeródromo a utilizar.</td><td colspan="2">El CIAC desarrollará un plan de gestión de riesgos respecto a diversos cambios de la organización y monitoreo hasta su finalización.</td></tr>
<tr><td rowspan="2">Mejora continua del SMS</td><td>El CIAC debe establecer y monitorear los indicadores de rendimiento, auditado su SMS y desarrollar un plan de acción simple para la implementación de acciones correctivas y preventivas.</td><td colspan="2">El CIAC debe tener un proceso formal y regular para asegurarse que dispone de un SMS eficaz y gestiona sus riesgos a través de la auditoria, la medición y monitoreo de su rendimiento, dando lugar a un plan de acción actualizado.</td></tr>
<tr><td>Seguimiento de los resultados de la auditoría.</td><td colspan="2">Procesos formales para el seguimiento de las no-conformidades de la auditoría y las acciones correctivas.</td></tr>
</table>

Tabla 12.4. Ejemplos de cumplimiento de los requisitos de promoción de la seguridad operacional

<table>
<tr><th colspan="4">4. Promoción de la seguridad operacional</th></tr>
<tr><th rowspan="2">Elementos</th><th colspan="3">Tamaño de la organización</th></tr>
<tr><th>Pequeña</th><th>Mediana</th><th>Grande</th></tr>
<tr><td rowspan="2">Instrucción y educación</td><td colspan="3">El CIAC desarrollará un programa de instrucción de SMS formal y documentado, que incluya como mínimo al gerente responsable, gerente del SMS y personal crítico para las actividades de instrucción en vuelo.</td></tr>
<tr><td>El CIAC tendrá un programa de capacitación de seguridad operacional general, con instrucción especial para el gerente del SMS.</td><td colspan="2">El CIAC desarrollará un análisis formal de las necesidades de capacitación para determinar la naturaleza y el alcance del programa de instrucción de seguridad operacional.</td></tr>
<tr><td rowspan="2">Comunicación de la seguridad operacional</td><td colspan="3">El CIAC desarrollará reuniones informativas periódicas para el personal, basadas en el alcance de sus responsabilidades.</td></tr>
<tr><td>El CIAC tendrá establecida una estructura de la comunicación de seguridad operacional, que permita que la información se transmita a todo el personal.</td><td>El CIAC tendrá un sistema formal de promoción y comunicación de la seguridad operacional.</td><td>El CIAC tendrá un sistema formal de promoción y comunicación de la seguridad operacional y estrategias establecidas para monitorear constantemente su eficacia.</td></tr>
</table>

Apéndice 14

Ejemplo de herramienta para la evaluación del SMS y desarrollo del plan de implementación

1. Introducción

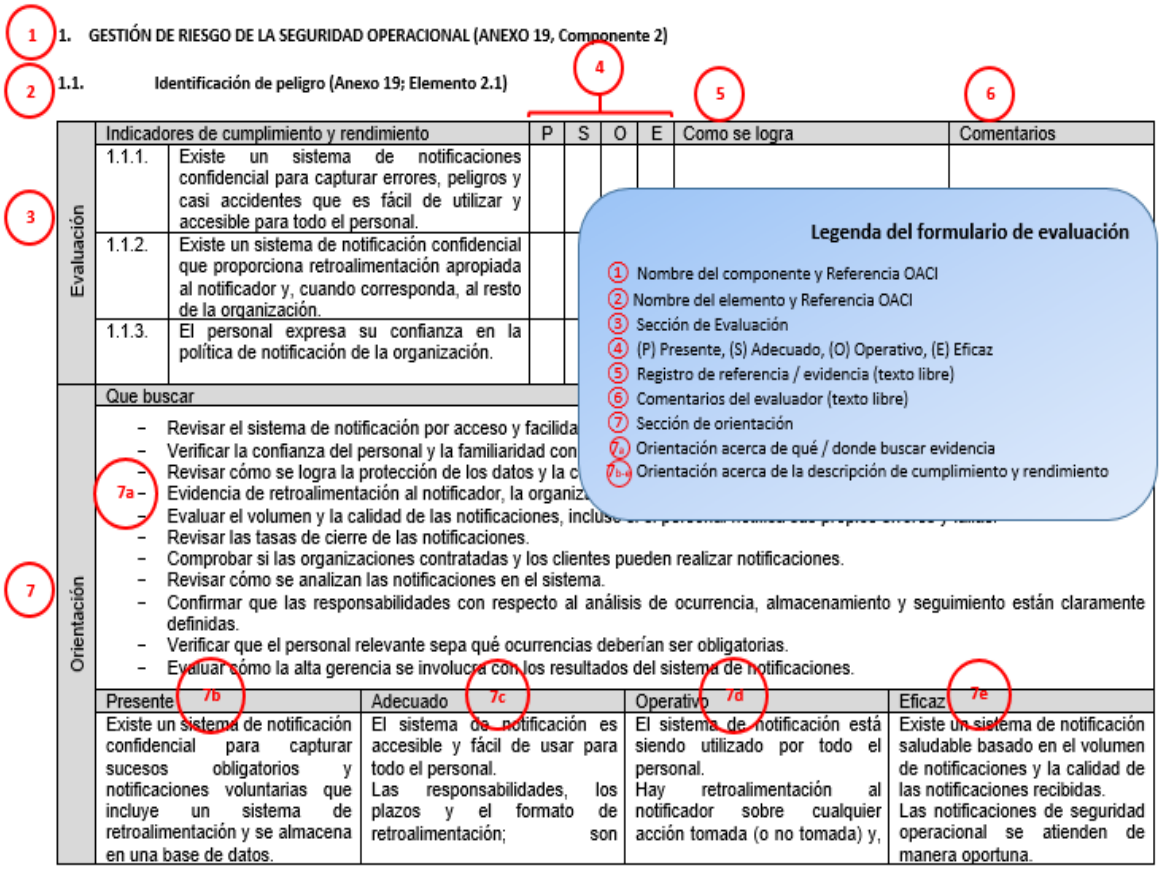
1.1 Este ejemplo de herramienta ha sido elaborada por el Comité Técnico (CT) del SRVSOP en base al documento editado por el Grupo de colaboración internacional para la gestión de la seguridad operacional / Safety Management International Collaboration Group (SM ICG).

1.2 Aunque la herramienta de evaluación sigue el marco SMS del Anexo 19, se ha cambiado el orden de los componentes para empezar con la gestión de riesgos de la seguridad operacional. Este es considerado el componente más importante del SMS de un CIAC y, por lo tanto, debe recibir la mayor atención durante la evaluación. Además, se ha añadido una sección dedicada a la gestión de interfaces, para reflejar el Anexo 19.

1.2 Al momento de aplicar esta herramienta, el postulante a una certificación o el CIAC certificado, pueden optar por individualizar el orden de los componentes para alinearlos con el orden del Anexo 19.

1.3 A continuación se describe una figura que refleja los componentes de la herramienta de evaluación e indicaciones para su correcto llenado.

Figura AP13.1 - Herramienta de evaluación el SMS



Definiciones utilizadas en la herramienta

Presente (P): 4 7b Hay evidencia que el indicador pertinente esté documentado dentro de la documentación SMS del CIAC.

Adecuado (S): 4 7c El indicador pertinente es adecuado en base al tamaño, naturaleza y

complejidad del CIAC y el riesgo inherente a su actividad.

Operativo (O): 4 7d Hay evidencia que el indicador está siendo utilizado y se está generando un resultado.

Eficaz (E): 4 7e Hay evidencia que el indicador pertinente está logrando el resultado deseado y tiene un impacto positivo en la seguridad operacional.

Generalmente, los términos *presente* y *adecuado* se utilizan para una aprobación o certificación inicial. *Operativo* y *eficaz* se utilizan al encontrar un SMS en funcionamiento.

Un elemento no puede ser considerado *operativo* o *eficaz* si no está *presente* y no puede ser considerado *presente* si no está documentado. La documentación asegura resultados consistentes, repetibles y sistemáticos.

Qué buscar: 7a Esta sección guía al evaluador al momento de analizar cada característica individual y no pretende ser una lista de verificación. Los puntos enumerados no son específicos para un nivel individual de *presente*, *adecuado*, *operativo* o *eficaz*, pero recuerda al evaluador las áreas que podría considerar. Algunos elementos de esta columna pueden no ser relevantes dependiendo del tamaño, tipo o naturaleza del CIAC.

2. Nivel de detalle a ser registrado

2.1 Es importante que quien realiza la evaluación registre las evidencias de cumplimiento correspondiente. Las evidencias incluyen documentación, informes y registros de entrevistas y discusiones. Por ejemplo, para que un elemento sea designado *presente*, es probable que la evidencia sólo esté documentada en el manual del SMS, mientras que para que un elemento sea designado *operativo*, la evaluación puede involucrar la evaluación de los registros que evidencien la implementación.

2.2 Para la evaluación inicial o como parte de una transición a los nuevos requisitos del SMS, todos los procesos deben ser *presentes* y *adecuados*. Si no es así, el CIAC deberá definir los faltantes para poder completarlos antes de la presentación de la solicitud formal.

3. El puntaje en la evaluación del SMS

3.1 El objetivo principal de esta herramienta es contribuir a la evaluación del SMS en términos de madurez y eficacia de una manera consistente.

3.2 Con esta herramienta, los CIAC podrán evaluar el cumplimiento de los componentes y elementos del marco de trabajo del SMS, distribuidos en cuarenta y siete (47) indicadores de cumplimiento y rendimiento que permiten determinar el nivel de madurez de los procesos del SMS.

3.3 Se aplicará un sistema de puntaje ponderado que expresa de manera lógica el estado de madurez de los procesos del SMS. Para cada indicador según su importancia en la madurez del SMS, se asignarán las siguientes ponderaciones: 0.5 baja, 1 moderada, 1.5 alta y 2 muy alta.

3.4 Para los niveles de madurez expresados como presente (P), adecuado (S), operativo (O) y eficaz (E), se asignarán valores aritméticos de 1, 2, 3 y 4 respectivamente. Una vez que se determine el nivel de madurez para cada indicador de cumplimiento y rendimiento, los valores aritméticos asignados se sumarán y multiplicarán por la ponderación. Asimismo, el resultado de cada indicador se totalizará en la sumatoria aritmética, resultando en una puntuación total.

Ejemplo de resumen de la evaluación

	Inicio	Presente y Adecuado	Operativo	Eficaz
El SMS como un todo	El SMS se encuentra en etapa de implementación.	Todos los elementos principales del SMS han sido establecidos.	Los sistemas y procesos del SMS están operativos.	El SMS funciona de manera eficaz y se hace esfuerzos por su mejora continua.
Gestión del riesgo de seguridad operacional	Los procesos para la gestión del riesgo de la seguridad operacional no se encuentran plenamente desarrollados.	Existe un sistema de información sobre seguridad operacional, así como un proceso para evaluar y gestionar los riesgos.	Se están creando registros de peligros y riesgos, y se está empezando a gestionar los riesgos de manera proactiva.	El CIAC identifica continuamente los peligros y es consciente de sus mayores riesgos y los gestiona activamente; esto se puede ver en su rendimiento en materia de seguridad operacional. La gestión de los riesgos de la seguridad operacional es proactiva.
Aseguramiento de la seguridad operacional	Las actividades de seguridad operacional, incluyendo los indicadores de rendimiento en materia de seguridad operacional (SPI) no se encuentran plenamente desarrollados.	Se han identificado los SPI iniciales relacionados con los objetivos de seguridad operacional y existe un proceso de gestión del cambio.	El CIAC ha establecido SPI, los cuales está supervisando, y está auditando y evaluando el SMS y sus resultados.	El CIAC se asegura de disponer de un SMS eficaz y gestiona sus riesgos mediante la auditoría, la evaluación y el seguimiento de su rendimiento en materia de seguridad operacional.
Políticas y objetivos en materia de seguridad operacional	Las políticas, los procesos y los procedimientos no se encuentran plenamente desarrollados.	Existen políticas, procesos y procedimientos que detallan cómo funcionará el SMS.	Existe una política sobre seguridad operacional y la alta dirección se ha comprometido en hacer que el SMS funcione y está proporcionando los recursos adecuados para la gestión de la seguridad operacional.	La alta dirección está claramente comprometida con el SMS y la política de seguridad operacional establece la voluntad del CIAC de gestionar la seguridad operacional. Esto es claramente evidente en las operaciones diarias.

	Inicio	Presente y Adecuado	Operativo	Eficaz
Promoción de la seguridad operacional	Las actividades relacionadas con la promoción de la seguridad operacional no se encuentran plenamente desarrolladas.	Existe un programa de instrucción, así como medios para comunicar la información sobre seguridad operacional.	El CIAC ha instruido a su personal y cuenta con varios medios para la promoción de la seguridad operacional, que utiliza para transmitir información sobre seguridad operacional.	El CIAC dedica considerables recursos y esfuerzos a la instrucción de su personal y a la divulgación de su cultura sobre seguridad operacional, así como cualquier otra información sobre seguridad operacional, y supervisa la eficacia de su promoción de la seguridad operacional.
Gestión de los recursos humanos	Los factores humanos son tomados en cuenta, pero no reflejados formalmente por el CIAC.	Las políticas y procesos sobre factores humanos han sido definidos y documentados en los casos en que así lo requiere la reglamentación.	Los factores humanos se están gestionando en todo el CIAC y están empezando a incluirse en el SMS del CIAC.	Los factores humanos están incorporados en el SMS y en las operaciones del CIAC. Todo el personal, incluida la dirección, es consciente de los factores humanos y los aplica en su forma de trabajar.

Nota.- *También se ha añadido una línea específica para factores humanos en este ejemplo, para resaltar la importancia de considerarlos como parte del SMS.*

Apéndice B – Herramienta para la evaluación del SMS

Centro de instrucción:	**Responsable de evaluación del CIAC:**
Revisión del SMS o del Manual SM:	**Fecha de evaluación**

Índice

B1 Gestión de riesgos de la seguridad operacional (Anexo 19, Componente 2)

B1.1 Identificación de peligros (Anexo 19, Elemento 2.1)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
1.1.1	Existe un sistema de notificación confidencial, que captura los errores, peligros y cuasicolisiones, que es fácil de usar y accesible a todo el personal.					2			
1.1.2	El sistema de notificación confidencial brinda retroalimentación a la persona que notifica sobre las medidas adoptadas (o no adoptadas) y, cuando sea adecuado, al resto del CIAC					1.5			
1.1.3	El personal expresa su confianza en la política y en los procesos de notificación del CIAC					1			

Orientación

¿Qué buscar?

- Revisar el sistema de notificación para verificar si es accesible y fácil de usar.
- Verificar la confianza y familiaridad del personal con el sistema de notificación, y si saben lo que se debe informar.
- Revisar cómo se logra la protección de datos y la confidencialidad.
- Evidencia de retroalimentación a la persona que notifica, al CIAC y a terceros.
- Evaluar el volumen y la calidad de las notificaciones, incluyendo si el personal está notificando sus propios errores y equivocaciones.
- Revisar las tasas de cierre de las notificaciones.
- Verificar si las organizaciones contratadas y los clientes son capaces de emitir notificaciones.
- Revisar cómo se analizan los informes en el sistema.
- Verificar que las responsabilidades con respecto al análisis de ocurrencias, almacenamiento y seguimiento estén claramente definidas.
- Verificar que el personal pertinente es consciente de los sucesos que deberían ser obligatorios.
- Evaluar cómo se relaciona la alta dirección con los productos del sistema de notificación.

Presente	Adecuado	Operativo	Eficaz
• Existe un sistema de notificación confidencial para capturar los sucesos obligatorios y las notificaciones voluntarias que incluye un sistema de retroalimentación y se almacena en una base de datos. • El proceso identifica la forma en que se actúa sobre las notificaciones y específica y aborda cronogramas.	• El sistema de notificación es accesible y fácil de usar para todo el personal. • Las responsabilidades, cronogramas y el formato de retroalimentación son pertinentes y están bien definidos. • La protección y confidencialidad de los datos están garantizadas.	• El sistema de notificación está siendo utilizado por todo el personal. • Se retroalimenta a la persona que notifica acerca de cualquier medida adoptada (o no adoptada) y, de ser el caso, al resto del CIAC. • Las notificaciones son evaluadas, procesadas, analizadas y almacenadas. • El personal conoce y cumple con sus responsabilidades con respecto al sistema de notificación. • Las notificaciones son procesadas dentro de los cronogramas definidos.	• Existe un sistema saludable de notificación basado en el volumen de notificaciones y la calidad de las notificaciones recibidas. • Las notificaciones de seguridad operacional son atendidas a tiempo. • El personal expresa confianza en la política y el proceso de notificación del CIAC. • El sistema de notificación se utiliza para tomar mejores decisiones de gestión y para la mejora continua. • El sistema de notificación está disponible para que terceros (socios, proveedores y contratistas) puedan notificar.

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	
1.1.4	Existe un proceso que define cómo se identifica peligros de múltiples fuentes utilizando métodos reactivos y proactivos (internos y externos).					2			
1.1.5	El proceso de identificación de peligros identifica los peligros relacionados con la actuación humana.					2			
1.1.6	Existe un proceso para analizar los datos y la información sobre seguridad operacional para buscar tendencias y obtener información de gestión utilizable.					2			
1.1.7	Las investigaciones sobre seguridad operacional son realizadas por personal debidamente capacitado para identificar las causas de fondo (no sólo lo que sucedió, sino por qué sucedió).					2			

Orientación

¿Qué buscar?

- Revisar cómo los peligros son identificados, analizados, abordados y registrados.
- Revisar la estructura y el diseño del registro de peligros.
- Considerar los peligros relacionados con:
  - Posibles escenarios de accidentes;
  - Factores humanos y organizacionales;
  - Decisiones y procesos de negocio;
  - Organizaciones de terceros; y
  - Factores reglamentarios.
- Analizar qué fuentes internas y externas de peligros son tomadas en cuenta, tales como notificaciones de seguridad operacional, auditorías, encuestas de seguridad operacional, investigaciones, inspecciones, tormenta de ideas, actividades de gestión del cambio, influencias comerciales y otras influencias externas, etc.
- Revisar si las investigaciones sobre seguridad operacional identifican los factores humanos y organizacionales contribuyentes.

Presente	Adecuado	Operativo	Eficaz
• Existe un proceso que define cómo son identificados los peligros mediante métodos reactivos y proactivos. • Se identifican los desencadenantes de las investigaciones de seguridad operacional.	• Se considera y revisa múltiples fuentes de peligros (internos y externos), según corresponda. • El proceso de análisis de datos permite obtener información de seguridad operacional útil. • Los peligros se documentan en un formato fácil de entender. • El nivel de aprobación de las investigaciones de seguridad operacional está definido y es adecuado al nivel de riesgo.	• Los peligros son identificados y documentados. Se están identificando los factores humanos y organizacionales relacionados con los peligros. • Se lleva a cabo y se registra las investigaciones de seguridad operacional.	• El CIAC tiene un registro de los peligros, el cual es mantenido y revisado para asegurar que se mantenga actualizado. Identifica de forma continua y proactiva los peligros relacionados con sus actividades y el entorno operativo e involucra a todo el personal clave y a las partes interesadas apropiadas, incluidas las organizaciones externas. • Los peligros son evaluados continuamente en forma sistemática y oportuna. • Las investigaciones de seguridad operacional identifican los factores causales/contribuyentes sobre los que se actúa.

B1.2 Evaluación y mitigación de los riesgos de seguridad operacional (Anexo 19, Elemento 2.2)

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	1.2.1	Existe un proceso para la gestión de riesgos que incluye el análisis y evaluación de los riesgos asociados con los peligros identificados, expresado en términos de probabilidad y gravedad (o alguna metodología alternativa).					2			
	1.2.2	Hay criterios para evaluar el nivel de riesgo que el CIAC está dispuesta a aceptar, y las evaluaciones y clasificaciones de riesgos están debidamente justificadas					2			

Orientación

¿Qué buscar?

- Revisar el esquema y los procedimientos de clasificación de riesgos.
- Verificar que se definan criterios de probabilidad y gravedad (o que se describa una metodología alternativa).
- Verificar si las evaluaciones de riesgos se llevan a cabo de forma coherente.
- Hacer un muestreo de un peligro identificado y analizar cómo es procesado y documentado.
- Revisar lo que desencadena una evaluación de riesgos.
- Verificar los supuestos y si éstos son revisados.
- Revisar cómo se clasifican los problemas cuando no se dispone de datos cuantitativos suficientes.
- Verificar que el proceso defina quién puede aceptar qué nivel de riesgo.
- Verificar que el registro de riesgos está siendo revisado y supervisado por el comité o comités de seguridad operacional correspondientes.
- Evidencia de que la aceptabilidad del riesgo se aplica rutinariamente en los procesos de toma de decisiones.

Presente	Adecuado	Operativo	Eficaz
• Existe un proceso para el análisis y la evaluación de los riesgos de seguridad operacional. • Se ha definido el nivel de riesgo que el CIAC está dispuesto a aceptar.	• Los criterios de probabilidad y gravedad están claramente definidos y se ajustan a las circunstancias reales del proveedor de servicios. • La matriz de riesgos y los criterios de aceptabilidad están claramente definidos y son utilizables. • Las responsabilidades y los plazos para aceptar el riesgo están claramente definidos.	• El análisis y las evaluaciones de riesgos se llevan a cabo de manera coherente sobre la base del proceso definido. • Se está aplicando la aceptabilidad definida del riesgo.	• Los análisis y evaluaciones de riesgos son revisados para asegurar la coherencia y para identificar las mejoras en los procesos. • Las evaluaciones de riesgos son revisadas periódicamente para asegurar que se mantienen actualizadas. • Los criterios de aceptabilidad del riesgo son utilizados de forma rutinaria, son aplicados en los procesos de toma de decisiones de la gerencia y son revisados periódicamente.

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
1.2.3	El CIAC cuenta con un proceso para tomar decisiones y aplicar controles de riesgo adecuados y eficaces.					2			
1.2.4	La alta gerencia tiene visibilidad de los peligros cuyo riesgo asociado es alto o medio, así como de su mitigación y control.					1.5			

Orientación

¿Qué buscar?

- Verificar que los controles de riesgo contemplen los factores humanos y organizacionales.
- Evidencia que se están tomando medidas respecto a los controles de riesgo y se hace el seguimiento respectivo.
- Se está considerando el riesgo agregado.
- Verificar si los controles del riesgo han reducido el riesgo residual.
- Los controles del riesgo están claramente identificados.
- Verificar el uso de controles de riesgos que se basan únicamente en la intervención humana.
- Verificar que los nuevos controles de riesgos no generen riesgos adicionales.
- Verificar si la aceptabilidad de los riesgos se realiza en el nivel de gestión adecuado.

Presente	Adecuado	Operativo	Eficaz
• El CIAC cuenta con un proceso para decidir y aplicar controles de riesgo.	• Se definen las responsabilidades y los plazos para determinar y aceptar los controles de riesgo.	• Se están aplicando controles de riesgo apropiados para reducir el riesgo a un nivel aceptable, incluidos plazos y asignación de responsabilidades. • Los factores humanos son considerados como parte del desarrollo de los controles de riesgo.	• Los controles de riesgo son prácticos y sostenibles, se aplican de manera oportuna y no crean riesgos adicionales. • Los controles de riesgo tienen en cuenta los factores humanos.

B2 Aseguramiento de la seguridad operacional (Anexo 19, Componente 3)

B2.1 Observación y medición del rendimiento en materia de la seguridad operacional (Anexo 19, Elemento 3.1)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
2.1.1	Los indicadores de rendimiento en materia de seguridad operacional (SPI) relacionados con los objetivos de seguridad operacional del CIAC han sido definidos, promulgados y son observados y analizados para buscar tendencias					2			

Orientación

¿Qué buscar?

- Evidencia que los SPI se basan en fuentes de datos confiables.
- Evidencia de cuándo se revisaron los SPI por última vez.
- Los SPI y metas definidas son apropiadas para las actividades, riesgos y objetivos del CIAC en materia de seguridad operacional.
- Los SPI se centran en lo que es importante y no en lo que es fácil de medir.
- Consideración de cualquier SPI estatal.
- Revisar si se ha tomado alguna acción cuando un SPI indica una tendencia negativa (que refleja un control de riesgo o un SPI inapropiado).
- Evidencia de que los resultados de la observación del rendimiento en materia de seguridad operacional son discutidos a nivel de la alta gerencia.
- Evidencia de retroalimentación proporcionada al ejecutivo responsable.

Presente	Adecuado	Operativo	Eficaz
• Existe un proceso para medir el rendimiento en materia de la seguridad operacional del CIAC, incluidos los SPI y las metas relacionadas con la seguridad operacional del CIAC, así como para medir la eficacia de los controles de riesgos en la seguridad operacional.	• Los SPI se centran en lo que es importante y no en lo que es fácil de medir. • La confiabilidad de las fuentes de datos se toma en consideración en el diseño de los SPI. • Los SPI están vinculados a los riesgos identificados y a los objetivos en materia de seguridad operacional. • La frecuencia y la responsabilidad del seguimiento de las tendencias de los SPI son adecuadas. • Se han establecido metas realistas. • Se consideran los SPI estatales, según corresponda.	• El rendimiento en materia de seguridad operacional del CIAC está siendo medido y los SPI significativos están siendo continuamente supervisados y analizados en busca de tendencias.	• Los SPI están demostrando el rendimiento en materia de seguridad operacional del CIAC y la efectividad de los controles de riesgo basados en datos confiables. • Los SPI son revisados y actualizados regularmente para asegurar que sigan siendo relevantes. • Cuando los SPI indican que un control de riesgos es ineficaz, se toman las medidas apropiadas.

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	2.1.2	Los controles y mitigaciones de los riesgos se verifican/auditan para confirmar que están funcionando y son eficaces.					2			
	2.1.3	El aseguramiento de la seguridad operacional toma en cuenta las actividades llevadas a cabo por todas las organizaciones directamente contratadas.					1.5			

Orientación

¿Qué buscar?

- Evidencia de que los controles de riesgo están siendo evaluados para determinar su eficacia (por ejemplo, auditorías, encuestas, revisiones, SPI y metas de rendimiento en materia de seguridad operacional [SPT], sistemas de notificación).
- Evidencia de los controles de riesgo aplicados por las organizaciones contratadas que están siendo evaluadas y supervisadas (por ejemplo, control de calidad, revisiones y reuniones regulares).
- La información procedente de las actividades de aseguramiento de la seguridad operacional y supervisión del cumplimiento se incorpora al proceso de gestión de riesgos de la seguridad operacional.
- Revisar dónde se han modificado los controles de riesgo como resultado de la evaluación.

Presente	Adecuado	Operativo	Eficaz
• Existe un proceso para evaluar si los controles de riesgo son aplicados y son eficaces.	• Se definen las responsabilidades, los métodos y los plazos para evaluar los controles de riesgo. • Las organizaciones contratadas están incluidas en el proceso de aseguramiento de la seguridad operacional.	• Se están verificando los controles de riesgo para evaluar si se aplican y si son eficaces.	• Se evalúan los controles de riesgo y se toman medidas para garantizar que sean eficaces y que presten un servicio seguro.

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	2.1.4	Se define las responsabilidades y la obligación de rendición de cuentas para garantizar el cumplimiento de las normas de la seguridad operacional y se identifica claramente los requisitos aplicables en los manuales y procedimientos del CIAC.					1.5			
	2.1.5	Existe un programa de auditoría interna que incluye detalles sobre el calendario de auditorías, los procedimientos para las auditorías, la notificación, el seguimiento y los registros.					1.5			
	2.1.6	Se define las responsabilidades del proceso de auditoría interna y existe una persona o grupo de personas con responsabilidades de auditoría interna con acceso directo al gerente responsable.					1.5			

Orientación

¿Qué buscar?

- Revisar la forma en que la alta gerencia se asegura que el CIAC sigue cumpliendo la reglamentación.
- Revisar las descripciones de los puestos de trabajo en cuanto a las responsabilidades de cumplimiento.
- Evidencia de que la alta dirección toma medidas sobre los resultados de la auditoría interna y externa.
- Revisar cómo se logra la independencia de la función de auditoría interna.
- Revisar cómo interactúa la función de auditoría interna con:
  - La alta gerencia,
  - Los gerentes de línea, y
  - El personal de gestión de la seguridad operacional.
- Evaluar el contenido del programa en relación con cualquier requisito reglamentario.

Presente	Adecuado	Operativo	Eficaz
• Se define las responsabilidades de cumplimiento. • El CIAC tiene un programa de auditoría interna, así como procedimientos de auditoría, notificaciones y registros. • Se ha identificado a una persona o grupo de personas con responsabilidades de auditoría interna y tienen acceso directo al ejecutivo responsable.	• El programa de auditoría interna abarca todas las normas aplicables e incluye detalles del calendario de auditorías. • Se logra la independencia de la función de auditoría interna.	• El programa de vigilancia del cumplimiento se está siguiendo y revisando periódicamente. • Todo el personal es consciente de sus responsabilidades y obligaciones de rendición de cuentas en cuanto al cumplimiento y de seguir los procesos y procedimientos. • Los resultados de las auditorías internas y externas se comunican al ejecutivo responsable y al personal directivo superior.	• Los individuos están identificando e informando proactivamente sobre posibles incumplimientos. • El ejecutivo responsable y el personal directivo superior solicitan regularmente información sobre la situación de las actividades de auditoría interna y externa.

Evaluación	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
	2.1.7	Después de una auditoría, se realiza un análisis apropiado de los factores causales y se toman medidas correctivas/preventivas.					2			

Orientación

¿Qué buscar?

- Revisar los métodos utilizados para el análisis de las causas
- Compruebe que el método se utiliza de forma coherente.
- Revise cualquier hallazgo repetido y verifique si las acciones no han sido implementadas o están atrasadas.
- Verificar la implementación oportuna de las acciones.
- Revisar la comprensión de la alta gerencia sobre el estado de las constataciones significativas y las acciones correctivas/preventivas conexas.
- Verifique que el personal apropiado participe en la determinación de las causas y los factores contribuyentes.
- Buscar la coherencia entre los resultados de la auditoría interna y los resultados de la auditoría externa.
- Revisar si los factores causales se consideran como peligros potenciales.

Presente	Adecuado	Operativo	Eficaz
• Se define el proceso de identificación y seguimiento de las acciones correctivas/preventivas. • Se describe la interfaz entre las auditorías internas y los procesos de gestión de riesgos de la seguridad operacional.	• Se definen las responsabilidades y los plazos para determinar, aceptar y dar seguimiento a las medidas correctivas/preventivas. • El control del cumplimiento incluye las actividades contratadas.	• La identificación y el seguimiento de las medidas correctivas/preventivas se llevan a cabo de acuerdo con los procedimientos, incluido el análisis de causas para abordar la causa raíz. • El estado de las medidas correctivas/preventivas se comunica periódicamente a la alta gerencia y al personal pertinente.	• El CIAC investiga las causas sistémicas y los factores contribuyentes de las constataciones. • El CIAC revisa proactivamente el estado de las medidas correctivas/preventivas. • Se verifica la efectividad de las medidas correctivas/preventivas.

B2.2 La gestión del cambio (Anexo 19, Elemento 3.2)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
2.2.1	El CIAC cuenta con un proceso para identificar si los cambios tienen un impacto en la seguridad operacional, así como para gestionar los riesgos identificados de acuerdo con los procesos de gestión de riesgos de seguridad operacional existentes.					1.5			
2.2.2	Las cuestiones relativas a los factores humanos (HF) se han considerado como parte del proceso de gestión del cambio y, donde corresponde, el CIAC ha aplicado los requisitos de diseño adecuados, centrados en el factor humano, para el diseño de los equipos y el entorno físico.					1			

Orientación

¿Qué buscar?

- Las principales partes interesadas participan en el proceso.
- Revisar qué es lo que desencadena el proceso.
- Revisar los cambios recientes que se han producido durante el proceso de evaluación de riesgos.
- Comprobar que el cambio ha sido firmado por una persona debidamente autorizada.
- Se están identificando y gestionando los riesgos de tipo transicional.
- Verificar las acciones de seguimiento, por ejemplo, si se ha validado los supuestos.
- Verificar si hay un impacto en las evaluaciones de riesgos anteriores y en los peligros existentes.
- Revisar si se tiene en cuenta el efecto acumulativo de múltiples cambios.
- Revisar que los cambios relacionados con el negocio han considerado los riesgos de seguridad operacional (reestructuración organizacional, aumento o reducción de personal, proyectos de informática (IT), etc.).
- Evidencia de los problemas de factores humanos (HF) que se abordan durante los cambios.
- Revisar el impacto del cambio sobre la instrucción y las competencias.
- Revisar los cambios anteriores para confirmar que permanecen bajo control.
- Considerar cómo se comunican los cambios a las personas afectadas por el cambio.

Presente	Adecuado	Operativo	Eficaz
• El CIAC ha establecido un proceso de gestión del cambio para identificar si los cambios tienen un impacto en la seguridad operacional y para gestionar cualquier riesgo identificado de acuerdo con los procesos de gestión de riesgos de la seguridad operacional existentes.	• Se definen los desencadenantes del proceso de gestión de cambios. • El proceso también considera los cambios relacionados con el negocio y las interfaces con otras organizaciones/departamentos. • El proceso está integrado con los procesos de gestión de riesgos y de aseguramiento de la seguridad operacional. • Se definen las responsabilidades y los plazos.	• Se está utilizando el proceso de gestión del cambio, que incluye la identificación de peligros y la evaluación de riesgos, y se han establecido controles de riesgos adecuados antes de que se tome la decisión de introducir el cambio. • Las cuestiones relativas a los factores humanos (HF) han sido consideradas y abordadas como parte del proceso de gestión del cambio.	• El proceso de gestión del cambio se utiliza para todos los cambios que pueden afectar la seguridad operacional, incluidos los problemas de factores humanos (HF), y considera la acumulación de múltiples cambios. Se inicia de manera planificada, oportuna y coherente e incluye acciones de seguimiento que garantizan que el cambio se implementó de manera segura. • El cambio se comunica a los afectados. • Las estrategias de control y mitigación de riesgos asociadas con los cambios están logrando el efecto previsto.

B2.3 Mejora continua del SMS (Anexo 19, Elemento 3.3)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
2.3.1	El CIAC supervisa y evalúa continuamente sus procesos de SMS para mantener o mejorar continuamente la eficacia total del SMS.					1			

Orientación

¿Qué buscar?

- Revisar la información y los datos sobre la seguridad operacional utilizados para la toma de decisiones de gestión y la mejora continua.
- Evidencia de:
  - Incorporación de las lecciones aprendidas en el SMS y en los procesos operacionales;
  - Se busca y adopta mejores prácticas;
  - Encuestas y evaluaciones de la cultura organizacional que se están llevando a cabo y sobre las que se está actuando;
  - Se analizan los datos y se comparte los resultados con los Comités de Seguridad Operacional; y
  - Acciones de seguimiento.
- La información de sucesos externos, informes de investigación, reuniones de seguridad operacional, informes de riesgos, auditorías y análisis de datos de la seguridad operacional contribuyen a la mejora continua del SMS.

Presente	Adecuado	Operativo	Eficaz
• Existe un proceso para supervisar y revisar la eficacia del SMS utilizando los datos y la información disponibles.	• El SMS es revisado periódicamente, y la revisión se apoya en información sobre seguridad operacional y en actividades de aseguramiento de la seguridad operacional. • La alta gerencia y los diferentes departamentos están involucrados. • La toma de decisiones se basa en datos. • Se toma en consideración la información externa, además de la información interna.	• Hay evidencia de que el SMS está siendo revisando periódicamente para apoyar la evaluación de su eficacia, y que se están tomando las medidas adecuadas.	• La evaluación de la eficacia de los SMS utiliza múltiples fuentes de información, incluido el análisis de los datos de la seguridad operacional, que respalda las decisiones de mejora continua.

B3 Políticas y objetivos de la seguridad operacional (Anexo 19, Componente 1)

B3.1 Compromiso de gestión (Anexo 19, Elemento 1.1)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
3.1.1	Existe una política de seguridad operacional, firmada por el Gerente Responsable, que incluye un compromiso hacia la mejora continua; cumple con todos los requisitos y disposiciones legales aplicables; y toma en consideración las mejores prácticas.					0.5			
3.1.2	La política de seguridad operacional incluye una declaración para proporcionar los recursos adecuados, y el CIAC está gestionándolos con el objetivo de anticipar y subsanar cualquier deficiencia.					0.5			
3.1.3	Existen políticas establecidas para las funciones críticas de seguridad operacional, relacionadas con todos los aspectos de aptitud para el trabajo (por ejemplo, la política sobre alcohol y drogas o la fatiga).					1			

Orientación

¿Qué buscar?

- Entrevistar al ejecutivo responsable para evaluar su conocimiento y comprensión sobre la política de seguridad operacional.
- Verificar que la política de seguridad operacional es revisada periódicamente en cuanto a contenido y vigencia.
- Verificar que la política de seguridad operacional cumple los requisitos.
- Entrevistar al personal para determinar hasta qué punto se conoce la política de seguridad operacional, así como su legibilidad y comprensión.
- Revisar los recursos disponibles, incluyendo el personal, el equipo y los recursos financieros.
- Hay personal suficiente y competente.
- Examinar los recursos previstos en relación con los recursos reales.
- Comprobar cómo se fomenta una cultura positiva de seguridad operacional y cómo repercute en la eficacia general.

Presente	Adecuado	Operativo	Eficaz
• Existe una política de seguridad operacional, firmada por el Gerente Responsable, que incluye un compromiso hacia la mejora continua; observa todos los requisitos y disposiciones legales aplicables; y considera las mejores prácticas. La política de seguridad operacional incluye una declaración para proporcionar los recursos adecuados.	• La política de seguridad operacional es fácil de leer. • El contenido se adapta al CIAC. • Existe un proceso para evaluar los recursos y subsanar cualquier deficiencia.	• La política de seguridad operacional se revisa periódicamente para garantizar que sigue siendo relevante para el CIAC. • El CIAC está evaluando los recursos que se están proporcionando para prestar un servicio seguro y tomando medidas para subsanar cualquier deficiencia.	• El ejecutivo responsable está familiarizado con el contenido de la política de seguridad operacional y la respalda. • El CIAC está revisando y tomando medidas para subsanar cualquier deficiencia de recursos prevista.

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	3.1.4	Existe un medio para la comunicación de la política de seguridad operacional.					0.5			
	3.1.5	El ejecutivo responsable y el equipo de la alta gerencia promueven una cultura positiva de seguridad operacional/justa y demuestran su compromiso con la política de seguridad operacional, a través de la participación activa y visible en el sistema de gestión de la seguridad operacional.					1			

Orientación

¿Qué buscar?

- Revisar cómo se comunica la política de seguridad operacional.
- La política de seguridad operacional es claramente visible para todo el personal, incluido el personal contratado y las organizaciones de terceros.
- Preguntar a los gerentes y al personal sobre el conocimiento de la política de seguridad operacional
- Todos los gerentes están familiarizados con los elementos clave de la política de seguridad operacional.
- Evidencia de la participación de la alta gerencia en reuniones de seguridad operacional, instrucción, conferencias, etc.
- Retroalimentación de encuestas de seguridad operacional que incluyen aspectos específicos de la cultura justa.
- Relación con el regulador y otras partes interesadas.
- Revisar cómo se promueve una seguridad operacional positiva y una mentalidad justa.

Presente	Adecuado	Operativo	Eficaz
• Existe un medio para la comunicación de la política de seguridad operacional. El compromiso de la dirección con la seguridad operacional está documentado en la política de seguridad operacional.	• La política de seguridad operacional es claramente visible para todo el personal (considerar múltiples lugares). • La política de seguridad operacional es comprensible (considerar múltiples idiomas). El Ejecutivo Responsable y el equipo de la alta gerencia tienen un papel bien definido en el sistema de gestión de la seguridad operacional.	• La política de seguridad operacional se comunica a todo el personal (incluido el personal contratado y las organizaciones pertinentes). El ejecutivo responsable y el equipo de la alta gerencia están promoviendo su compromiso con la política de seguridad operacional, a través de la participación activa y visible en el sistema de gestión de la seguridad operacional.	• Las personas de todo el CIAC están familiarizadas con esta política y pueden describir sus obligaciones con respecto a la política de seguridad operacional. La toma de decisiones, las acciones y los comportamientos reflejan una actitud positiva hacia la seguridad operacional y la cultura justa, y existe un buen liderazgo en materia de seguridad operacional, que demuestra el compromiso con la política de seguridad operacional.

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	3.1.6	La política sobre seguridad operacional fomenta activamente la elaboración de informes sobre seguridad operacional					1			
	3.1.7	Se ha definido una política y principios de una cultura justa que identifican claramente los comportamientos aceptables e inaceptables para promover una cultura justa.					1			

Orientación

¿Qué buscar?

- Evidencia de cuándo se han aplicado los principios de actitud justa después de un evento.
- Evidencia de intervenciones a partir de investigaciones de seguridad operacional que se ocupen de cuestiones organizativas, en lugar de centrarse únicamente en el individuo.
- Revisar la forma en que el CIAC está monitoreando las tasas de notificación.
- Revisar el número de notificaciones de seguridad operacional de la aviación apropiados para las actividades.
- Las notificaciones de seguridad operacional incluyen los propios errores de la persona que notifica y los eventos en los que está involucrado (eventos en los que nadie estaba observando).
- Retroalimentación sobre la cultura de equidad, a partir de encuestas al personal sobre la cultura justa de la seguridad operacional.
- Entrevistar a los representantes del personal para confirmar que están de acuerdo con la política y los principios de la cultura justa.
- Comprobar que el personal es consciente de la política y los principios de la cultura justa.

Presente	Adecuado	Operativo	Eficaz
• Se han definido una política y unos principios de la cultura de equidad.	• La política sobre la cultura justa identifica claramente los comportamientos aceptables e inaceptables. • Los principios garantizan que la política pueda aplicarse de forma coherente en todo el CIAC. • La política y los principios de la cultura justa son comprensibles y claramente visibles.	• Hay pruebas de que la política sobre la cultura justa y los principios que la sustentan se aplican y se promueven entre el personal.	• La política sobre la cultura justa se aplica de manera justa y coherente y el personal confía en ella. • Hay pruebas de que la línea divisoria entre comportamiento aceptable e inaceptable se ha determinado en consulta con el personal y los representantes del personal.

Evaluación	**Indicadores de cumplimiento y rendimiento**		**P(1)**	**S(2)**	**O(3)**	**E(4)**	**W**	**Puntos**	**¿Cómo se logra?**	**Comentarios**
	3.1.8	Se han establecido objetivos de seguridad operacional coherentes con la política de seguridad operacional y éstos son comunicados a todo el CIAC.					1			
	3.1.9	El programa estatal de seguridad operacional (SSP) está siendo considerado y abordado según corresponda.					1			

Orientación

¿Qué buscar?

- Evaluar si los objetivos de seguridad operacional son adecuados y pertinentes.
- Se definen objetivos que conducirán a una mejora de los procesos, de los resultados y al desarrollo de una cultura positiva de seguridad operacional.
- Evaluar cómo se comunican los objetivos de seguridad operacional en todo el CIAC.
- Se están midiendo los objetivos de seguridad operacional para supervisar los logros a través de los SPI y los SPT.
- Evaluar si los objetivos de seguridad operacional han tenido en cuenta los objetivos estatales en materia de seguridad operacional del SSP.

Presente	**Adecuado**	**Operativo**	**Eficaz**
• Se han establecido objetivos de seguridad operacional que son coherentes con la política de seguridad operacional y existe un medio para comunicarlos a toda el CIAC.	• Los objetivos de seguridad operacional son relevantes para el CIAC y sus actividades. • Los objetivos de la seguridad operacional son comprensibles y claramente visibles. • Los objetivos de seguridad operacional están alineados con el SSP.	• Los objetivos de seguridad operacional son revisados periódicamente y comunicados a todo el CIAC.	• El alcance de los objetivos de seguridad operacional está siendo supervisado por la alta dirección y se están tomando medidas para garantizar su cumplimiento.

B3.2 Obligaciones de rendición de cuentas y responsabilidades en materia de seguridad operacional (Anexo 19, Elemento 1.2)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
3.2.1	Se ha nombrado un ejecutivo responsable con plena responsabilidad y obligación de rendición de cuentas para garantizar que el SMS se aplique correctamente y funcione con eficacia.					1			
3.2.2	El ejecutivo responsable es plenamente consciente de sus funciones y responsabilidades en materia del SMS con respecto a la política de seguridad operacional, los requisitos de seguridad operacional y la cultura de seguridad operacional del CIAC.					1			

Orientación

¿Qué buscar?

- Evidencia de que el ejecutivo responsable tiene la autoridad para proporcionar recursos suficientes para proporcionar las mejoras de seguridad operacional relevantes.
- Evidencia de la toma de decisiones sobre la aceptabilidad del riesgo.
- Las actividades de revisión de SMS se están llevando a cabo de manera oportuna y el SMS cuenta con recursos suficientes.
- Evidencia de que las actividades se han interrumpido debido a un nivel inaceptable de riesgo de seguridad operacional.
- Buscar pruebas de que las acciones del ejecutivo responsable son consistentes con la promoción activa de una cultura positiva de seguridad operacional en el CIAC.

Presente	Adecuado	Operativo	Eficaz
• Se ha nombrado un ejecutivo responsable con plena responsabilidad y con total rendición de cuentas de la gestión del SMS.	• El ejecutivo responsable tiene control de los recursos.	• El ejecutivo responsable se asegura de que el SMS cuente con los recursos adecuados, se implemente y se mantenga, y tiene la autoridad para detener la operación si existe un nivel inaceptable de riesgo para la seguridad operacional. • El ejecutivo responsable es plenamente consciente de sus funciones y responsabilidades en materia del SMS. • El ejecutivo responsable es accesible al personal del CIAC.	• El ejecutivo responsable se asegura de que el rendimiento del SMS sea supervisado, revisado y mejorado.

Evaluación	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
	3.2.3	Las obligaciones de rendición de cuentas, las autoridades y las responsabilidades están definidas y documentadas en todo el CIAC y el personal comprende sus propias responsabilidades.					0.5			

Orientación

¿Qué buscar?

- Preguntar a los gerentes y al personal sobre sus funciones y responsabilidades.
- Confirmar que los altos directivos son conscientes del rendimiento del CIAC en materia de seguridad operacional y de sus riesgos más significativos.
- Evidencia de que los gerentes tienen objetivos de rendimiento relacionados con la seguridad operacional.
- Buscar la participación activa del equipo directivo en el SMS.
- Evidencia de una adecuada mitigación de riesgos, acción y apropiación.
- Se definen y aplican los niveles de gestión autorizados para tomar decisiones sobre la aceptación de riesgos.
- Compruebe si existen conflictos de intereses y si han sido identificados y gestionados.

Presente	Adecuado	Operativo	Eficaz
• La obligación de rendición de cuentas, las autoridades y responsabilidades están claramente definidas y documentadas.	• Las personas tienen acceso a su responsabilidad en materia de seguridad operacional, autoridades y responsabilidades (por ejemplo, a través de descripciones de puestos de trabajo o de organigramas).	• Todos los miembros del CIAC conocen y cumplen con sus responsabilidades, sus autoridades y obligaciones de rendición de cuentas en materia de seguridad operacional, y se les anima a contribuir al SMS.	• El ejecutivo responsable y el equipo de la alta gerencia son conscientes de los riesgos a los que se enfrenta el CIAC, y los principios del SMS existen en todo el CIAC para que la seguridad operacional forme parte del lenguaje cotidiano.

B3.3 Nombramiento de personal clave (Anexo 19, Elemento 1.3)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
3.3.1	Se ha nombrado un gerente de seguridad operacional competente, responsable de la implementación y el mantenimiento del SMS, que depende directamente del ejecutivo responsable.					1			
3.3.2	El CIAC ha asignado recursos suficientes para gestionar el SMS, incluido, entre otros, personal competente para la investigación, el análisis, la auditoría y la promoción de la seguridad operacional.					2			

Orientación

¿Qué buscar?

- Revisar el rol del gerente de seguridad operacional, incluyendo la credibilidad y el estatus.
- Revisar la capacitación que ha recibido el gerente de seguridad operacional.
- Evidencia de competencia mantenida.
- Revisar cómo el gerente de seguridad operacional tiene acceso a la información sobre seguridad operacional interna y externa.
- Revisar cómo se comunica y se relaciona el gerente de seguridad operacional con el personal operacional y la gerencia superior.
- Revisar la carga de trabajo/tiempo asignado al gerente de seguridad operacional para cumplir con su función.
- Comprobar que existen recursos suficientes para las actividades del SMS, tales como investigación de la seguridad operacional, análisis, auditoría, asistencia a reuniones sobre seguridad operacional y promoción.
- Revisión de los plazos de actuación y cierre de las notificaciones de seguridad operacional.
- Entrevistas con el ejecutivo responsable y el gerente de seguridad operacional.
- Comprobar si existen conflictos de intereses y si han sido identificados y gestionados.

Presente	Adecuado	Operativo	Eficaz
• Se ha nombrado a un gerente de seguridad operacional responsable de la implementación y el mantenimiento del SMS, que depende directamente del ejecutivo responsable.	• El gerente de seguridad operacional es competente. • Se asignan tiempo y recursos suficientes para mantener el SMS.	• El gerente de seguridad operacional ha implementado y mantiene el SMS. El gerente de seguridad operacional está en comunicación regular con el ejecutivo responsable y se encarga de los problemas de seguridad operacional cuando es apropiado. • El personal del CIAC tiene acceso al gerente de seguridad operacional.	• El gerente de seguridad operacional es competente para gestionar el SMS e identifica las mejoras de forma oportuna. • Existe una estrecha relación de trabajo con el ejecutivo responsable, y el gerente de seguridad operacional es considerado un asesor de confianza al que se le otorga la condición adecuada en el CIAC.

Evaluación	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
	3.3.3	El CIAC ha establecido uno o varios comités de seguridad operacional que debaten y resuelven los riesgos de la seguridad operacional y las cuestiones de cumplimiento, e incluye al ejecutivo responsable y a los jefes de las áreas funcionales.					1.5			

Orientación

¿Qué buscar?

- Revisar el comité de seguridad operacional, la estructura del mismo y los términos de referencia de cada comité/reunión.
- Revisar los niveles de asistencia a las reuniones.
- Revisar las actas de las reuniones y las acciones a tomar.
- Comprobar que los resultados se comunican al resto del CIAC.
- La evidencia de los objetivos de seguridad operacional, el rendimiento en materia de seguridad operacional y el cumplimiento están siendo revisados y discutidos en las reuniones.
- Los participantes cuestionan lo que se presenta cuando hay poca evidencia.
- La alta gerencia es consciente de los riesgos más significativos a los que se enfrenta el CIAC y del rendimiento general del CIAC en materia de seguridad operacional.

Presente	Adecuado	Operativo	Eficaz
• El CIAC ha establecido comité(s) de seguridad operacional.	• La estructura y frecuencia de los comités de seguridad operacional respaldan las funciones del SMS en todo el CIAC. • El alcance de los comités de seguridad operacional incluye riesgos en la seguridad operacional, así como cuestiones de cumplimiento. • La asistencia del comité de seguridad operacional del más alto nivel incluye por lo menos al ejecutivo responsable y a los jefes de las áreas operacionales.	• Hay evidencia de reuniones que se llevan a cabo, detallando la asistencia, las discusiones y las acciones a tomar. • El comité o comités de seguridad operacional supervisa(n) la eficacia del SMS y la función de supervisión del cumplimiento, revisando que haya recursos suficientes. • Se están supervisando las acciones y se han establecido los objetivos de seguridad operacional y los SPI adecuados.	• Los comités de seguridad operacional incluyen a las principales partes interesadas. Los resultados de las reuniones son documentados y comunicados y cualquier acción es acordada, tomada y seguida de manera oportuna. Los objetivos y rendimiento en materia de seguridad operacional son revisados, y se toma las medidas apropiadas.

B3.4 Coordinación de la planificación de la respuesta ante emergencias (Anexo 19, Elemento 1.4)

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	3.4.1	Se ha desarrollado y distribuido un plan de respuesta ante emergencias (ERP) que define los procedimientos, roles, responsabilidades y acciones de las diversas organizaciones y personal clave.					1			
	3.4.2	Periódicamente se comprueba la idoneidad del ERP y se examina los resultados para mejorar su eficacia.					0.5			

Orientación

¿Qué buscar?

- Revisar el plan de respuesta ante emergencias.
- Revisar cómo se planifica la coordinación con otras organizaciones.
- Revisar cómo se distribuye el ERP y dónde se guardan las copias.
- Entrevistar al personal clave y comprobar que tiene acceso al ERP.
- Comprobar que se han considerado diferentes tipos de emergencias previsibles.
- Verificar cuándo se revisó y probó el ERP por última vez y qué medidas se tomaron.

Presente	Adecuado	Operativo	Efectivo
• Un ERP coordinado ha sido desarrollado y definido.	• El personal clave tiene fácil acceso a las partes relevantes del ERP en todo momento. • El ERP define los procedimientos, roles, responsabilidades y acciones de las distintas organizaciones y del personal clave. • Se definen la frecuencia y los métodos para probar el ERP. • La coordinación con otras organizaciones (incluidas las que no son de aviación) se define con los mecanismos adecuados.	• Se revisa el ERP y se prueba para asegurarse de que esté actualizado. Existen pruebas de coordinación con otras organizaciones, según proceda.	• Se analizan los resultados de la revisión y evaluación al ERP y se adopta medidas para mejorar su eficacia.

B3.5 Documentacion SMS (Anexo 19, Elemento 1.5)

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se alcanza?	Comentarios
Evaluación	3.5.1	La documentación del SMS incluye las políticas y los procesos que describen el sistema y los procesos de gestión de la seguridad operacional del CIAC y está a disposición de todo el personal pertinente.					1			
	3.5.2	La documentación SMS, incluido los registros relacionados con el SMS, se revisa y actualiza periódicamente con el adecuado control de versiones.					0.5			

Orientación

¿Qué buscar?

- Revisar la documentación del SMS y los procedimientos de enmienda.
- Comprobar si hay referencias cruzadas a otros documentos y procedimientos.
- Verificar la disponibilidad de la documentación SMS para todo el personal.
- Comprobar que el personal sepa dónde encontrar la documentación relacionada con la seguridad operacional, incluidos los procedimientos adecuados para su función.
- Revisar la documentación de apoyo del SMS (registros de peligros, actas de reuniones, informes sobre el desempeño de la seguridad operacional, evaluaciones de riesgos, etc.).
- Comprobar cómo se almacenan los registros de la seguridad operacional y cómo se controlan las versiones.
- Verificar que el personal apropiado esté al tanto de los procesos y procedimientos de control de registros.

Presente	Adecuado	Operativo	Eficaz
• La documentación del SMS incluye las políticas y procesos que describen el SMS y los procesos del CIAC. La documentación SMS define los productos SMS y los registros de las actividades SMS que se almacenarán. • Se identifica los registros que deben almacenarse, el período de almacenamiento y la ubicación.	• La documentación SMS está fácilmente disponible para todo el personal pertinente. • La documentación SMS es comprensible. • La documentación SMS es coherente con otros sistemas de gestión interna y representativa de los procesos reales existentes. • Se han definido requisitos de protección de datos y de confidencialidad.	• Se gestionan los cambios en la documentación SMS. • Todos están familiarizados con las partes relevantes de la documentación SMS, y las siguen. • Las actividades SMS son almacenadas adecuadamente y se comprueba que son completas y coherentes con los requisitos de protección de datos y de control de la confidencialidad.	• La documentación SMS es revisada de forma proactiva para mejorarla. • Los registros SMS se utilizan rutinariamente como datos para efectuar tareas relacionadas con la gestión de la seguridad operacional y la mejora continua del SMS.

B4 Promoción de la seguridad operacional (Anexo 19, Componente 4)

B4.1 Instrucción y educación (Anexo 19, Elemento 4.1)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
4.1.1	Existe un programa de instrucción en SMS que incluye instrucción inicial y periódica. La instrucción cubre las tareas de seguridad operacional individuales (incluyendo roles, responsabilidades y obligación de rendición de cuentas) y cómo funciona el SMS del CIAC.					2			
4.1.2	Hay un proceso en vigor para medir la eficacia de la instrucción y para adoptar las medidas adecuadas para mejorar la instrucción posterior.					1.5			
4.1.3	La instrucción incluye factores humanos y organizacionales, incluyendo cultura justa y habilidades no técnicas, con la intención de reducir el error humano.					1			

Orientación

¿Qué buscar?

- Revisar el programa de instrucción en SMS, incluyendo el contenido del curso y el método de entrega.
- Comprobar los registros de instrucción en relación con el programa de instrucción.
- Revisar cómo se está evaluando y manteniendo la competencia de los instructores.
- La instrucción considera la retroalimentación de sucesos externos, informes de investigación, reuniones de seguridad operacional, informes de riesgos, auditorías, análisis de datos de seguridad operacional, formación, evaluaciones de cursos, etc.
- Revisar cómo se evalúa la instrucción del personal nuevo y para los cambios de puesto.
- Revisar cualquier evaluación de la instrucción.
- Comprobar que la instrucción incluye factores humanos y organizacionales.
- Consultar al personal sobre su propia comprensión de su papel en el SMS del CIAC y sus funciones de seguridad operacional.
- Verificar que todo el personal esté informado sobre su cumplimiento.

Presente	Adecuado	Operativo	Eficaz
• Existe un programa de instrucción SMS que incluye instrucción inicial y periódica.	• La instrucción cubre las tareas individuales de seguridad operacional (incluyendo roles, responsabilidades y obligaciones de rendición de cuentas) y cómo funciona el SMS del CIAC. • El material y la metodología de la capacitación se adaptan a la audiencia e incluyen factores humanos. • Se identifica a todo el personal que requiere instrucción.	• El programa de instrucción SMS está impartiendo la instrucción adecuada a los diferentes miembros del personal del CIAC y está siendo impartido por personal competente.	• La instrucción SMS se evalúa en todos sus aspectos (objetivos de aprendizaje, contenido, métodos y estilos de enseñanza, pruebas, etc.) y está vinculada a la evaluación de competencias. • La instrucción es revisada rutinariamente para tener en cuenta los comentarios de diferentes fuentes.

	Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
Evaluación	4.1.4	Hay un proceso que evalúa la competencia del individuo y toma las medidas correctivas apropiadas cuando sea necesario.					1			
	4.1.5	Se define y evalúa la competencia de los instructores y se adoptan las medidas correctivas adecuadas cuando es necesario.					1			

Orientación

¿Qué buscar?

- Revisar cómo se lleva a cabo la evaluación de competencias en la contratación inicial y de forma periódica.
- Comprobar que incluye las funciones y responsabilidades en la seguridad operacional, así como la gestión del cumplimiento.

Presente	Adecuado	Operativo	Eficaz
• Se define un marco de competencias para todo el personal, incluidos los instructores.	• Existe un proceso para evaluar periódicamente la competencia real del personal en relación al marco de trabajo.	• Hay pruebas de que el proceso se está utilizando y registrando.	• El programa y proceso de evaluación de competencias se revisa y mejora de forma rutinaria. • La evaluación de las competencias adopta las medidas correctivas adecuadas cuando es necesario y se incorpora al programa de instrucción.

B4.2 Comunicación de la seguridad operacional (Anexo 19, Elemento 4.2)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
4.2.1	Existe un proceso para determinar qué información crítica de seguridad operacional debe comunicarse y cómo se comunica a todo el personal del CIAC, según corresponda. Esto incluye a las organizaciones y al personal contratado, cuando proceda.					0.5			

Orientación

¿Qué buscar?

- Revisar las fuentes de información utilizadas para la comunicación en materia de seguridad operacional.
- Revisar los métodos utilizados para comunicar información sobre seguridad operacional (por ejemplo, reuniones, presentaciones, correos electrónicos, acceso al sitio web, boletines, carteles, etc.).
- Evaluar si el medio de comunicación es apropiado.
- Se revisan la eficacia de los medios de comunicación en materia de seguridad operacional y el material utilizado para actualizar la formación pertinente.
- Se están comunicando los eventos significativos, los cambios y los resultados de la investigación.
- Comprobar la accesibilidad a la información sobre seguridad operacional.
- Consultar con el personal sobre cualquier comunicación reciente en materia de seguridad operacional.
- Revisar si la información de los sucesos se comunica oportunamente a todo el personal pertinente (interno y externo) y si ha sido debidamente desidentificada.

Presente	Adecuado	Operativo	Eficaz
• Existe un proceso para comunicar información crítica sobre la seguridad operacional.	• El proceso determinó *qué*, *cuándo* y *cómo* debe comunicarse la información sobre la seguridad operacional. • El proceso incluye, en su caso, a las organizaciones y al personal contratado. • Los medios de comunicación se adaptan al público y al significado de lo que se está comunicando.	• La información crítica sobre la seguridad operacional se identifica y se comunica en todo el CIAC a todo el personal, según proceda, incluidas las organizaciones contratadas y el personal, cuando proceda.	• El CIAC analiza y comunica la información crítica sobre seguridad operacional de manera efectiva, a través de una variedad de métodos apropiados para maximizar su comprensión. • La comunicación de la seguridad operacional se evalúa para determinar cómo se está utilizando y entendiendo, para mejorarla cuando sea necesario.

B5 Gestión de la interfaz (Anexo 19, Apéndice 2, Nota 2)

Evaluación

Indicadores de cumplimiento y rendimiento		P(1)	S(2)	O(3)	E(4)	W	Puntos	¿Cómo se logra?	Comentarios
5.1.1	El CIAC ha identificado y documentado las interfaces internas y externas relevantes y la naturaleza crítica de dichas interfaces.					2			
						Puntuación total			

Orientación

¿Qué buscar?

- Revisar cómo se han documentado las interfaces. Puede incluirse en una descripción del sistema.
- Prueba de ello:
  - Se identifican los temas críticos de la seguridad operacional, las áreas y los peligros asociados;
  - Los incidentes en la seguridad operacional están siendo notificados y abordados;
  - Las medidas de control de riesgos son aplicadas y revisadas regularmente; y
  - Las interfaces se revisan periódicamente.
- Se organiza sesiones de instrucción y promoción de la seguridad operacional con las organizaciones externas pertinentes.
- Las organizaciones externas participan en actividades SMS y comparten información sobre seguridad operacional.
- Comprobar las interfaces identificadas (por ejemplo, interfaces con aeródromos, control de tráfico aéreo (ATC), otros centros de instrucción, organizaciones contratadas y el Estado).

Presente	Adecuado	Operativo	Eficaz
• El CIAC ha identificado y documentado las interfaces internas y externas relevantes y la naturaleza crítica de dichas interfaces.	• Se contemplan todas las interfaces relevantes. • La forma en que se gestionan las interfaces es apropiada para la criticidad en términos de seguridad operacional. • Se definen los medios para comunicar la información sobre seguridad operacional.	• El CIAC está gestionando las interfaces a través de la identificación de peligros y la gestión de riesgos. • Existe una actividad de aseguramiento para evaluar las mitigaciones de los riesgos que están siendo entregadas por organizaciones externas.	• El CIAC tiene un buen conocimiento de la gestión de la interfaz y existen pruebas de que se están identificando los riesgos de la interfaz y se está actuando en consecuencia. • Las organizaciones que interactúan entre sí comparten información sobre seguridad operacional y toman medidas cuando es necesario.

Apéndice 14

Ejemplo del plan de implementación

1. Definición de tareas de implementación en base al análisis de brechas

Luego de completar la herramienta de evaluación del SMS en el Apéndice 13 de esta circular, se debe elaborar un plan detallado sobre “Acciones/Tareas requeridas” como el del ejemplo de la Tabla 14-1, que incluye el detalle sobre las brechas y como transformar éstas en tareas requeridas específicas relacionadas con los procesos y procedimientos de la organización. Cada tarea debe estar asignada a una persona o grupo de personas para que asuma las acciones respectivas. Es importante que se provea la correlación entre las tareas requeridas, los elementos del SMS y el manual del SMS como figura en la tabla.

2. Cronograma de implementación de las tareas/acciones

La Tabla 14-2 es una continuación de la Tabla 14-1 en forma de una hoja de cálculo. Esta tabla ilustra los hitos (puntos de inicio y fin) de cada tarea. En el enfoque de implementación por años, cada tarea/acción requerida debe estar relacionada con los requisitos del SMS, utilizando un cuadro en Excel, un software como es el MS Project/Diagrama de Gantt o similar, conforme a la elección del CIAC, en donde pueda establecer la planificación de las tareas, responsables, hitos a cumplir, así como demostrar el monitoreo de su cumplimiento.

Tabla 14-1 – Identificación de las tareas de implementación (Ejemplo del formato)

Ref. PAC	Pregunta de la evaluación del SMS	Respuesta: Si/ No/ Parcial	Descripción de la brecha	Acción/tarea requerida para subsanar la brecha	Persona o grupo asignado	Ref. manual SMS	Estado de la acción (Abierta/ en proceso/ Cerrada)
1. 1-1	*¿Se ha introducido y se aplica una política de seguridad operacional?*	*Parcial*	*La política de seguridad existente no contempla todos los elementos que figuran en el Apéndice 1.*	*a) Mejorar la política de seguridad existente para incluir las políticas y los objetivos del SMS, o desarrollar una nueva política de seguridad.* *b) Difundir la política de seguridad operacional por parte del gerente responsable.*	*Grupo de acción 1*	*Capítulo 1, Sección 1.3*	*Abierta*

Tabla 14-2 – Cronograma de implementación del SMS (Ejemplo de formato)

Acción/tarea requerida para subsanar la brecha	Ref. manual SMS	Persona o grupo asignado	Estado de la acción	Cronograma												
				1Q/10	2Q/10	3Q/10	4Q/10	1Q/11	2Q/11	3Q/11	4Q/11	1Q/12	2Q/12	3Q/12	4Q/12	Etc.
1. 1-1 a) Mejorar la política de seguridad existente para incluir las políticas y los objetivos del SMS, o desarrollar una nueva política de seguridad.	Capítulo 1, Sección 1.3	Grupo de acción 1	Abierta													
1. 1-1 b) Difundir la política de seguridad operacional al personal por parte del gerente responsable.																