REPUBLICA DEL PARAGUAY

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL

CIRCULAR DE ASESORAMIENTO

CA Nº: 141-001

Implementación de un Sistema de Gestión de la Seguridad Operacional (SMS) en Centros de Instrucción de Aeronáutica Civil (DINAC R 141)

Aprobado por Resolución Nº:1695/2017

Primera Edición - Año 2017

REGISTRO DE ENMIENDAS Y CORRECCIONES

ENMIENDAS			
Num.	Fecha de aplicación	Fecha de anotación	Anotada por

CORRECCIONES			
Num.	Fecha de aplicación	Fecha de anotación	Anotada por

CIRCULAR DE ASESORAMIENTO 141-001

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN CENTROS DE INSTRUCCIÓN DE AERONÁUTICA CIVIL (DINAC R 141)

INDICE

PAGINA DEJADA INTENCIONALMENTE EN BLANCO

CIRCULAR DE ASESORAMIENTO 141-001

IMPLEMENTACIÓN Y ACEPTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN CENTROS DE INSTRUCCIÓN DE AERONÁUTICA CIVIL (DINAC R)

1. PROPÓSITO

Esta circular de asesoramiento (CA) provee información de orientación para el desarrollo, implementación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS) y establece los métodos aceptables de cumplimiento (MAC) para los requisitos establecidos en la Sección 141.275 y el Apéndice 10 del DINAC R 141.

2. APLICABILIDAD

Esta circular de asesoramiento es aplicable al postulante o titular de una certificación de centro de instrucción de aeronáutica civil (CIAC), conforme a los requisitos del DINAC R 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.

Un CIAC puede utilizar otros métodos alternos de cumplimiento, siempre que dichos métodos sean aceptables para la DINAC.

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 DEL DINAC R 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.

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

5. DEFINICIONES Y ABREVIATURAS

5.1 Definiciones

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

b) **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.

c) **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.

d) **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.

e) **Indicadores de alto impacto.-** Indicadores de rendimiento en materia de seguridad operacional relacionados con el control y la medición de sucesos de alto impacto, como accidentes o incidentes graves. A menudo, los indicadores de alto impacto se conocen como indicadores reactivos.

f) **Indicadores de bajo impacto.-** Indicadores de rendimiento en materia de

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

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

h) **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.

i) **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.

j) **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.

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

l) **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.

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

n) **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.

o) **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)	CP	Puesto de comando
d)	CVR	Registrador de la voz en el puesto de pilotaje
e)	EC	Control de intensificación
f)	EF	Factor de intensificación
g)	EMC	Centro de control de la emergencia
h)	ERP	Plan de respuesta ante emergencias
i)	FDR	Registrador de datos de vuelo
j)	H	Peligro

k)	HIRM	Identificación de peligros y mitigación de los riesgos
l)	MOR	Informe obligatorio de sucesos
m)	OACI	Organización de Aviación Civil Internacional
n)	OSHE	Seguridad ocupacional, salud y medio ambiente
o)	PC	Control preventivo
p)	QA	Garantía de calidad
q)	QMS	Sistema de gestión de calidad
r)	RM	Medida de recuperación
s)	SAG	Grupo de acción de seguridad operacional
t)	SAR	Búsqueda y rescate
u)	SDCPS	Sistemas de recopilación y procesamiento de datos de seguridad operacional
v)	SMM	Manual de gestión de la seguridad operacional
w)	SMS	Sistema de gestión de la seguridad operacional
x)	SMSM	Manual de sistemas de gestión de la seguridad operacional
y)	SPI	Indicadores de rendimiento en materia de seguridad operacional
z)	SSP	Programa estatal de seguridad operacional
aa)	UC UE	Consecuencia final
bb)		Evento inseguro

6. INTRODUCCIÓN AL SISTEMA DE GESTIÓN DE SEGURIDAD OPERACIONAL

6.1 El SMS es un sistema que sirve para garantizar la operación segura de la aeronave mediante una gestión de riesgos de la seguridad operacional eficaz. Este sistema está diseñado para mejorar continuamente la seguridad de las operaciones mediante la identificación de peligros, la recopilación de datos, identificación de peligros y la evaluación continua de los riesgos de la seguridad operacional. El SMS busca contener o mitigar proactivamente los riesgos antes de que se produzcan accidentes e incidentes de aviación.

6.2 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.

6.3 La planificación y desarrollo del sistema que llevará a cabo el CIAC deberá incluir las interfaces del SMS dentro 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.

6.4 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.

6.5 Resulta útil para una buena comprensión del SMS, considerar como complemento de la descripción básica del sistema y sus procedimientos, un diagrama de la organización, con sus respectivas referencias cruzadas de cada uno de los elementos que establece la Sección141.275 del Reglamento DINAC

7. ESTRUCTURA DEL SMS

7.1 Dentro de la estructura del SMS se incluyen cuatro componentes fundamentales y 12

elementos que representan los requisitos mínimos establecidos por la OACI en el Anexo 19, los cuales se especifican a continuación:

1. Política y objetivos de seguridad operacional

1.1 Responsabilidad funcional y compromiso de la dirección

1.2 Obligación de rendición de cuentas sobre la seguridad operacional

1.3 Designación del personal clave de seguridad operacional

1.4 Coordinación de la planificación de respuestas ante emergencias

1.5 Documentación SMS

2. Gestión de riesgos de seguridad operacional

2.1 Identificación de peligros

2.2 Evaluación y mitigación de riesgos de seguridad operacional

3. Aseguramiento de la seguridad operacional

3.1 Observación y medición del rendimiento en materia de seguridad

3.2 Gestión del cambio

3.3 Mejora continua del SMS

4. Promoción de la seguridad operacional

4.1 Instrucción y educación

4.2 Comunicación de la seguridad operacional

7.2 **Política y objetivos de la seguridad operacional.-** La política de seguridad operacional es el documento mediante el cual el ejecutivo responsable como la más alta autoridad de la organización, describe los principios, procesos y métodos del SMS del CIAC para lograr los resultados deseados de seguridad operacional. La política establece el compromiso del más alto nivel organizacional para incorporar y mejorar continuamente la seguridad operacional en todos los aspectos de sus actividades. Asimismo, establece los objetivos de seguridad operacional a nivel de la organización medibles y asequibles que puedan alcanzarse.

7.3 **Gestión de riesgos de la seguridad operacional.-** Este componente proporciona un proceso de toma de decisiones para la identificación y mitigación de riesgos basado en un conocimiento profundo de la organización y su entorno operativo. Asimismo, incluye la toma de decisiones respecto a la aceptación de la gestión de riesgo para sus operaciones y constituye la forma que el CIAC tiene para cumplir el compromiso de aceptar y reducir el riesgo en sus operaciones a un nivel aceptable. En ese sentido, este componente es un proceso de diseño, una manera de incorporar el control de riesgos en los procesos y servicios que ofrece, así como para rediseñar los controles en los procesos existentes que no están cumpliendo con las necesidades organizacionales de seguridad.

7.4 **Aseguramiento de la seguridad operacional**.- El aseguramiento ofrece los procesos necesarios para contar con la confianza que el SMS cumple con los objetivos organizacionales de seguridad operacional del CIAC, la mitigación y el control de los riesgos establecidos. Por lo tanto, en el aseguramiento la meta es ver qué está pasando y qué ha sucedido para asegurar que los objetivos de seguridad operacional estén siendo cumplidos. Por lo tanto, este componente requiere el monitoreo y medición del desempeño de los procesos operativos de seguridad operacional y la mejora continua del nivel de desempeño de seguridad operacional. Un buen proceso de aseguramiento proporcionará información a ser utilizada para mantener la integridad de los controles de riesgo. En tal sentido, este componente es un medio de asegurar la eficacia de la seguridad operacional del CIAC, mantener la aplicación correcta de los requisitos del SMS, realizar los ajustes necesarios para mejorar el desempeño e identificar nuevas necesidades de la organización para reformular los

procesos existentes.

7.5 **Promoción de la seguridad operacional.-** El último componente del SMS está diseñado para asegurar que el personal del CIAC tienen una base sólida en cuanto a sus responsabilidades de seguridad, las políticas y expectativas de la organización en seguridad operacional, el procedimiento de presentación de informes y está familiarizado con los controles de riesgo. En ese sentido, la instrucción y la comunicación son las dos áreas claves de la promoción de la seguridad. La promoción también permite al CIAC compartir y proveer evidencia del éxito y lecciones aprendidas.

7.6 En resumen, un SMS no tiene que ser voluminoso, complejo o costoso para añadir valor a la seguridad operacional. Si un CIAC tiene la participación de los líderes operativos, mantiene abiertas las líneas de comunicación de arriba abajo en la organización y entre pares, se mantiene vigilante en lo que atañe a la gestión de los riesgos y se asegura que su personal tiene presente que la seguridad operacional es una parte esencial de su desempeño en el trabajo, logrará tener un SMS eficaz que le permita tomar las mejores decisiones de gestión de la seguridad operacional.

8. INTEGRACIÓN DE LOS SISTEMAS DE GESTIÓN

8.1 Dependiendo de los contextos organizacional, operacional y reglamentario, el CIAC puede implementar un SMS integrado. La integración tiene el potencial de generar sinergias, al gestionar los riesgos de seguridad a través de distintas áreas de la organización, así como de otros sistemas con los que pudiera contar como por ejemplo el de gestión de calidad, salud ocupacional y medio.

8.2 Asimismo, todos estos sistemas tienen procesos de gestión de riesgos y si el SMS funcionara aislado de estos otros sistemas de gestión, puede existir la tendencia de enfocarse solamente en los riesgos de seguridad operacional, sin comprender la naturaleza de la calidad o las amenazas del entorno de la organización.

8.3 Integración del SMS y el QMS

8.3.1 *Los CIAC implementan sistemas de gestión que abarcan toda la empresa.* La eficacia de la seguridad organizacional depende de la integración efectiva de estos sistemas para apoyar la producción de los servicios de instrucción que realizan. En el contexto del SMS el aspecto más significante de integración es con el sistema de gestión de la calidad (QMS) del CIAC. El QMS comúnmente se define como la estructura organizacional, las responsabilidades, recursos, procesos y procedimientos necesarios para establecer y promover un sistema de gestión de calidad y mejoramiento continuo, mientras se producen los productos o servicios.

8.3.2 El QMS y el SMS son complementarios. El QMS está enfocado en el cumplimiento de requisitos reglamentarios para alcanzar las expectativas del cliente y las condiciones contractuales, mientras que el SMS está enfocado en la eficacia de la seguridad operacional. Los objetivos de un SMS son identificar los peligros relacionados con la seguridad, evaluar los riesgos asociados a estos peligros e implementar medidas efectivas para el control de estos riesgos. En congruencia con el SMS, el QMS se enfoca desde el punto de vista de la seguridad operacional a verificar el cumplimiento de los requisitos reglamentarios que se aplican a los proveedores de servicio por lo que ambos sistemas convergen en beneficio de la seguridad operacional. Por tanto el SMS como el QMS:

a) requieren planificación y gestión;

b) dependen de la medición y monitoreo de indicadores de eficacia;

c) involucran todas funciones de la organización relacionadas con la entrega de productos o servicios; y

d) buscan la mejora continua.

8.3.3 *El SMS y el QMS utilizan procesos de gestión de los riesgos y de garantía similares*. El objetivo del SMS es identificar los peligros que la organización debe confrontar y controlar. El SMS está designado para gestionar los riesgos y medir el rendimiento en

materia de seguridad operacional durante la producción de bienes o servicios. El proceso de gestión de riesgos elimina los peligros o provee controles efectivos para mitigar los riesgos, por medio del balance apropiado en la asignación de recursos para la producción y protección, cumpliendo los niveles de eficacia de la seguridad requeridos. En el caso del QMS, la última edición de la Norma ISO 9001 (2015), establece dentro de los requisitos de planificación y operación, las acciones para identificar riesgos y afrontarlos con lo cual se facilita la interrelación con el SMS.

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

8.3.5 Dadas las características complementarias entre el SMS y el QMS, es posible establecer una relación sinérgica entre ambos sistemas que puede resumirse de la siguiente manera:

a) un SMS está apoyado por los procesos del QMS como las auditorías, inspecciones, investigaciones, análisis de causa raíz, procesos de diseño, análisis estadístico y medidas preventivas;

b) un QMS puede anticipar problemas de seguridad independientes al cumplimiento de los estándares y especificaciones de calidad; y

c) los principios, políticas y prácticas de calidad están vinculados con los objetivos de la gestión de la seguridad operacional.

8.3.6 La relación entre el SMS y el QMS conduce a la contribución complementaria de ambos sistemas al logro de los objetivos de seguridad y calidad de la organización. Una comparación resumida puede reflejarse de la siguiente manera:

Tabla 1: Relación QMS y SMS

QMS	SMS
Calidad	Seguridad operacional
Aseguramiento de la calidad	Aseguramiento de la seguridad operacional
Control de la calidad y acciones para afrontar riesgos.	Identificación de peligros y control de riesgos
Cultura de calidad	Cultura de seguridad operacional
Cumplimiento de requisitos	Nivel aceptable de rendimiento en materia de seguridad operacional
Prescriptivo	Basado en rendimiento
Normas y especificaciones	Factores institucionales y humanos
Reactivo > Proactivo	Proactivo > Predictivo

8.3.7 En conclusión, el CIAC podría contar con un sistema integrado de gestión de modo que los requisitos de la seguridad operacional se definan y apliquen de forma coherente con los demás requisitos de otros sistemas, como por ejemplo de calidad y medio ambiente, dado que la integración tiene el potencial de proporcionar sinergias al gestionar riesgos de seguridad operacional en varias áreas de las actividades de la aviación.

9. DATOS DE LA SEGURIDAD OPERACIONAL

9.1 Recopilación y calidad de los datos de seguridad operacional

9.1.1 La toma de decisiones basada en datos es una de las facetas más importantes de cualquier sistema de gestión. El tipo de datos de seguridad operacional que se recopila puede incluir accidentes e incidentes, eventos no cumplimientos o desvíos e

informes de peligros. Desafortunadamente, muchas bases de datos carecen de calidad de datos necesaria para ofrecer una base confiable a fin de evaluar las prioridades y la eficacia de las medidas de mitigación de riesgos. Si no se consideran las limitaciones de los datos usados para respaldar las funciones de la gestión de riesgos de seguridad operacional y su aseguramiento, se generan resultados erróneos del análisis, lo que, a su vez, puede producir decisiones incompletas y desacreditación del proceso de gestión.

9.1.2 Es fundamental para el correcto funcionamiento del SMS del centro de instrucción, contar con medios adecuados para la recolección de datos que puedan ser analizados para convertirse en información de seguridad operacional para la toma de decisiones del CIAC.

9.1.3 En el contexto de la recopilación de datos de seguridad operacional, el término "base de datos de seguridad" puede incluir el siguiente tipo de datos:

a) Datos de la investigación de accidentes;

b) datos de la investigación de incidentes;

c) datos de la notificación voluntaria;

d) datos de la notificación de la aeronavegabilidad continua;

e) datos del control de rendimiento operacional;

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

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

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

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

9.1.4 Dada la importancia de la calidad de los datos, el CIAC debe evaluar los datos usados para respaldar la gestión de riesgos de seguridad operacional y los procesos de aseguramiento de la seguridad operacional mediante los siguientes criterios:

a) Validez. Los datos recopilados son aceptables según los criterios establecidos para su uso previsto.

b) Integridad. No falta ningún dato relevante.

c) Congruencia. Se puede reproducir el grado hasta donde la medición de un parámetro determinado es congruente y evita errores.

d) Accesibilidad. Los datos están fácilmente disponibles para su análisis.

e) Puntualidad. Los datos son relevantes para el período de interés y están disponibles de forma oportuna.

f) Seguridad. Los datos están protegidos contra modificación accidental o maliciosa.

g) Precisión. Los datos no contienen errores.

9.1.5 Al considerar estos siete criterios para la calidad de datos, los análisis de datos de seguridad operacional generarán la información más precisa posible que se usará para respaldar la toma de decisiones estratégica.

9.2 Análisis de datos de la seguridad operacional

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

a) ayudar a decidir qué hechos son necesarios;

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

c) ayudar a alcanzar conclusiones válidas; y

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

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

9.2.3 Los criterios humanos pueden estar sometidos a algún grado de parcialidad según experiencias pasadas, lo que podría influenciar la interpretación de los resultados del análisis o la prueba de hipótesis. Una de las formas más frecuentes de error de criterio se conoce como "sesgo de confirmación". Esta es una tendencia a buscar y conservar información que confirme lo que una persona ya cree que es cierto.

9.2.4 Para el análisis de datos se pueden usar los siguientes métodos:

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

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

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

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

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

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

9.3 Gestión de información de la seguridad operacional

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

9.3.2 El establecimiento y mantenimiento de una base de datos de seguridad operacional

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

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

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

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

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

d) operar a un costo relativamente bajo.

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

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

a) Registrar eventos de seguridad operacional en varias categorías;

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

c) controlar tendencias;

d) compilar análisis, gráficos e informes;

e) revisar registros históricos;

f) compartir datos de seguridad operacional con otras organizaciones;

g) controlar investigaciones de eventos; y

h) controlar la implementación de medidas correctivas

9.4 Protección de datos de la seguridad operacional

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

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

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

c) eliminación de la identificación, al borrar todos los detalles que puedan causar que un tercero infiera la identidad de las personas (por ejemplo, números de

vuelo, fechas/horas, ubicaciones y tipos de aeronave); 17/8+2345d) seguridad de los sistemas de información, almacenamiento de datos y redes de comunicación; prohibiciones en el uso no autorizado de los datos.

10. COMPONENTES, ELEMENTOS Y CRITERIOS DE ACEPTACIÓN DE UN SMS

10.1 Componente 1: Política y objetivos de seguridad operacional

La política de seguridad operacional es el documento mediante el cual el ejecutivo responsable como la más alta autoridad de la organización, describe los principios, procesos y métodos del SMS del CIAC para lograr los resultados deseados de seguridad operacional. La política establece el compromiso del más alto nivel organizacional para incorporar y mejorar continuamente la seguridad operacional en todos los aspectos de sus actividades. Asimismo, establece los objetivos de seguridad operacional a nivel de la organización medibles y asequibles que puedan alcanzarse.

10.1.1 Responsabilidad funcional y compromiso de la dirección

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

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

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

c) incluir procedimientos de notificación de seguridad operacional;

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

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

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

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

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

10.1.1.3 Luego de haber desarrollado una política de seguridad operacional, el ejecutivo responsable deberá:

a) respaldar visiblemente la política;

b) comunicar la política a todo el personal correspondiente;

c) establecer objetivos de seguridad operacional para el SMS y la organización (de acuerdo con 10.1.1.4); y

d) establecer objetivos de seguridad operacional que identifiquen lo que intenta alcanzar la organización en términos de gestión de la seguridad operacional (de acuerdo con 10.1.1.4).

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

a) Minimizar las consecuencias y la gravedad de los accidentes e incidentes cuando ocurran.

b) Reducir la cantidad de accidentes e incidentes.

c) Incorporar la seguridad operacional en todas las actividades operativas, de mantenimiento e instrucción.

d) Evitar daños y lesiones a la propiedad y el personal de la empresa.

e) Considerar las implicaciones en materia de seguridad operacional cuando se incorporan nuevos equipos de vuelo, instalaciones o procedimientos.

f) Cumplir con las leyes, reglamentos y políticas y procedimientos internos relacionados con la seguridad operacional.

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

- *Se ha desarrollado la política de acuerdo con el Adjunto A y está firmada por el gerente responsable del CIAC.*
- *La alta dirección ha respaldado abiertamente esta política, por ejemplo con asignación de una partida presupuestaria adecuada para las actividades relacionadas con el SMS.*
- *Existe evidencia objetiva de que se ha comunicado la política y es accesible a todo el personal del CIAC.*
- *Se han establecido y publicado en el manual del SMS o documento equivalente los objetivos de seguridad operacional del CIAC, según el Párrafo 10.1.1.4, y están alineados a los ALoSP del Estado si éstos han sido desarrollados.*

10.1.2 Obligación de rendición de cuentas sobre la seguridad operacional

10.1.2.1 El CIAC:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nota.- *Las responsabilidades descritas anteriormente no pueden delegarse*.

10.1.2.5 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 consejo de directores;

c) un socio principal; o

d) el propietario.

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

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

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

10.1.2.9 El CIAC debe garantizar que:

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

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

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

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

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

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

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

10.1.2.11 La función del gerente de seguridad operacional se describe en detalle en la Sección 10.1.3.

10.1.2.12 A partir de una perspectiva de responsabilidad, la persona que realiza la función del gerente de seguridad operacional es responsable del rendimiento del SMS ante el gerente responsable y de la entrega de servicios de seguridad operacional a las otras áreas de la organización.

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

- *El gerente responsable está plenamente identificado y ha sido designado observando la orientación de 10.1.2.3 y 10.1.2.6.*
- *Las obligaciones en materia de seguridad operacional así como las líneas de obligación de rendición de cuentas sobre la seguridad operacional, para toda la organización, incluidos la de la administración superior, el encargado o gerente del SMS y los directivos o responsables de área están claramente definidas, documentadas y disponibles.*
- *Los niveles de atribución para la toma de decisiones sobre la tolerabilidad de los riesgos de seguridad operacional están claramente definidas, documentadas y disponibles.*
- *La autoridad y responsabilidades del ejecutivo responsable incluyen al menos aquellas señaladas en 10.1.2.4.*
- *Existe una declaración expresa de que las responsabilidades del ejecutivo responsable en materia de seguridad operacional no pueden delegarse.*
- *Los puestos, las responsabilidades y las autoridades relacionadas con la seguridad operacional han sido definidas, publicadas y comunicadas a toda la organización.*
- *Existe una declaración expresa de que el CIAC es responsable del rendimiento en materia de seguridad operacional de los productos o servicios que proporcionan los subcontratistas.*
- *Se han establecido y publicado los procedimientos del CIAC que garantizan el cumplimiento de 10.1.2.9 con relación a los subcontratistas.*
- *Todos los puntos anteriores están documentados en el manual de SMS del CIAC.*

10.1.3 Designación del personal clave de seguridad operacional

10.1.3.1 El CIAC designará un gerente de seguridad operacional que será responsable de la implementación y el mantenimiento de un SMS eficaz.

10.1.3.2 El nombramiento de un gerente de seguridad operacional calificado es clave para la

implementación y el funcionamiento eficaces de una oficina de servicios de seguridad operacional. Las funciones del gerente de seguridad operacional incluyen, entre otras:

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

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

c) controlar las medidas correctivas y evaluar sus resultados;

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

e) mantener registros y documentación de la seguridad operacional;

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

g) proporcionar consejos independientes sobre asuntos de seguridad operacional;

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

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

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

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

a) experiencia de gestión de seguridad operacional/calidad;

b) experiencia operacional;

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

d) habilidades para relacionarse con las personas;

e) habilidades analíticas y de solución de problemas;

f) habilidades de gestión de proyectos; y

g) habilidades de comunicaciones oral y escrita.

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

10.1.3.5 La distribución de la información de seguridad operacional mediante la oficina de servicios de seguridad operacional es el primer paso en el proceso de gestión de riesgos de seguridad operacional. Esta información la deberán usar los gerentes de línea para mitigar los riesgos de seguridad operacional, que inevitablemente requieren la asignación de los recursos. Los recursos necesarios podrían estar disponibles fácilmente para los gerentes de línea para este propósito.

10.1.3.6 Además, se requiere de un proceso formal para evaluar la eficacia y eficiencia de cualquier estrategia de mitigación usada para lograr los objetivos de rendimiento en materia de seguridad operacional acordados de la organización. Es recomendable la creación de un comité de revisión de seguridad operacional (SRC). El SRC proporciona la plataforma para lograr los objetivos de la asignación de recursos y para evaluar la eficacia y eficiencia de las estrategias de mitigación de riesgos. El SRC es un comité de muy alto nivel, liderado por un ejecutivo responsable y se

compone de gerentes superiores, lo que incluye gerentes de línea responsables de las áreas funcionales, así como también, de aquellos departamentos administrativos pertinentes. El gerente de seguridad operacional participa en el SRC solo en una función de asesoría. El SRC puede reunirse con poca frecuencia, a menos que circunstancias excepcionales indiquen lo contrario. El SRC:

a) controla la eficacia del SMS;

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

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

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

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

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

10.1.3.7 El SRC es estratégico y aborda temas de alto nivel relacionados con políticas, la asignación de recursos y el control del rendimiento institucional. Luego que el SRC desarrolla una dirección estratégica, se deben coordinar las estrategias de seguridad operacional en toda la organización.

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

- *El CIAC ha definido los requisitos y ha designado un gerente de seguridad operacional que será responsable de la implementación y el mantenimiento de un SMS eficaz debidamente calificado según la orientación de 10.1.3.3.*
- *En el manual del SMS se describen las funciones del gerente de seguridad operacional que incluyen como mínimo los criterios de 10.1.3.2*
- *Se han establecido y documentado en el manual del SMS el comité de revisión de seguridad operacional (SRC), incluyendo la descripción de sus funciones, sus miembros, la frecuencia y circunstancias de sus reuniones, etc. según la orientación de 10.1.3.6 y 10.1.3.7.*

10.1.4 Coordinación de la planificación de respuestas ante emergencias

10.1.4.1 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.

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

10.1.4.3 La coordinación de la planificación de respuestas ante emergencias será aceptable

para la DINAC si se han observado los siguientes criterios:

- *El CIAC ha desarrollado y documentado una planificación de respuesta ante emergencias.*
- *La planificación de respuesta ante emergencias puede ser parte integral del manual del SMS o puede desarrollarse como un manual independiente.*

10.1.5 Documentación SMS

10.1.5.1 La documentación del SMS está compuesta por el manual del SMS, los registros del SMS y, si aplica, el plan de implementación.

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

a) su política y objetivos de seguridad operacional;

b) sus requisitos del SMS;

c) todos los procesos y procedimientos del SMS;

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

e) sus resultados esperados del SMS.

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

10.1.5.4 En el caso de CIAC certificados, además del manual, la documentación deberá incluir un plan de implementación del SMS, aprobado formalmente por la organización, en el que se definirá el enfoque de la organización respecto de la gestión de la seguridad operacional, de manera que se cumplan los objetivos de la organización en materia de seguridad operacional.

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

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

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

i) gestión de documentos y registros;

ii) requisitos del SMS reglamentarios;

iii) marco de trabajo, alcance e integración;

iv) política y objetivos de seguridad operacional;

v) responsabilidades de la seguridad operacional y personal clave;

vi) sistema de notificación de peligros voluntaria;

vii) procedimientos de notificación e investigación de incidentes;

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

ix) indicadores de rendimiento en materia de seguridad operacional;

x) capacitación y comunicación de seguridad operacional;

xi) mejora continua y auditoría de SMS;

xii) gestión de cambio; y

xiii) planificación de contingencia de emergencia u operaciones.

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

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

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

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

iv) registros de revisión o auditoría internas de SMS;

v) registros de promoción de seguridad operacional;

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

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

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

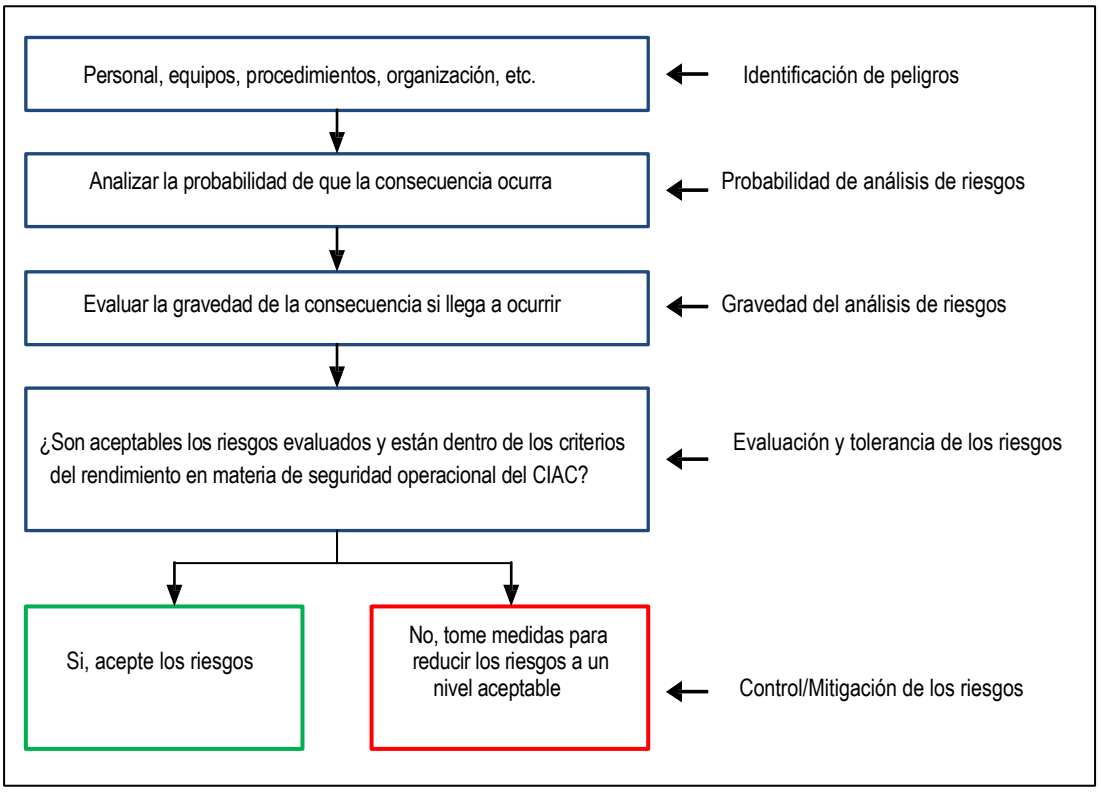
10.1.5.7 La documentación SMS será aceptable para la DINAC si se han observado los siguientes criterios:

- *El CIAC ha desarrollado un manual del SMS de acuerdo con 10.1.5.2, 10 1.5.6 (a).*
- *El CIAC mantiene un sistema de registros adecuado, de acuerdo con 10.1.5.6 (b).*
- *El CIAC ha desarrollado, si aplica, un plan de implementación por fases.*

10.2 Componente 2: Gestión de riesgos de seguridad operacional

Este componente proporciona un proceso de toma de decisiones para la identificación y mitigación de riesgos basado en un conocimiento profundo de la organización y su entorno operativo. Asimismo, incluye la toma de decisiones respecto a la aceptación de la gestión de riesgo para sus operaciones y constituye la forma que el CIAC tiene para cumplir el compromiso de aceptar y reducir el riesgo en sus operaciones a un nivel aceptable. En ese sentido, este componente es un proceso de diseño, una manera de incorporar el control de riesgos en los procesos y servicios que ofrece, así como para rediseñar los controles en los procesos existentes que no están cumpliendo con las necesidades organizacionales de seguridad.

Figura 1 – El proceso de gestión de riesgos de la seguridad operacional



10.2.1 Identificación de peligros

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

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

10.2.1.3 La identificación de los peligros se basará en una combinación de métodos reactivos, preventivos y de predicción para recopilar datos sobre seguridad operacional, como se describe en el Párrafo 10.2.1.4.

10.2.1.4 Las tres metodologías para identificar peligros son:

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

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

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

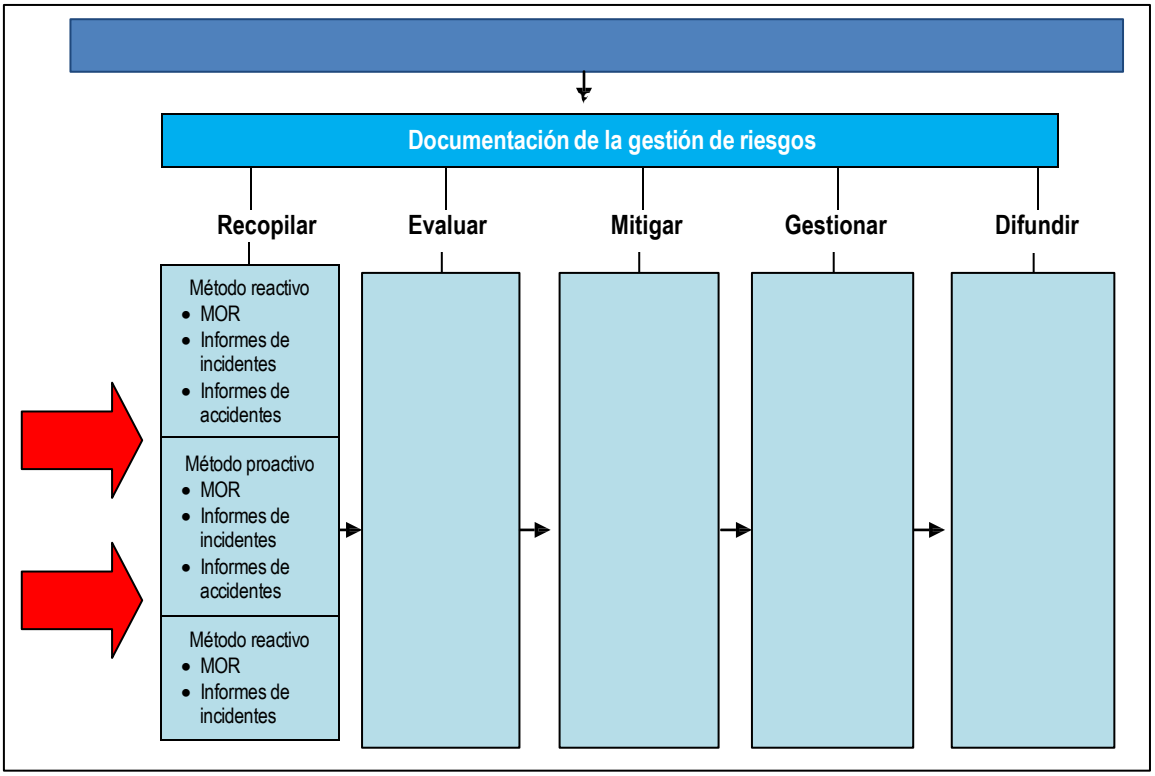
10.2.1.5 La gestión de riesgos de seguridad operacional requiere que el CIAC desarrolle y mantenga un proceso formal para identificar peligros que pueden contribuir con los sucesos relacionados con la aviación. Los peligros pueden existir en las actividades de aviación continuas o introducirse accidentalmente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

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

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

10.2.1.8 La **Figura 2** ilustra la documentación de peligros y el proceso de gestión de riesgos de seguimiento. Los peligros se identifican constantemente mediante varias fuentes de datos. Se espera que el CIAC identifique peligros, elimine estos peligros o mitigue los riesgos asociados. En el caso de peligros identificados en los productos o servicios suministrados mediante subcontratistas, una mitigación podría ser el requisito del CIAC para que tales organizaciones tengan un SMS o un proceso equivalente para la identificación de peligros y la gestión de riesgos.

Figura 2 - Documentación de peligros y seguimiento del proceso de gestión de riesgos



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

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

a) diagramas de control de operación normal;

b) sistemas de notificación voluntaria y obligatoria;

c) estudios de seguridad operacional;

d) auditorías de seguridad operacional;

e) comentarios de la capacitación; y

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

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

a) informes de accidentes industriales;

b) sistemas de notificación de incidentes obligatoria estatal;

c) sistemas de notificación de incidentes voluntaria estatal;

d) auditorías de vigilancia estatal; y

e) sistemas de intercambio de información.

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

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

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

- *El CIAC ha definido de manera clara y detallada en su manual del SMS los medios y procedimientos que garanticen la identificación de los peligros asociados a sus productos o servicios de aviación.*
- *La identificación de peligros del CIAC está compuesta por una combinación de métodos reactivos, preventivos y de predicción para recopilar datos sobre seguridad operacional.*
- *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.

- *Existe un método adecuado para la documentación y registro de los peligros identificados.*

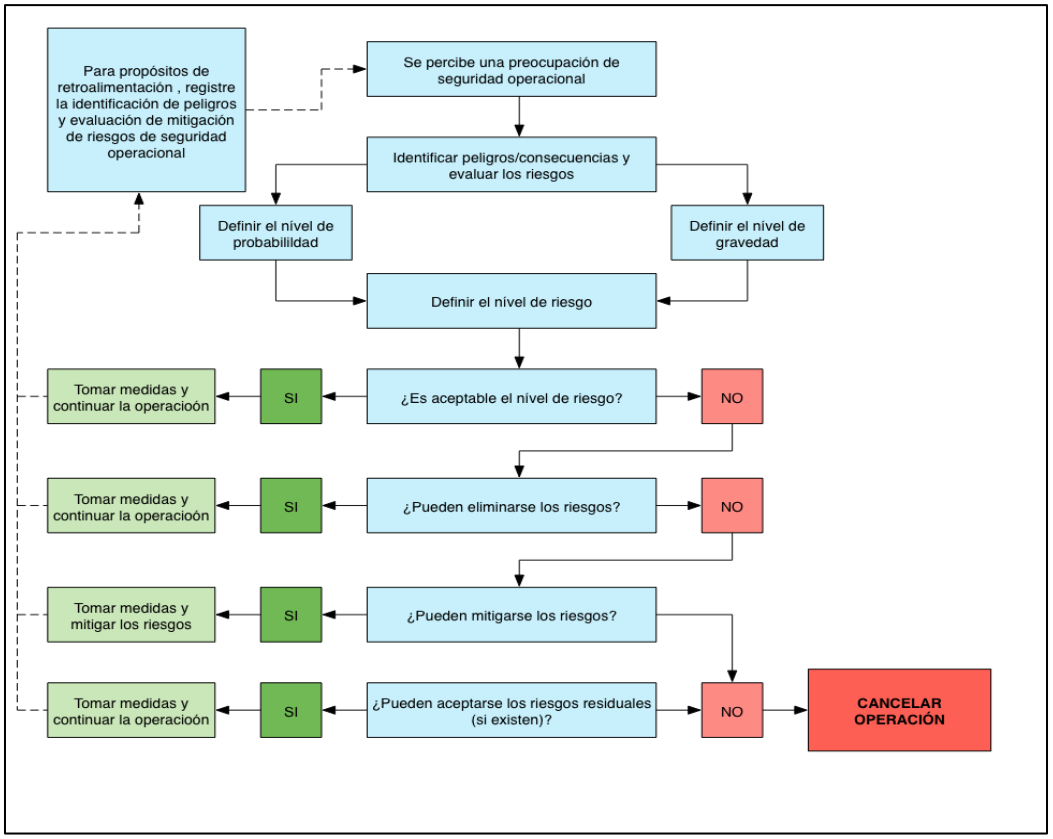
10.2.2 Evaluación y mitigación de riesgos de seguridad operacional

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

10.2.2.2 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.

10.2.2.3 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). 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



10.2.2.4 En muchos casos será necesario priorizar los peligros de acuerdo con la gravedad/probabilidad de sus consecuencias proyectadas. Esto facilita la priorización de las estrategias de mitigación de riesgos, tanto como para usar recursos limitados de

la forma más eficaz. La **Figura 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 2-13 de este capítulo);
b) en relación con la matriz de tolerabilidad relacionada, determine la categoría de tolerabilidad del índice de riesgo (es decir, intolerable, tolerable o aceptable) o terminología/categorización equivalente;
c) concluir que la priorización del peligro es:
<table><tr><th>Índice de riesgo proyectado</th><th>Nivel de peligro</th></tr><tr><td>Intolerable/alto riesgo
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>

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

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

b) la probabilidad que sucederá.

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

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

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

10.2.2.8 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

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

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

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

10.2.2.10 La evaluación de gravedad debe considerar todas las posibles consecuencias relacionadas con una condición o un objeto inseguros, considerando la peor situación predecible. La **Figura 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	5
Peligroso	• Una gran reducción de los márgenes de seguridad operacional estrés físico o una carga de trabajo tal que ya no se pueda confiar en los CIACs para que realicen sus tareas con precisión o por completo • Lesiones graves • Daño importante al equipo	4
Grave	• Una reducción importante de los márgenes de seguridad operacional, una reducción en la capacidad de los 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	3

Leve	• Molestias • Limitaciones operacionales • Uso de procedimientos de emergencia • Incidente leve	2
Insignificante	• Pocas consecuencias	1

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

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

10.2.2.13 El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a una matriz de tolerabilidad del riesgo de seguridad operacional (véase la Figura 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.

10.2.2.14 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

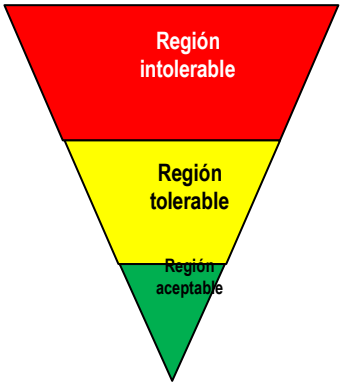
Descripción de la tolerabilidad	Índice de riesgo evaluado	Criterios sugeridos
	5A, 5B, 5C, 4A, 4B, 3A	Inaceptable según las circunstancias existentes
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Aceptable según la mitigación de riesgos. Puede necesitar una decisión de gestión.
	3E, 2D, 2E, 1B, 1C,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

10.2.2.15 Al usar esta matriz, los riesgos pueden categorizarse de acuerdo con una evaluación de su posible gravedad y probabilidad. La matriz de evaluación de riesgos puede personalizarse para reflejar el contexto de cada estructura institucional y actividades de aviación del 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.

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

10.2.2.17 Cada ejercicio de mitigación de riesgos se documentará de manera progresiva. Esto

puede lograrse al usar una variedad de aplicaciones, desde hojas de cálculo o tablas básicas hasta software personalizado de mitigación de riesgos comercial. Los documentos de mitigación de riesgos completos deben recibir la aprobación del nivel correspondiente de la administración.

10.2.2.18 La evaluación y mitigación de riesgos de seguridad operacional será aceptable para la DINAC 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 10.2.2.17.*
- *El CIAC ha desarrollado tablas de probabilidad y severidad para identificar los valores y definiciones respectivas, de acuerdo con 10.2.2.8, 10.2.2.9 y 10.2.2.10.*
- *El CIAC ha desarrollado una matriz de evaluación del riesgo de seguridad operacional de acuerdo con 10.2.2.11.*
- *El CIAC ha desarrollado una matriz de tolerabilidad de riesgo de acuerdo con 10.2.2.13 y 10.2.2.14.*
- *Como parte de la estrategia de control de riesgos, está considerada la posibilidad de cancelar las actividades de instrucción en vuelo cuando la mitigación no fuera posible.*

10.3 Componente 3: Aseguramiento de la seguridad operacional

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

10.3.1 Observación y medición del rendimiento en materia de seguridad operacional

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

10.3.1.2 El rendimiento en materia de seguridad operacional del CIAC se verificará en referencia a los indicadores y las metas de rendimiento en materia de seguridad operacional del SMS.

10.3.1.3 La información usada para medir el rendimiento en materia de seguridad operacional de la organización se genera mediante sus sistemas de notificación de la seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional se

analizan en detalle a partir del Párrafo 10.3.1.7 de esta sección.

10.3.1.4 Existen dos tipos de sistemas de notificación:

a) sistemas de notificación de incidentes obligatoria; y

b) sistemas de notificación de incidentes voluntaria.

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

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

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

a) revisiones de seguridad operacional,

b) estudios de seguridad operacional,

c) auditorías auditoría, e

d) investigaciones internas.

10.3.1.8 El resultado final del control y la medición del rendimiento en materia de seguridad operacional es el desarrollo de indicadores de rendimiento en materia de seguridad operacional, basado en el análisis de los datos recopilados mediante las fuentes nombradas anteriormente. El proceso de control y medición implica el uso de indicadores de rendimiento en materia de seguridad operacional seleccionados y niveles de objetivos y alertas del rendimiento en materia de seguridad operacional correspondientes. A partir del Párrafo 8.3.1.8 de esta sección y Adjunto D podrá encontrar una guía sobre el desarrollo de indicadores de rendimiento en materia de seguridad operacional y su configuración de objetivos y alertas.

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

10.3.1.10 Los indicadores de rendimiento en materia de seguridad operacional también proporcionan evidencia objetiva para que la DINAC evalúe la eficacia del SMS del CIAC y controle el logro de sus objetivos de seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional del CIAC consideran factores como la tolerancia de los riesgos de seguridad operacional de la organización, el costo/beneficios que conlleva la implementación de las mejoras al sistema, los requisitos reglamentarios y las expectativas públicas. Se deben seleccionar y desarrollar indicadores de rendimiento en materia de seguridad operacional en coordinación y con el asesoramiento de la DINAC. Este proceso es necesario para facilitar la agregación de la DINAC y la armonización de los indicadores de rendimiento en materia de seguridad operacional del CIAC para el mismo sector de aviación. Aún en caso que la DINAC no hubiera implementado su SSP o no hubiera definido los indicadores y objetivos de seguridad operacional del Estado, el CIAC deberá establecer sus propios indicadores, alertas y objetivos de seguridad operacional en estrecha coordinación con la DINAC.

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

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

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

10.3.1.14 En el caso de un CIAC nuevo, que carece de datos históricos, debe utilizarse inicialmente indicadores genéricos y objetivos de seguridad operacional de fuentes externas. Estas fuentes pueden ser organizaciones internacionales o del SSP de su Estado, u otros CIACs que operan en el mismo segmento y contexto operacional. A medida que el CIAC reúne experiencia mediante su operación, irá reuniendo información de seguridad operacional por medio de sus propias fuentes y podrá migrar gradualmente hacia indicadores, objetivos y niveles de alerta propios. El periodo de transición deberá ser acordado con la DINAC en función a la dimensión y complejidad del CIAC.

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

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

10.3.1.17 Los indicadores de alto impacto deben abordarse primero, mientras que los indicadores de bajo impacto pueden desarrollarse en una etapa más madura de la implementación del SMS.

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

10.3.1.19 También se puede compilar/agregar un resumen consolidado del resultado de rendimiento general de objetivos y alertas de todo el paquete de indicadores de rendimiento en materia de seguridad operacional para un período de control determinado. Se pueden asignar valores cualitativos (satisfactorio/insatisfactorio) para

cada “objetivo logrado” y cada “nivel de alerta no violado”. O bien, se pueden usar valores numéricos (puntos) para proporcionar una medición cuantitativa del rendimiento general del paquete de indicadores. En el Adjunto D de esta circular se ofrecen ejemplos de los indicadores de rendimiento en materia de seguridad operacional y sus criterios de configuración de objetivos y alertas.

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

- El CIAC ha desarrollado métodos y procedimientos para verificar el rendimiento en materia de seguridad operacional para confirmar la eficacia de los controles de riesgo de la seguridad operacional que incluya al menos:
    - Los indicadores, objetivos y alertas de seguridad operacional en base a datos históricos del CIAC o a los criterios indicados en 10.3.1.13, de acuerdo con esta sección y con el Adjunto D de esta circular.
    - Los indicadores, objetivos y alertas de seguridad operacional alineados con los del SSP del Estado si están disponibles.
    - Procedimientos para el monitoreo continuo del Estado de los indicadores y para las acciones a tomar frente a la activación de los niveles de alerta.
    - Procedimientos para el control y actualización regular de los indicadores, alertas y objetivos de seguridad operacional.
    - Procedimientos para la producción y emisión de resúmenes consolidados para periodos determinados de tiempo (Por ejemplo, meses, años, etc.)

10.3.2 Gestión del cambio

10.3.2.1 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, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios. Un ejemplo de los cambios que deben gestionarse es la incorporación de un nuevo tipo de aeronaves, la apertura de una nueva rutas de travesía para la instrucción, modificaciones importantes en la dimensión del CIAC, la incorporación de un nuevo tipo de operación o tecnología, las adquisiciones o funciones entre empresas, cambio de base principal de operaciones, etc.

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

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

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

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

c) Rendimiento pasado. El rendimiento pasado de los sistemas críticos y el análisis de tendencias en el proceso de aseguramiento de la seguridad operacional debe usarse para anticipar y controlar el rendimiento en materia de seguridad operacional bajo situaciones de cambio. El control del rendimiento pasado también garantiza la eficacia de las medidas correctivas tomadas para abordar deficiencias de seguridad operacional identificadas como resultado de auditorías, evaluaciones, investigaciones o informes.

10.3.2.4 La gestión del cambio será aceptable para la DINAC 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.*
- *El proceso de identificación y efecto de los cambios también incluye los arreglos que deberán incorporarse con anterioridad a la implementación de los cambios, así como los controles y mitigación de riesgos que ya no serán necesarios o efectivos una vez que el cambio haya surtido efecto.*
- *La gestión del cambio incluye un análisis de los riesgos asociados a dicho cambio.*

10.3.3 Mejora continua del SMS

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

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

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

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

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

10.3.3.6 En resumen, los procesos de evaluación y auditoría contribuyen con la capacidad del CIAC de lograr una mejora continua en el rendimiento en materia de seguridad

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

10.3.3.7 La mejora continua del SMS será aceptable para la DINAC 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.*
- *Existen en el manual del SMS disposiciones relativas a que las auditorías internas serán realizadas por personas u organizaciones funcionalmente independientes de los procesos técnicos evaluados.*
- *Las auditorías internas incluyen al menos la evaluación de:*
  - *Las funciones de la gestión de la seguridad operacional;*
  - *El diseño de las políticas;*
  - *La gestión de los riesgos;*
  - *El aseguramiento de la seguridad operacional; y*
  - *L promoción de la seguridad operacional en toda la organización*
- *El CIAC ha establecido la frecuencia y las circunstancias para recibir auditorías externas u otras empresas seleccionadas por el CIAC para la evaluación de su SMS.*
- *Las políticas y procedimientos relacionados con las auditorías externas incluyen los criterios de selección de las organizaciones auditoras, y el compromiso y procedimientos para el tratamiento de los hallazgos y no conformidades.*

10.4 Componente 4: Promoción de la seguridad operacional

El último componente del SMS está diseñado para asegurar que el personal del CIAC tienen una base sólida en cuanto a sus responsabilidades de seguridad, las políticas y expectativas de la organización en seguridad operacional, el procedimiento de presentación de informes y familiarizado con los controles de riesgo. En ese sentido, la instrucción y la comunicación son las dos áreas claves de la promoción de la seguridad. La promoción también permite al CIAC compartir y proveer evidencia del éxito y lecciones aprendidas.

10.4.1 Instrucción y educación

10.4.1.1 El CIAC 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.

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

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

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

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

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

d) sistemas de notificación de la seguridad operacional;

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

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

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

h) adoctrinamiento inicial documentado y requisitos de capacitación recurrente.

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

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

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

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

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

10.4.1.9 La instrucción y educación será aceptable para la DINAC si se han observado los siguientes criterios:

- *El CIAC ha establecido dentro de su programa de instrucción, la instrucción inicial y recurrente 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 Jefe responsable;*
  - *jefe de Instructores y los instructores;*
  - *alumnos*
- *El alcance y duración de cada curso de instrucción del SMS es apropiado para cada área de actividad.*
- *El contenido de la instrucción aborda al menos lo establecido por 10.4.1.3.*

- *Está claramente establecida la responsabilidad por el desarrollo de los contenidos de los cursos, la programación y el mantenimiento de los registros de capacitación.*

- *La capacitación del ejecutivo responsable ha sido especialmente diseñada para ser una sesión de alto nivel, que asegure la comprensión sus responsabilidades con relación al SMS, así como la descripción general del SMS y su relación con la estrategia comercial de la organización.*

10.4.2 Comunicación de la seguridad operacional

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

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

b) difunda información crítica para la seguridad operacional;

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

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

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

10.4.2.3 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;

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

e) sitios web o correo electrónico.

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

- *El CIAC ha establecido un método oficial de comunicación sobre seguridad operacional que cumpla con 10.4.2.1 y 10.4.2.3.*

- *Se han comunicado debidamente a todo el personal de operaciones los objetivos y procedimientos del SMS.*

- *Se han desarrollado y documentado procedimientos para la comunicación regular de información sobre tendencias de rendimiento en materia de seguridad operacional y temas de seguridad relevantes, incluyendo la responsabilidad por la preparación y publicación de esta información.*

- *Se han determinado los medios apropiados para distribuir la información del punto anterior, de tal forma de garantizar su amplia distribución.*

- *Se han establecido mecanismos para alentar al personal de operaciones que identifique e informe sobre los peligros.*

- *Todo el personal del CIAC está familiarizado con el acceso y el uso de los medios de notificación de peligros.*

11. EVALUACIÓN DE LA IMPLEMENTACIÓN DEL SMS

11.1 A partir del 1 de enero del 2016, todo postulante a una certificación de centro de instrucción de aeronáutica civil (CIAC) conforme al DINAC R 141 (Tipo 2 y Tipo 3) o aquellos que se encuentran en las Fases I o II del proceso de certificación, deberán incluir el desarrollo de un manual del SMS como parte del manual de instrucción y procedimientos (MIP) o como documento independiente, para la implementación de todos los elementos que se detallan en la Sección 10 de esta circular de asesoramiento, con excepción de los aquellos aspectos identificados en el Figura 11 que deberán ser incluidos en un plan de implementación, el cual deberá ser aceptado por la DINAC junto con el manual del SMS.

11.2 Para aquellos CIAC 141 certificados o aquellos que se encuentren en las Fases III o IV del proceso de certificación, se prevé un proceso de adecuación o implantación del SMS por etapas, en virtud a que diversos elementos del SMS descritos en la Sección 10 de esta circular, ya forman parte del sistema de calidad y otros procesos anteriores al desarrollo del concepto de los SMS. En este sentido, lo que hace falta es en primer lugar identificar los elementos que ya están desarrollados y ajustarlos a los criterios del SMS y lógicamente, desarrollar aquellos elementos faltantes. El contenido de estas etapas se detalla en la Figura 10.

11.3 Una descripción en detalle de las etapas de implementación se incluye a partir de la Sección 13 de esta circular. Las 4 etapas de implementación se aplican solamente a centros de instrucción certificados.

11.4 El proceso de transición o adaptación, también llamado de implementación del SMS puede durar desde algunos meses hasta varios años. Para facilitar la implementación, la misma se ha dividido en etapas. El número de etapas y la duración de cada una de éstas dependerán del resultado del análisis de brechas, y del tamaño, naturaleza y complejidad de las operaciones del CIAC. En el **Adjunto B** de esta circular se ofrece una lista de las preguntas para el análisis de brechas.

11.5 El plan de implementación de SMS se desarrolla con el asesoramiento del ejecutivo responsable y los gerentes o directivos responsables de las actividades de instrucción en vuelo para la operación segura de la aeronave o en respaldo de ésta. Luego de completarse, el ejecutivo responsable apoya el plan. El plan de implementación del SMS incluye cronologías e hitos coherentes con los requisitos identificados en el proceso de análisis de brechas, la envergadura del CIAC y la complejidad de sus servicios. El plan debe abordar la coordinación con organizaciones o contratistas externos, donde corresponda, y deberá ser aceptado por la DINAC.

11.6 El plan de implementación del CIAC puede documentarse de diferentes formas, lo que varía de una simple hoja de cálculos hasta software especializado de gestión de proyectos. El plan de implementación debe abordar las brechas mediante la finalización de medidas e hitos específicos de acuerdo con la cronología determinada. La asignación de cada tarea garantiza una responsabilidad en todo el proceso de implementación. El plan debe revisarse y actualizarse regularmente, según sea necesario. En el **Adjunto B** de esta circular se incluye ejemplos de este plan.

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

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

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

b) la necesidad de permitir la implementación de elementos del marco de trabajo

del SMS en varias secuencias, según los resultados de cada análisis de brechas efectuado por el CIAC;

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

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

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

11.10 Se describen como ejemplo cuatro etapas de implementación para un SMS. Cada etapa se asocia con varios elementos (o subelementos) según el marco de trabajo del SMS; sin embargo, la configuración particular de los elementos que figura en esta circular no está diseñada para ser absoluta. La DINAC y el CIAC pueden hacer ajustes que consideren convenientes según las circunstancias.

11.11 En la Figura 10 se muestra el contenido de las cuatro etapas de la implementación del SMS y sus elementos correspondientes para los CIAC 141 certificados, y en la Figura 11 se muestran los elementos que deben ser incluidos en el plan de implementación del SMS de un CIAC nuevo.

Figura 10 - Contenido de las cuatro etapas de implementación del SMS de un CIAC existente

Etapa 1 (12 meses*)	Etapa 2 (12 meses)	Etapa 3 (18 meses)	Etapa 4 (18 meses)
1. Elemento 1.1 a. Identificar al ejecutivo responsable del SMS. b. Establecer un equipo de implementación del SMS. c. Definir el alcance del SMS. d. Realizar un análisis de las brechas. **2. Elemento 1.5** a. Desarrollar un plan de implementación del SMS. **3. Elemento 1.3** a. Establecer una persona /oficina clave responsable de la administración y mantenimiento del SMS. **4. Elemento 4.1** a. Establecer un programa de capacitación del SMS para todo el personal, con prioridad para el personal a cargo de la implementación del SMS **5. Elemento 4.2** a. Iniciar los canales de comunicación del SMS.	**1. Elemento 1.1** a. Establecer la política y objetivos de seguridad operacional. **2. Elemento 1.2** a. Definir las responsabilidades de la gestión de seguridad operacional en las áreas pertinentes del CIAC. b. Establecer un mecanismo o comité de coordinación del SMS. c. Establecer un grupo de acción seguridad operacional (SAG). **3. Elemento 1.4** a. Establecer un plan de respuesta ante emergencias. **4. Elemento 1.5** a. Iniciar el desarrollo progresivo de un documento o manual del SMS y otra documentación de respaldo.	**1. Elemento 2.1** a. Establecer un procedimiento de notificación de peligros voluntaria. **2. Elemento 2.2** a.Establecer procedimientos de gestión de gestión de riesgos de la seguridad operacional. **3. Elemento 3.1** a. Establecer procedimiento de notificación e investigación de sucesos. b. Establecer un sistema de recopilación y procesamiento de datos de seguridad operacional para los resultados de alto impacto. c.Desarrollar el indicador de rendimiento en materia de seguridad operacional de alto impacto y una configuración de objetivos y alertas asociada. **4. Elemento 3.2** a. Crear un procedimiento de gestión del cambio que incluye la evaluación de riesgos de la seguridad operacional. **5. Elemento 3.3** a. Establecer un programa interno de auditoría de la calidad. b. Establecer un programa externo de auditoría de calidad.	**1. Elemento 1.1** a. Mejorar el procedimiento disciplinario/política existente con una debida consideración de los errores o las equivocaciones accidentales de las infracciones deliberadas o graves. **2. Elemento 2.1** a. Integrar los peligros identificados a partir de los informes de investigación de sucesos con el sistema de notificación de peligros voluntaria. b. Integrar procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o el cliente, según corresponda. **3. Elemento 3.1** a. Mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto. b. Desarrollar SPI de bajo impacto y una configuración de objetivos y alertas asociadas. **4. Elemento 3.3** a. Establecer programas de auditoría de SMS o integrarlos en programas de auditoría internos y externos existentes. b. Establecer otros programas de revisión /estudio de SMS operacional, donde corresponda. **5. Elemento 4.1** a. Garantizar que se haya completado el programa de capacitación de SMS para todo el personal pertinente. **6. Elemento 4.1** a. Promover la distribución e intercambio de información de la seguridad operacional en forma interna y externa.
El elemento 1.5: Documentación del SMS se desarrolla a lo largo de todas las fases			
Los elementos 4.1 y 4.2: Capacitación, educación y comunicación del SMS se desarrolla a lo largo de todas las fases			
Los periodos de implantación incluidos en esta tabla constituyen tan solo referencias aproximadas. El tiempo real dependerá del alcance y la complejidad de la organización.			

Figura 11 - Contenido del plan de implementación del SMS de un CIAC nuevo

Etapa 1 (12 meses*)	Etapa 2 (12 meses)	Etapa 3 (18 meses)	Etapa 4 (18 meses)
1. Elemento 1.1 a. Identificar al ejecutivo responsable del SMS. b. Establecer un equipo de implementación del SMS. c. Definir el alcance del SMS. d. Realizar un análisis de las brechas. **2. Elemento 1.5** a. Desarrollar un plan de implementación del SMS. **3. Elemento 1.3** a. Establecer una persona /oficina clave responsable de la administración y mantenimiento del SMS. **4. Elemento 4.1** a. Establecer un programa de capacitación del SMS para todo el personal, con prioridad para el personal a cargo de la implementación del SMS **5. Elemento 4.2** a. Iniciar los canales de comunicación del SMS.	**1. Elemento 1.1** a. Establecer la política y objetivos de seguridad operacional. **2. Elemento 1.2** a. Definir las responsabilidades de la gestión de seguridad operacional en las áreas pertinentes del CIAC. b. Establecer un mecanismo o comité de coordinación del SMS. c. Establecer un grupo de acción seguridad operacional (SAG). **3. Elemento 1.4** a. Establecer un plan de respuesta ante emergencias. **4. Elemento 1.5** d. Iniciar el desarrollo progresivo de un documento o manual del SMS y otra documentación de respaldo.	**1. Elemento 2.1** a. Establecer un procedimiento de notificación de peligros voluntaria. **2. Elemento 2.2** a.Establecer procedimientos de gestión de gestión de riesgos de la seguridad operacional. **3. Elemento 3.1** a. Establecer procedimiento de notificación e investigación de sucesos. e. Establecer un sistema de recopilación y procesamiento de datos de seguridad operacional para los resultados de alto impacto. **f.** Desarrollar el indicador de rendimiento en materia de seguridad operacional de alto impacto y una configuración de objetivos y alertas asociada. **4. Elemento 3.2** a. Crear un procedimiento de gestión del cambio que incluye la evaluación de riesgos de la seguridad operacional. **5. Elemento 3.3** a. Establecer un programa interno de auditoría de la calidad. b. Establecer un programa externo de auditoría de calidad.	**1. Elemento 1.1** a. Mejorar el procedimiento disciplinario/política existente con una debida consideración de los errores o las equivocaciones accidentales de las infracciones deliberadas o graves. **2. Elemento 2.1** a.Integrar los peligros identificados a partir de los informes de investigación de sucesos con el sistema de notificación de peligros voluntaria. b. Integrar procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o el cliente, según corresponda. **3. Elemento 3.1** a. Mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto. b. Desarrollar SPI de bajo impacto y una configuración de objetivos y alertas asociadas. **4. Elemento 3.3** a. Establecer programas de auditoría de SMS o integrarlos en programas de auditoría internos y externos existentes. b.Establecer otros programas de revisión/estudio de SMS operacional, donde corresponda. **5. Elemento 4.1** a. Garantizar que se haya completado el programa de capacitación de SMS para todo el personal pertinente. **6. Elemento 4.1** a. Promover la distribución e intercambio de información de la seguridad operacional en forma interna y externa.
El elemento 1.5: Documentación del SMS se desarrolla a lo largo de todas las fases			
Los elementos 4.1 y 4.2: Capacitación, educación y comunicación del SMS se desarrolla a lo largo de todas las fases			
Los periodos de implantación incluidos en esta tabla constituyen tan solo referencias aproximadas. El tiempo real dependerá del alcance y la complejidad de la organización.			

12. DETALLE DE LAS ETAPAS DE IMPLEMENTACIÓN DEL SMS

12.1 Etapa 1

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

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

Al finalizar la Etapa 1, se deben finalizar las siguientes actividades de tal forma que cumplan las expectativas de la DINAC, como se establece en los requisitos de la Sección 141.275 y Apéndice 10 del DINAC R 141:

Compromiso y responsabilidad de la gestión — Elemento 1.1

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

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

(i) Desarrollar el plan de implementación del SMS;

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

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

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

d) Realizar un análisis de brechas de los sistemas y procesos actuales de la organización en relación con los requisitos del marco de trabajo del SMS (o los requisitos reglamentarios de SMS pertinentes).

Plan de implementación del SMS — Elemento 1.5

a) Desarrollar un plan de implementación acerca de cómo la organización implementará el SMS sobre la base del sistema identificado y las brechas del proceso que se generan del análisis de brechas.

Nombramiento del personal de seguridad operacional clave — Elemento 1.3

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

b) Establecer la oficina de servicios de seguridad operacional.

Capacitación y educación — Elemento 4.1

a) Realizar un análisis de las necesidades de capacitación.

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

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

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

ii) la capacitación periódica.

d) Identificar los costos asociados con la capacitación.

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

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

Comunicación de la seguridad operacional — Elemento 4.2

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

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

i. Folletos informativos, noticias y boletines de seguridad operacional:

ii. Sitios web;

iii. Correo electrónico

Etapa 2

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

Compromisos y responsabilidades de la gestión — Elemento 1.1

a) Desarrollar una política de seguridad operacional.

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

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

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

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

i) indicadores de rendimiento en materia de seguridad operacional;

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

iii) planes de acción.

f) Establecer los requisitos del SMS para los subcontratistas:

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

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

Nota.- *Véase el Adjunto A de esta circular un ejemplo de política de seguridad operacional para el CIAC.*

Responsabilidades de la seguridad operacional — Elemento 1.2

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

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

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

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

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

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

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

Coordinación de la planificación de respuesta ante emergencias — Elemento 1.4

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

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

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

d) Evaluar los ERP respectivos de las entidades externas.

e) Establecer la coordinación entre los diferentes ERP.

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

Nota.- *Véase el Adjunto E de esta circular una guía detallada sobre ERP.*

Documentación del SMS — Elemento 1.5 (ii)

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

i) desarrollar un documento de SMS que sea un manual independiente o una sección distinta dentro del MIP existente.

Nota.- Véase el Adjunto C de esta circular una orientación sobre el desarrollo de un manual de SMS.

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

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

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

12.3 Etapa 3

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

Identificación de peligros — Elemento 2.1 (i)

a) Establecer un procedimiento de notificación voluntaria.

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

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

Nota.- *Véase el Adjunto F de esta circular una orientación sobre el procedimiento de notificación voluntaria.*

Evaluación y mitigación de riesgos de seguridad operacional — Elemento 2.2

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

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

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

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

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

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

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

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

Nota.- *Véase en el Adjunto D de esta circular los ejemplos de indicadores de rendimiento en materia de seguridad operacional.*

Gestión de cambio — Elemento 3.2

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

i) la vulnerabilidad de los sistemas y actividades;

ii) la estabilidad de los sistemas y entornos operacionales;

iii) rendimiento pasado;

iv) cambios reglamentarios, industriales y tecnológicos.

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

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

Mejora continua del SMS — Elemento 3.3 (i)

a) Desarrollar formularios para las evaluaciones internas.

b) Definir un proceso de auditoría interna.

c) Definir un proceso de auditoría externa.

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

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

12.4 Etapa 4

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

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

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

Identificación de peligros — Elemento 2.1

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

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

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

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

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

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

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

Mejora continua del SMS — Elemento 3.3 (ii)

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

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

Capacitación y educación — Elemento 4.1 (ii)

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

Comunicación de seguridad operacional — Elemento 4.2 (ii)

a) Establecer mecanismos para promover la distribución y el intercambio de información

de seguridad operacional de forma interna y externa.

12.5 Elementos del SMS implementados progresivamente a través de las Etapas 1 a la 4.

En la implementación del enfoque en etapas, los siguientes tres elementos clave se implementan progresivamente en cada una de las etapas:

Documentación del SMS — Elemento 1.5

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

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

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

13. 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 aprobación oportuna del su SMS.

13.1 Fase I – Pre-solicitud

13.1.1 La DINAC 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

13.1.2 En la reunión de pre-solicitud y durante las reuniones sucesivas que podrían requerirse antes de pasar a la Fase II, la DINAC 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. También es importante adelantar los criterios que serán utilizados para definir el plazo para establecer los indicadores y objetivos de seguridad operacional una vez que el CIAC inicie sus operaciones. 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.

13.1.3 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.

13.2 Fase II – Solicitud formal

13.2.1 Durante la Fase II y con anterioridad a la presentación de la carta de solicitud formal, el CIAC deberá desarrollar el contenido de todos los elementos descritos en la Sección 10 de esta circular, salvo aquellos sub-elementos en color más oscuro

resaltados en la Figura 11. Los elementos resaltados en negrilla deberán formar parte del plan de implementación, que también deberá ser presentado junto con la carta de solicitud formal, de acuerdo a los criterios y plazos previamente acordados entre la DINAC y el solicitante.

13.2.2 El análisis del faltante no es requerido para un CIAC nuevo, pero si puede ser de gran ayuda para realizar una referencia cruzada con cada uno de los elementos.

13.2.3 El manual del SMS y el plan de implementación deberán ser presentados a la DINAC junto con la carta de solicitud formal y el resto de los documentos del CIAC. Es importante recordar que el manual del SMS forma parte del manual de instrucción y procedimientos (MIP), aún si se ha desarrollado como un documento separado. Una vez que se ha presentado la carta de solicitud formal, la DINAC 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 DINAC 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.

13.2.4 En caso de que el documento sea rechazado por la DINAC, 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 DINAC por lo que se recomienda que los CIAC los utilicen como guía para la confección de su SMS.

13.3 Fase III – Evaluación de la documentación

13.3.1 Una vez que el documento ha sido admitido como parte de la solitud formal, a la DINAC 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 DINAC para poder resolver oportunamente cualquier observación que surja durante la revisión del manual y el resto de los documentos.

13.3.2 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.

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

13.3.4 Durante esta etapa la DINAC 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.

13.3.5 En función de la disponibilidad de recursos, los inspectores de la DINAC 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.

13.3.6 En la Sección 10 de esta circular, se incluye una explicación del contenido de cada elemento, así como los criterios de aceptabilidad que deberán ser tomados en cuenta por el inspector de la DINAC durante la revisión de la documentación del SMS del solicitante.

13.3.7 Resumiendo la Fase III, al inspector de la DINAC le corresponde revisar y aceptar 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 CIAC.

13.4 Fase IV – Inspección y demostración

13.4.1 La Fase IV del proceso de certificación ofrece a la DINAC 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.

13.4.2 La DINAC 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.

13.4.3 Como parte de las demostraciones, la DINAC 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.

13.4.4 Si la DINAC 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 DINAC tenga algunas observaciones o que hubiera determinado que alguno 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 DINAC, todas las observaciones.

13.5 Fase V – Aceptación provisional

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

15.5.2 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 DINAC durante el proceso de certificación. A partir de este día, el CIAC recopilará datos de seguridad operacional, identificará peligros, determinará sus consecuencias, gestionará los riesgos e implementará las medidas de mitigación correspondientes.

15.5.3 Paralelamente, el CIAC iniciará gradualmente el desarrollo de aquellos sub-elementos contemplados en letra más oscura en la Figura 11, de acuerdo con las condiciones y plazos acordados entre el CIAC y la DINAC en el plan de implementación aceptado

15.5.4 Al cabo de un período determinado, el CIAC procederá a acordar con la DINAC sus indicadores y niveles de objetivos y alertas, una vez que cuente con suficiente información de seguridad operacional, con lo cual se dará por finalizado el proceso de aceptación del SMS (aceptación final) del centro de instrucción y se continuará con la vigilancia del mismo.

15.5.5 Durante el período de implementación, el CIAC revisará su sistema para hacer las mejoras en sus procesos y procedimientos y completará los ítems referidos en la Etapa 4.

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

Adjunto A

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.*

Firmado: _____

Gerente responsable

Adjunto B

Análisis de brechas de los recursos existentes en la organización y ejemplo del plan de implementación

1. La Tabla 1 que se describe a continuación contiene un ejemplo de lista de verificación para el análisis inicial de las brechas, que puede ser utilizado como una plantilla para realizar el primer paso del análisis de las brechas del SMS. El formato sugerido con respuestas **SI**, **NO** y **PARCIAL** permite identificar de manera general las brechas existentes y por tanto la carga de trabajo y los recursos requeridos para la implementación del SMS. El cuestionario puede modificarse para adecuarse a las condiciones y naturalezas propias de la organización, sin embargo, para asegurar los mayores niveles de armonización regional, se recomienda enfáticamente desviarse lo menos posible del material sugerido. Al uso de esta lista de verificación, debe seguir un plan de implementación como el de las Tablas 2 y 3.

2. Una respuesta **SI** indica que la organización cumple o excede las expectativas de la pregunta. Una respuesta **NO** indica que existen brechas significativas entre la situación actual y las expectativas de la pregunta. Una respuesta **PARCIAL** indica que se necesita trabajos de mejora en los procesos específicos existentes para alcanzar las expectativas de la pregunta.

Tabla 1 – Lista de verificación para el análisis inicial de las brechas

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

3	¿Tiene el ejecutivo responsable la autoridad final sobre todas las actividades de aviación del CIAC?	Si No Parcial	
4	¿Ha identificado y documentado el CIAC las responsabilidades de seguridad operacional de la gestión, así como también, del personal de operaciones, en relación con el SMS?	Si No Parcial	
No.	***Aspecto a ser analizado o pregunta por responder***	***Respuesta***	***Estado de implementación***
5	¿Existe un comité de seguridad operacional o consejo de revisión para el propósito de revisión del SMS y el rendimiento en materia de seguridad operacional?	Si No Parcial	
6	¿Lidera al comité de seguridad operacional un ejecutivo responsable o un delegado asignado correctamente, confirmado debidamente en el manual del SMS?	Si No Parcial	
7	¿Incluye el comité de seguridad operacional a líderes de departamento u operacionales pertinentes, según corresponda?	Si No Parcial	
8	¿Existen grupos de acción de seguridad operacional que trabajan junto con el comité de seguridad operacional (en particular para las organizaciones grandes/complejas)?	Si No Parcial	
9	¿Ha identificado el CIAC al directivo que, independientemente a sus funciones, tiene la responsabilidad funcional y obligación de rendición de cuentas definitivas, en nombre de la organización, sobre la implementación y mantenimiento del SMS?	Si No Parcial	
10	¿Están definidas claramente las líneas de rendición de cuentas sobre seguridad operacional por parte de toda la organización?	Si No Parcial	
11	¿Está determinada la obligación de rendición de cuentas de todos los directivos, independiente de otras funciones, así como de los empleados, en relación al rendimiento en materia de seguridad operacional del SMS?	Si No Parcial	
12	¿Está documentada y comunicada la información relativa a las responsabilidades funcionales, la obligación de rendición de cuentas y las atribuciones de seguridad operacional en todo el CIAC?	Si No Parcial	
13	¿Están definidos los niveles de gestión con atribuciones para tomar decisiones sobre la tolerabilidad de riesgos de la seguridad operacional?	Si No Parcial	
Elemento 1.3 – Designación del personal clave de seguridad operacional			
1	¿Ha asignado el CIAC a una persona calificada para gestionar y vigilar la operación diaria del SMS?	Si No Parcial	
2	¿Tiene la persona calificada acceso o notificación directa al ejecutivo responsable, acerca de la implementación y operación del SMS?	Si No Parcial	
3	¿Tiene el gerente responsable de administrar el SMS otra responsabilidad más que pueda entrar en conflicto o perjudicar su papel como gerente de SMS?	Si No Parcial	
4	¿Es el puesto de gerente de SMS un puesto administrativo superior que no es inferior jerárquicamente o subordinado a otros puestos operacionales o de producción?	Si No Parcial	

No.	Aspecto a ser analizado o pregunta por responder	Respuesta	Estado de implementación
Elemento 1.4 – Coordinación de la planificación de respuestas ante emergencias			
1	¿Tiene el CIAC un plan de respuesta ante emergencias/contingencia adecuado para la envergadura, naturaleza y complejidad de la organización?	Si No Parcial	
2	¿Aborda el plan de emergencia/contingencia todos los escenarios de emergencia/crisis posibles o probables, en relación con los suministros de productos o servicios de aviación del CIAC?	Si No Parcial	
3	¿Incluye el ERP procedimientos para la producción, la entrega y el respaldo seguros y continuos de los productos o servicios de la aviación durante tales emergencias o contingencias?	Si No Parcial	
4	¿Existe un plan y registro para los ensayos o ejercicios en relación con el ERP?	Si No Parcial	
5	¿Aborda el ERP la coordinación necesaria de sus procedimientos de respuesta ante emergencias/contingencia con los procedimientos de contingencia de emergencia/respuesta de otras organizaciones, donde corresponda?	Si No Parcial	
6	¿Tiene el CIAC un proceso para distribuir y comunicar el ERP a todo el personal pertinente, incluidas las organizaciones externas pertinentes?	Si No Parcial	
7	¿Existe un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continuas?	Si No Parcial	
Elemento 1.5 Documentación de SMS			
1	¿Existe un resumen de SMS de nivel superior o documento de exposición que esté aprobado por el gerente responsable y aceptado por la DINAC?	Si No Parcial	
2	¿Aborda la documentación del SMS el SMS de la organización y sus componentes y elementos asociados?	Si No Parcial	
3	¿Está el marco de trabajo de SMS del CIAC en alineación con el marco de trabajo del SMS reglamentario?	Si No Parcial	
4	¿Mantiene el CIAC un registro de documentación de respaldo pertinente para la implementación y operación del SMS?	Si No Parcial	
5	¿Tiene el CIAC un plan de implementación de SMS para establecer su proceso de implementación de SMS, incluidas las tareas específicas y sus hitos de implementación pertinentes?	Si No Parcial	
6	¿Aborda el plan de implementación de SMS la coordinación entre el SMS del proveedor de servicios y el SMS de las organizaciones externas, donde corresponde?	Si No Parcial	
7	¿Respalda el ejecutivo responsable el plan de implementación de SMS?	Si No Parcial	

No.	Aspecto a ser analizado o pregunta por responder	Respuesta	Estado de implementación
Componente 2 – GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL			
Elemento 2.1 – Identificación de peligros			
1	¿Existe un proceso para la notificación de peligros/amenazas voluntaria de todos los empleados?	Si No Parcial	
2	¿Es simple la notificación de peligros/amenazas voluntaria, está disponible a todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios?	Si No Parcial	
3	¿Incluye el SDCPS del CIAC los procedimientos para la notificación de incidentes/accidente mediante personal operacional o producción?	Si No Parcial	
4	¿Es simple la notificación de incidentes/accidentes, es accesible para todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios?	Si No Parcial	
5	¿Tiene el CIAC procedimientos para la investigación de todos los incidentes/accidentes notificados?	Si No Parcial	
6	¿Existen procedimientos para garantizar que los peligros/amenazas identificados o descubiertos durante los procesos de investigación de incidentes/accidentes se explican correctamente y se integran en la recopilación de peligros y el procedimiento de mitigación de riesgos de la organización?	Si No Parcial	
7	¿Existen procedimientos para revisar peligros/amenazas de informes industriales pertinentes para medidas de seguimiento o la evaluación de riesgos, donde corresponda?	Si No Parcial	
Elemento 2.2 – Evaluación y mitigación de riesgos de seguridad operacional			
1	¿Existe un procedimiento de identificación de peligros y mitigación de riesgos (HIRM) documentado que implique el uso de herramientas de análisis de riesgos objetivas?	Si No Parcial	
2	¿Aprobaron el personal directivo o un nivel superior los informes de evaluación de riesgos, donde corresponda?	Si No Parcial	
3	¿Existe un procedimiento para la revisión periódica de los registros de mitigación de riesgos existentes?	Si No Parcial	
4	¿Existe un procedimiento para explicar las medidas de mitigación cada vez que se identifican niveles de riesgos inaceptables?	Si No Parcial	
5	¿Existe un procedimiento para priorizar los peligros identificados para las medidas de mitigación de riesgos?	Si No Parcial	
6	¿Existe un programa para la revisión sistemática y progresiva de todas las operaciones, los procesos, las instalaciones y los equipos relacionados con la seguridad operacional de la aviación sujetos al proceso de HIRM, como lo identificó la organización?	Si No Parcial	

No.	Aspecto a ser analizado o pregunta por responder	Respuesta	Estado de implementación
Componente 3 – ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL			
Elemento 3.1 – Observación y medición del rendimiento en materia de seguridad operacional			
1	¿Existen indicadores de rendimiento en materia de seguridad operacional identificados para medir y controlar el rendimiento en materia de seguridad operacional de las actividades de aviación del CIAC?	Si No Parcial	
2	¿Son los indicadores de rendimiento en materia de seguridad operacional relevantes con la política de seguridad operacional así como con los objetivos y metas de seguridad asumidos por el ejecutivo responsable?	Si No Parcial	
3	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional alertas y objetivos de seguridad operacional que definan las regiones de rendimiento inaceptable y las metas de mejora establecidas?	Si No Parcial	
4	¿Se basa la configuración de niveles de alerta o los criterios fuera de control en principios de métricas de seguridad operacional objetivos?	Si No Parcial	
5	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional un control cuantitativo de resultados de seguridad operacional de alto impacto (por ejemplos, tasas de incidentes de accidentes e incidentes graves), así como también, eventos de bajo impacto (por ejemplo, tasa de no cumplimiento, desviaciones)?	Si No Parcial	
6	¿Están los indicadores de rendimiento en materia de seguridad operacional y su configuración de rendimiento asociada desarrollados en función del acuerdo de la autoridad de aviación civil y sujetos a éste?	Si No Parcial	
7	¿Existe un procedimiento para una medida correctiva o de seguimiento que puede tomarse cuando no se logran los objetivos o se violan los niveles de alerta?	Si No Parcial	
8	¿Se revisan periódicamente los indicadores de rendimiento en materia de seguridad operacional?	Si No Parcial	
Elemento 3.2 Gestión del cambio			
1	¿Existe un procedimiento para la revisión de instalaciones y equipos existentes relacionados con la seguridad operacional de la aviación (incluidos los registros de HIRM) cada vez que haya cambios pertinentes a aquellas instalaciones y equipos?	Si No Parcial	
2	¿Existe un procedimiento para revisar las operaciones y los procesos existentes relacionados con la seguridad operacional de la aviación pertinente (como cualquier registro de HIRM) cada vez que haya cambios a aquellas operaciones o procesos?	Si No Parcial	
3	¿Existe un procedimiento para revisar las nuevas operaciones y los procesos relacionados con la seguridad operacional de la aviación en busca de peligros/riesgos antes de implementarlos?	Si No Parcial	

4	¿Existe un procedimiento para revisar las instalaciones, los equipos, las operaciones o los procesos existentes pertinentes (incluidos los registros de HIRM) cada vez que existan cambios pertinentes que sean externos a la organización, como normas reglamentarias/industriales, mejores prácticas o tecnología?	Si No Parcial	
No.	***Aspecto a ser analizado o pregunta por responder***	***Respuesta***	***Estado de implementación***
Elemento 3.3 – Mejora continua del SMS			
1	¿Existe un procedimiento para la evaluación/auditoría interna periódica del SMS?	Si No Parcial	
2	¿Existe un plan actual de la auditoría/evaluación de SMS interna?	Si No Parcial	
3	¿Incluye la auditoría de SMS la toma de muestras de las evaluaciones existentes completadas/de riesgos de seguridad operacional?	Si No Parcial	
4	¿Incluye el plan de auditoría del SMS la toma de muestras de los indicadores de rendimiento en materia de seguridad operacional para conocer la actualidad de los datos y el rendimiento de su configuración de objetivos/alertas?	Si No Parcial	
5	¿Aborda el plan de auditoría de SMS la interfaz de SMS con los subcontratistas o clientes, donde corresponda?	Si No Parcial	
6	¿Existe un proceso para que los informes de auditoría/evaluación de SMS puedan enviarse o destacarse para la atención del gerente responsable, cuando sea necesario?	Si No Parcial	
Componente 4 – PROMOCIÓN DE LA SEGURIDAD OPERACIONAL			
Elemento 4.1 – Instrucción y educación			
1	¿Existe un programa para proporcionar la instrucción/familiarización de SMS al personal que participa en la implementación u operación del SMS?	Si No Parcial	
2	¿Ha tomado el ejecutivo responsable un curso de familiarización, sesión informativa o capacitación de SMS adecuado?	Si No Parcial	
3	¿Se brinda al personal que participa en la evaluación de riesgos capacitación o familiarización adecuadas de la gestión de riesgos?	Si No Parcial	
4	¿Existe evidencia de esfuerzos de educación o toma de conciencia del SMS a nivel de la organización?	Si No Parcial	
Elemento 4.2 – Comunicación de la seguridad operacional			
1	¿Participa el CIAC en la distribución de información de seguridad operacional a proveedores de productos y servicios u organizaciones industriales externos pertinentes, incluidas las organizaciones reglamentarias de aviación pertinentes?	Si No Parcial	
2	¿Existe evidencia de una publicación, un circular o un canal de seguridad operacional (SMS) para comunicar la seguridad operacional y asuntos de SMS a los empleados?	Si No Parcial	
3	¿Hay un manual de SMS del CIAC y material guía relacionado accesible o distribuido a todo el personal pertinente?	Si No Parcial	

3. Análisis detallado de las brechas y de las tareas de implementación

Luego de completar la Tabla 1 - Lista de verificación para el análisis inicial de las brechas" debe elaborarse un plan detallado sobre "Acciones/Tareas requeridas" como el del ejemplo de la Tabla 2. En la Tabla 2, debe incluirse un 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 SMM como figura en la tabla.

4. Cronograma de implementación de las tareas/acciones

La Tabla 3 es una continuación de la Tabla 2 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 fases, cada tarea/acción requerida debe estar organizada de acuerdo con sus elementos y fases respectivas. Puede consultar la sección de este documento referida a la implementación por etapas para mayor información.

Asimismo, en la Tabla 4 se muestra la asignación de tareas relacionadas a los requisitos del SMS, utilizando un software como es el MS Project/Diagrama de Gantt o similar, que puede ser utilizado por el CIAC conforme a su conveniencia.

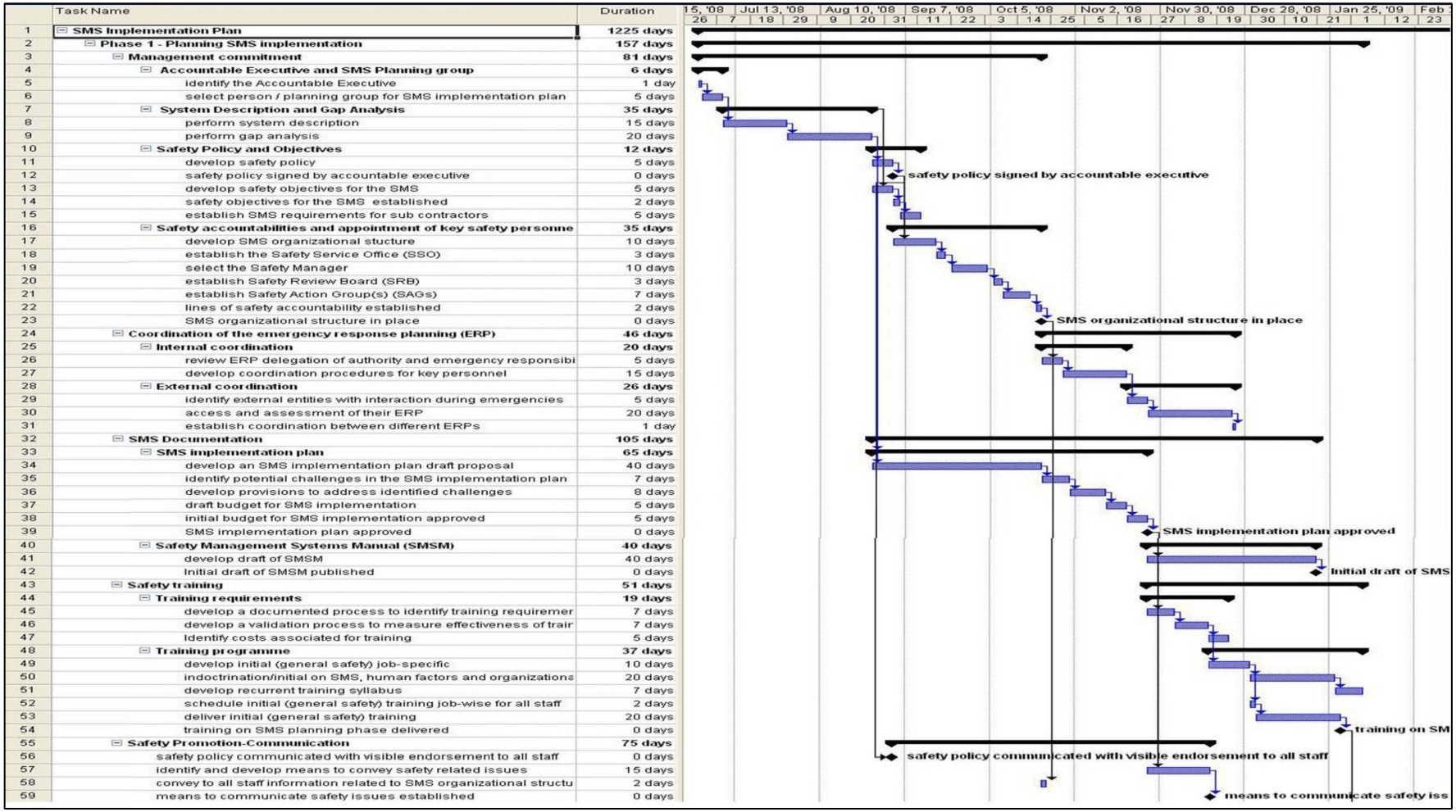
Tabla 2 – Análisis de las brechas del SMS e identificación de las tareas de implementación (Ejemplo del formato)

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

Tabla 3 – Cronograma de implementación del SMS (Ejemplo de formato)

Acción/tarea requerida para subsanar la	Ref. manual SMS	Persona o grupo asignado	Estado de la acción	Cronograma												
				1Q/10	2Q/10	3Q/10	4Q/10	1Q/11	2Q/11	3Q/11	4Q/11	1Q/12	2Q/12	3Q/12	4Q/12	Etc.
1. 1-1 a) Mejorar la política de seguridad existente para incluir las políticas y los objetivos del SMS, o desarrollar una nueva política de seguridad.	Capítulo 1, Sección 1.3	Grupo de acción 1	Abierta													
1. 1-1 b)Hacer aprobar y firmar la política de seguridad por el ejecutivo responsable.																

Tabla 4 – Ejemplo de asignación de tareas en Diagrama Gantt



	Task Name	Duration
1	**SMS Implementation Plan**	**1225 days**
2	**Phase 1 - Planning SMS implementation**	**157 days**
3	**Management commitment**	**81 days**
4	**Accountable Executive and SMS Planning group**	**6 days**
5	identify the Accountable Executive	1 day
6	select person / planning group for SMS implementation plan	5 days
7	**System Description and Gap Analysis**	**35 days**
8	perform system description	15 days
9	perform gap analysis	20 days
10	**Safety Policy and Objectives**	**12 days**
11	develop safety policy	5 days
12	safety policy signed by accountable executive	0 days
13	develop safety objectives for the SMS	5 days
14	safety objectives for the SMS established	2 days
15	establish SMS requirements for sub contractors	5 days
16	**Safety accountabilities and appointment of key safety personne**	**35 days**
17	develop SMS organizational stucture	10 days
18	establish the Safety Service Office (SSO)	3 days
19	select the Safety Manager	10 days
20	establish Safety Review Board (SRB)	3 days
21	establish Safety Action Group(s) (SAGs)	7 days
22	lines of safety accountability established	2 days
23	SMS organizational structure in place	0 days
24	**Coordination of the emergency response planning (ERP)**	**46 days**
25	**Internal coordination**	**20 days**
26	review ERP delegation of authority and emergency responsibi	5 days
27	develop coordination procedures for key personnel	15 days
28	**External coordination**	**26 days**
29	identify external entities with interaction during emergencies	5 days
30	access and assessment of their ERP	20 days
31	establish coordination between different ERPs	1 day
32	**SMS Documentation**	**105 days**
33	**SMS implementation plan**	**65 days**
34	develop an SMS implementation plan draft proposal	40 days
35	identify potential challenges in the SMS implementation plan	7 days
36	develop provisions to address identified challenges	8 days
37	draft budget for SMS implementation	5 days
38	initial budget for SMS implementation approved	5 days
39	SMS implementation plan approved	0 days
40	**Safety Management Systems Manual (SMSM)**	**40 days**
41	develop draft of SMSM	40 days
42	Initial draft of SMSM published	0 days
43	**Safety training**	**51 days**
44	**Training requirements**	**19 days**
45	develop a documented process to identify training requiremer	7 days
46	develop a validation process to measure effectiveness of trair	7 days
47	Identify costs associated for training	5 days
48	**Training programme**	**37 days**
49	develop initial (general safety) job-specific	10 days
50	indoctrination/initial on SMS, human factors and organizations	20 days
51	develop recurrent training syllabus	7 days
52	schedule initial (general safety) training job-wise for all staff	2 days
53	deliver initial (general safety) training	20 days
54	training on SMS planning phase delivered	0 days
55	**Safety Promotion-Communication**	**75 days**
56	safety policy communicated with visible endorsement to all staff	0 days
57	identify and develop means to convey safety related issues	15 days
58	convey to all staff information related to SMS organizational structu	2 days
59	means to communicate safety issues established	0 days

PAGINA DEJADA INTENCIONALMENTE EN BLANCO

Adjunto C

Orientación para el desarrollo de un 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 **aprobación** de la DINAC como una evidencia de aceptación 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

El SMSM propuesto ha sido estructurado de la siguiente manera:

a) Encabezado de sección

b) Objetivo

c) Criterios

d) Documentos de referencia cruzada

Debajo del cada ***encabezado de sección*** se encuentra la descripción del ***objetivo*** para esa sección, seguido del ***criterio*** para su cumplimiento, y las referencias a los documentos relacionados.

- El ***objetivo*** es lo que la organización pretende lograr al hacer lo que describe en una sección específica. El ***criterio*** define la forma y el alcance que deben tomarse en cuenta al escribir cada sección. Los ***documentos de referencia cruzada***, vinculan la información con otros manuales pertinentes o SOP de la organización, los que contienen detalles del elemento o proceso, según corresponda.

3. Contenido

El contenido del manual debe incluir como mínimo:

a) Control de documentos.

b) Requisitos reglamentarios del SMS.

c) Alcance e integración del SMS.

d) Política de seguridad operacional.

e) Objetivos de seguridad operacional.

f) Responsabilidades de la seguridad operacional y personal clave.

g) Notificación de seguridad operacional y medidas correctivas.

h) Identificación de peligros y evaluación de riesgos.

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

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

k) Capacitación y comunicación de seguridad operacional.

l) Mejora continua y auditoría de SMS.

m) Gestión de los registros de seguridad operacional.

n) Gestión de cambio y

o) Plan de respuesta ante emergencias/contingencia-

4. Control de documentos

Objetivo

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

Criterio

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

b) Explicación sobre la correlación del SMSM con el MIP y otros manuales existentes.

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

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

Documentos de referencia cruzada: MIP y otros manuales existentes.

5. Requisitos reglamentarios

Objetivo

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

Criterios

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

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

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

Documentos de referencia cruzada: Reglamentos relacionados con el SMS, material de referencia relacionado con el SMS, etc.

6. Alcance e integración del SMS

Objetivo

Describir la amplitud y el alcance de la implementación del SMS dentro de la organización. Definir el alcance, en términos de procesos, equipos y operaciones, que tendrá la identificación de peligros y gestión de riesgos (HIRM).

Criterio

a) Precisar la naturaleza del centro de instrucción, modelo de negocios y su posición o rol dentro del ámbito aeronáutico como un todo.

b) Identificar las áreas e instalaciones principales donde se aplicará el SMS.

c) Identificar los procesos, las operaciones y los equipos principales que se consideran idóneos para el programa HIRM de la organización, especialmente aquellos que son pertinentes para la seguridad operacional de la aviación. Si el alcance de los

procesos, las operaciones y los equipos idóneos de HIRM es demasiado detallado o extenso, se puede controlar de acuerdo con un documento complementario, según corresponda.

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

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

Documentos de referencia cruzada: MIP, manual de calidad (si es independiente), etc.

7. Política de seguridad operacional

Objetivo

Describir las intenciones y los principios de gestión de la organización, así como el compromiso de mejorar la seguridad operacional de la aviación, en términos del proveedor servicios. La política de seguridad operacional debería ser corta, clara y objetiva, parecida a una declaración de la misión.

Criterios

a) La política de seguridad operacional debe ser apropiada para el tamaño y la complejidad de la organización.

b) La política de seguridad operacional debe reflejar claramente las intenciones de la organización, los principios gerenciales y el compromiso para la mejora continua de la seguridad operacional de la aviación.

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

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

e) La política de seguridad operacional debe revisarse periódicamente.

f) El personal en todos los niveles debe estar involucrado en el establecimiento y mantenimiento del SMS.

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

Documentos de referencia cruzada: Política de seguridad operacional, etc.

8. Objetivos de seguridad operacional

Objetivo

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

Criterios

a) Se hayan establecido los objetivos de seguridad operacional.

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

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

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

e) Se han asignado recursos para lograr los objetivos.

f) Los objetivos de seguridad operacional deben estar vinculados con los indicadores de

seguridad operacional para facilitar su medición y control cuando sea necesario.

Documentos de referencia cruzada: Documentos que incluyen los indicadores de rendimiento en materia de seguridad operacional.

9. Funciones y responsabilidades

Objetivo

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

Criterios

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

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

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

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

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

Documentos de referencia cruzadas: Manual de exposición de la empresa, manual de administración, etc.

10. Notificación de seguridad operacional

Objetivo

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

Criterios

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

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

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

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

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

f) Los informes son almacenados en una base de datos que facilite su análisis y revisión.

Documentos de referencia cruzada: Política de seguridad operacional

11. Identificación de peligros y evaluación de riesgos

Objetivo

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

Criterios

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

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

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

d) El proceso de evaluación de los riesgos debe llevarse a cabo mediante el uso de formularios, hojas de cálculo o un software especializado, apropiados para la complejidad de la organización y sus operaciones.

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

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

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

12. Control y medición del rendimiento en materia de a seguridad operacional

Objetivo

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

Criterios

a) Debe existir un proceso formal y documentado para desarrollar y mantener un conjunto de indicadores de rendimiento en materia de seguridad operacional así como sus objetivos de eficacia asociados.

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

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

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

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

Objetivo

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

Criterios

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

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

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

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

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

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

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

Documentos de referencia cruzada: Política de seguridad operacional

14. Capacitación y comunicación de seguridad operacional

Objetivo

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

Criterios

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

b) Debe existir un procedimiento de validación para medir la eficacia de la capacitación.

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

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

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

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

Documentos de referencia cruzada: MIP.

15. Mejora continua y auditorías del SMS

Objetivo

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

Criterios

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

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

Documentos de referencia cruzada: MIP, manual de calidad (si es independiente).

16. Gestión de los registros de seguridad operacional

Objetivo

Describir el método utilizado para almacenar todos los, registros y documentos relacionados con el SMS.

Criterios

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

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

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

17. Gestión del cambio

Objetivo

Describir el proceso para la gestión de los cambios que tienen o pueden tener un impacto en los riesgos de la seguridad operacional, y la manera en la que estos procesos se integran con el SMS.

Criterios

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

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

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

Documentos de referencia cruzada: Procedimientos de instrucción relacionados con la gestión del cambio.

18. Plan de respuesta ante emergencia/contingencia

Objetivo

Describir las intenciones de la organización acerca de situaciones de emergencia y sus controles de recuperación correspondientes, además de su compromiso para abordar dichas situaciones. Describir las funciones y responsabilidades del personal clave. El plan de respuesta ante emergencias puede ser un documento separado o puede ser parte del manual de SMS.

Criterios

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

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

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

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

e) Existe un procedimiento para vigilar el bienestar de todas las personas afectadas y

para notificar al familiar más cercano.

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

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

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

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

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

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

Documentos de referencia cruzada: Manual de ERP, etc.

Adjunto D

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 DINAC, por tanto es necesaria la coordinación y el acuerdo entre los CIAC y los funcionarios responsables de la DINAC.

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 alto nivel. 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 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 alto impacto:

Nivel de alerta no violado	(Si=4, No=0)	Objetivo alcanzado	(Si=3, No=0)

Indicadores de bajo impacto:

Nivel de alerta no violado	(Si=2, No=0)	Objetivos alcanzada	(Si=1, No=0)

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

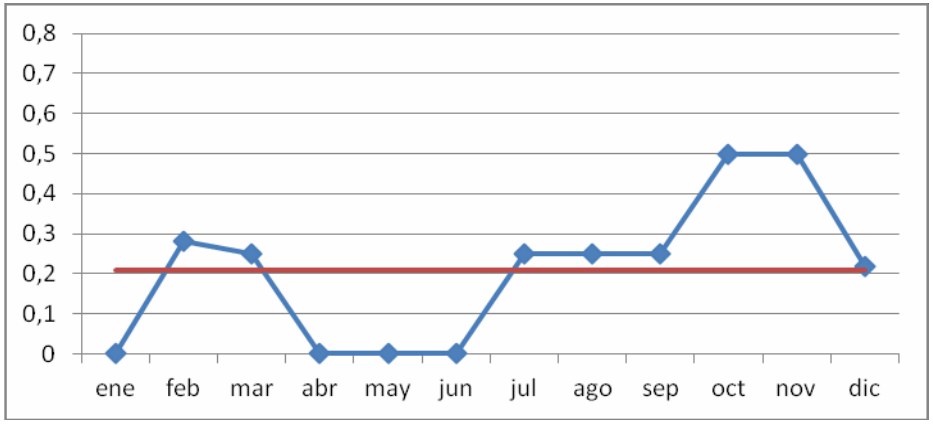
Tabla 5: Ejemplos de indicadores de cuestiones sistémicas

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.

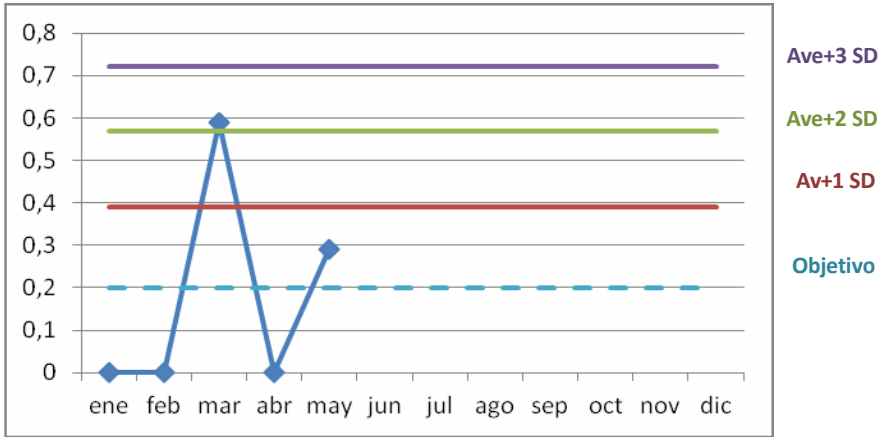
Tabla 1: Ejemplos de indicadores de rendimiento en materia de seguridad operacional

Indicadores de seguridad operacional del SSP (Estado)						Indicadores de rendimiento en materia de seguridad operacional del SMS (CIAC					
Indicadores de alto impacto (basado en sucesos//resultados)			Indicadores de bajo impacto			Indicadores de alto impacto			Indicadores de bajo impacto		
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/1000 HV)	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 2: Ejemplos de indicadores de rendimiento en materia de seguridad operacional

<table>
<tr>
<td> 

TASA MENSUAL DE INCIDENTES REPORTABLES (POR/1000 HV) CIAC 141 DEL PERIODO ANTERIOR

PROMEDIO DEL PERIODO ANTERIOR</td>
<td> 

TASA MENSUAL DE INCIDENTES REPORTABLES (POR/1000 HV) CIAC 141 DEL PERIODO ACTUAL

OBJETIVO PROMEDIO DEL PERIODO ACTUAL</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>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.

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 3: Ejemplos de indicadores de rendimiento en materia de seguridad operacional

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

Año anterior				
Mes	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**, esta basado en (Ave+1/2/3) 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 4: Ejemplo de medición de la eficacia de la seguridad operacional

Indicadores de alto nivel de la eficacia de la seguridad operacional					
Descripción del indicador (S.I.)		**Criterio/Nivel de alerta del S.I.**	**Nivel de alerta superado? (Si/No)**	**Criterio/Objetivo S.I.**	**Objetivo alcanzado /Si/no)**
1	Tasa 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 bajo nivel de la eficacia de la seguridad operacional					
Descripción del indicador (S.I.)		**Criterio/Nivel de alerta del S.I.**	**Nivel de alerta superado? (Si/No)**	**Criterio/Objetivo S.I.**	**Objetivo alcanzado /Si/no)**
1	Tasa combinada de incidentes de 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 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 revisados con respecto a la seguridad operacional en relación al año anterior.

Área	Enfoque de medición	Métrica
	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 que no habían sido percibidos por el personal/gestión previamente en comparación con el año anterior.

Área	Enfoque de medición	Métrica
		– 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 relación a los 10 últimos cambios.

Área	Enfoque de medición	Métrica
		– 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.

Adjunto E

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 DINAC 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 (DINAC, 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 DINAC 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 PRE 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.

Adjunto F

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 DINAC 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 DINAC.

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;*
- *alumnos;*
- *personal del aeródromo;*
- *personal de mantenimiento;*
- *Personal de aviación general*

¿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:…