CIRCULAR DE ASESORAMIENTO

CA	:	**145-6-A**
FECHA	:	**19/01/2021**
REVISIÓN	:	**01**
EMITIDA POR	:	**CTA/DSA**

ASUNTO: IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA (OMA) BAJO LA RAP 145

A. OBJETIVO

a) Proporcionar una guía para las organizaciones que solicitan una aprobación como organización de mantenimiento o para la modificación de una aprobación ya existente (Sección 145.100 de la RAP 145).

b) Proporcionar una guía a las organizaciones de mantenimiento aprobadas según la RAP 145, para la correcta interpretación del requisito establecido en su Sección 145.225 *"Implementación del sistema de gestión de la seguridad operacional (SMS)".*

c) Proporcionar lineamientos de como cumplir de una manera aceptable con los requisitos antes listados y verificar la implementación de los requisitos del Capítulo C de la RAP 145 en la OMA, en los plazos máximos establecidos por la DGAC.

B. APLICACIÓN

1. La presente circular de asesoramiento (CA) proporciona medios aceptables de cumplimiento y orientaciones para asistir a las organizaciones de mantenimiento RAP 145 en el establecimiento, implementación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS).

2. La RAP 145 especifica el marco para la implementación y mantenimiento de un SMS Independientemente del tamaño y la complejidad de la organización de mantenimiento, se aplican todos los elementos del marco de SMS. La implementación debe adaptarse a la organización y sus actividades. Asimismo, esta CA establece textos de orientación que contienen un ordenamiento propuesto y las acciones mínimas para cumplir con los requisitos de las siguientes secciones de la RAP 145:

   a) 145.205 - Política y objetivos de seguridad operacional;

   b) 145.210 - Gestión de riesgos de seguridad operacional;

   c) 145.215 - Aseguramiento de la seguridad operacional; y

   d) 145.220 - Promoción de la seguridad operacional.

3. Se incluye material de orientación sobre cómo desarrollar un manual de SMS y la

documentación asociada para organizaciones pequeñas. Como tal, aborda la escalabilidad en el extremo inferior del tamaño, la naturaleza y la complejidad de una organización, y los peligros y riesgos asociados inherentes a las actividades realizadas por la organización.

4. Esta CA describe recomendaciones con la intención de proporcionar una guía para la elaboración de procedimientos aceptables por la DGAC, a partir de lineamientos establecidos por el Estado Peruano, y las recomendaciones proporcionadas por la OACI y la industria aeronáutica civil. Como una CA no es de naturaleza obligatoria ni reglamentaria, los términos utilizados en sus textos forman parte del sentido de orientación para garantizar la aplicabilidad de su contenido. Estas recomendaciones no son las únicas; sin embargo, los procedimientos basados en otras diferente a lo descrito, requerirá una evaluación integral por parte de la DGAC para su aceptación como equivalentes.

***Nota**. — La definición del término Escalabilidad se muestra en la Sección DEFINICIONES.*

C. BASE LEGAL y DOCUMENTOS RELACIONADOS

1. Documento 9859, Manual de Gestión de la Seguridad Operacional, 4ta Edición – OACI
2. RAP 43, Mantenimiento.
3. Rap 145, Organizaciones de Mantenimiento Aprobadas.
4. RAP 11 Capitulo B. Reglas para la elaboración de la Reglamentación

D. CONTENIDO

Sección **Páginas**

E. DEFINICIONES Y ABREVIATURAS

1. Accidente.- Todo suceso relacionado con la utilización de una aeronave, que, en el caso de una aeronave tripulada, ocurre entre el momento en que una persona entra a bordo de la aeronave, con la intención de realizar un vuelo, y el momento en que todas las personas han desembarcado, o en el caso de una aeronave no tripulada, que ocurre entre el momento en que la aeronave está lista para desplazarse con el propósito de realizar un vuelo y el momento en que se detiene, al finalizar el vuelo, y se apaga su sistema de propulsión principal, durante el cual:

a) cualquier persona sufre lesiones mortales o graves a consecuencia de:

- hallarse en la aeronave, o
- por contacto directo con cualquier parte de la aeronave, incluso las partes que se hayan desprendido de la aeronave, o
- por exposición directa al chorro de un reactor, excepto cuando las lesiones obedezcan a causas naturales, se las haya causado una persona a sí misma o hayan sido causadas por otras personas o se trate de lesiones sufridas por pasajeros clandestinos escondidos fuera de las áreas destinadas normalmente a los pasajeros y la tripulación; o

b) la aeronave sufre daños o roturas estructurales que:

- afectan adversamente su resistencia estructural, su performance o sus características de vuelo; y que normalmente exigen una reparación importante o el recambio del componente afectado, excepto por falla o daños del motor, cuando el daño se limita a un solo motor (incluido su capó o sus accesorios); hélices, extremos de ala, antenas, sondas, álabes, neumáticos, frenos, ruedas, carenas, paneles, puertas de tren de aterrizaje, parabrisas, revestimiento de la aeronave (como pequeñas abolladuras o perforaciones), o por daños menores a palas del rotor principal, palas del rotor compensador, tren de aterrizaje y a los que resulten de granizo o choques con aves (incluyendo perforaciones en el radomo); o

c) la aeronave desaparece o es totalmente inaccesible.

***Nota 1**. — Para uniformidad estadística únicamente, toda lesión que ocasione la muerte dentro de los 30 días contados a partir de la fecha en que ocurrió el accidente, está clasificada por la OACI como lesión mortal.*

***Nota 2**. — Una aeronave se considera desaparecida cuando se da por terminada la búsqueda oficial y no se han localizado los restos.*

***Nota 3**. — El tipo de sistema de aeronave no tripulada que se investigará se trata en 5.1 del Anexo 13.*

***Nota 4**. — En el Adjunto E del Anexo 13 figura orientación para determinar los daños de aeronave.*

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

3. **Clima de SMS. -** El valor percibido que se otorga a la seguridad operacional en una organización en un momento determinado.

4. **Control del riesgo. -** Un medio para reducir o eliminar los efectos de los peligros.

5. **Cultura justa. -** Una cultura en la que las personas no son castigadas por acciones, omisiones o decisiones tomadas por ellos que sean acordes con su experiencia y formación, pero donde no se toleran negligencias graves, violaciones intencionales y actos destructivos.

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

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

7. **Datos de seguridad operacional. -** Conjunto de hechos definidos o conjunto de valores de seguridad operacional recopilados de diversas fuentes de aviación, que se utiliza para mantener o mejorar la seguridad operacional.

   ***Nota**. — Dichos datos sobre seguridad operacional se recopilan a través de actividades preventivas o reactivas relacionadas con la seguridad operacional, incluyendo, entre otros, lo siguiente:*

   a) investigaciones de accidentes o incidentes;

   b) notificaciones de seguridad operacional;

   c) notificaciones sobre el mantenimiento de la aeronavegabilidad;

   d) supervisión de la eficiencia operacional;

   e) inspecciones, auditorías, constataciones; o

   f) estudios y exámenes de seguridad operacional.

8. **Dato de SMS. -** Datos utilizados para garantizar el rendimiento de SMS. Ejemplos:

   - Registro de informes de peligros y muestras de informes.
   - Resultados de las evaluaciones de riesgos.
   - Indicadores de rendimiento de seguridad operacional y gráficos relacionados.
   - Registro de evaluaciones de seguridad operacional completadas o en curso.
   - Registros de auditoría o revisión interna de SMS.
   - Registros de promoción de la seguridad operacional.
   - Registros de capacitación en seguridad operacional / SMS del personal.

- Actas de la reunión del comité de seguridad operacional / SMS.
- Plan de implementación de SMS (durante el proceso de implementación).

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

10. **Escabilidad. -** es la propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para reaccionar y adaptarse sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

11. **Evento. -** Cualquier anomalía en la operación de un producto de aviación o en el desempeño de la actividad de una organización.

12. **Falla de calidad. -** Cualquier producto certificado por la organización que posteriormente se determine que no cumple con los requisitos del contrato o de la especificación del producto, o ambos.

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

14. **Gestión del mantenimiento de la aeronavegabilidad. -** Un proceso por el cual una aeronave certificada de tipo se mantiene en condiciones de aeronavegabilidad, cumpliendo con las condiciones técnicas fijadas para la emisión del certificado de aeronavegabilidad y es mantenida en condiciones de operación segura (técnicamente apta para vuelo).

15. **Gestión del riesgo de la seguridad operacional (SRM). -** Un proceso dentro del SMS que identifica el peligro, analiza, evalúa y controla los riesgos relacionados.

16. **Incidente. -** Todo suceso relacionado con la utilización de una aeronave, que no llegue a ser un accidente, que afecte o pueda afectar la seguridad de las operaciones.

    Nota**. — Entre los tipos de incidentes que son de interés para los estudios relacionados con la seguridad operacional figuran los incidentes enumerados en el **Anexo 13, Adjunto C.

17. **Mantenimiento de la aeronavegabilidad. -** Conjunto de procedimientos que permite asegurar que una aeronave, motor, hélice o pieza cumple con los requisitos aplicables de aeronavegabilidad y se mantiene en condiciones de operar de modo seguro durante toda su vida útil.

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

19. **Objetivo de seguridad operacional. -** Una declaración breve y de alto nivel del logro de seguridad operacional o resultado deseado que ha de conseguirse

mediante el programa estatal de seguridad operacional o el sistema de gestión de la seguridad operacional del proveedor de servicios.

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

20. Organización. - En el alcance de esta circular de asesoramiento, cualquier entidad, aprobada o no aprobada, independientemente de su tamaño, que realice una actividad de diseño, fabricación o mantenimiento de aeronaves, hélices, motores de aeronaves o partes y aparatos. La OACI está utilizando el término "proveedor de servicios" para esas organizaciones.

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

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

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

***Nota**. — Cuando se documenta un procedimiento, el término "procedimiento escrito" o "procedimiento documentado" se utiliza con frecuencia. El documento que contiene un procedimiento puede denominarse "documento de procedimiento".*

24. Producto. - Un término amplio que incluye aeronave, motor de aeronave, hélice de aeronave, parte o dispositivo de aeronave o ambos, sus subcomponentes (hardware y software) y servicios asociados como la documentación necesaria para la operación y mantenimiento (por ejemplo, Instrucciones para el mantenimiento de la aeronavegabilidad, manual de vuelo de la aeronave).

25. Promoción de la seguridad operacional. - Una combinación de capacitación y comunicación de información de seguridad operacional para apoyar la implementación y operación de un SMS en una organización que mejora su cultura de seguridad operacional.

26. Rendimiento 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.

27. Riesgo de seguridad operacional. - La probabilidad y la gravedad previstas de las consecuencias o resultados de un peligro.

28. 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 y controlan a un nivel aceptable.

29. Sistema de gestión. - Un marco de políticas, procesos y procedimientos utilizados por una organización para garantizar que puede cumplir con todas las tareas necesarias para lograr sus objetivos.

30. Sistema de gestión de seguridad operacional (SMS). - Enfoque sistemático para la gestión de la seguridad operacional que incluye las estructuras orgánicas, la

obligación de rendición de cuentas, las responsabilidades, las políticas y los procedimientos necesarios.

31. **SMS corporativo. -** La gobernanza, la estructura y los procesos corporativos para cubrir algunos o todos los elementos comunes en todos los dominios (como la responsabilidad, la política de seguridad operacional, la identificación de peligros y los principios de gestión de los riesgos de seguridad operacional, la recopilación y evaluación de datos de seguridad operacional, la conciencia y capacitación en seguridad operacional)
Los SMS corporativos no son obligatorios, pero podrían facilitar la implementación consistente de SMS en empresas que tienen múltiples aprobaciones y/o certificados.

32. **Suceso. -** Todo accidente o incidente relacionado con la operación de una aeronave.

CCA . - Análisis de Causa Común
DMS . - Sistema de Gestión de la Documentación
DOA . - Aprobaciones a Organizaciones de Diseño
EMS . - Sistema de Gestión Ambiental
ERP . - Plan de Respuesta ante Emergencia
FHA . - Evaluación de Riesgos Funcionales
FMEA . - Análisis de Modos de Falla y Efectos
FRMS . - Sistema de Gestión de Riesgo de la Fatiga
MDR . - Informe Obligatorio de Defectos
MRO . - Organizaciones de Mantenimiento, Reparación y revisión general
MSMS . - Manual del Sistema de Gestión de Seguridad Operacional
MTBF . - Tiempo Medio Entre Fallos
MTBUR . - Tiempo Medio Entre Cambios No Programados
OHSMS . - Sistema de Gestión de la Seguridad Operacional y Salud Ocupacional
PFMEA . - Análisis de Modos de Falla y Efectos en Proceso
POA . - Organizaciones de Producción Aprobadas
PSSA . - Evaluación Preliminar de Seguridad Operacional del Sistema
QMS . - Sistema de Gestión de Calidad
SA . - Aseguramiento de la Seguridad Operacional
SAA . - Evaluación de la Seguridad Operacional del Sistema
SAG . - Grupo de Acción de Seguridad Operacional
SMS . - Sistema de Seguridad Operacional
SPI . - Indicador de Rendimiento en materia de Seguridad Operacional
SPT . - Metas de Rendimiento en materia de Seguridad Operacional
SRB . - Junta de Revisión de Seguridad Operacional
SRM . - Gestión de Riesgos de la Seguridad Operacional

SSP . - Seguridad Operacional del Estado

ZSA . - Análisis de Seguridad Operacional Zonal

F. ANTECEDENTES

F.1 Componentes y Elementos

1. El marco de un Sistema de Gestión de Seguridad Operacional SMS contiene los 4 componentes y 12 elementos que se muestran en la siguiente tabla:

COMPONENTE	ELEMENTO
1. Política y Objetivos de Seguridad Operacional	1.1 Compromiso de la Dirección
	1.2 Obligación de Rendición de cuentas y responsabilidades en materia de Seguridad Operacional.
	1.3 Designación del Personal Clave de Seguridad Operacional.
	1.4 Coordinación de la Planificación de Respuesta ante Emergencia.
	1.5 Documentación SMS.
2. Gestión de riesgos de Seguridad Operacional	2.1 Identificación de peligros
	2.2 Evaluación y mitigación del rendimiento en materia de Seguridad.
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

2. El primer componente del marco de SMS se centra en la creación de un entorno en el que la gestión de la seguridad operacional puede ser eficaz. Se basa en una política y objetivos de seguridad operacional que establecen el compromiso de la alta dirección con la seguridad operacional, sus metas y la estructura organizacional de apoyo.
3. El segundo componente proporciona un marco para ayudar a las organizaciones a gestionar sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional (SRM), que incluye la identificación de peligros, la evaluación de riesgos, y la gestión de riesgos.
4. El tercer componente proporciona los medios para verificar el rendimiento de seguridad operacional de la organización y para validar la eficacia de los controles de riesgos de seguridad operacional.

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

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

F.2 Gestión de Proveedores

1. Las actividades de aviación son realizadas y respaldadas por una multitud de negocios interconectados. La OMA es responsable de administrar y monitorear cómo interactúan con esas organizaciones, también conocidas como terceros. Es probable que el nivel general de seguridad operacional en la industria de la aviación aumente cuando se comprendan y controlen mejor los riesgos de seguridad operacional relacionados con esas conexiones.

2. Un SMS no solo se aplica a la OMA, se extiende a terceros (personas y organizaciones) que suministran productos y servicios para que la OMA realice el mantenimiento, y a terceros que son suministrados con productos o servicios proporcionados por la OMA. Es posible que algunos de estos terceros no tengan (o requieran) un SMS, pero todos tienen el potencial de afectar los riesgos de seguridad operacional para la organización certificada. Al identificar y administrar estas interfaces, la organización tendrá más control sobre los riesgos de seguridad operacional relacionados con las interfaces. Estas interfaces de terceros deben definirse y describirse en el sistema de gestión de seguridad operacional de la organización (descripción del sistema). En el Capitulo H se expresan las interfases entre organizaciones, las cuales considera también las Interfases internas.

F.3 Escalabilidad del SMS

NOTA. - *"El sistema de la organización para la gestión de la seguridad operacional debe corresponder al tamaño, la naturaleza y complejidad de las actividades realizadas por la OMA, y los peligros y riesgos asociados inherentes a las actividades realizadas por la organización*

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

2. Independientemente del tamaño de la organización, la escalabilidad también deberá ser una función del riesgo de seguridad operacional inherente de las actividades realizadas. Incluso las OMAs pequeñas pueden participar en actividades que pueden entrañar importantes riesgos para la seguridad operacional

de la aviación. Por lo tanto, la capacidad de gestión de la seguridad operacional debe estar en consonancia con el riesgo de seguridad operacional a gestionar.

3. La Figura 1 muestra la relación de los peligros y los riesgos asociados para las actividades realizadas, conectadas como un todo dentro del contexto organizacional y el entorno empresarial y físico.

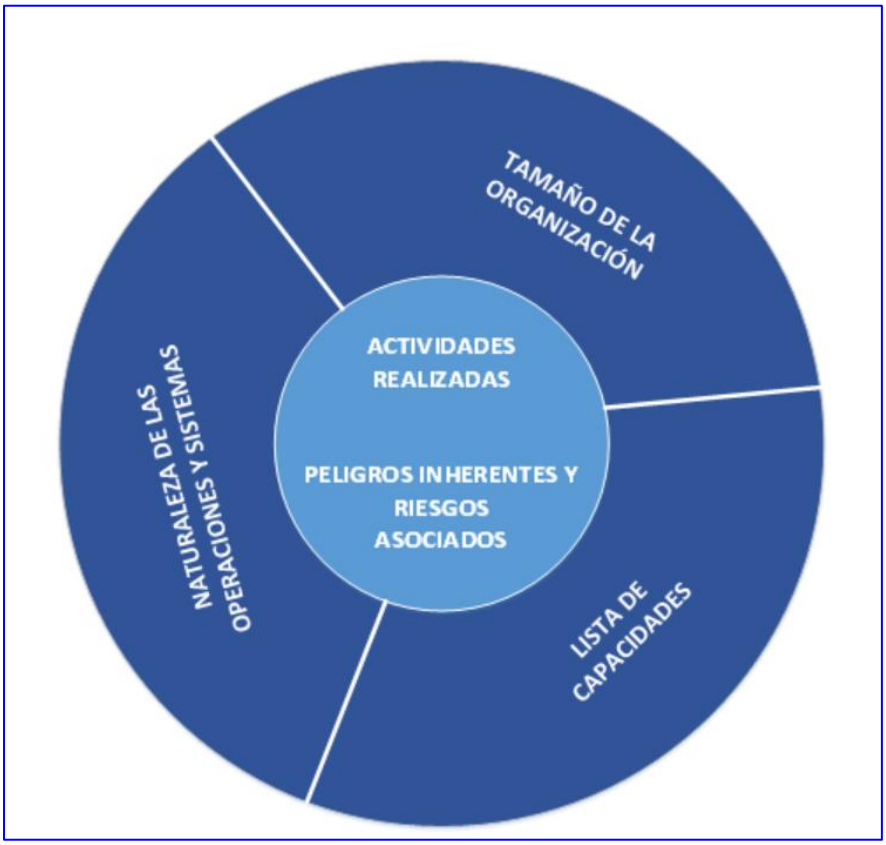


Figura 1. Concepto de tamaño, naturaleza y complejidad en relación con el riesgo de la actividad

4. La siguiente tabla muestra ejemplos de tres tipos diferentes de trabajos, con un tamaño aproximado en términos de empleados equivalentes a tiempo completo. En la columna que muestra los indicadores de complejidad, el tipo en negrita indica el factor de riesgo de cada ejemplo (OMA para dar mantenimiento a aeronaves: de menos de 5,700 Kg, nueva OMA, múltiples bases adicionales, diferentes tipos de aeronaves). A medida que se acumula la experiencia, la familiaridad con la gestión de varios tipos y la operación en áreas remotas evoluciona, por lo que cambia el nivel de riesgo. Con cambios en esas mismas organizaciones de ejemplo (nueva aeronave, fusión organizacional, organización corporativa), pueden surgir otros riesgos. Es importante reconocer estas relaciones, que son fundamentales para el enfoque de SMS basado en riesgos.

NATURALEZA DE LAS OPERACIONES Y SISTEMAS	TAMAÑO	INDICADORES DE COMPLEJIDAD
OMA para mantener aeronaves < 5,700 Kg	< 5 personas	***Nueva organización*** con sistemas inmaduros, un solo modelo de aeronave, trabajos solo diurnos.
OMA corporativa para mantener aeronaves > 5,700 Kg y componentes	> 20 personas	***Múltiples bases adicionales*** nacionales y extranjeras, alta experiencia en gestión, personal competente, diferentes talleres de componentes.
OMA para mantener aeronaves y componentes < 5,700 Kg.	> 5 < 20 personas	Número medio de habilitaciones, con ***5 marcas y modelos de aeronaves***, 5 ***bases adicionales*** de mantenimiento.

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

5. Para determinar la dimensión y complejidad de la organización referirse a la CA 145-001, MAC 145.200.

F.4 Desafíos para organizaciones más pequeñas

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

2. Las organizaciones deben hacerse las siguientes preguntas en todas las etapas del desarrollo, implementación y funcionamiento de su SMS:

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

- ¿Es eficaz y produce los resultados esperados?

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

F.5 Escalabilidad y evaluación de los SMS de una OMA

1. Cada OMA es diferente. Los SMS están diseñados para adaptarse a las necesidades específicas de la organización.
2. Todos los componentes y todos los elementos del SMS están interconectados y son interdependientes, y son necesarios para funcionar de manera eficaz. El sistema está diseñado para ofrecer los resultados deseados para cada organización sin una carga indebida. Los SMS, bien implementados, están destinados a complementar y mejorar los sistemas y procesos existentes de la organización.
3. Se logrará una gestión de seguridad operacional eficaz mediante una planificación e implementación cuidadosa que garanticen que cada requisito se aborde de manera que se adapte a la cultura y el entorno operacional de la OMA.
4. La DGAC al evaluar el SMS de una OMA, tendrá en cuenta la escalabilidad. La DGAC proporciona la herramienta de evaluación de SMS, la cual puede ser obtenida de la página web https://www.gob.pe/institucion/mtc/colecciones/331-manual-del-inspector-de-aeronavegabilidad-de-la-dgac, MIA, Parte I, Capítulo 14, para ayudar a las organizaciones a determinar cómo evaluar, desarrollar e implementar mejor los diversos elementos de un SMS eficaz adaptado a su organización. La herramienta proporciona orientación durante la implementación inicial y la certificación para evaluar los procesos y sistemas de una organización para un SMS que se escala para que sea acorde con el tamaño de la organización, la naturaleza y la complejidad de sus actividades y los peligros y riesgos asociados inherentes a las actividades.
5. La herramienta se divide en 13 elementos, y cada elemento se subdivide para proporcionar más detalles para ayudar a la organización y a la DGAC a evaluar el sistema. No se aplicarán todos los sub-elementos, dependiendo de la escala de la organización.
6. Es posible que las organizaciones más pequeñas y menos complejas que realizan actividades con menos peligros inherentes y menores riesgos asociados solo necesiten demostrar cómo cumplen los requisitos para cada elemento en el requisito de alto nivel que se muestra en la parte superior de cada tabla en el formulario.
7. Para organizaciones más grandes y complejas o aquellas que participan en actividades con más peligros inherentes y mayores riesgos asociados, es probable que se deban abordar progresivamente más sub-elementos a medida que la organización desarrolla sus procesos de gestión de la seguridad operacional.

Nota. *— Consulte las secciones J (Implementación del SMS) y K (Madurez de su SMS) de esta circular de asesoramiento para obtener más información y orientación sobre la implementación de los elementos de un SMS.*

F.6 Integración del SMS con otros sistemas de gestión

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

2. Un sistema típico de gestión integrado puede incluir:

   a) Sistema de Gestión de la Calidad (QMS);

   b) Sistema de Gestión de la Seguridad Operacional (SMS);

   c) Sistema de Gestión de la Seguridad de la Aviación (SeMS);

   d) Sistema de Gestión Ambiental (EMS);

   e) Sistema de Gestión de la Seguridad Operacional y Salud Ocupacional (OHSMS);

   f) Sistema de Gestión Financiera (FMS);

   g) Sistema de Gestión de la Documentación (DMS); y

   h) Sistema de Gestión del Riesgo de la Fatiga (FRMS)

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

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

reglamentarios, estatutarios y de las partes interesadas. Sea cual sea la opción tomada, deberá garantizar que reúna los requisitos de SMS.

5. Beneficios y desafíos de la integración de sistemas de gestión:

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

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

b) reducción de las responsabilidades y relaciones potencialmente conflictivas.

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

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

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

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

b) podría haber resistencia al cambio para el personal afectado por la integración, ya que esto requerirá una mayor cooperación y coordinación;

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

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

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

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

8. Integración de SMS y QMS:

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

2. Ambos sistemas son complementarios, el SMS se centra en la gestión de los riesgos y el rendimiento de la seguridad operacional mientras que el QMS se centra en el cumplimiento de los reglamentos y requisitos prescriptivos para

cumplir con las expectativas del cliente y las obligaciones contractuales. Los objetivos de un SMS son identificar los peligros, evaluar el riesgo asociado de seguridad operacional asociado e implementar controles efectivos de riesgos de seguridad operacional. En contraste, el QMS se enfoca en la entrega consistente de productos y servicios que cumplen con las especificaciones aplicables. No obstante, ambos el SMS como el QMS:

a) deberán ser planificados y gestionados;

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

c) identifican procesos y procedimientos ineficaces;

d) se esfuerzan por mejorar continuamente; y

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

3. El SMS se centra en:

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

b) evaluación del riesgo de seguridad operacional asociado;

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

d) medición del rendimiento de seguridad operacional; y

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

4. El QMS se centra en:

a) cumplimiento de los reglamentos y requisitos;

b) consistencia en la entrega de productos y servicios;

c) cumplimiento con los estándares de rendimiento especificados:

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

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

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

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

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

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

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

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

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

F.7 Cultura de la seguridad operacional

1. Introducción

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

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

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

4. Cuando la organización tiene una cultura de seguridad operacional positiva, y esto es visiblemente respaldado por el Gerente responsable y el personal clave, el personal de primera línea tiende a sentir un sentido de responsabilidades compartidas hacia el logro de los objetivos de seguridad operacional de la organización. La gestión de seguridad operacional eficaz también respalda los esfuerzos para impulsar una cultura de seguridad

operacional cada vez más positiva al aumentar la visibilidad del apoyo de la dirección y mejorar la participación activa del personal en la gestión de riesgos de seguridad operacional.

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

Vínculo entre SMS y cultura de seguridad operacional
U otra forma de verlo

SMS + Cultura = Desempeño en seguridad operacional

(marco) + (comportamientos) = (logro)

"*Los SMS nunca son suficientes si se practican mecánicamente, se requiere una cultura de seguridad operacional eficaz para florecer*". *(Hudson, 2001).*

7. La cultura de seguridad operacional puede describirse mediante seis características de alto nivel, como se muestra a continuación y se amplía en el numeral F.7.4) Desarrollo de una cultura de seguridad operacional positiva:

2. <u>Cultura de Seguridad Operacional y notificaciones de seguridad operacional</u>

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

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

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

3. Toma de decisiones basada en datos

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

a) cultura de presentación de notificaciones: ¿la organización fomenta la presentación de notificaciones?

b) cultura de aprendizaje: ¿la organización trata la información como una oportunidad para hacer crecer su cultura de seguridad operacional?

c) cultura flexible: ¿la organización actúa sobre la información para mejorar la seguridad operacional?

4. Desarrollo de una cultura de seguridad operacional positiva

1. Debemos tener cuidado con los intentos de "implementar" o "crear" una cultura como se haría con un interruptor. Las culturas no se transforman de la noche a la mañana, pero puede cambiar el entorno de trabajo y la forma en que las personas trabajan juntas, y explicar claramente los comportamientos que se esperan de todos. Puede evaluar actitudes y comportamientos, pero las personas no cambiarán a menos que las nuevas formas se acepten como una mejora.

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

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

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

Característica	Habilitadores	Deshabilitadores
actividades • Desde la perspectiva del Estado el personal es consciente de los riesgos de seguridad operacional inducidos por sus propias actividades y las organizaciones que supervisan. Los empleados y la administración deberían mantener constantemente un alto grado de vigilancia con respecto a la seguridad operacional	• Las investigaciones procuran establecer las causas básicas • La organización está siempre al tanto de importantes mejoras de la seguridad operacional y se adapta a las mismas según sea necesario • La organización evalúa sistemáticamente si se aplican y funcionan según lo previsto las mejoras de la seguridad operacional • Los miembros apropiados de la organización están bien conscientes de los riesgos de seguridad operacional inducidos por sus acciones individuales y las operaciones o actividades de la compañía	viable sin procurar determinar la causa básica • La organización no está al tanto de importantes mejoras de seguridad operacional • La organización no evalúa si se implantan adecuadamente las mejoras de seguridad • Cuando corresponde, los miembros de la organización no están conscientes de los riesgos de seguridad operacional inducidos por sus acciones individuales y operaciones de la compañía • Los datos de seguridad operacional se recopilan pero no se analizan ni se toman medidas al respecto
COMPORTAMIENTO		
El comportamiento con respecto a la seguridad operacional refleja el grado en que todos los niveles de la organización se comportan para mantener y mejorar el nivel de seguridad operacional. La importancia de la seguridad operacional debería reconocerse y se deberían instituir procesos y procedimientos necesarios para mantenerla	• Los empleados se automotivan para actuar en forma segura y como ejemplos • Se practica la observación continua del comportamiento de seguridad operacional • El comportamiento inseguro intencional no es tolerado por la administración y los colegas • Las condiciones de trabajo apoyan la seguridad operacional de la aviación en todo momento	• Los empleados no son castigados por el comportamiento inseguro intencional en beneficio de sus propios intereses o los de terceros • Las condiciones de trabajo provocan comportamientos y acciones alternativas que van en detrimento de la seguridad operacional de la aviación • No se vigila la seguridad operacional de la aviación dentro de los productos al servicio de la organización • No se ven con agrado las críticas constructivas para beneficiar la seguridad operacional de la aviación
INFORMACIÓN		
• La información refleja el grado en que se distribuyen los conocimientos y datos a todas las personas necesarias dentro de la organización. Debería permitirse y fomentarse que los empleados notifiquen preocupaciones de seguridad operacional de la aviación y reciban comentarios sobre sus	• Existe un entorno abierto y justo para notificar problemas de seguridad operacional • Se brinda a los empleados información sobre seguridad operacional en forma oportuna para permitir la realización de operaciones o la toma de	• Es evidente un entorno de notificación de seguridad operacional con asignación de culpas • Se retiene la información sobre seguridad operacional • No se vigila la eficacia de las comunicaciones de

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

5. Monitoreo de la cultura de seguridad operacional

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

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

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

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

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

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

G. PROCESO DE IMPLEMENTACION

G.1 Los primeros objetivos y tareas del proceso de implementación del SMS en la organización de mantenimiento nacen de la necesidad de establecer cuál es la condición en que se encuentra la organización, en relación al desarrollo de los requisitos de aceptación del SMS que deben ser implementados, de acuerdo con los requisitos reglamentarios de la RAP 145 aplicables.

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

G.3 Inicialmente la OMA junto con los miembros del equipo de implementación del SMS, deberán establecer el alcance de su SMS, en base a un análisis de su accionar, procesos de mantenimiento, política y objetivos del SMS, y fundamentalmente establecer las interfaces del sistema con otras organizaciones o contratistas. Con el alcance, será posible establecer las brechas existentes entre los requisitos del SMS y las capacidades, procesos y procedimientos que posee la OMA, a fin de determinar la magnitud del trabajo a realizar, la envergadura y los costos del proceso de implementación del SMS a realizar, y la manera como este trabajo será efectuado en un plazo definido (plan de implementación).

G.4 Definido esto, también será necesario establecer en que tiempo se establecerán e implementaran los elementos del marco de trabajo del SMS (los tiempos variarán de acuerdo a la dimensión y complejidad de la organización de mantenimiento), cuáles serán los medios humanos y materiales que se asignarán y la estructura funcional que se ocupará para efectuar esta actividad, en forma simultánea al funcionamiento normal de la OMA, según sea aplicable.

G.5 Conjuntamente y por su importancia, se debe iniciar la instrucción y la comunicación del SMS en la OMA para la preparación y concientización del personal en este nuevo sistema de gestión de los riesgos en la organización y sobre la importancia de su participación en estos procesos. Estas actividades son parte del proceso de implementación y en el caso de la capacitación se irán incorporando paulatinamente los nuevos requisitos y procedimientos al programa de capacitación que la OMA tenía implementado al certificarse. Al iniciar la implementación del SMS el convencimiento de la alta dirección sobre la importancia de este sistema y su involucramiento en este proceso serán fundamentales para su éxito.

G.6 Este hito se completará cuando estén definidas y solucionadas estas interrogantes y se encuentre coordinado con la DGAC los plazos de cumplimiento y las metas a lograr en cada una de las actividades de implementación del SMS (plan de implementación).

G.7 En el siguiente paso, la organización que ya definió como efectuará la implementación de su SMS, establecerá la política y los objetivos que orientarán el desarrollo de la documentación y procedimientos, asimismo definirá las responsabilidades internas que deberán ser asumidas en todos los niveles de la organización como consecuencia de incorporar este nuevo sistema. Esto último requiere ser difundido por el gerente responsable, dada su importancia y trascendencia y por la necesidad de hacer comprender que la implementación del SMS es responsabilidad de toda la organización.

G.8 Una vez que la organización ha definido la política, objetivos y las responsabilidades internas, se dará inicio a la confección del manual del SMS (MSMS) y de los primeros documentos orientados al funcionamiento interno de la OMA. Asimismo, se designará a la **junta de revisión de seguridad operacional** (SRB) y al **grupo**

de acción de seguridad operacional (SAG), cuando sea aplicable. Durante esta etapa y de ser necesario, la organización de mantenimiento también desarrollará el plan de respuesta ante emergencias para accidentes e incidentes en coordinación con los explotadores de aeronaves y otras emergencias de aviación, según sea aplicable. Este plan deberá estar coordinado de forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que la organización deba interactuar al suministrar sus servicios o productos.

G.9 El siguiente paso se corresponde con establecer los elementos que tiene como objetivo establecer procesos de gestión de riesgos del marco de trabajo del SMS. con el establecimiento de estos elementos la OMA estará lista para recopilar datos de seguridad operacional y realizar análisis basados en la información obtenida mediante diversos sistemas de notificación.

G.10 Se deben implementar los procedimientos e indicadores con que deberá trabajar la nueva oficina o departamento creado bajo la dirección de un responsable de SMS, nominado por el gerente responsable, que está participando en la implementación. Con estas herramientas y el desarrollo de la documentación en ejecución es posible empezar a recibir y procesar en la oficina o departamento de seguridad operacional la información de SMS de la OMA.

G.11 También, para las organizaciones de mantenimiento ya certificadas, es el momento de incorporar al sistema toda aquella información que la OMA posee de los accidentes e incidentes en los que ha estado involucrado previamente, con sus correspondiente evaluaciones y acciones correctivas, las acciones de prevención desarrolladas y las auditorias de calidad internas y externas que la OMA realiza como parte de los requisitos de calidad que debe cumplir desde su certificación. Esta información permitirá el desarrollo de indicadores de alta gravedad/baja probabilidad y alta probabilidad/baja gravedad, y empezar a completar las bases de información o de datos de seguridad operacional de la OMA. La DGAC deberá aceptar los indicadores presentados por la OMA, desarrollados en base a la experiencia y sustentados en datos de seguridad operacional.

G.12 Los elementos de la implementación y funcionamiento maduro del SMS se corresponden a la consolidación del sistema y a la incorporación plena de esta nueva organización interna de SMS (sección o departamento) en la OMA; a la consolidación de una nueva cultura de trabajo con responsabilidades, procedimientos y manuales complementarios en la organización; indicadores que permitan orientar su desempeño con una optimización de los recursos asignados y una mejora potencial en la seguridad operacional en el producto o servicio que entrega, en su imagen corporativa, en su relación con sus operadores, y subcontratistas; y finalmente en el compromiso de su personal con la OMA y su sistema de seguridad operacional.

G.13 Para las OMA ya certificadas, todo el desarrollo efectuado deberá mostrar sus resultados, así como su efectividad y eficiencia. Será la demostración de si la OMA efectuó en buena forma la incorporación del SMS a sus actividades normales, luego de su certificación inicial previa.

G.14 También, se debe asegurar que los procesos de capacitación normales de la OMA incorporen en forma permanente estos nuevos temas de SMS y se mantenga la

motivación, compromiso y participación del personal en el sistema, mediante una buena difusión de los logros alcanzados, el compromiso permanente de la alta dirección y la retroalimentación de los análisis de causa raíz realizados a la información de peligros por ellos informados, junto a las acciones tomadas para solucionarlos, en los casos que lo amerite.

G.15 Una vez completado el plan de implementación aceptado por la DGAC se culminará el proceso de aceptación, al demostrar a la DGAC que se ha completado en forma efectiva y eficiente la implementación del SMS, de acuerdo a la dimensión y complejidad de la OMA.

G.16 La **Figura 2** proporciona una descripción general de los componentes del SMS y las interacciones entre ellos, con un enfoque específico en la Gestión de Riesgos de Seguridad Operacional y Garantía de Seguridad Operacional.

G.17 Los componentes y elementos que se muestran en la Tabla del literal F.1.1) y los párrafos y referencias relacionados con la **Figura 1** se describen con más detalle en esta circular de asesoramiento.

G.18 La mejora continua del SMS se basa en el seguimiento y la medición del rendimiento de la seguridad operacional, que se detallan con más detalle en las secciones relacionadas al Monitoreo y medición del desempeño de seguridad operacional (literal G.22.1) y Mejora continua del SMS (literal G.22.3).

G.19 La estructura de este Sección es la siguiente:

- Dentro de bloques grises: Las Normas y métodos recomendados de SMS del Anexo 19 del Apéndice 2 de la OACI para cada componente y elemento de SMS.
- Por debajo de cada bloque gris: orientación para una mayor comprensión de cada componente y elemento de SMS y de los medios de cumplimiento asociados.

***Nota**. — Es posible que algunas partes de los requisitos del Anexo 19 no necesiten ninguna declaración adicional de "comprensión". La amplia trazabilidad a los requisitos del Anexo 19 se proporciona en el capítulo 6 con los 12 elementos. Sin embargo, no se aplica la trazabilidad línea a línea*.

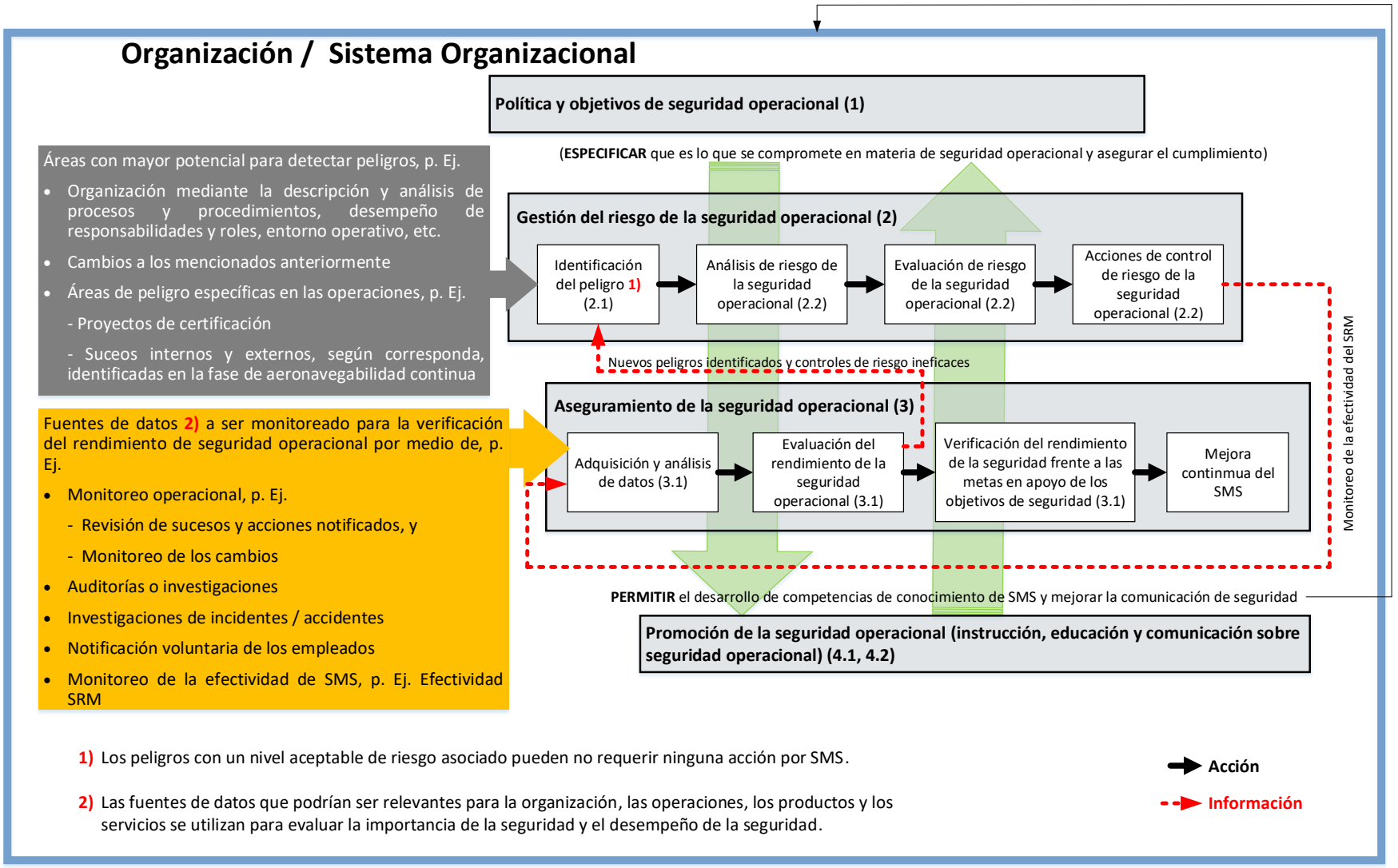


Figura 2. Descripción general de SMS e interacciones entre componentes de SMS

G.20 Componente 1 – Política y objetivos de seguridad operacional

G.20.1 Compromiso de la dirección

1. Política de seguridad operacional

1. Comprensión

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

La política de seguridad operacional define los objetivos de la organización, asigna responsabilidades y establece estándares. La política de seguridad operacional deberá describir en términos amplios la visión de la organización para la gestión de la seguridad operacional; cómo se propone abordar los temas relacionados con la seguridad operacional; y cómo reaccionará y fomentará una cultura de seguridad operacional en todos los niveles de la estructura organizativa, con un compromiso activo y visible.

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

a) Transmite el compromiso de la administración con el rendimiento de seguridad operacional de la organización hacia sus empleados.

b) Aborda la provisión de recursos materiales, humanos y financieros suficientes para realizar las actividades planificadas del SMS.

c) Incluye (pero no se limita a) los procedimientos de informes de seguridad operacional relacionados con la seguridad operacional de los servicios que ofrece la OMA, incluida la recopilación continua de datos de aeronavegabilidad y los informes de eventos que se hayan producido en aeronaves a las cuales les da el servicio de mantenimiento, así como los informes internos de la organización sobre problemas y riesgos de seguridad operacional, como notificaciones voluntarias de empleados.

d) Incluye el establecimiento de una política de "Cultura Justa". Las personas no son sancionadas por acciones, omisiones o decisiones erróneas acordes con su experiencia, formación y procedimientos internos. Sin embargo, no se toleran la negligencia grave, las infracciones deliberadas y los actos destructivos. Otras organizaciones pueden considerar esta definición al establecer políticas para comportamientos que son inaceptables y las circunstancias bajo las cuales no se aplicarían medidas disciplinarias.

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

e) Estará firmada por el Gerente responsable como el adalid de seguridad operacional de la organización.

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

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

2. Medios de cumplimiento

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

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

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

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

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

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

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

En el **Apéndice 3** "Manual o Documento de SMS" se propone un ejemplo de declaración de política de seguridad operacional.

G.20.2. Objetivos de seguridad operacional

1. Comprensión

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

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

Otros objetivos están relacionados con el desarrollo y rendimiento de la propia OMA.

Los objetivos de seguridad operacional deberán ser lo suficientemente detallados para garantizar que se pueda demostrar su cumplimiento, en la medida de lo posible mediante un mecanismo de medición (cualitativo o cuantitativo). El propósito del monitoreo del rendimiento de seguridad operacional es evaluar apropiadamente el logro de los objetivos de seguridad operacional de la organización (ver el literal G.22 correspondiente a "Aseguramiento de la seguridad operacional" para más detalles).

Por ejemplo, si uno de los objetivos de la organización era promover una cultura de seguridad operacional positiva, esto podría estar respaldado por un objetivo que aborde las características de la cultura de seguridad operacional descritas en la sección anterior. Con el objetivo de llevar a los inhabilitadores a una cultura positiva y promover los habilitadores, durante un período de

tiempo, la organización podría crear un programa con indicadores mensurables de su progreso.

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

2. Medios de Cumplimiento

a) La OMA deberá definir objetivos de seguridad operacional que reflejen el rendimiento de seguridad operacional en servicio del mantenimiento que proporciona (por ejemplo, basados en los análisis realizados a través del proceso de mantenimiento que realiza a los explotadores aéreos o mantenimiento a los componentes de aeronaves) así como objetivos relacionados con la función del SMS mismo. Estos objetivos deberían incluir el seguimiento del correcto despliegue del SMS, la medición de su actividad y la asignación de los medios y competencias del personal adecuados. Estos objetivos de seguridad operacional deberán reflejar la mejora de seguridad operacional identificada, con base en la situación actual. Deberán definirse como específicos, medibles, alcanzables, pertinentes y de duración determinada (SMART).

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

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

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

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

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

alineada con la publicación de los resultados de rendimiento de seguridad operacional en términos de lograr los objetivos.

G.20.3. Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional

1. Comprensión

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

a) Proporcionar y asignar recursos humanos, técnicos, financieros o de otro tipo necesarios para el rendimiento eficaz y eficiente del SMS.

b) Responsabilidad directa por la conducción de los asuntos de la organización.

c) Autoridad final sobre las operaciones bajo el certificado y lista de capacidades de la organización.

d) Establecer y promover la política de seguridad operacional.

e) Establecer los objetivos y las metas de seguridad operacional de la organización.

f) Actúa como el líder de la seguridad operacional de la organización.

g) Responsabilidad final por la resolución de todos los problemas de seguridad operacional.

h) Establecer y mantener la competencia de la organización para aprender del análisis de los datos recopilados a través de su sistema de notificaciones de seguridad operacional.

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

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

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

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

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

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

2. Medios de cumplimiento

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

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

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

Los ejemplos de esquemas incluyen, pero no se limitan a:

- Un Responsable de la seguridad operacional para cada organización (por ejemplo, explotador aéreo y OMA).
- Un solo Responsable de seguridad operacional en un nivel de gestión adecuado para cubrir el SMS general de la empresa.

G.20.4 Rendición de cuentas y responsabilidades con respecto a las organizaciones externas

La OMA es responsable del rendimiento de seguridad operacional de las organizaciones externas donde hay una interfaz de SMS. La organización de mantenimiento puede ser responsable de la rendición de cuentas de seguridad operacional de los productos o servicios proporcionados por organizaciones externas que respaldan sus actividades, incluso si las organizaciones externas no están obligadas a tener un SMS. Es esencial que los SMS de la organización de mantenimiento interactúen con los sistemas de

seguridad operacional de cualquier organización externa que contribuya a la entrega segura de sus productos o servicios.

G.20.5 Designación de personal clave de seguridad operacional

1. Medios de cumplimiento

La asignación de responsabilidades de gestión de SMS queda a discreción de la organización.

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

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

La organización es responsable de:

- Asegurarse de que el SMS funcione según lo definido y sea eficaz.
- Recopilar y analizar información de seguridad operacional de manera oportuna.
- Administrar encuestas relacionadas con la seguridad operacional.
- Seguimiento y evaluación de los resultados de las acciones correctivas.
- Asegurar que se lleven a cabo evaluaciones de riesgo, cuando corresponda;
- Monitorear los problemas de seguridad operacional reportadas en otras organizaciones que podrían afectar a la OMA o sus productos / servicios.
- Garantizar que la información relacionada con la seguridad operacional, incluidas los logros y los objetivos de la organización, esté disponible para todo el personal a través de los procesos de comunicación establecidos.
- Proporcionar notificaciones periódicas sobre el rendimiento en seguridad operacional.

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

operacional a los otros departamentos de la organización.

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

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

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

c) monitorear acciones correctivas y evaluar sus resultados;

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

e) mantener documentación y registros de SMS;

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

g) proporcionar asesoramiento independiente sobre problemas de seguridad operacional;

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

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

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

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

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

b) prioridades conflictivas para los recursos; y

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

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

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

a) experiencia en gestión de seguridad operacional / calidad;

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

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

d) habilidades interpersonales;

e) habilidades analíticas y de resolución de problemas;

f) habilidades de gestión de proyectos;

g) habilidades de comunicación oral y escrita; y

h) una comprensión de los factores humanos.

***Nota**. — Si la organización de mantenimiento lo considera necesario los requisitos de competencia los puede desarrollar en el documento/manual de SMS.*

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

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

La junta de revisión de seguridad operacional (SRB), incluye al gerente responsable y los gerentes de alta dirección con el gerente de seguridad operacional participante en carácter de asesor. El SRB es estratégico y se ocupa de cuestiones de alto nivel relacionadas con las políticas, la asignación de recursos y el monitoreo del rendimiento organizacional. La SRB monitorea:

a) La efectividad del SMS;

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

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

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

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

1) la prioridad organizativa declarada de la gestión de la seguridad operacional; y

2) Promoción de la seguridad operacional en toda la organización.

Nota. *— Este SRB debe ser establecido en organizaciones de mantenimiento de grandes organizaciones de mantenimiento y podría establecerse también en organizaciones de mantenimiento medianas. Para determinar si una organización es pequeña, mediana o grande de acuerdo a su dimensión y la complejidad se debe recurrir a la CA-145-001.*

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

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

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

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

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

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

Nota*. — Este SAG debe ser establecido en grandes organizaciones de mantenimiento y podría establecerse también en organizaciones de mantenimiento medianas. Para determinar si una organización es pequeña, mediana o grande de acuerdo a su dimensión y la complejidad se debe recurrir a la CA-145-001*

G.20.6 Coordinación de la planificación de respuesta ante emergencias

1. Compresión

Un plan de respuesta ante emergencias (ERP) documenta las acciones que debe tomar todo el personal responsable durante las emergencias. El propósito de un ERP es garantizar que haya una transición ordenada y eficiente hacia y desde las operaciones de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de autoridad.

El plan también contiene la autorización para la acción del personal clave, así como los medios para coordinar los esfuerzos necesarios para hacer frente a la emergencia.

El objetivo general es la continuación segura de las operaciones.

Un ERP no se aplica a las organizaciones de mantenimiento aprobadas.

Sin embargo, establecer un ERP se considera una buena práctica en las OMAs cuando la organización está realizando mantenimiento a los explotadores aéreos. Es posible que dichas organizaciones también necesiten coordinar actividades relevantes con las organizaciones que necesitan tener un ERP.

También se puede utilizar un artefacto o método similar cuando se produce una interrupción significativa (no relacionada con la seguridad de las operaciones de vuelo) en la propia organización, para garantizar la continuidad del negocio y la gestión de crisis.

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

2. Medios de cumplimiento

La coordinación de la planificación de respuesta ante emergencias se aplica solo a los proveedores de servicios requeridos a establecer y mantener un ERP como es el caso de los aeropuertos y explotadores aéreos. Sin embargo, las organizaciones de mantenimiento que brindan soporte de mantenimiento a los explotadores aéreos o que tienen sus instalaciones dentro de un aeropuerto, se encargarán de brindar su apoyo en los planes de respuestas ante emergencias de dichos proveedores de servicio. Para ello, se deberán establecer los procedimientos en donde se detallen funciones y responsabilidades que deberán cumplirse en caso de un accidente o incidente grave en el cual se solicite su colaboración.
Una organización de mantenimiento que realiza trabajos de mantenimiento a componentes de aeronaves no es necesario que tenga un plan de respuesta ante emergencias.

G.20.7 Documentación SMS

1. Comprensión

El alcance de la documentación de SMS puede diferir de una OMA a otra debido a:

- Dimensión (tamaño) de la organización y tipo de actividades.
- Complejidad de procesos y sus interacciones.

Cada OMA deberá garantizar el control y mantenimiento adecuados de estos documentos.

Deberán revisarse periódicamente y actualizarse según sea necesario (por ejemplo, anualmente):

a) **Política y objetivos de seguridad operacional**

La política de seguridad operacional tal como se entiende en el literal G.20.1 (Compromiso de la Dirección) determina los objetivos de seguridad operacional. Los objetivos deben ser prácticos, alcanzables, revisados y reevaluados periódicamente y comunicados al personal.

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

b) **Requisitos de SMS**

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

c) **Procesos y procedimientos de SMS**

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

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

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

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

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

e) **Manual de SMS**

La documentación de SMS puede incluir un documento de nivel superior (Manual de SMS o similar), que describe la implementación de SMS de la OMA de los cuatro componentes y doce elementos descritos en esta Sección.

El Manual de SMS puede ser un documento independiente o puede integrarse en el MOM existente. Cuando los detalles de los procesos de SMS de la organización ya se abordan en documentos existentes, es suficiente la referencia cruzada adecuada a dichos documentos.

2. Medios de cumplimiento

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

En el **Apéndice 3** se proporcionan ejemplos de documentación de SMS (por ejemplo, manual de SMS, política de seguridad operacional).

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

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

b) SPI y gráficos relacionados;

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

d) revisión interna del SMS o registros de auditoría;

e) registros de auditoría interna;

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

g) minutas de reuniones del SRC / SMS;

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

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

G.21 Componente 2 – Gestión de riesgos de seguridad operacional (SRM)

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

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

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

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

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

G.21.1 Identificación de peligros

1. Comprensión

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

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

Con respecto a las actividades de la OMA, los peligros son las condiciones que previsiblemente podrían conducir a un servicio realizado por la organización como no conforme o no conforme que, si no se abordan, podrían llegar a un nivel de riesgo inaceptable.

2. Medios de cumplimiento

La identificación de peligros consiste de:

- Análisis de las áreas de alto riesgo de las actividades de la organización o cambios organizacionales.

- Análisis de datos de fuentes internas y externas (por ejemplo, datos de retornos de aeronaves por mantenimiento, comentarios de los explotadores, información de los subcontratistas, peligros identificados por la DGAC u otra AAC o datos de notificaciones voluntarias).

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

Las OMAs deberán haber establecido y documentado metodologías y procesos para monitorear eventos y sucesos reportados como los siguientes:

- Para actividades de mantenimiento:
  - FOD (daños por objetos extraños).
  - Cualquier trabajo realizado que no está de acuerdo con los datos aprobados.
  - Cualquier desviación de una herramienta detectada durante la calibración.
- Para actividades que ocasionen problemas con el mantenimiento de la aeronavegabilidad de los explotadores a los que provee servicio:
  - Sucesos durante la operación del explotador (por ejemplo, fallas, mal funcionamiento o defectos).
  - Fallas de calidad
  - Retorno de las aeronaves a la zona de despacho por problemas de mantenimiento.
  - Incumplimientos relacionados con certificaciones de conformidad de mantenimiento (CCMs).

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

Para mejorar la identificación de peligros, la OMA deberá implementar un sistema de notificación voluntario de los empleados, basado en la política de cultura justa definida e implementada por la organización. Ver G.20.1.1. (política de seguridad operacional)

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

3. Sistema de notificación de seguridad operacional

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

errores. Pueden proporcionar información valiosa a la organización de mantenimiento sobre eventos de bajo impacto.

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

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

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

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

Es posible que sea necesario filtrar las notificaciones de entrada cuando hay una gran cantidad de notificaciones de seguridad operacional. Esto puede implicar una evaluación inicial de riesgos de seguridad operacional para

determinar si es necesaria una mayor investigación y qué nivel de investigación se requiere.

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

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

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

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

G.21.2. Evaluación y mitigación de riesgos de seguridad operacional

1. Comprensión

La SRM requiere el análisis de los riesgos de seguridad operacional para determinar la gravedad y la probabilidad asociadas con los peligros identificados. varias orientaciones / métodos (ver medios de cumplimiento a continuación) se encuentran disponibles para analizar el riesgo.

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

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

- Durante la fase del mantenimiento que ofrece la OMA (incluyendo el mantenimiento de las aeronaves y los componentes de las aeronaves), la aceptabilidad del riesgo de seguridad operacional se define por el mantenimiento de la aeronavegabilidad de la aeronave y de los productos en servicio. La aceptabilidad de los riesgos de seguridad operacional durante la fase de mantenimiento que se proporciona debe basarse en la consideración de los requisitos de aeronavegabilidad aplicables y la garantía de que no existe ninguna condición insegura. Un producto en una condición insegura implica un riesgo de seguridad operacional inaceptable y requiere una gestión de riesgos de seguridad operacional adecuada.

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

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

  1) Descripción del sistema.

  2) Identificación de peligros y consecuencias.

  3) Estimación de la gravedad y probabilidad de las consecuencias de la ocurrencia del peligro.

  4) Evaluación del riesgo y toma de decisiones asociadas.

  5) Mitigación de riesgos y medidas de seguridad operacional.

  6) Reclamaciones, argumentos y evidencia de que las acciones de seguridad operacional se han cumplido y documentado en un caso de seguridad operacional.

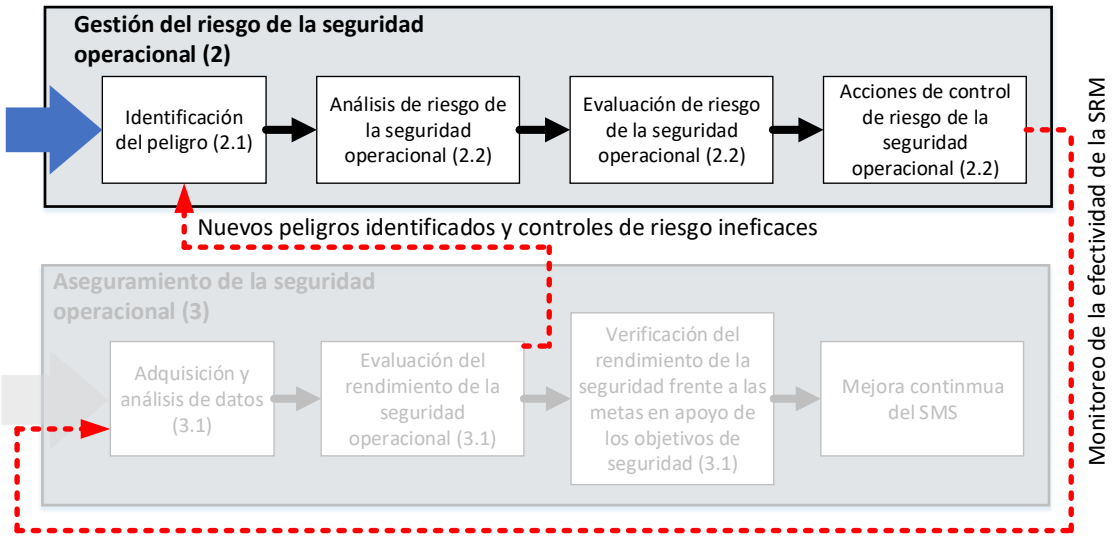


Figura 3. Pasos de la SRM

***Nota**. — La Figura 2 destaca parte del proceso con fines ilustrativos, al igual que la Figura 3.*

2. Medios de cumplimiento

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

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

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

- Técnicas de evaluación de riesgos (fuente ISO 31010):
  - Lluvia de ideas.
  - Lista de verificación.
  - Análisis de causa raíz.
  - Análisis de modos y efectos de falla (FMEA).
  - Análisis de árbol de fallas (FTA).
  - Árbol de decisiones.
  - Análisis de Bow tie.
  - Simulación de Monte Carlo.
  - Matriz de consecuencias / probabilidades.
- Sistema Europeo de Clasificación de Riesgos (ERCS) (fuente: publicado como vinculado al reglamento de la UE 2015/1018).
- Matriz de evaluación de riesgos de seguridad operacional (fuente CS / FARxx.1309). (https://gama.aero/wp-content/uploads/SMS-Standard_final-issue-A_20180917-1.pdf)
- Soluciones de gestión de riesgos de aerolíneas (ARMS).
- Métodos de análisis de riesgos a nivel de producto (fuente: SAE ARP4761):
  - Evaluación de riesgos funcionales (FHA).
  - Evaluación preliminar de seguridad operacional del sistema (PSSA).
  - Evaluación de la seguridad operacional del sistema (SSA).
  - Diagramas de dependencia.
  - Análisis de Markov.
  - Análisis de seguridad operacional zonal (ZSA).

- Análisis de causa común (CCA).

***Nota**. — No es posible ni deseable realizar evaluaciones de riesgos de seguridad operacional para todos los cambios. Solo los cambios que potencialmente tengan un impacto sustancial en la seguridad operacional o la gestión de la seguridad operacional están sujeta a la SRM (ver G.**22.3.2 Gestión** de cambios) o ambos.*

En el **Apéndice 1** "Mejores prácticas para la Gestión de Riesgos de Seguridad Operacional SRM" se enumeran ejemplos de situaciones en las que la SRM debería ser aplicada.

Las OMAs ya tienen las bases principales para recolectar, analizar y mitigar los riesgos relacionados con el servicio de mantenimiento que ofrecen.

Este proceso, que incluye recopilación de fallas, mal funcionamiento y defectos, análisis de riesgos y acciones para mantener la aeronavegabilidad del producto que se entrega a los explotadores, es un factor importante para la SRM y una entrada al proceso de aseguramiento de la seguridad operacional, como se describe en el literal G.22.

Las actividades de mantenimiento que ofrece la OMA y que soportan el mantenimiento de la aeronavegabilidad de las aeronaves de los explotadores deberán complementarse con una gestión proactiva de riesgos de seguridad operacional.

De hecho, los datos / información de mantenimiento de la aeronavegabilidad también son datos de origen clave para la evaluación proactiva de riesgos de los productos en funcionamiento.

G.22. Componente 3 – Aseguramiento de la seguridad operacional

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

- Monitoreo y medición del desempeño de la seguridad operacional.
- Proceso de gestión de cambios.
- Mejora continua del SMS.

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

La medición del rendimiento de la seguridad operacional (ver el literal G.22.1.) se entiende mejor como una evaluación de la capacidad para gestionar el riesgo. Es una determinación del éxito de los procesos en la gestión del riesgo y la eficacia resultante de los controles de riesgo implementados, tanto desde la perspectiva del producto como de la OMA.

El SA también requiere un proceso para gestionar cambios (ver el literal G.22.2.) que monitorea cambios sustanciales en el entorno operacional, ya sean planeados o no planeados, auto-inducidos o como resultado de influencias externas, para asegurar que los cambios no conducirán a riesgo inaceptable. Los cambios

sustanciales en el SMS también necesitan una evaluación para medir que el rendimiento del SMS no se degrada.
El SA también se utiliza para identificar áreas y para impulsar la mejora continua de los procesos de SMS (ver el literal G.22.c)).

El SA es un proceso reiterativo en el que los requisitos de rendimiento evolucionarán con la madurez de SMS (consulte la Sección J “Plan de implementación de SMS”).

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

¿Cómo realizar la adquisición de datos?

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

Para la adquisición de datos se debe establecer lo siguiente:

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

Los datos pueden ser:

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

Ejemplos de datos relacionados con productos:

- Número de eventos informados a la organización (de fuentes internas, externas o ambas).

- Número de sucesos notificados a las autoridades.
- Número de sucesos recurrentes.
- Número de fallas de calidad en productos, clasificados por criticidad con respecto a la seguridad operacional.
- Número de daños por objetos extraños (FOD) (por ejemplo, material dejado en la aeronave, motor, escombros que caen en sistemas abiertos).
- Número de datos incorrectos o incompletos dentro de las instrucciones para realizar el mantenimiento de las aeronaves y que podrían afectar a la aeronavegabilidad continua
- Número de errores de instalación (por ejemplo, equipo / parte no instalada, orientación incorrecta, instalación incompleta).
- Numere los errores de servicio (por ejemplo: no hay suficiente / demasiado fluido, acceso no cerrado, sistema / equipo no desactivado / reactivado).
- Tiempo medio entre fallos (MTBF) luego de haber realizado una revisión general (overhaul) a componentes de aeronaves.
- Tiempo medio entre cambios no programadas (MTBUR) a componentes que han recibido una revisión general (overhaul) a componentes de aeronaves.

Ejemplos de datos relacionados con el rendimiento de la OMA:

- Estado de las iniciativas en curso que contribuyen a los objetivos de seguridad operacional.
- Estado de las acciones de mitigación de riesgos.
- Asistencia a revisiones de SMS.
- Número de empleados capacitados en temas de seguridad operacional.
- Limitaciones de la DGAC u otra AAC por suspensión o revocación de privilegio / delegación.
- Respuesta a tiempo a los hallazgos relacionados con la seguridad operacional (por ejemplo: auditorías internas; auditorías de la DGAC.
- Gestión de recursos o competencias (por ejemplo: cumplimiento de puestos clave de seguridad operacional como personal de gestión de seguridad operacional, personal de mantenimiento o ambos).
- Factores relacionados con el entorno operativo (por ejemplo, ruido y vibraciones ambientales, temperatura, iluminación y disponibilidad de equipo y ropa de protección).
- Plazo para emitir mitigaciones o medidas correctivas en el proceso de mantenimiento o ambos.
- Deficiencias identificadas en la gestión de interfaces.

Los ejemplos antes mencionados de datos recopilados deben procesarse o analizarse o ambos para establecer indicadores de rendimiento relevantes, como se detalla en el literal G.22.1) - Observación y medición del rendimiento en materia de seguridad operacional.

Se requiere que la organización recopile datos para respaldar el aseguramiento de la seguridad operacional. Esto puede incluir, entre otros: notificaciones de datos automáticos, un sistema obligatorio de notificación de eventos, revisiones sistemáticas o auditorías, o un sistema voluntario de notificación de los empleados, o ambos, según la política de cultura justa (consulte G.20.1.1. y G.21.1.3.) y puede ser uno de los medios para adquirir datos. Todos los empleados deben conocer los sistemas que se utilizan que son apropiados para sus funciones y dónde hay sistemas disponibles para permitir la notificación anónima de datos (por ejemplo, peligros potenciales y, si están disponibles, soluciones propuestas o mejoras de seguridad operacional).

G.22.1. Observación y medición del rendimiento en materia de seguridad operacional

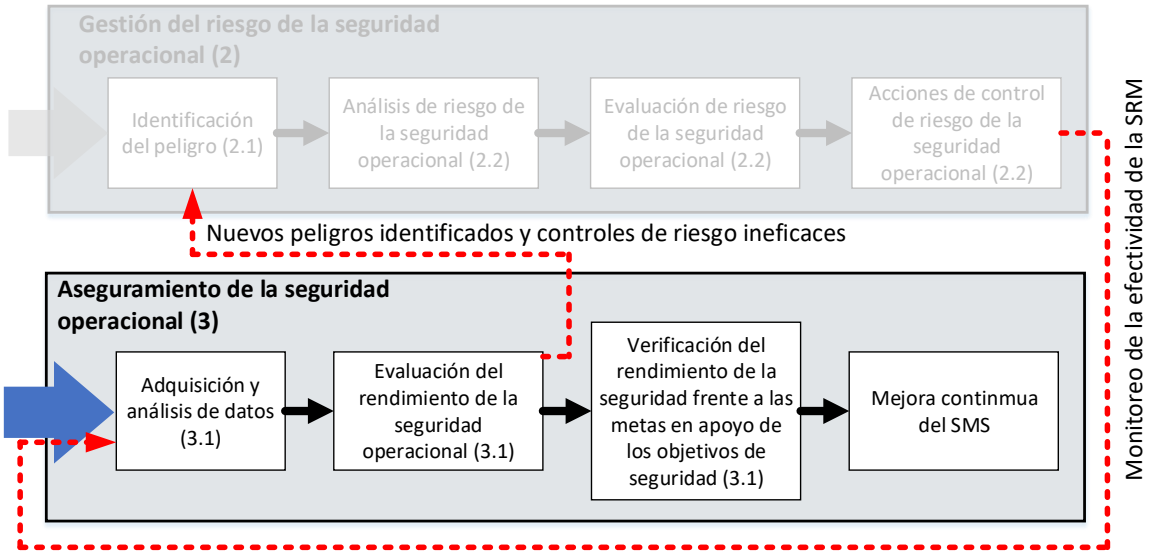


Figura 4. Pasos del aseguramiento de la seguridad operacional

1. Comprensión

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

La SRM es fundamental para el funcionamiento del SMS. Si se implementa correctamente, proporcionará a la OMA los medios para determinar si sus

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

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

- ¿Cuáles son los principales riesgos de seguridad operacional de la OMA?
- ¿Qué quiere lograr la OMA en términos de seguridad operacional y cuáles son los principales riesgos de seguridad operacional que deben abordarse? (objetivos de seguridad operacional de la organización).
- ¿Cómo sabrá la OMA si está progresando hacia sus objetivos de seguridad operacional? (a través de SPI).
- ¿Qué datos e información de seguridad operacional se necesitan para tomar decisiones de seguridad operacional informadas? (incluida la asignación de los recursos de la organización).

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

2. Medios de cumplimiento

La adquisición de datos a ser analizados, tal y como se describe en G.4.22. se realiza de acuerdo con criterios previamente establecidos que deben ser proporcionales a la diversidad, complejidad y criticidad de los servicios de mantenimiento que se ofrece y a la propia OMA. Independientemente de qué parte de la organización esté a cargo de procesar los datos recopilados y de implementar las acciones correctivas, los datos deben informarse a la función del SA con el fin de evaluar el rendimiento de la seguridad operacional.

Los indicadores de rendimiento de seguridad operacional (SPI) se utilizan para ayudar a la alta dirección a saber si es probable que la organización logre su objetivo de seguridad operacional; pueden ser cualitativos o cuantitativos. Los indicadores cualitativos son descriptivos y se miden por calidad, como una imagen descriptiva de la situación de seguridad operacional (¿cómo se ve bien?). Los indicadores cuantitativos pueden expresarse como un número (x fallas después de trabajos de mantenimiento) o como una tasa (x fallas después de trabajos de mantenimiento por n certificaciones de conformidad realizadas). En algunos casos, una expresión numérica será suficiente. Sin embargo, el solo uso de números puede crear una impresión distorsionada de la situación real de seguridad operacional si el nivel de

actividad fluctúa.

Por ejemplo, si el explotador aéreo reporta cinco (5) fallas o mal funcionamiento de algún sistema del avión luego del despacho del avión en el mes de julio y ocho (8) en el mes de agosto, puede haber una gran preocupación por el deterioro significativo en el rendimiento de seguridad operacional. Pero en agosto pueden haber realizado el doble de vuelos que, en julio, lo que significa que los aumentos de fallas o mal funcionamientos, o la tasa, ha disminuido, no ha aumentado. Esto puede cambiar o no el nivel de escrutinio, pero proporciona otra información valiosa que puede ser vital para la toma de decisiones de seguridad operacional basada en datos.

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

Indicadores avanzados y resultados

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

Los SPI de resultados ayudan a la organización a comprender lo que ha sucedido en el pasado y son útiles para determinar tendencias a largo plazo. Se pueden utilizar como indicadores de alto nivel o como una indicación de tipos específicos de sucesos o ubicaciones, como “tipos de accidentes por tipo de aeronave” o “tipos de incidentes específicos por región”. Debido a que los indicadores de resultados miden los resultados de seguridad operacional, pueden medir la efectividad de las medidas de mitigación de la seguridad operacional. También resultan eficaces para validar el rendimiento de seguridad operacional general del sistema. Por ejemplo, monitorear el número de apagados de motor en vuelo después de un trabajo de mantenimiento por número de horas de vuelo de la aeronave, proporciona una medida de la efectividad de las nuevas marcas (asumiendo que nada más ha cambiado). La reducción de apagado de motor en vuelo valida una mejora en el rendimiento de seguridad operacional general del sistema de mantenimiento; que puede ser atribuible al cambio en cuestión.

Las tendencias en los SPI de resultados pueden analizarse para determinar las condiciones existentes en el sistema que deberían abordarse. Utilizando el ejemplo anterior, una tendencia creciente en el número de apagados de motor en vuelo después de un trabajo de mantenimiento por número de horas de vuelo de la aeronave pudo haber sido lo que llevó a la identificación de una mala aplicación de los procedimientos durante los trabajos en los motores.

Los indicadores de resultado se dividen además en dos tipos: **baja probabilidad / alta gravedad** (accidentes o incidentes graves); **alta probabilidad / baja gravedad**: resultados que no necesariamente resultaron en un accidente o incidente grave, también conocidos como indicadores precursores.

Las medidas de seguridad operacional de la aviación han estado históricamente sesgadas hacia los SPI que reflejan resultados de “baja probabilidad/alta gravedad”. Esto es comprensible ya que los accidentes e incidentes graves son eventos de alto perfil y son fáciles de contar. Sin embargo, desde una perspectiva de gestión de rendimiento en materia de la seguridad operacional, existen inconvenientes en una dependencia excesiva de accidentes e incidentes graves como un indicador fiable del rendimiento en materia de seguridad operacional. Por ejemplo, los accidentes e incidentes graves son poco frecuentes (puede haber un solo accidente en un año, o ninguno) lo que hace difícil la realización de análisis estadísticos para identificar tendencias. Esto no indica necesariamente que el sistema es seguro. Una consecuencia de confiar en este tipo de datos es un falso sentido de confianza potencial en que el rendimiento en materia de seguridad operacional de una organización o sistema es eficaz, cuando de hecho puede estar peligrosamente cerca de un accidente.

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

Los SPI avanzados también pueden informar a la organización sobre cómo su operación se enfrenta al cambio, incluyendo los cambios en su entorno operacional. La atención se centrará en anticipar puntos débiles y vulnerabilidades como resultado del cambio o la supervisión del rendimiento después de un cambio. Un ejemplo de SPI para vigilar un cambio en las operaciones de la OMA sería “el porcentaje de sitios que han implementado el procedimiento X”.

Para una indicación más precisa y útil del rendimiento en materia de la seguridad operacional, los SPI de resultados, que miden tanto eventos de “baja probabilidad/alta gravedad” como eventos de “alta probabilidad/baja gravedad”, deben combinarse con los SPI avanzados. En la Figura 5 se ilustra el concepto de indicadores avanzados y de resultados que proporciona una imagen más completa y realista del rendimiento de la organización en materia de seguridad operacional.

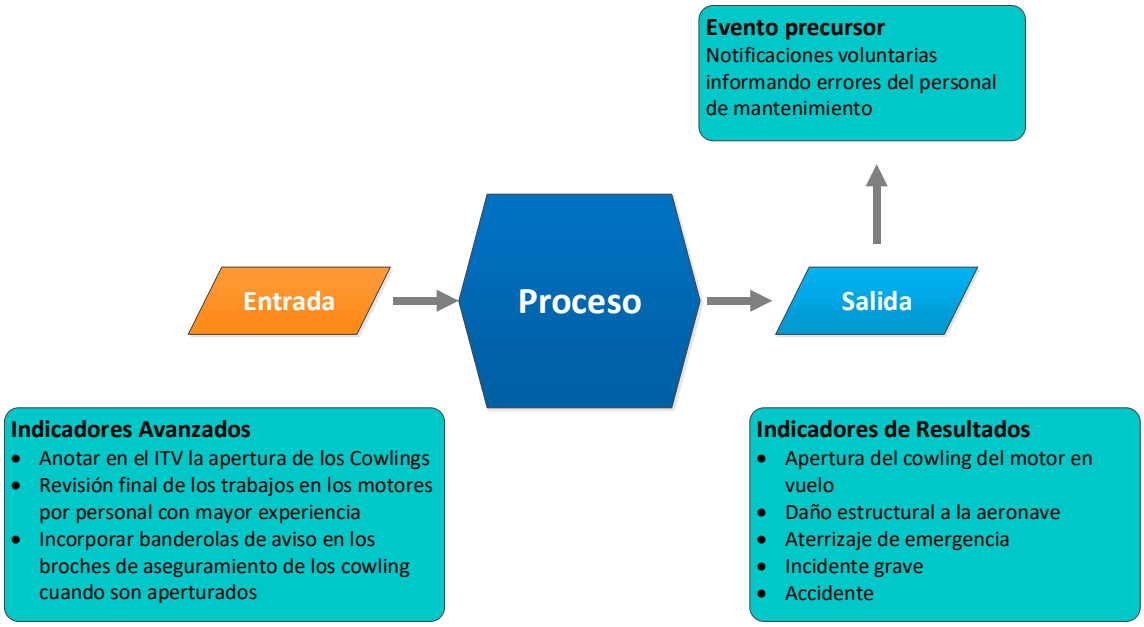


Figura 5. Indicador avanzado versus indicador de resultado

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

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

Documentar los indicadores de desempeño de seguridad operacional

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

Metas de rendimiento de seguridad operacional

Las metas de rendimiento en materia de seguridad operacional (SPT) definen los

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

Los objetivos de seguridad operacional pueden ser difíciles de comunicar y pueden parecer difíciles de lograr; al dividirlos en metas de seguridad operacional concretos más pequeños, el proceso de entrega es más fácil de gestionar. De esta manera, las metas forman un vínculo crucial entre la estrategia y las operaciones del día a día. Las organizaciones deberán identificar las áreas clave que impulsan el rendimiento en seguridad operacional y establecer una forma de medirlas. Se recomienda que las OMAs comiencen por apuntar a las tasas de tendencia de aumento (por ejemplo, aumento de la tasa de notificación de peligros) o disminución (por ejemplo, reducción de las fallas, mal funcionamiento y defectos después del servicio brindado por la OMA durante ...), en lugar de cifras arbitrarias (por ejemplo, reducción del 20%) hasta que el SMS haya estado funcionando durante mucho tiempo. suficiente para proporcionar datos fiables en los que basar objetivos específicos.

También debe tenerse en cuenta lo siguiente al decidir el SPT apropiado:

- conducir comportamientos indeseables; si el personal clave está demasiado enfocado en el logro de los números como un indicador de éxito, es posible que no logren la mejora deseada en el rendimiento de seguridad operacional
- metas operacionales; demasiado enfoque en el logro de las metas operativas (tales como: entrega de la aeronave a tiempo, reducción de los costos generales, etc.) sin un equilibrio de SPT puede llevar a "lograr los objetivos operativos" sin que necesariamente mejore el rendimiento de seguridad operacional
- donde la atención se centra en la cantidad más que en la calidad; Esto puede alentar al personal o los departamentos a alcanzar el objetivo, pero al hacerlo, entregar un producto o servicio deficiente.
- inhibir la innovación; Aunque no es la intención, una vez que se alcanza una meta, esto puede conducir a una relajación y que no se necesitan más mejoras y puede establecerse la complacencia.
- conflicto organizacional; Las metas pueden crear conflictos entre departamentos y otras organizaciones, ya que discuten sobre quién es responsable en lugar de centrarse en tratar de trabajar juntos.

¿Cómo medir la seguridad operacional?

El SMS se ocupa de la seguridad operacional de la aviación (es decir, muertes o lesiones de pasajeros y tripulación a bordo, o muertes y lesiones de personas

sobrevoladas o en tierra alrededor de la aeronave, o daños a la aeronave y al medio ambiente).

Debido a múltiples contribuyentes en la cadena de circunstancias que conducen a un evento de seguridad operacional (por ejemplo, explotadores, organizaciones de mantenimiento aprobadas, organización de capacitación, cada uno desempeñando su papel en la seguridad operacional), los datos recopilados para su procesamiento por el SMS de la organización son por naturaleza parciales y limitados.

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

¿Cómo construir indicadores?

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

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

Indicadores de rendimiento de seguridad operacional típicos

Cada OMA necesitará definir la categoría de eventos que se considerarán para la recopilación y el análisis de datos y los criterios para la evaluación, según su propia actividad (por ejemplo: eventos en aeronaves producidos luego del mantenimiento realizado por la OMA o fallas de calidad).

Puede ser útil monitorear algunos SPI contra el número de movimientos (por ejemplo, CCMs, horas hombre, vuelos, horas de vuelo, ciclos de vuelo).

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

Accidentes e incidentes

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

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

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

También puede ser de interés adquirir estadísticas de toda la industria para comparar el funcionamiento de la organización con empresas similares que realizan los mismos tipos de actividades.

Eventos de la flota

El término “Eventos de la flota” se utiliza para describir lo que se informa sobre la operación de aeronaves (o productos presentes en estas aeronaves) de interés para la OMA. Las actividades de mantenimiento de la aeronavegabilidad para los titulares de certificados de tipo (TCH) se incluyen en esta categoría. El proceso de la SRM del SMS debe clasificar la criticidad de los eventos. Cada organización puede establecer categorías (basadas en parámetros técnicos, organizacionales o de criticidad o ambos) y vincular los datos de eventos a una o varias categorías. Las relaciones entre el número de eventos (por categoría) y la actividad de vuelo (por ejemplo, horas de vuelo, ciclos de vuelo) pueden producir SPI. Se pueden establecer tendencias para cada categoría y se espera que muestren mejoras.

Las organizaciones deben identificar las condiciones (por ejemplo, nuevas capacidades o equipos o ambos) que podrían afectar negativamente las tendencias observadas sin constituir una degradación real.

El tiempo necesario para procesar un evento (posiblemente con umbrales) puede constituir un indicador, pero es más adecuado como indicador de operación de la organización de SMS.

Clima de SMS

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

Notificaciones voluntarias

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

Indicadores de operaciones de SMS típicos

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

Durante las fases de implementación de SMS (ver Sección J "Plan de implementación de SMS"); Los indicadores pueden ser específicos para medir el progreso del aumento de las actividades de SMS. Ejemplos de tales indicadores son:

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

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

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

- Una tendencia positiva (disminución) en el número de eventos en las aeronaves a las que se le brinda mantenimiento o con los componentes de aeronaves durante un período razonable (el período debe estar relacionado con la cantidad de eventos para lograr significación estadística).
- Una tendencia positiva (aumento) en el número de notificaciones voluntarias en la OMA (esto mostrará la adherencia a los principios de SMS).
- El tiempo de procesamiento de incidentes o acciones de mitigación o ambos (esto podría dividirse en la fase de definiciones / investigaciones y la fase de implementación real de las acciones relacionadas).
- El número de entrada de peligros confirmados al SRM.

Los indicadores anteriores reflejan la madurez del SMS y podrían combinarse en una Matriz de Madurez de SMS para resumir y mapear el rendimiento operacional, y luego usarse para la comunicación (ver **Apéndice 2** "Ejemplo de Método de Evaluación de Madurez de SMS").

Necesidad de medición adicional

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

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

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

Como uno de los medios de seguimiento, las auditorías podrían cubrir temas relacionados con:

- Organización (incluido el rendimiento de responsabilidades, gestión de recursos de conocimiento, documentación, medios y herramientas) y el despliegue y madurez de la cultura de seguridad operacional.
- SPI, que representa la efectividad de las mitigaciones y controles de riesgos en el contexto de la SRM.
- Efectividad de los procesos operacionales, tales como:
  - Proceso de mantenimiento y reparación.
  - Proceso de mantenimiento de la aeronavegabilidad (por ejemplo, mal funcionamiento de la aeronave, falla o recolección de defectos o ambos, reporte, análisis o corrección o ambos).

Cuando la organización mantiene la aprobación de una organización, dichas auditorías deberán ser coordinadas y contabilizadas por la función de monitoreo del cumplimiento requerida por dicha aprobación.

En organizaciones no aprobadas, las auditorías deben realizarse en el contexto del sistema de gestión de la organización con las adaptaciones necesarias del programa de auditoría.

¿Cómo comunicar la medición del rendimiento en seguridad operacional?

Se puede utilizar un dashboard de rendimiento de seguridad operacional para mostrar la medición del rendimiento de seguridad operacional de la organización.

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

complejidad de la organización (ver ejemplo de plantilla del dashboard o de rendimiento de seguridad operacional en el **Apéndice 3** "Ejemplo de Manual SMS / Documentación").

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

G.22.2. Gestión del Cambio

1. Comprensión

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

Si una organización elige usar métodos y procesos nuevos o no establecidos, o revisar sustancialmente los existentes, deberá desarrollar y usar procesos de identificación de peligros para identificar condiciones nuevas o existentes que previsiblemente podrían conducir a un riesgo inaceptable.

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

La evaluación del rendimiento de seguridad operacional incluye la evaluación de cambios significativos.
La gestión de los riesgos de seguridad operacional que resultan de los cambios debe considerar lo siguiente:

- Criticidad de los sistemas y actividades, incluido el impacto en organizaciones externas.
- Estabilidad de sistemas y entornos operativos.
- Rendimiento pasado (¿Qué datos e información está disponible que se puede utilizar para ayudar en el análisis del cambio?).

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

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

2. Medios de cumplimiento

Aunque cada organización es única, una serie de características del entorno operacional son comunes o similares entre las OMAs. Por lo tanto, hay cambios

típicos que podrían tener un impacto sustancial en la gestión de la seguridad operacional.

La descripción de una organización es necesaria para determinar el alcance de la aplicabilidad del SMS y los cambios a los que podría estar sujeto.

Algunos ejemplos de cambios típicos incluyen:

- Cambios en la organización:
  - Cambio de propietario.
  - Reubicación.
  - Apertura de una base adicional.
  - Cambio en el alcance de la lista de capacidades.
  - Introducción de una nueva tecnología (por ejemplo, máquina, inspección).
  - Cambio en la organización (trabajo compartido internamente entre instalaciones o externamente con socios / proveedores).
  - Cambio en las partes de la organización que contribuyen directamente a la conformidad que se otorga.
  - Cambio a los principios de aseguramiento de la calidad o monitoreo independiente.
  - Cambio de proveedor (es).
- Cambios de responsabilidades:
  - Cambio del Gerente Responsable.
  - Cambio del Responsable de la seguridad operacional.
  - Cambios del personal clave.
- Cambios en los principios de los procedimientos relacionados con:
  - Clasificación de cambios y reparaciones en mayores o menores.
  - La aprobación de cambios y reparaciones.
  - Sistema de manejo de calidad.
  - La aceptación de las tareas realizadas por socios o proveedores.
- Cambios en los recursos:
  - Reducción sustancial del número, calificaciones y / o experiencia del personal.
  - Aumento sustancial de la plantilla.

Las OMAs deben considerar cambios significativos según se definen en la reglamentación aplicable.

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

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

Disponibilidad de expertos en la materia: es importante que las partes interesadas clave estén disponibles y participen en la gestión de los cambios. Esto puede incluir personas de organizaciones externas.

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

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

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

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

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

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

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

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

Cambios notificables al Gerente Responsable

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

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

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

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

G.22.3. Mejora Continua del SMS

1. Comprensión

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

La mejora continua deberá aumentar el rendimiento con planes de acción que se basan en el monitoreo y la medición del rendimiento de la seguridad operacional (consulte el literal G.22.1).

2. Medios de cumplimiento

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

Sobre la base de los datos de seguridad operacional recopilados de acuerdo con el literal G.22 (aseguramiento de la seguridad operacional), la organización debería garantizar que:

- se hace análisis de datos a nivel organizacional para establecer un plan de acción, con los grupos de interés a cargo de la implementación de las acciones. El plan de acción debe abordar las causas fundamentales de las fallas o mal funcionamiento a nivel del sistema donde el rendimiento de seguridad operacional no ha alcanzado el nivel esperado.
- se implementan acciones de mejora.
- se consideran las mejores prácticas y lecciones aprendidas para mejorar el SMS. Además, estas mejores prácticas deben difundirse en toda la organización mediante actividades de promoción de la seguridad (literal G.23).

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

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

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

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

Programa de auditoria interna

Una auditoría es una revisión metódica y planificada para determinar cómo se llevan a cabo las actividades y si se llevan a cabo de acuerdo con los procedimientos publicados. La auditoría de seguridad operacional está estrechamente relacionada con los procesos de aseguramiento de la calidad y se considera una actividad de gestión de la seguridad operacional proactiva que proporciona los medios para identificar problemas potenciales antes de que tengan un impacto en la seguridad operacional. Las auditorías de seguridad operacional se centran en evaluar la efectividad de los SMS y los sistemas de apoyo de la OMA. Las auditorías de

seguridad operacional son una de las herramientas que se pueden utilizar para evaluar la efectividad de los controles de riesgos de seguridad operacional implementados o para monitorear el cumplimiento de los reglamentos de seguridad operacional. Garantizar la independencia y la objetividad es un desafío para las auditorías de seguridad operacional. La independencia y la objetividad se pueden lograr mediante la participación de entidades externas o auditorías internas con protecciones establecidas a través de políticas, procedimientos, roles y protocolos de comunicación.

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

Deben utilizarse auditorías de seguridad operacional para identificar que:

- el riesgo de seguridad operacional se está gestionando y los controles de riesgo son eficaces
- se cumplen los procedimientos e instrucciones de la OMA
- el SMS de la organización tiene una estructura sólida y niveles adecuados de personal
- se alcanza el nivel requerido de competencia e instrucción del personal para operar equipos e instalaciones, y para mantener sus niveles de rendimiento
- el rendimiento del equipo es adecuado para los niveles de seguridad operacional del servicio prestado
- existen arreglos efectivos para promover la seguridad operacional, monitorear el rendimiento de la seguridad operacional y procesar los problemas de seguridad operacional
- existen arreglos adecuados para manejar emergencias previsibles
- si es necesario, el área de la OMA que se audita identifica las medidas correctivas.

<u>Establecimiento de un programa de auditoría</u>

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

Establecer el alcance y la frecuencia de la auditoría

El alcance de la auditoría describe la amplitud de las disciplinas o áreas de la OMA que se cubrirán y depende del área de enfoque de la auditoría. La naturaleza y el alcance de las auditorías será un equilibrio entre la necesidad basada en el riesgo y la basada en el cumplimiento, impulsada principalmente por la importancia para la seguridad operacional de un área de la OMA, mientras se mantiene el cumplimiento (es probable que una falla en el cumplimiento sea un riesgo para la seguridad operacional) operacional. La mayoría de las organizaciones estarán familiarizadas con la auditoría basada en el cumplimiento; algunos también habrán utilizado técnicas de auditoría de procesos mediante muestreo de productos o para procesos organizacionales específicos.

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

El uso del riesgo de seguridad operacional como base para el alcance y la frecuencia de las auditorías requerirá que la organización considere al menos algunos o todos estos puntos:

- ¿Cuáles son los principales riesgos que gestiona la OMA y dónde ocurren?
- ¿Cuántos controles de riesgo existen y qué tan efectivos son (ingeniería, administrativos, equipos de protección del personal)?
- ¿Qué está funcionando bien y por qué? ¿Ayudaría una auditoría a comprender las lecciones que podrían aplicarse a otras partes de la operación de la OMA?
- datos de seguridad operacional de las notificaciones y los resultados de investigaciones y auditorías previas: ¿se identificaron fallas de control que podrían ser aplicables a otras áreas?
- ¿Se están produciendo cambios que requieren un seguimiento más detenido para verificar que las medidas de control planificadas son eficaces?
- ¿Cómo realiza el seguimiento la OMA con sus indicadores de rendimiento en seguridad operacional?

Establecer objetivos de la auditoria

Los objetivos de la auditoría definen los logros tangibles que se esperan de cada auditoría. Es aconsejable establecer los objetivos detallados mucho antes de la auditoría para ayudar a los auditores a planificar y realizar la auditoría. Por ejemplo, para una auditoría dirigida a verificar la “atención de mantenimiento de aeronaves en la línea”, un objetivo de la auditoría podría ser "determinar cómo se identifican, gestionan y notifican los errores de despacho de las aeronaves para determinar la eficacia de los procesos de seguridad operacional".

Descripción de la metodología de auditoría

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

Documentación de procesos

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

Realización de auditorías de seguridad operacional y seguimiento de resultados

Una auditoría debe incluir los siguientes pasos:

a) Planificación de la auditoría

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

b) Realización de la auditoría

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

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

Redacción del informe de auditoría

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

- la consistencia de hallazgos, recomendaciones y observaciones;

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

Difusión y seguimiento de los resultados de la auditoría

El informe de auditoría debe presentarse formalmente a los auditados para que puedan abordar cualquier hallazgo. Es necesario realizar un seguimiento de las acciones para abordar los hallazgos de manera transparente y sistemática (por ejemplo, un tema de la agenda en una reunión mensual de la SRB).

Selección y formación de auditores

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

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

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

Revisión de gestión

Como cualquier sistema de gestión empresarial (por ejemplo, financiero, de salud y seguridad operacional), para garantizar la adecuación y eficacia continua del SMS, el Gerente Responsable deberá realizar revisiones periódicas de los procesos y procedimientos del SMS y evaluar el rendimiento de seguridad operacional de la OMA. Hay muchas formas en que el Gerente Responsable puede revisar el SMS, como recibir y revisar un informe generado por el Responsable de seguridad operacional u otro personal, comunicación electrónica, como parte de una reunión regular de la gerencia o realizada una reunión separada. La organización necesita describir cómo se llevará a cabo el proceso de revisión por la dirección. Si es por reunión, entonces con qué frecuencia se reunirán, quiénes estarán en la reunión, qué se discutirá como una agenda permanente y cómo se documentarán las acciones acordadas y el seguimiento de su progreso.

Actividades de revisión por la dirección

Es importante que la Gerente Responsable revise la eficacia del SMS. Esto puede llevarse a cabo como una de las funciones de la SRB. Puntos a revisar por la gerencia:

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

Entradas para la revisión por el Gerente Responsable

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

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

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

Resultados de la revisión por el Gerente Responsable

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

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

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

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

Frecuencia de las revisiones por la dirección

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

La organización deberá considerar lo siguiente al establecer la frecuencia de sus revisiones por la dirección:

- cambios anticipados o amenazas a las operaciones y SMS. Los nuevos sistemas requieren más atención y asignación de recursos para dar seguimiento y cerrar los puntos de acción.

- establecer una lista de elementos de seguridad operacional importantes que desencadenarían una revisión por la dirección entre las sesiones planificadas.

G.23. Componente 4 – Promoción de la seguridad operacional

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

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

G.23.1. Instrucción y educación

***Nota**. — En esta circular de asesoramiento se utiliza el término "instrucción" a fin de estar coherente con lo que establece el Anexo 19. Es posible utilizar los términos capacitación, formación, educación o aprendizaje, el material de orientación que se proporciona no pretende ser tomado como material definitivo dentro del campo de aprendizaje, pero es específico para la competencia del SMS.*

1. Comprensión

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

La organización debería definir y mantener un programa de instrucción en seguridad operacional. La capacitación en seguridad operacional debe adaptarse a los empleados de la organización, según sea apropiado para las competencias requeridas por cada función laboral. La organización debería identificar a la población destinataria de la formación en seguridad operacional. Esto incluye a los empleados cuyas actividades pueden afectar la seguridad operacional del producto o servicio, además de los que están a cargo del SMS. La capacitación en seguridad operacional basada en roles debe garantizar que los empleados:

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

2. Medios de cumplimiento

La OMA deberá definir un programa de instrucción en seguridad operacional para cumplir con los objetivos de la política de seguridad operacional.

Este programa debe cubrir, como mínimo, el alcance, el contenido, los métodos de entrega (por ejemplo, capacitación en el aula, aprendizaje virtual (E-learning), notificaciones, capacitación en el trabajo) y la frecuencia de la capacitación que

mejor satisfaga las necesidades de la organización considerando el tamaño, el alcance requerido. competencias y complejidad de la organización.

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

La formación debería ser específica para el SMS y las operaciones de la organización y debería impartirse de acuerdo con las necesidades de competencia.

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

La instrucción de seguridad operacional deberá considerar:

a) capacitación para el Gerente Responsable, incluidas las responsabilidades de seguridad operacional, la supervisión y la gobernanza y su relación con la estrategia comercial de la organización y otros sistemas de gestión;

b) capacitación para el personal clave y jefes sobre cómo liderar de manera efectiva el desarrollo, implementación y sostenimiento continuo del SMS

c) competencia para el liderazgo organizacional y el personal clave de seguridad operacional en la aplicación de prácticas de gestión de riesgos

d) capacitación que proporciona competencia al personal superior del sistema de gestión de la seguridad operacional (responsable de seguridad operacional) en la gestión y administración del SMS y las prácticas de gestión de riesgos. Referirse al Material de orientación sobre capacitación y competencias;

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

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

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

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

Análisis de las necesidades de instrucción

Se deberá realizar un análisis de las necesidades de capacitación (TNA) para identificar el programa de instrucción apropiado para todo el personal, el alcance del programa de instrucción debe ser apropiado para el papel y la participación de cada individuo en el SMS de la organización. Se puede realizar un análisis de las necesidades de formación mediante:

- analizar el trabajo:
  - iniciar por consultar la documentación específica que describe el trabajo, como la descripción del puesto. Identifique frases que especifiquen habilidades, procesos o áreas de conocimiento importantes requeridas.
- determinar las brechas de habilidades / conocimientos:
  - desarrollar una lista de áreas en las que se requeriría capacitación para mejorar la efectividad del trabajo en cuestión
  - decidir si hay una brecha en las habilidades o conocimientos, o si se requiere alguna revisión para mejorar el conjunto de habilidades generales
  - obtener retroalimentación de un grupo representativo de personas que realizan el trabajo sobre las áreas que consideran que deben abordarse.
- identificar soluciones de instrucción:
  - establecer la mejor manera de cerrar las brechas de habilidades / conocimientos identificadas en el paso anterior. Las diferentes opciones pueden incluir cursos de instrucción realizados interna o externamente, aprendizaje auto-dirigido, instrucción individual o tutoría en el entorno laboral.
- evaluar el rendimiento después de la instrucción para determinar si aún existen brechas de rendimiento y si la solución de instrucción seleccionada era apropiada. Esto se puede lograr mediante:
  - pedir al personal y/o al responsable de ese personal que evalúen su efectividad en la tarea;
  - preguntar al personal si las brechas de rendimiento que fueron el motivo de la capacitación aún persisten.
  - evaluar al personal a medida que realiza tareas para determinar si todavía hay evidencia de deficiencia de habilidades o conocimientos.

Determinar los plazos del programa de instrucción en seguridad operacional

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

Programa de instrucción de seguridad operacional

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

- políticas, logros y objetivos de seguridad operacional organizacionales
- roles y responsabilidades de seguridad operacional organizacional relacionados con la seguridad operacional
- fundamentos de SMS, incluida la relación con factores humanos
- principios de gestión de riesgos de seguridad operacional
- identificación de peligros e informes de seguridad operacional
- comunicación de seguridad operacional.

El programa de instrucción deberá identificar el alcance y la profundidad del programa de instrucción para las diversas tareas y funciones relacionadas con la seguridad operacional de acuerdo con las necesidades y la complejidad de la organización. La orientación del programa de instrucción para el puesto de responsable de seguridad operacional se encuentra en el Material de orientación sobre capacitación y competencias.

Programa de instrucción y documentación de cualificación

Los requisitos de instrucción y calificación deben documentarse para cada área de actividad en la organización. Se debe desarrollar un archivo de instrucción para todo el personal, incluido el Gerente Responsable, para identificar y registrar sus requisitos y logros de instrucción y competencia.

Quién necesita recibir instrucción en seguridad operacional

Todo el personal debe participar en el programa de instrucción en seguridad operacional de la organización apropiado para sus responsabilidades de seguridad operacional. En particular, todo el personal operativo de la OMA / de apoyo, supervisores, certificadores de conformidad de mantenimiento, jefes, personal clave y el Gerente Responsable deben estar capacitados y ser competentes para realizar sus funciones de SMS.

Los subcontratistas también pueden requerir instrucción sobre el uso del SMS o cómo integrar sus prácticas con el SMS de la organización, y sobre las expectativas de la organización con respecto a las prácticas de trabajo seguras, la identificación de peligros y los procesos de informes de seguridad operacional.

Material de orientación sobre capacitación y competencias

El Responsable de seguridad operacional es la persona responsable del desarrollo, implementación, operación y mejora continua del SMS de la OMA. Deberán actuar como punto focal para la seguridad operacional en la organización.

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

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

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

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

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

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

G.23.2. Comunicación de la Seguridad Operacional

1. Comprensión

La comunicación deberá complementar la instrucción al proporcionar un flujo continuo de información de seguridad operacional y garantizar que el SMS sea

visible y se demuestre que es efectivo e integrado. El Responsable de seguridad operacional también deberá asegurarse de que las lecciones aprendidas de las investigaciones y los historiales de casos o experiencias, tanto internamente como de otras organizaciones, se distribuyan ampliamente.

2. Medios de cumplimiento

Qué comunicar en toda la organización

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

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

Qué comunicar fuera de la organización

La siguiente información debe comunicarse según sea necesario:

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

Métodos de comunicación

La comunicación de seguridad operacional deberá entregarse por el método más apropiado según el rol del individuo y la necesidad de recibir información

relacionada con la seguridad operacional. Esto se puede hacer a través de reuniones, hojas informativas de seguridad operacional, avisos, boletines, sesiones informativas o cursos de capacitación. Algunos paquetes de software de SMS tienen funciones de notificación por correo electrónico o aplicaciones de mensajería. Es importante utilizar más de un medio, asegurándose de que haya una combinación de comunicación activa (por ejemplo, la capacidad de interactuar y recibir comentarios) y comunicación pasiva. Algunos ejemplos son:

Métodos activos de comunicación

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

Métodos pasivos de comunicación

- La publicación de una revista u hoja informativa de seguridad operacional organizacional
- Presentación basada en la web
- Foros
- Correos electrónicos.

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

Promoción de seguridad operacional

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

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

La promoción de la seguridad operacional proporciona un mecanismo a través del cual las lecciones de las investigaciones de seguridad operacional y otras

actividades relacionadas con la seguridad operacional se ponen a disposición de todo el personal afectado.

Cómo promover la seguridad operacional de manera efectiva

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

- Palabra hablada: quizás el método más eficaz, especialmente si se complementa con una presentación visual
- Palabra escrita: el método más popular debido a su rapidez y economía, el material impreso de promoción de la seguridad operacional también compite por la atención con cantidades considerables de otro material impreso
- Medios electrónicos: el uso de Internet ofrece un importante potencial de mejora en la promoción de la seguridad operacional. Esto podría incluir hojas informativas electrónicas, blogs, herramientas de retroalimentación como encuestas, etc.

H. INTERFACES ENTRE LAS ORGANIZACIONES

H.1. Principios de Interfaz

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

Las interfaces entre organizaciones se pueden expresar:

- Internamente dentro de una empresa / grupo / entidad legal:
  - Cada organización tiene su propio SMS (por ejemplo, SMS en la OMA, SMS en el explotador aéreo).
  - Cada organización tiene su propio SMS con el apoyo de un enfoque de SMS corporativo (consulte el literal H.5.3).
  - Un único SMS corporativo en varias organizaciones (por ejemplo, SMS que cubren las organizaciones de un explotador aéreo y el de una OMA con un solo Gerente responsable).
- Externamente con empresas / entidades legales separadas:
  - Haber implementado un SMS (por ejemplo, explotadores aéreos, organización de mantenimiento aprobadas).
  - No haber implementado un SMS (por ejemplo, proveedores de servicios de ingeniería, proveedores de fabricación).

***Nota**. — La descripción del sistema de una organización con un SMS implementado debe capturar las interfaces con otras organizaciones para asegurar el flujo de requisitos hacia los proveedores externos. También se debe considerar la interfaz con otras organizaciones que tienen su propio SMS implementado. Independientemente, la descripción del sistema debe adaptarse a la dimensión de la organización. Por ejemplo, es imposible hacer una descripción detallada del sistema que cubra todas las interfaces SMS para un gran fabricante que trata con cientos de proveedores, clientes, etc.*

- Externamente con la DGAC y otras Autoridades de Aviación Civil (AAC):
  - Según lo requiera el reglamento aplicable.
  - Teniendo en cuenta que todos los datos provenientes de la SRM y el SA no están necesariamente sujetos a ser reportados a las AACs.

***Nota.** — La DGAC puede recibir de otros canales (explotadores, otras AAC, diversas entidades bajo su jurisdicción) información valiosa relacionada con la seguridad operacional de un producto o pueden tener acceso a datos de seguridad operacional genéricos (por ejemplo, recomendaciones de organismos oficiales de investigación). Estas pueden ser fuentes potenciales de información para la organización.*

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

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

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

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

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

El rendimiento de la seguridad operacional podría contabilizarse durante la evaluación de los proveedores (para la calificación inicial o el monitoreo continuo). El intercambio y la gestión de los datos de seguridad operacional o SMS que excedan las necesidades deberán acordarse entre las organizaciones y documentarse. Esto debería evitar una interacción excesiva del sistema entre organizaciones (por ejemplo, una OMA en el contexto de su propio SMS solicitando auditar el SMS de un titular de CT).

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

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

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

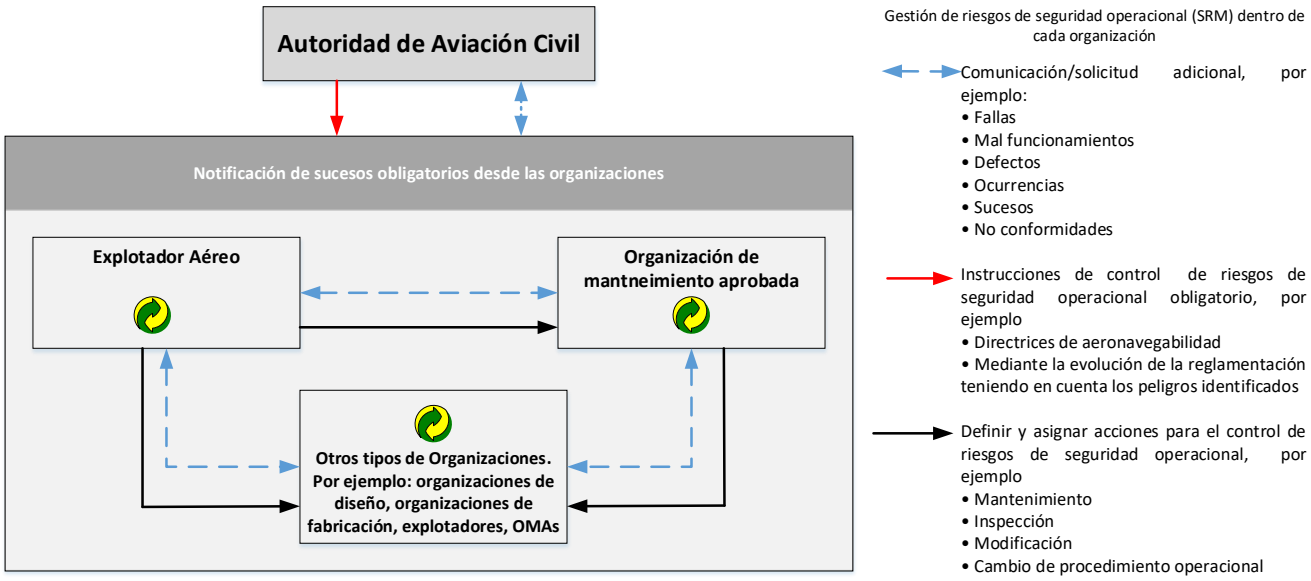


Figura 6. Ejemplo de flujo de datos de seguridad operacional y comunicación asociada entre organizaciones para la gestión de sucesos

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

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

H.2. Documentación de interfaz

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

Esta documentación debe considerar los siguientes objetivos:

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

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

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

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

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

H.3. Enfoque de SMS corporativos

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

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

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

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

I. RESUMEN DE ALTO NIVEL DE COMPONENTES Y ELEMENTOS DE SMS

Esta sección proporciona una "versión abreviada" de la descripción detallada de cada elemento, es decir, qué buscar en los componentes y elementos de un SMS. La información presentada destaca los medios aceptables de cumplimiento, las notas de orientación, así como más información para que las OMAs puedan encontrar lo que funciona mejor, teniendo en cuenta la cultura y el entorno operativo de la organización.

Información más detallada sobre lo que se debe considerar al implementar SMS se podrá encontrar bajo el título de cada componente.

COMPONENTE 1 – POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL	
Elemento 1 – Compromiso de la dirección	
Medios aceptables de cumplimiento	Existe una política de seguridad operacional firmada por el Gerente Responsable y comunicada a todo el personal. El Gerente Responsable y el personal clave promueven y demuestran su compromiso con la política de seguridad operacional a través de una participación activa y visible en el sistema de gestión de la seguridad operacional. La política de seguridad operacional se ha desarrollado considerando lo siguiente: • Compromiso e intenciones del Gerente Responsable con respecto al establecimiento de la seguridad operacional como un valor fundamental. • un compromiso a la mejora continua del rendimiento del SMS. • provisión de recursos apropiados. • política de notificación no punitiva (cultura justa) • reconocimiento de que el cumplimiento de los procedimientos, normas y reglas es obligación de todo el personal. Evidencia de evaluación regular y revisión según sea necesario.
Notas guías	Existe una política de seguridad operacional que se utiliza en toda la organización y se implementa en todos los niveles de la organización. La organización tiene un sistema de gestión de la seguridad operacional que hace interfaz con otras funciones del sistema de gestión (por ejemplo: calidad, medio ambiente, finanzas, etc.). Los objetivos de la política de seguridad operacional impulsan el rendimiento de seguridad operacional del SMS. La organización se asegura periódicamente de que el personal de toda la organización esté familiarizado y haya comprendido la política y sus responsabilidades de seguridad operacional. La política de notificaciones no punitivas (cultura justa) cuenta con el respaldo activo de los representantes del Gerente Responsable y el personal clave. Existe evidencia de toma de decisiones, acciones y comportamientos que reflejan una cultura de seguridad operacional positiva.
Más información	Para obtener más información sobre el desarrollo de una política de seguridad operacional efectiva y significativa, metas y objetivos de seguridad operacional, investigue utilizando las siguientes frases clave:

	• establecer y mantener la responsabilidad de la seguridad operacional • establecer metas y objetivos de seguridad operacional • demostrando rendición de cuentas y compromiso.
Elemento 2 – Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional	
Medios aceptables de cumplimiento	Se ha designado a un gerente responsable con total responsabilidad y rendición de cuentas final para el SMS para garantizar que se implemente correctamente y funcione de manera eficaz. Las rendiciones de cuentas, autoridades y responsabilidades de seguridad operacional están definidas y documentadas en toda la organización. El personal de todos los niveles, esta consiente, y comprende sus rendiciones de cuentas, autoridades y responsabilidades de seguridad operacional con respecto a todos los procesos, decisiones y acciones de gestión de la seguridad operacional. Existen diagramas organizacionales de gestión documentados y descripciones de trabajo para todo el personal. La gestión de la seguridad operacional se comparte en toda la organización (y no es solo responsabilidad del gerente responsable y el personal clave).
Notas guías	Las actividades clave de seguridad operacional se describen claramente en las funciones y responsabilidades del gerente responsable y se incorporan en las metas del rendimiento del personal. El personal clave reconoce los comportamientos de seguridad operacional positivos y las contribuciones para mantener el SMS de la organización. Hay evidencia de participación y consulta del personal en el establecimiento y operación del SMS.
Elemento 3 – Designación del personal clave de seguridad operacional	
Medios aceptables de cumplimiento	Se ha designado o contratado a una persona competente con los conocimientos, las habilidades y la experiencia adecuados para gestionar el funcionamiento del SMS y cumple las funciones y responsabilidades laborales requeridas. La organización ha asignado recursos suficientes para gestionar el SMS incluidos, pero no limitados, mano de obra para la investigación, el análisis, la auditoría y la promoción de la seguridad operacional.

Notas guías	La persona responsable de la gestión del SMS recibe un estatus apropiado en la organización que refleja la importancia del rol de seguridad operacional dentro de la organización y es una gerencia independiente. Si la organización está combinando a la persona responsable de la gestión del SMS con otras funciones de otra gerencia, en situaciones de conflicto de intereses, la organización empleará o contrata a una persona independiente para mantener la integridad del sistema. Las personas dentro de la organización que tienen un papel clave en la seguridad operacional, mantienen sus conocimientos a través de capacitación adicional y asistencia a conferencias, seminarios y talleres relevantes para la industria.
Elemento 4 – Coordinación de la planificación de respuestas ante emergencias	
Medios aceptables de cumplimiento	Se ha desarrollado un plan de respuesta ante emergencias (ERP) que refleja el tamaño, la naturaleza y la complejidad de la OMA y define los procedimientos, roles, responsabilidades y acciones de las diversas departamentos y personal clave. El personal clave en caso de emergencia tiene fácil acceso al ERP en todo momento. La organización tiene un proceso para distribuir los procedimientos ERP y comunicar el contenido a todo el personal. La OMA participa periódicamente en los ensayos de los ERP para determinar la idoneidad del plan y los resultados se revisan para mejorar su eficacia.
Notas guías	Se ha delegado la autoridad de emergencia. Se han asignado responsabilidades de emergencia durante las actividades coordinadas. Se han implementado procesos para registrar las actividades durante una respuesta ante emergencia. Se ha establecido la compatibilidad con la planificación de respuesta ante emergencias de otras partes interesadas (por ejemplo, otros usuarios del aeródromo, operaciones de aviación vecinas, socios de alianzas, etc.). La organización se ha puesto en contacto con proveedores de servicios de emergencia y autoridades gubernamentales. El proceso de actualización de cambios de personal / organización y listas de contactos está en marcha. La organización ha implementado un programa de manejo del estrés por incidentes críticos para su personal.

Más información	Para obtener más información sobre el desarrollo de un ERP eficaz, investigue utilizando las siguientes frases clave: • beneficios de implementar un ERP • acciones de respuesta inicial • establecer un centro de respuesta a crisis • registros que deben mantenerse durante y después de un ejercicio o suceso de ERP • las responsabilidades de la OMA en el lugar del accidente • sesión informativa sobre el estrés posterior a un incidente crítico • mantener referencias en papel.
Elemento 5 – Documentación SMS	
Medios aceptables de cumplimiento	Existe documentación que describe el sistema de gestión de la seguridad operacional y las interrelaciones entre todos sus elementos. Los procedimientos del sistema de seguridad operacional son proporcionales a la complejidad de la organización y están disponibles para todo el personal. La documentación de SMS esta fácilmente disponible para todo el personal. La documentación de SMS, incluidos los registros relacionados con SMS, se revisan y actualizan periódicamente con un control adecuado. La documentación de SMS detalla y hace referencia a los medios para el almacenamiento de otros registros relacionados con SMS. Los registros de seguridad operacional se conservan y demuestran el rendimiento del sistema.
Notas guías	Se han creado plantillas específicas que respaldan la gestión de riesgos de seguridad operacional y las actividades de garantía de seguridad operacional. La organización puede demostrar que los procesos de gestión de la seguridad operacional están integrados en otros sistemas organizacionales. La organización ha analizado y utiliza el medio más adecuado para la entrega de documentación tanto a nivel corporativo como operativo.
Más información	Para obtener más información sobre el desarrollo de un sistema de control de documentos eficaz, investigue utilizando las siguientes frases clave: • estructurar un manual de gestión de la seguridad operacional

	• registros de seguridad operacional.
COMPONENTE 2 – GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL	
Elemento 6 – Identificación de peligros	
Medios aceptables de cumplimiento	Medios documentados y demostrados que garantizan la identificación de los peligros para la seguridad operacional, incluidos los cuasi accidentes y los errores. Proceso documentado que garantiza que los peligros identificados se registren, analicen y se actúe de manera oportuna. Proceso documentado para proporcionar retroalimentación al notificador de las acciones tomadas (o no tomadas) y, en su caso, cómo difundirlas al resto de la organización. Proceso documentado para establecer factores contribuyentes causales, es decir, por qué ocurrió el evento y no solo qué sucedió.
Notas guías	Diferenciar entre diferentes tipos de peligros. Determinar un proceso de identificación de peligros adecuado para la organización. Determinar los procesos formales de registro y notificación de peligros. Determine un proceso de control de peligros adecuado, incluidas las responsabilidades. Determine los procesos de seguimiento adecuados. Asegúrese de que haya un rastro documentado desde la identificación hasta la resolución de cada peligro identificado. Mantenga un registro de peligros. Capacite a todo el personal en la identificación y notificación de peligros. Integrar factores humanos en la identificación y reducción de peligros.
Más información	Para obtener más información sobre el desarrollo de procesos efectivos de identificación de peligros, investigue utilizando las siguientes frases clave: • identificación de peligros para la seguridad operacional • peligros relacionados con el rendimiento humano en la aviación
Elemento 7 – Evaluación y mitigación de riesgos de seguridad operacional	
Medios aceptables de	Proceso documentado para la gestión del riesgo que incluye la evaluación del riesgo asociado con los peligros identificados.

cumplimiento	Proceso y criterios documentados para evaluar el nivel de riesgo que la organización está dispuesta a aceptar. Método documentado para registrar los riesgos y las estrategias de tratamiento tomadas, incluidos los plazos y las responsabilidades. Procedimientos documentados para revisar y modificar los procesos de gestión de riesgos de forma periódica.
Notas guías	Implementación de diferentes procesos de identificación de riesgos, como la realización de evaluaciones de riesgos cuando se producen cambios operacionales (por ejemplo, inclusión en la lista de capacidades de un nuevo tipo de aeronave, nueva instalación de mantenimiento, cambios en el personal clave). Implementación de procesos de notificación y registro de riesgos, disponibles para todo el personal e involucrando al personal clave en el proceso de análisis. Desarrollo de procesos de control y seguimiento de riesgos, como el uso de un registro de riesgos y reuniones periódicas para discutir estrategias de tratamiento de riesgos. Desarrollo de procesos de comunicación de riesgos como mensajes regulares de alerta al personal, formación, etc. El desarrollo e implementación de perfiles de riesgo operacional puede ser una forma de lograr todo lo anterior.
Más información	Para obtener más información sobre el desarrollo de un sistema de gestión de riesgos eficaz, investigue utilizando las siguientes frases clave: • gestión del riesgo operacional • perfil de riesgo: gestión de riesgo estratégico • gestión de riesgos empresariales • ALARP • conceptos de gestión de riesgos • tres líneas de garantía de defensa.
COMPONENTE 3 – ASEGURAMIENTO DE SEGURIDAD OPERACIONAL	
Investigaciones de seguridad operacional	
Medios aceptables de cumplimiento	Medios documentados y demostrados para realizar investigaciones de seguridad operacional interna. Investigadores internos de seguridad operacional designados y debidamente capacitados.
Notas guías	Hay un rastro documentado desde la identificación hasta la resolución cuando se completa una investigación.

	Existe un registro claro del proceso de investigación, los hallazgos y las acciones requeridas. Existen procedimientos formales para desencadenar investigaciones, procesos para recopilar evidencia y realizar el análisis, procesos para desarrollar recomendaciones y para distribuir el informe. Existen procesos para monitorear y revisar las acciones tomadas en respuesta a la investigación de seguridad operacional. Se establecen y documentan los criterios para las habilidades y conocimientos del investigador de seguridad operacional.
Más información	Para obtener más información sobre la implementación de una capacidad de investigación de seguridad operacional efectiva, investigue utilizando las siguientes frases clave: • métodos y procesos de recopilación de datos • teorías y métodos de análisis de la investigación de seguridad operacional • redactar un informe de investigación de seguridad operacional • cualidades y calificaciones de un investigador de seguridad operacional • factores humanos • técnicas de investigación y análisis • análisis de causa y efecto • modelo de Reason.
Elemento 8 – Observación y medición del rendimiento en materia de seguridad	
Medios aceptables de cumplimiento	Medios documentados y demostrados para monitorear el rendimiento de seguridad operacional. Proceso documentado para identificar fuentes reactivas, proactivas e interactivas de datos de seguridad operacional. Medios documentados y demostrados para medir el rendimiento en seguridad operacional a través de indicadores establecidos. Metas de rendimiento de seguridad operacional establecidos en consonancia con los objetivos de seguridad operacional de la organización.
Notas guías	Implementación de un sistema de notificación de seguridad operacional. Encuesta de las percepciones de seguridad operacional del personal dentro de la organización (por ejemplo, una encuesta de cultura de seguridad operacional).

	Captura sistemática de datos para ayudar a contextualizar las estadísticas (por ejemplo, número de sucesos por mes, número de informes de defectos por mes, etc.). Comunicación de resultados a todo el personal. Desarrollar métodos para rastrear cómo está funcionando el sistema de gestión de la seguridad operacional (por ejemplo, cuadro de mando integral). Establecer reuniones periódicas para revisar el desempeño en seguridad operacional.
Más información	Para obtener más información sobre el desarrollo de una supervisión y medición eficaces del rendimiento, investigue utilizando las siguientes frases clave: • indicadores de rendimiento avanzados y resultados • medir el rendimiento en seguridad operacional para los proveedores de servicios.
Elemento 9 – Gestión del cambio	
Medios aceptables de cumplimiento	Proceso documentado para realizar análisis de peligros y evaluaciones de riesgos para los cambios que se han identificado dentro de la OMA, incluidos los cambios en la alta dirección y la lista de capacidades que pueden afectar la seguridad operacional. Proceso documentado para asegurar que las partes interesadas internas y externas apropiadas estén involucradas en la gestión del proceso de cambio. La gestión documentada del proceso de cambio incluye la revisión de evaluaciones de riesgos anteriores y peligros existentes, según corresponda. Proceso documentado para registrar el resultado de cada etapa del plan.
Notas guías	Se establecen procesos para: • identificación de peligros y riesgos • notificación y registros de riesgos • control de riesgos (incluidas las responsabilidades) • seguimiento de riesgos (incluidas las responsabilidades) • comunicación de riesgos.
Más información	Para obtener más información sobre el desarrollo y la implementación de procesos de gestión del cambio, investigue utilizando las siguientes frases clave:

	• principios de gestión del cambio • proceso de gestión del cambio • gestión del cambio en la gestión de proyectos • gestión de riesgos.
Elemento 10 – Mejora continua del SMS	
Medios aceptables de cumplimiento	Proceso documentado que muestra cómo la organización utiliza sus procedimientos de monitoreo y medición del rendimiento y su programa de auditoría interna para notificar el proceso de revisión por el gerente responsable y el personal clave de modo que se puedan tomar acciones para mejorar la efectividad del SMS. Plan de acción documentado y asignación de recursos para lograr mejoras.
Notas guías	Se realizan encuestas u otros mecanismos de retroalimentación para medir el rendimiento de la seguridad operacional (por ejemplo, encuestas de clima de seguridad operacional). Se implementa el mantenimiento de los procesos y sistemas de gestión de la seguridad operacional para facilitar la mejora continua. Se implementan mecanismos de mejora de la calidad y la seguridad operacional (por ejemplo, buzones de sugerencias, sistema de notificaciones internos, equipos de revisión de seguridad operacional).
Más información	Para obtener más información sobre cómo lograr una mejora continua, investigue utilizando las siguientes frases clave: • mejora continua • etapas de madurez de la seguridad operacional • Kaizen • Modelo "Planificar, Hacer, Verificar, Actuar".
Programa de auditorías internas	
Medios aceptables de cumplimiento	**Auditoría de seguridad operacional** Programa de auditoría documentado. Un procedimiento de auditoría interna que define los tipos de auditoría y los procedimientos asociados, e identifica al personal que realizará la auditoría. Auditorías realizadas por personal de auditoría capacitado e independiente. Resultados de la auditoría informados al personal responsable de la

	actividad. Acción preventiva o correctiva tomada en respuesta a problemas identificados durante la auditoría. Estas acciones son monitoreadas para asegurar que sean apropiadas, se hayan implementado de manera oportuna y sean efectivas. El análisis de la causa raíz se utiliza para identificar las causas de las no conformidades o no cumplimientos. El funcionamiento del programa de auditoría interna está sujeto a una auditoría independiente. **Notificaciones de auditoria** Documentado y comunicado.
Notas guías	**Auditoría de seguridad operacional** Asegúrese de que el programa de auditoría se haya desarrollado y se haya dotado de recursos para que sea lo suficientemente flexible para que pueda adaptarse a un enfoque basado en el riesgo. La persona o personas designadas para realizar la auditoría deben ser independientes de la función, operación o grupo que se audita. Adopte un enfoque evaluativo de la auditoría para aprovechar al máximo los recursos y el tiempo necesarios. Asegurarse de que las auditorías estén planificadas y bien documentadas; Todos los hallazgos y acciones subsiguientes deben ser rastreados y monitoreados. Asegúrese de que el personal que realiza las auditorías tenga la formación y la experiencia adecuadas y mantenga sus habilidades. **Informes de auditoria** Los informes de auditoría son fáciles de leer y los resultados y las acciones correctivas se indican claramente. Se especifican los plazos para implementar acciones correctivas.
Más información	Para obtener más información sobre el desarrollo y la conducción de un programa de auditoría eficaz, investigue utilizando las siguientes frases clave: • principios y procesos de auditoría • programación de auditorías • competencia del auditor.
Revisión de la gestión	
Medios	Métodos documentados y demostrados para realizar revisiones

aceptables de cumplimiento	formales y regulares por parte del gerente responsable de la eficacia del SMS. Agenda estructurada. Procesos documentados que especifican la frecuencia de las revisiones por el gerente responsable. Los resultados de la revisión se evalúan y registran.
Notas guías	Se implementan procesos para documentar reuniones, decisiones y responsabilidades. Se implementan procesos para dar seguimiento a decisiones y acciones y para revisar la efectividad. Se utilizan métodos de análisis documentados. Se publica y circula una agenda antes de las reuniones. La revisión incluye resultados tanto reactivos como proactivos.
Más información	Para obtener más información sobre el proceso de realización de revisiones de gestión efectivas, investigue utilizando las siguientes frases clave: • gobernanza y supervisión de la seguridad operacional • métodos de comunicación de seguridad operacional • rendición de cuentas de la gestión.
COMPONENTE 4 – PROMOCIÓN DE LA SEGURIDAD OPERACIONAL	
Elemento 11 – Instrucción y educación	
Medios aceptables de cumplimiento	Proceso documentado para identificar los requisitos de instrucción en SMS para que el personal sea competente para desempeñar sus funciones. Proceso documentado para medir la eficacia de la formación y tomar las medidas adecuadas para mejorar la formación posterior. Proceso documentado que evalúa la competencia del individuo y toma medidas correctivas cuando es necesario. El programa de instrucción incluye formación inicial y periódica. Proceso documentado que especifica las responsabilidades para el desarrollo de contenido de instrucción, programación y gestión de registros de instrucción.
Notas guías	Análisis de las necesidades de instrucción (para determinar las deficiencias y los requisitos de todo el personal) se revisa periódicamente. Se implementa un plan de estudios de capacitación que atiende las

	diferentes responsabilidades de seguridad operacional del personal involucrado en el SMS. Consulte el Material de orientación sobre instrucción y competencias. Se desarrolla material de formación coherente con el contenido del SMS de la organización. Dependiendo de los requisitos de personal, se consideran diferentes métodos de impartición de instrucción. El seguimiento de la instrucción garantiza que todo el personal sea competente para desempeñar sus funciones.
Más información	Para obtener más información sobre el desarrollo de un programa de instrucción y educación en seguridad operacional eficaz, investigue utilizando las siguientes frases clave: • análisis de necesidades de instrucción (TNA) • principios de instrucción en seguridad operacional • instrucción en seguridad operacional en la aviación (incluida los factores humanos).
Elemento 12 – Comunicación de la seguridad operacional	
Medios aceptables de cumplimiento	Medios de comunicación de seguridad operacional demostrados y documentados que garantizan que el personal conozca el SMS de acuerdo con sus responsabilidades de seguridad operacional. Transmite información crítica de seguridad operacional y explica por qué se toman acciones de seguridad operacional particulares y por qué se introducen o modifican procedimientos de seguridad operacional.
Notas guías	Se desarrollan e implementan procesos regulares de comunicación de seguridad operacional (por ejemplo, revista de seguridad operacional, boletines informativos, correos electrónicos regulares, reuniones del consejo de revisión de seguridad operacional (SRC), etc.). Se desarrollan métodos para que el personal proporcione comentarios sobre problemas de seguridad operacional. Se fomenta la conciencia de la importancia de comunicar información de seguridad operacional relevante en todos los niveles de la organización y a las organizaciones externas cuando sea apropiado. Las actividades de promoción de la seguridad operacional específicas se llevan a cabo, no solo dentro de la propia organización, sino también con otras organizaciones de terceros relevantes.
Más información	Para obtener más información sobre el proceso de llevar a cabo procesos efectivos de promoción y comunicación de la seguridad

	operacional, investigue utilizando las siguientes frases clave: • estrategias efectivas de promoción de la seguridad operacional de la aviación • procesos para comunicar información crítica para la seguridad operacional • determinar la eficacia de las actividades de comunicación y promoción de la seguridad operacional.

J. IMPLEMENTACION DEL SMS

J.1. Planificación de la Implementación

1. Muchas organizaciones han implementado formas de gestión de la seguridad operacional a lo largo de los años. Algunos se han basado en enfoques de seguridad ocupacional, incluidas metodologías de gestión de peligros y de gestión riesgos. Algunos de los primeros usuarios utilizaron métodos reactivos (notificaciones de seguridad operacional) en combinación con un sistema de gestión de la calidad. Estos sistemas son un buen punto de partida, pero no se puede considerar que el SMS de una organización demuestre el cumplimiento con el Capítulo C del RAP 145 hasta que se realice una solicitud, la DGAC haya evaluado formalmente a la OMA y emitidos documentos de certificado operativo enmendados para demostrar que el SMS ha sido aceptado.

2. A excepción de una nueva organización que implementará SMS como parte de la certificación inicial, las organizaciones deberán realizar una transición planificada del sistema actual (por ejemplo, sistema de calidad interna) a la gestión de la seguridad operacional. Este cambio no puede ser instantáneo, ya que implica cambios como la forma en que las organizaciones abordan y gestionan los riesgos, recopilan y analizan datos y establecen y miden el desempeño de la seguridad operacional. En consecuencia, las organizaciones necesitarán algún tiempo para ajustar los procesos actuales, establecer otros nuevos cuando sea necesario y hacerlos efectivos.

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

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

PRESENTE	Hay evidencia que el indicador pertinente esté documentado dentro de la documentación del SMS de la organización de mantenimiento
ADECUADO	El indicador pertinente es adecuado en base al tamaño, naturaleza y complejidad de la organización de mantenimiento y el riesgo inherente a su actividad
OPERATIVO	Hay evidencia que el indicador está siendo utilizado y se está generando un resultado
EFICAZ	Hay evidencia que el indicador pertinente está logrando el resultado deseado y tiene un impacto positivo en la seguridad operacional
NO INICIADO	No hay evidencia de que la organización haya iniciado la implementación del SMS
MEJORES PRACTICAS	Las organizaciones que buscan mejorar continuamente pueden utilizar los indicadores de mejores prácticas para lograr un mayor nivel de rendimiento en seguridad operacional.

Descripción de los indicadores de rendimiento individuales

5. La herramienta puede ayudar a las OMAs a evaluar si los elementos requeridos de un SMS están "presentes y adecuados" durante la implementación y en una etapa posterior "operativa y eficaz" reconociendo también las" mejores prácticas ". La herramienta se basa en una serie de indicadores para cada elemento de SMS.

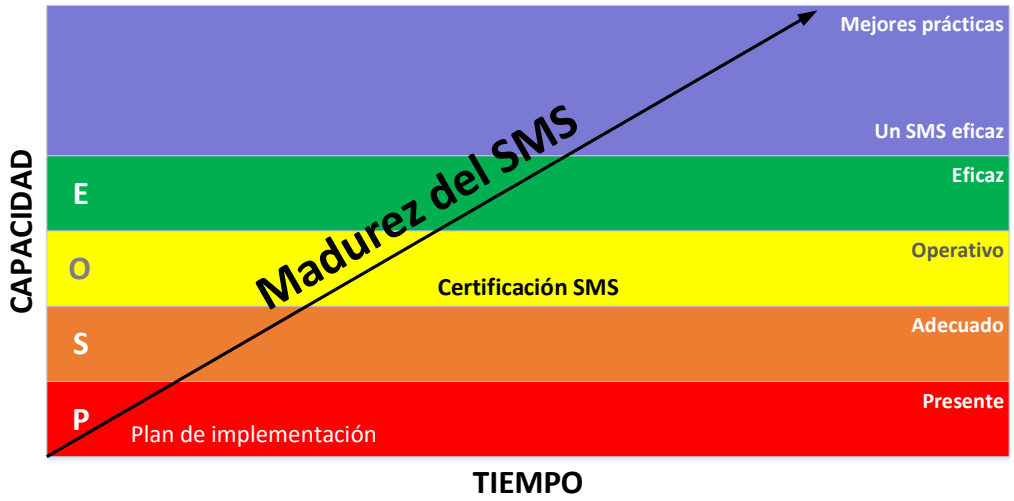
6. La siguiente figura muestra los diferentes niveles de madurez de SMS a medida que una organización implementa y desarrolla su SMS.

J.2. El trayecto de los SMS

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

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

2. Dependiendo del elemento SMS, las Etapas pueden no ser secuenciales sino concurrentes.



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

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

J.3. Análisis de Brechas

1. La mayoría de las OMAs se componen de una red compleja de interfaces e interacciones que involucran a diferentes departamentos internos, así como a diferentes organizaciones externas que contribuyen a la operación segura de la organización. Una descripción general del sistema ayuda a identificar los procesos organizacionales, incluidas las interfaces para definir el alcance del SMS y una oportunidad para identificar cualquier brecha entre el estado actual y los requisitos de un SMS. Una descripción general del sistema también puede servir como punto de partida para identificar los peligros organizacionales y operacionales. Una descripción del sistema puede incluir una lista con viñetas con referencias a políticas y procedimientos. Una descripción gráfica, como un diagrama de flujo del proceso o un organigrama anotado, puede ser suficiente para algunas organizaciones. Una organización debe utilizar un método y formato que les funcione.

2. Un análisis de brechas compara los procesos y procedimientos de gestión existentes de la organización con los elementos de SMS requeridos. El establecimiento de un SMS debe basarse en las estructuras y sistemas organizacionales existentes. Una vez que se ha completado y documentado el análisis de brechas, los recursos y procesos que se han identificado como faltantes o inadecuados formarán la base del plan de implementación. Los enlaces a materiales de recursos adicionales para ayudar a identificar el contenido requerido

para cada elemento se pueden encontrar en referencias y más información.

3. El orden en el que se abordan las brechas puede verse influido por impulsores únicos para cada organización, como la capacidad de vincularse con otros procesos existentes (por ejemplo, gestión de riesgos de seguridad ocupacional) o la introducción planificada de iniciativas comerciales como la metodología Lean.

4. El análisis de brechas identificará lo que se requiere para construir los elementos estructurales del sistema; Es igualmente importante considerar qué puede ser necesario para cambiar la cultura de la organización. Estas actividades serán parte de la gestión del cambio, parte de la promoción de la seguridad operacional y dependerán en gran medida del liderazgo de seguridad operacional en todos los niveles de la organización. Para fomentar un rendimiento de seguridad operacional eficaz, una OMA requiere un sistema de gestión de seguridad operacional y una cultura de seguridad operacional positiva; ambos requieren estrategias de planificación e implementación.

5. Es importante que, como parte del proceso, una vez que se hayan identificado las brechas y se haya establecido un plan para implementar el componente faltante, la OMA también deberá demostrar a través de su plan de implementación que tiene los recursos para construir su sistema de acuerdo con el plan.

J.4. Organizaciones nuevas

1. Las solicitudes para un nuevo certificado (no una organización que solicite la renovación del certificado) enviadas después del 01 de enero del 2018, deben incluir un plan de implementación para SMS que cumpla con los requisitos RAP 145.100 (b). El plan de implementación es por aquellos elementos del SMS que se han desarrollado, pero que aún no están “Operativos”.

2. En este caso, no habrá brechas y se aplicarán todos los componentes y elementos. En este caso, el plan de implementación debería mostrar cómo la organización tiene la intención de implementar el SMS como parte del proceso de certificación. Una forma de evidenciar esto sería completando la herramienta de evaluación.

J.5. Plan de Implementación

J.5.1 Procesos de evaluación

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

2. La DGAC evaluará el plan y proporcionará retroalimentación a la organización. La DGAC, si es aceptable, aprobará el plan de implementación de la organización y establecerá la fecha de implementación (certificación) teniendo en cuenta lo siguiente:

   - capacidad de la organización
   - complejidad de la organización

- riesgos inherentes a las actividades de la organización
- fecha de cualquier renovación de certificado
- cualquier impacto de recursos o programación en la organización o la Autoridad o ambos

3. Para las organizaciones existentes, la fecha de implementación se registrará mediante un documento emitido por la DGAC dirigido al Gerente Responsable de la OMA. En caso de no cumplirse la implementación en la fecha establecida por parte de la OMA, se considera un incumplimiento al Capítulo C de la RAP 145 y la organización pondrá en riesgo su certificado, pudiendo ser suspendida en primera instancia hasta completar la implementación y de no demostrar avance y compromiso de implementación, podría cancelarse la certificación.

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

   a) Identifique al Gerente responsable (consulte el literal G.20.2).

      Sujeto a variaciones en cada organización, se espera que el Gerente Responsable tenga:

      - Plena autoridad para asuntos financieros y de recursos humanos.
      - Responsabilidad directa por la conducción de los asuntos de la organización.
      - Responsabilidad final por todos los asuntos de seguridad operacional.

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

   c) Designe al Responsable de seguridad operacional. El Responsable de seguridad operacional deberá implementar el plan de implementación del SMS en nombre del Gerente responsable además de sus funciones operativas (consulte el literal G.20.3).

5. El desarrollo del plan de implementación del SMS podría considerarse como un proyecto de mejora del sistema de gestión de la organización. Los métodos/herramientas de gestión de proyectos (por ejemplo: proyecto de mejora del ciclo de vida del negocio - LBIP) podrían ayudar a la organización a enmarcar y ejecutar el plan de implementación de SMS.

Etapa 1 – Análisis de Brechas

Esta Etapa es fundamental para definir un plan de implementación de SMS eficiente y eficaz.

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

Las organizaciones aprobadas por la DGAC deberán encontrar que una gran parte

de los requisitos de SMS ya se cumplen mediante el cumplimiento de los requisitos de aprobación de la organización.

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

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

Etapa 2 – Definición, Planificación y Preparación.

Esta Etapa debe considerarse completada cuando se cumplan los siguientes elementos:

- Objetivos de seguridad definidos y aprobados por el Gerente responsable.
- Política de seguridad operacional firmada por el Gerente responsable y comunicada dentro de la organización.
- Estructura de gobernanza de SMS implementada con responsabilidades de seguridad operacional establecidas.
- Personal que apoyará la implementación del plan de implementación de SMS identificado, designado y consciente de los conceptos básicos y objetivos de SMS.
- Plan de implementación de SMS aprobado.

El plan de implementación de SMS deberá:

- Abordar las brechas identificadas como resultado de la Etapa 1, definiendo acciones y responsabilidades.
- Incluya cronogramas e hitos.
- Abordar la coordinación con las organizaciones interconectadas como se define en la Sección H, cuando corresponda.
- Ser aprobado por el Gerente responsable.
- Ser revisado periódicamente y actualizado, según sea necesario.

Etapa 3 – Desarrollo e Implementación

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

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

- Sistema de recolección de datos, comenzando con el mecanismo de notificación (incluyendo fuentes de datos, métodos y medios para recolectar y filtrar, etc.).

- Proceso de identificación de peligros.
- Procesos de mitigación y evaluación de riesgos de seguridad operacional:
  - La organización estará, al menos, preparada para realizar análisis de seguridad operacional basados en la información obtenida a través del sistema de notificación.
  - Esquema de la capacitación de la SRM.
- Aseguramiento de la seguridad operacional:
  - Monitoreo y medición del desempeño en seguridad operacional.
  - Gestión de cambios.
- Promoción de la seguridad operacional:
  - Comunicación de seguridad operacional, teniendo en cuenta que el personal de alta y media dirección es el motor de un SMS eficaz.
  - Plan de sensibilización/capacitación para todo el personal, según sea apropiado.
- Documentación del SMS.
- Evaluación de la preparación del SMS:
  - El SMS implementado se evalúan contra el plan de implementación. Esta evaluación podría realizarse utilizando el método de evaluación propuesto en el **Apéndice 2** “Ejemplo de método de evaluación de madurez de SMS”.
  - Según corresponda, se podría emitir una declaración de cumplimiento para respaldar la aceptación por parte de la DGAC.

Fase 4 – Mejora continua

Con la finalización de la Fase 3, la organización deberá tener todos los componentes/elementos de SMS requeridos operativos.

La implementación de iniciativas de mejora continua es clave para gestionar nuevos peligros o amenazas asociados a las continuas evoluciones del sistema de aviación global con el objetivo de mantener el más alto nivel de seguridad operacional de la aviación. Estas iniciativas deben estar sujetas a un plan de acción de mejora continua (consulte el literal G.22.3.) “Mejora continua del SMS”).

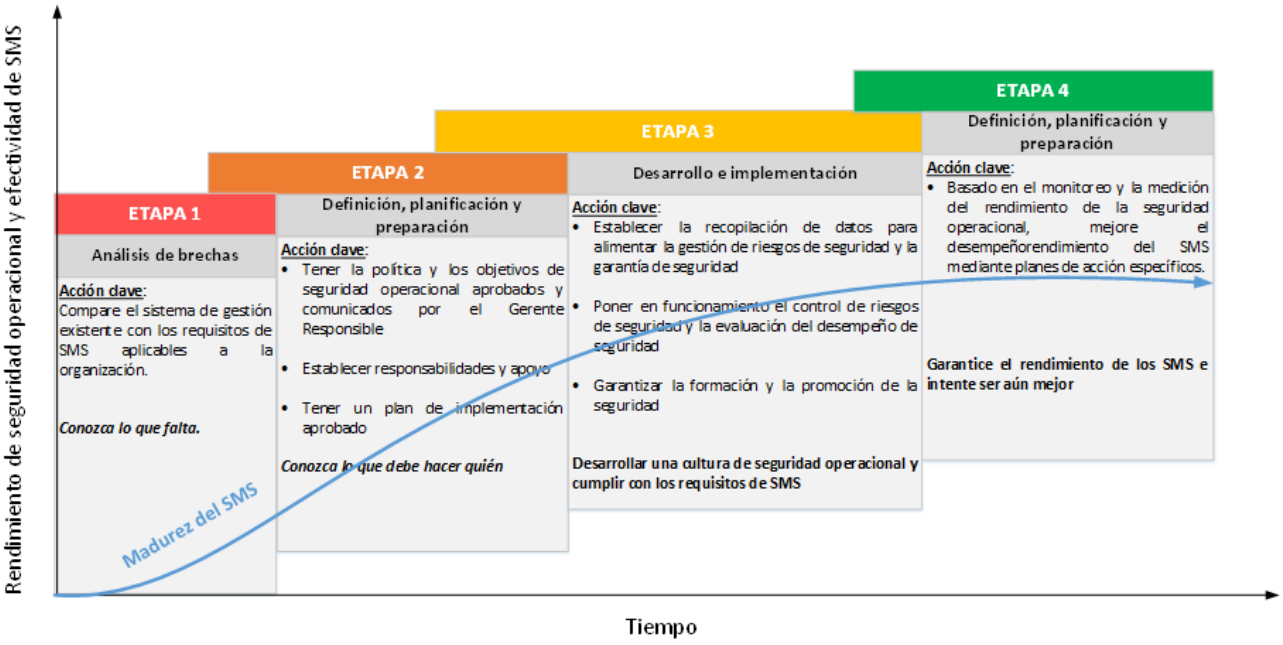


Figura 7. Viaje de la implementación general del SMS

J.5.2 Contenido del Plan

1. El plan de implementación es una hoja de ruta que describe cómo la organización tiene la intención de implementar procesos que cumplen con los requisitos del Capítulo C de la RAP 145 y los requisitos de certificación. Por lo tanto, el plan de implementación deberá ser una estrategia para gestionar la implementación de SMS, incluyendo recursos adecuados y un cronograma realista. Como cualquier cambio comercial, la implementación de SMS requerirá cierto nivel de inversión para abordar la capacitación, los cambios de documentación, el tiempo de desarrollo y posiblemente las herramientas del sistema para administrar los flujos de datos y ayudar con el análisis. Los cambios que son necesarios para implementar el SMS deben gestionarse de forma estructurada para garantizar que existe una conciencia de los impactos y las posibles consecuencias, y que estos se gestionan de forma adecuada.

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

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

4. El plan de implementación debe documentarse en un formato que sea apropiado

para dimensión, el contenido y la complejidad, y debe abordar lo siguiente:

- una descripción general de la implementación que describe: lista de capacidades; gestión; sistema de gestión (relación con otros sistemas, etc.); servicio prestado; proceso de planificación, incluidos los puntos identificados a continuación;
- las tareas identificadas durante el proceso de análisis de brechas, de acuerdo con los requisitos del tamaño de la organización y la complejidad de sus productos o servicios;
- cronogramas e hitos para cada tarea o grupo de tareas desde la etapa de planificación, hasta la implementación completa de SMS;
- para un enfoque de implementación por fases o etapas, las tareas se ordenan en una progresión lógica de acuerdo con la asignación de fases de sus elementos relacionados;
- información sobre quién es responsable de completar la tarea o grupo de tareas identificado, incluida la gobernanza general del plan de implementación;
- un proceso identificado mediante el cual el estado y el rendimiento del plan de implementación del SMS se monitorea regularmente y se toman los pasos para mitigar el rendimiento deficiente;
- información que muestre cómo la coordinación de la integración de contratistas y proveedores externos relacionados con la seguridad operacional sin un SMS, están dentro del alcance del SMS de la organización;
- requerimientos de recursos;
- gestión de riesgos asociados con la implementación de SMS.

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

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

J.6. Multiples certificados

Muchas organizaciones tienen varios certificados, por ejemplo, explotador aéreo y OMA. La DGAC esperaría que estas organizaciones implementen su sistema de gestión de la seguridad operacional (SMS) en todos sus certificados al mismo tiempo y en el mismo

período de transición. Esto debe abordarse a través del plan de implementación.

J.7. Guía de Implementación

Estos pasos proporcionan una guía para implementar un SMS.

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

Paso 5: Desarrollar políticas, procesos / procedimientos y otra documentación.	Es esencial para garantizar que exista un SMS integrado, bien entendido y bien comunicado. Se requiere una declaración de política de seguridad operacional diseñada por la alta dirección (OMAs grandes) y respaldada por el Gerente Responsable que describa su compromiso con la seguridad operacional. El manual de gestión de la seguridad operacional (MSMS) debe cubrir los procesos, acciones y flujos de trabajo involucrados.
Paso 6: Establecer el kit de herramientas de SMS	Un conjunto de herramientas contiene las acciones, los procesos y las herramientas de apoyo que son el corazón de un SMS. Puede incluir cualquiera o todo de lo siguiente: • procesos de identificación de peligros, incluidos los resultados de las investigaciones de seguridad operacional • procesos de evaluación de riesgos y plantillas de apoyo • procesos internos de notificación de seguridad operacional (incluida una base de datos que una organización puede utilizar para capturar notificaciones). • procedimientos de investigación de seguridad operacional interna • un sistema de auditoría interna • procesos de comunicación de seguridad operacional, como reuniones del SRC, y cómo se escala y difunde la información relacionada con la seguridad operacional. • programa de instrucción en seguridad operacional.
Paso 7: Implementar un programa de instrucción en SMS	Una vez que los planes, las políticas, los procedimientos y el conjunto de herramientas están en su lugar, la justificación para implementar un SMS debe comunicarse a todo el personal. Esto se puede hacer a través de un programa de instrucción estructurado que puede incluir una presentación para todo el personal, un paquete basado en la web o una serie de boletines informativos o correos electrónicos. Considerar el nivel de capacitación requerido por aquellos con responsabilidades de seguridad operacional (por ejemplo, los ejecutivos responsables, el responsable de seguridad operacional, los certificadores de conformidad de mantenimiento y el personal operativo (supervisores, mecánicos, ayudantes, entre otros).
Paso 8: Certificación SMS – Fecha de implementación	Antes de la fecha establecida para la implementación (al menos 60 días), envíe toda la documentación pertinente junto con los formularios de certificación de la organización correspondientes. Esto debe incluir un formulario de herramienta de evaluación de SMS completo.
Paso 9: Vigilar y revisar	Una vez que se han implementado los componentes de un sistema de gestión de la seguridad operacional, es importante asegurarse de que realmente estén funcionando. Las medidas de rendimiento descritas

	originalmente en el plan de gestión se pueden utilizar para rastrear el éxito del SMS. La forma de rastrearlos podría ser a través de una reunión del SRC o a través de una revisión periódica de la gestión del SMS.

J.8. Certificación SMS: fecha de implementación

J.8.1. Generalidades

1. Los procesos de certificación de la DGAC actuales se utilizarán para la certificación de SMS de una organización. Consistirá en una evaluación de la exposición y la documentación de apoyo, seguida de una inspección y demostración.

2. Se requiere la aceptación de la DGAC el SMS de una organización existente antes de la fecha de implementación establecida en la aprobación del plan de implementación. La fecha no es posterior a la (s) fecha (s) prescritas en las disposiciones de certificación de cada organización.

3. Consultar la Implementación de un SMS para obtener una descripción general del plan de implementación y la fecha para los plazos y el proceso de implementación.

4. Para las solicitudes enviadas después del 1 de enero de 2018 la aceptación de la DGAC el SMS de la OMA se llevará a cabo como parte del proceso de certificación general para el certificado solicitado.

J.8.2. Evaluación y Revisión

1. Como parte del proceso de evaluación, se revisará el manual y la documentación de respaldo para confirmar que la organización ha desarrollado e implementado su SMS. Si bien esta circular de asesoramiento proporciona el marco para un medio aceptable de cumplimiento de los requisitos, no tiene por objeto proporcionar el único medio de cumplimiento y se considerarán otros métodos de cumplimiento que puedan presentarse. Los solicitantes deben presentar documentación que demuestre que han abordado todos los elementos del SMS.

2. Esto se logra mejor utilizando un formulario de la herramienta de evaluación del sistema de gestión de seguridad operacional que la DGAC utilizará para ayudar a evaluar la capacidad del SMS de la organización. Los procesos y procedimientos de SMS pueden documentarse en un manual de la organización de mantenimiento (MOM) o incorporarse en otro manual, el cual debe ser referenciado en el MOM.

3. Los cambios organizacionales, como el nombramiento de un Responsable de seguridad operacional (la persona responsable de facilitar y gestionar el SMS de la organización) también deberán enviarse al mismo tiempo. Los cambios del personal clave de una OMA asociada con la implementación de SMS estarán sujetos al proceso normal de evaluación de alto nivel de la DGAC. Las entrevistas con las personas se pueden realizar como parte de las actividades in situ de la DGAC. Para la transición de una persona del personal clave a una función similar, o sujeta a la aceptación por parte del Gerente Responsable, combinando la función del sistema para la gestión de la seguridad operacional con otras funciones del personal clave

para funciones operacionales, la atención se centrará en satisfacer las calificaciones y experiencia, y tener los recursos suficientes según corresponda para ese rol.

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

J.8.3. Inspección y Demostración

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

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

J.8.4. Monitoreo Continuo

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

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

J.8.5. Cambios en la Organización del Titular del Certificado

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

    - metodologías para:

        - establecer logros, objetivos y medidas de rendimiento de seguridad operacional (nota: solo la metodología del proceso, no las medidas

individuales)

- identificación de peligros y gestión de riesgos
- desarrollo del programa de auditoría
- revisión de la gestión
- cambios en el programa de instrucción de seguridad operacional, p. ej. cambios de alto nivel en el programa de instrucción en seguridad operacional.

• los cambios deben dirigirse a la DGAC, como es el caso actualmente para otros cambios en el MSMS que requieren la aprobación previa del Gerente Responsable.

J.8.6. Renovación

1. Para las organizaciones que tienen un SMS aceptado, la DGAC evaluará el SMS en la renovación del certificado. En esa etapa, el nivel de madurez debería haber progresado desde el nivel “presente y adecuado” a “operativo” y en desarrollo hacia eficaz. Se recomienda encarecidamente que las organizaciones utilicen la herramienta de evaluación de SMS para evaluar y demostrar la progresión en su madurez y cualquier cambio introducido como parte de las actividades de mejora continua.
2. El mismo proceso de certificación se aplica de acuerdo con la política de certificación de la DGAC, en un proceso de cuatro pasos:

APLICACIÓN	El solicitante debe presentar una solicitud de renovación que incluya La herramienta de evaluación del sistema de gestión de seguridad operacional actualizada y documentación de respaldo.
EVALUACIÓN	La AAC realiza una revisión de escritorio al 100%. A partir de esta revisión, se identifican las áreas de enfoque del sistema de gestión para una evaluación detallada durante la inspección del sitio.
INSPECCIÓN Y DEMOSTRACIÓN	Dependiendo del resultado de esta revisión, las áreas típicas de enfoque podrían ser: ERP, gestión de riesgos, gestión de cambios, monitoreo y medición del rendimiento y auditoría interna. Las entrevistas con personas de alto nivel continuarán enfocándose en el conocimiento de los cambios organizacionales o reglamentarios, la conciencia del riesgo y la actitud de las personas hacia la seguridad operacional, y el personal de toda la organización se involucrará para evaluar si el SMS opera en todos los niveles de la organización.
CERTIFICACIÓN	El SMS se evalúa contra la herramienta de eficacia del SMS. Esto forma parte de la decisión más amplia sobre el cumplimiento general de la OMA con los requisitos para permanecer en el sistema de aviación y obtener una renovación de su certificado.

K. MADUREZ DE SU SMS

K.1. ¿Cómo te va?

Así que ahora ha implementado su SMS y ha sido certificado que cumple con un estándar de madurez de Presente y Adecuado: tiempo para volver a lo de siempre ("Business as Usual (BAU)). En realidad, este es el nuevo negocio y debería haber pocas cosas "habituales" al respecto, aparte de que su organización aplica rutinariamente la gestión de riesgos de seguridad operacional a las decisiones diarias y está activamente intranquila: ¿qué podría salir mal todavía?

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

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

Intente concentrarse en lo que está funcionando bien; Aproveche la oportunidad de compartir y aplicar esos procesos y prácticas en toda la organización y, cuando sea posible, terceros relacionados.

K.2. ¿Cómo sé que el sistema está madurando?

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

Proceso	Etapa de implementación		Mayor capacidad / Madurez	
	Presente	Adecuado	Operativo	Eficaz
Gestión del cambio	El proceso está establecido y documentado.	Existen desencadenantes para utilizar el proceso de gestión del cambio. El proceso considera a las partes interesadas internas / externas.	El proceso se está utilizando y se establecen controles de riesgo antes de que se produzca el cambio.	El proceso se utiliza para todos los cambios que pueden afectar la seguridad operacional. Iniciado de manera planificada, oportuna y consistente.

Proceso	Etapa de implementación		Mayor capacidad / Madurez	
	Presente	Adecuado	Operativo	Eficaz
Nombramiento de personal clave / comunicación de seguridad operacional	La organización ha establecido comités de seguridad operacional.	• El alcance de los comités de seguridad operacional incluye riesgos de seguridad operacional y problemas de cumplimiento. • La asistencia del comité de seguridad operacional de más alto nivel incluye al menos el Gerente responsable y el personal clave de la OMA.	Muestra de actas: reuniones en curso; asistencia; discusiones; acciones identificadas. Se está monitoreando la efectividad del SMS, incluidos los recursos suficientes, las acciones tomadas y se han establecido las medidas apropiadas.	Las reuniones incluyen partes interesadas clave. Los resultados se documentan y comunican y cualquier acción se acuerda, se toma y se realiza un seguimiento de manera oportuna. Las medidas de rendimiento de seguridad operacional se revisan y se toman las acciones apropiadas.

K.3. Inspección y seguimiento de la DGAC

Como resultado del proceso de inspección y monitoreo, la DGAC Canalizará las siguientes áreas para cada participante:

- ¿La organización está empleando eficazmente sus procesos de SMS?
- ¿La organización está monitoreando y midiendo efectivamente su rendimiento en seguridad operacional y el progreso / efectividad del SMS?
- ¿La organización está empleando eficazmente la gestión de riesgos?
- ¿Los resultados de los procesos de SMS han dado lugar a que se identifiquen y aborden deficiencias, así como a mejoras de seguridad operacional significativas?
- ¿Cuál es la cultura de seguridad operacional de la organización?

El proceso de inspección y monitoreo se aplicará de acuerdo con la política de la DGAC sobre inspección y monitoreo del rendimiento de la seguridad operacional.

No se pretende que la herramienta de evaluación de SMS se utilice como una “lista de verificación” completa, elemento por elemento. Más bien, es una herramienta para guiar a los inspectores y capturar la efectividad de aquellos elementos que han sido evaluados durante una inspección. La evaluación se realizará utilizando un enfoque de auditoría de procesos, informado por diversas fuentes de información de riesgo y cumplimiento, como para las actividades de auditoría actual basadas en riesgos. Por lo tanto, esto proporciona un método y una herramienta para:

- evaluar el desempeño de los participantes en función de un conjunto de criterios y orientación;
- registrar esa evaluación;
- informar los resultados, tanto internamente (para generar inteligencia para la DGAC) como externamente al participante (para establecer y promover un compromiso significativo que se enfoque en resultados importantes de seguridad operacional).

Apéndice 1

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

1. Propósito

El propósito de este apéndice es introducir algunas de las mejores prácticas para la gestión de riesgos de seguridad operacional, pero no detallar más los ejemplos de métodos, técnicas y herramientas con referencias cruzadas en el Sección G de este documento.

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

2. Alcance de la gestión de riesgos de la seguridad operacional (SRM)

SRM debe cubrir las siguientes áreas:

- Descripción del sistema: para establecer el marco para la identificación de peligros.
- Identificación de peligros: para identificar peligros de acuerdo con un método.
- Identificación de riesgos de seguridad operacional: para identificar los riesgos de seguridad operacional asociados con los peligros identificados.
- Análisis de riesgos de seguridad operacional: para determinar la gravedad y la probabilidad de un riesgo asociado con los peligros identificados.
- Evaluación de riesgos de seguridad operacional: a partir de los resultados del análisis de riesgos, para determinar si un riesgo es inaceptable según los criterios definidos.
- Control de riesgos de seguridad operacional: para eliminar, reducir o mitigar un riesgo de seguridad operacional mediante acciones que se definirán cuando el riesgo es inaceptable.

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

- Organizaciones que no tienen una aprobación o certificado.

  Las organizaciones no aprobadas deberían aplicar la gestión de riesgos de seguridad operacional a lo siguiente:

  - Implementación de nuevos sistemas.
  - Revisión significativa de sistemas existentes.
  - Desarrollo de procedimientos operativos.
  - Identificación de peligros o controles de riesgo ineficaces a través de los procesos de garantía de seguridad operacional

- Organizaciones de mantenimiento aprobadas (OMA):
  - Los cambios significativos en la OMA deberían desencadenar la SRM (por ejemplo, cambio en la lista de capacidades, estructura de la organización, instalaciones, personal, documentación, procesos, herramientas),
  - Identificación de peligros o controles de riesgo ineficaces a través del proceso de garantía de seguridad operacional.

3. Mejores prácticas para la identificación de peligros

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

N°	Mejores prácticas para la identificación de peligros
1	Evitar tratar de identificar todos los peligros concebibles o teóricamente posibles. Esto no es posible ni deseable. Se requiere juicio para determinar el nivel adecuado de detalle en la identificación de peligros. Debe ejercerse la debida diligencia para determinar los peligros importantes y razonablemente previsibles relacionados con las operaciones de la organización.
2	Centrarse en las áreas con mayor potencial para introducir peligros que puedan conducir a riesgos de seguridad operacional inaceptables, por ejemplo: • escenarios de accidentes (por ejemplo, de investigaciones) si aún no están cubiertos por el actual proceso de mantenimiento de la aeronavegabilidad. • Factores humanos y organizacionales (por ejemplo, actividad que puede conducir a riesgos inaceptables y afectar la seguridad operacional de los trabajos que realiza la OMA). • Cambios en las decisiones y procesos del negocio (por ejemplo, cambios significativos en los principios de un procesador en la estructura de la organización o ambos). • Interfaz con otras organizaciones (por ejemplo, subcontratistas).

N°	Mejores prácticas para la identificación de peligros
	• Novedad, criticidad o complejidad o ambas cosas en el mantenimiento que realiza la OMA (por ejemplo, inspección de la estructura compuesta).
3	Identificar el peligro a partir de la revisión/análisis de los datos de seguridad operacional disponibles, por ejemplo: • Notificaciones/publicaciones de seguridad operacional (por ejemplo, informes de la OACI, AAC, explotadores, otras organizaciones). • Informes de auditoría. • Estudios de seguridad operacional. • Investigaciones (por ejemplo, en el marco de la aeronavegabilidad continuada). • Análisis de seguridad operacional en el marco de las iniciativas de mejora de la seguridad operacional. • (Véase la definición de datos de seguridad operacional en la parte correspondiente a "Términos y definiciones").
4	No mezclar los peligros con **factores desencadenantes/contribuyentes** para mantener un número razonable de peligros confirmados necesarios para ser considerados para la evaluación de riesgos basada en la complejidad de la organización.
5	Agrupar los peligros en categorías, por ejemplo: <u>Peligros sistémicos</u>: • Organizacionales: gestión, recursos, documentación, procedimientos. • Humano: limitaciones de la persona que en el sistema tiene el potencial de causar daño, fatiga, estrés. <u>Peligros operacionales</u>: • Técnico: diseño. • Funcionamiento del producto. <u>Peligros para el medio ambiente</u>: • Regulación, finanzas y presupuesto, instalaciones, cambio climático.
6	No mezclar el peligro con sus consecuencias previsibles. Un peligro no está sujeto a la clasificación de gravedad o probabilidad, pero su riesgo de seguridad operacional asociado sí lo está.
7	Considerar que, dependiendo de su naturaleza, categorización y escenario de identificación: • No todos los peligros identificados deben resultar en acción por el SMS (p.ej. análisis de riesgos de seguridad operacional y acciones de control de riesgos).

N°	Mejores prácticas para la identificación de peligros
	• Varios peligros pueden resultar en acciones combinadas de SMS (ver figura A.1 y A-2)
8	Considerar que varios peligros ya están sujetos a una evaluación sistemática del riesgo y la mitigación del riesgo en el marco de la certificación del producto o de la aeronavegabilidad continuada, o ambos, y que pueden no necesitar más actividades de SMS a nivel del producto, por ejemplo: • "Peligro" se tiene en cuenta en la evaluación del diseño del producto mediante condiciones de incumplimiento para demostrar el cumplimiento de los criterios de certificación de tipo. • "Peligro" identificado en el actual proceso de Mantenimiento de la Aeronavegabilidad con evaluación de riesgos / acciones correctivas (p. Ej., AD) a nivel de producto. Sin embargo, las evaluaciones de los riesgos sistémicos pueden ser pertinentes (por ejemplo, en los procesos de mantenimiento, las herramientas y las competencias). Si se utilizan otras evaluaciones del riesgo, comprobar (cuando proceda) que los peligros, riesgos y gravedades resultantes identificados por estos métodos son coherentes con los niveles existentes conservados durante la certificación y resolver las discrepancias.
9	Considere la posibilidad de identificar los peligros de manera incremental desde la implementación inicial de SMS hasta cuando el SMS este totalmente operativo.
10	Considere revisar los peligros en un ciclo cerrado de mejora continua.

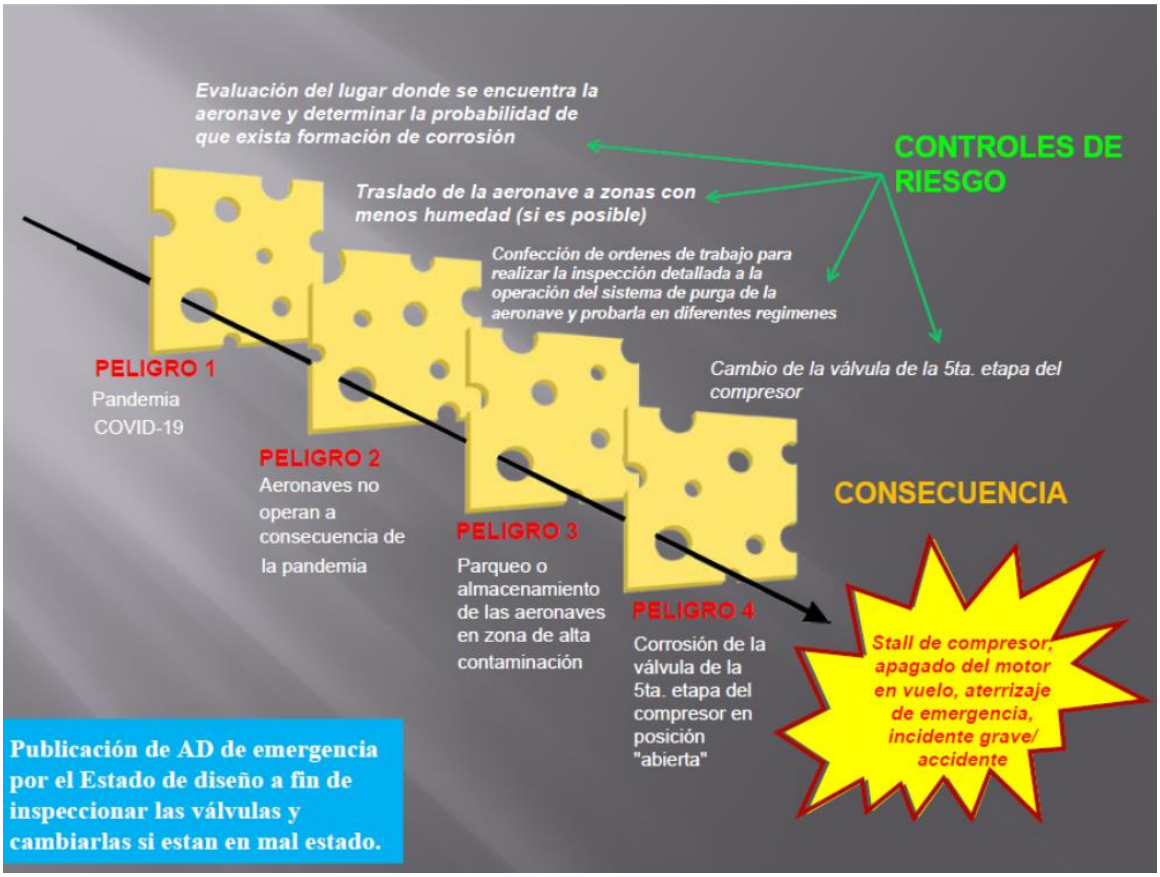


Figura A-1: Identificación del peligro

La Figura A-1 muestra que múltiples peligros (problemas / amenazas de seguridad operacional) pueden producir riesgos de seguridad operacional con consecuencias finales no deseadas, como se muestra en la Figura A-2.

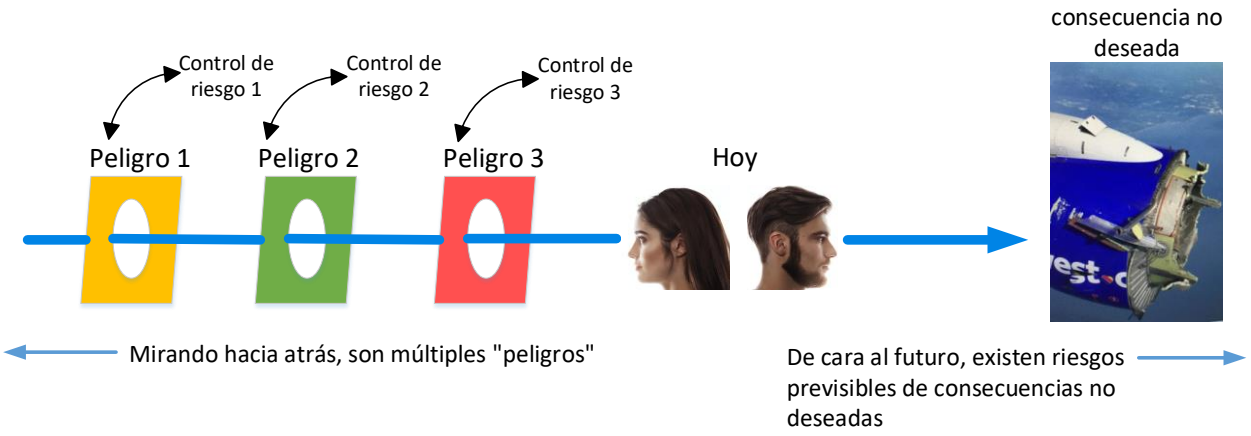


Figura A-2: Múltiples "peligros producen riesgos de seguridad operacional"

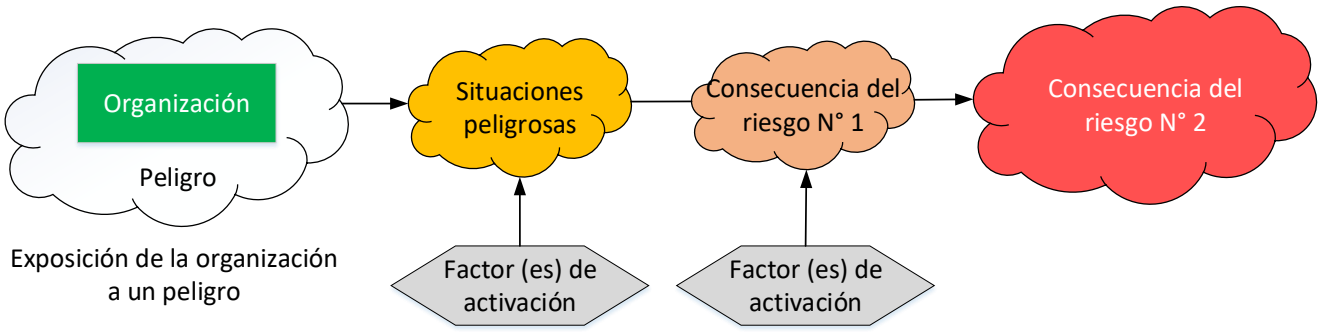


Figura A-3: Peligro único con múltiples factores desencadenantes para producir riesgo (s) de seguridad operacional

La Figura A-3 muestra que un solo peligro que combina los factores desencadenantes puede producir consecuencias no deseadas.

4. Evaluación y control de riesgos de seguridad operacional

El riesgo de seguridad operacional debe identificarse utilizando los métodos, técnicas y/o herramientas más apropiadas como se menciona en la Sección G de esta circular de asesoramiento.

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

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

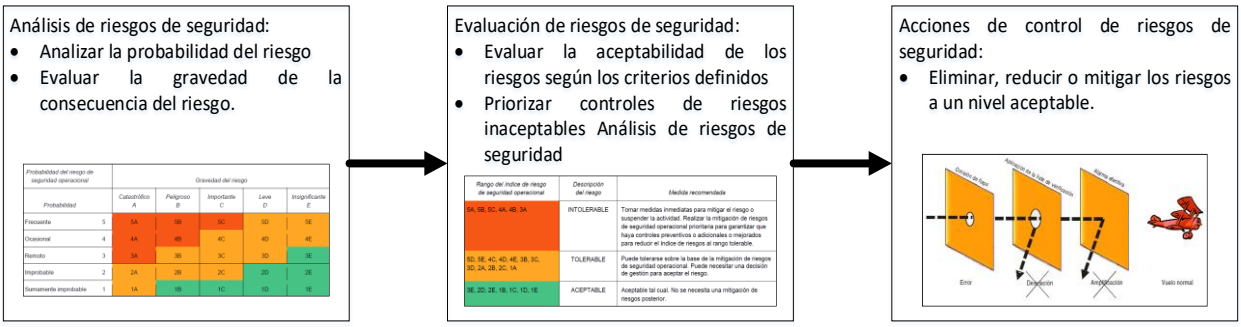


Figura A-4: Análisis, evaluación y control de riesgos de seguridad operacional

Se pueden utilizar varias matrices de evaluación de riesgos de seguridad operacional.

En la Figura A-5 se muestra una matriz de evaluación de riesgos de seguridad operacional genérica con ejemplos personalizados en las Figuras A-6, A-7 y A-8.

Probabilidad del riesgo de seguridad operacional		Gravedad del riesgo				
Probabilidad		Catastrófico A	Peligros 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**

Figura A-5: Matriz genérica de evaluación de riesgos de seguridad operacional

Probabilidad del riesgo de seguridad operacional		Gravedad del riesgo				
Probabilidad		Catastrófico A	Peligros 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**

Figura A-6: Matriz de evaluación de riesgos de seguridad operacional del Doc. 9859 (SMM)

MATRIZ DE EVALUACIÓN DE RIESGO				
Gravedad / Probabilidad	Catastrófico (1)	Crítico (2)	Marginal (3)	Despreciable (4)
Frecuente (A)	**Alto**	**Alto**	**Serio**	**Mediano**
Probable (B)	**Alto**	**Alto**	**Serio**	**Mediano**
Ocasional (C)	**Alto**	**Serio**	**Mediano**	**Bajo**
Remoto (D)	**Serio**	**Mediano**	**Mediano**	**Bajo**
Improbable (E)	**Mediano**	**Mediano**	**Mediano**	**Bajo**
Eliminado (F)	**Eliminado**			

Figura A-7: Matriz de evaluación de riesgos de seguridad operacional de AIA Standard NAS 9927

Nota: *Para una comprensión detallada de esta matriz, consulte NAS 9927*

		Probabilidad		
Gravedad		Improbable (1)	Posible (2)	Probable (3)
	Accidente fatal (5)	Revisar (5)	Inaceptable (10)	Inaceptable (10)
	Accidente serio (3)	Revisar (5)	Revisar (5)	Inaceptable (10)
	Insignificante	Aceptable (1)	Aceptable (1)	Revisar (5)

Figura A-8: Matriz de evaluación con información de aceptabilidad desde el documento SMICG: "SMS para organizaciones pequeñas"

Nota*: Para una comprensión detallada de esta matriz, consulte el documento SMICG "SMS para organizaciones pequeñas"*

El formato de una matriz de evaluación de riesgos de seguridad operacional puede ser personalizado por cada organización dependiendo de la complejidad de sus actividades y prácticas existentes.

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

Apéndice 2

Ejemplo de método de evaluación de madurez de SMS

1. Antecedentes y objetivo

Este apéndice proporciona orientación y propone un método para la evaluación de la madurez del SMS durante la implementación inicial y la mejora continua.
La organización debe utilizarlo como una autoevaluación, pero las autoridades de aviación también podrían considerarlo para evaluar la madurez del SMS de la organización.

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

Esta guía:

- Se basa en una herramienta de evaluación de SMS que es parte del manual del inspector de aeronavegabilidad (MIA), Parte I, Capitulo 14.
- Se basa en un conjunto de criterios[1] y evidencias para ayudar a determinar la madurez general de un SMS con respecto a los 12 elementos del marco de SMS según se captura en este estándar y como resultado de lo establecido en el DGAC RAP 145, Capítulo C.
- Considera el tránsito de mejora de la madurez de SMS desde Presente (P), Adecuado (S) hasta ser Operativo (O) y el Eficaz (E).

***Nota**. — En este documento, "criterios" significa los puntos de verificación/preguntas registrados en las columnas "Presente", "Adecuado", "Operativo" y "Eficaz". "Qué buscar" significa la evidencia.*

2. Definiciones

- **Niveles de madurez**. – Los niveles de madurez se pueden definir de la siguiente manera:
  - **Nivel Presente (P)**: Hay evidencia de que el elemento (mencionado en los "criterios") está definido y documentado.
  - **Nivel Adecuado (S)**: Es apropiado al tamaño, naturaleza y complejidad de la organización de mantenimiento y el riesgo inherente a su actividad.
  - **Nivel Operativo (O)**: Hay evidencia de que el elemento (mencionado en los "criterios") se implementa con resultados/entregables.
  - **Nivel Eficaz (E):** Existe evidencia de que el ítem (al que se hace referencia en los "criterios") está logrando el resultado deseado y tiene un impacto positivo en la seguridad operacional.
- **Evidencia**. – Documentación, notificaciones, registros de entrevistas y discusiones. Si bien la finalización del nivel de madurez "Presente y Adecuado" se basa en la documentación de procedimiento disponible, la

finalización de los niveles de madurez "Operativo" y "Eficaz" se basa en la aplicación consistente de procesos documentados para producir y evaluar hechos, cifras y registros.

3. Utilizando el método

Este método se puede utilizar por primera vez para completar el análisis de brechas como se menciona en el numeral J.5.1.5. Este análisis de brechas y el plan de implementación resultante son los principales insumos para la (s) próxima (s) evaluación (es) de madurez del SMS.

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

Para cada elemento de SMS, se enumera una serie de "criterios de cumplimiento y rendimiento" seguidos de evidencia (es decir, "qué buscar"). Cada criterio debe revisarse para determinar si se encuentra en el nivel de madurez Presente, Adecuado, Operativo o Eficaz, de modo que se pueda evaluar la madurez general del elemento SMS, teniendo en cuenta los demás elementos interrelacionados (por ejemplo, “La política de seguridad operacional debe ser comunicada, con visible respaldo, en toda la organización”). Este requisito puede declararse a nivel operativo bajo las condiciones de que se nombre a un gerente responsable y se le informe sobre los SMS y se defina y promueva la política de seguridad operacional. Estos aspectos están sujetos a otros elementos dentro de esta herramienta de evaluación (como G.20.1.1.2. “Responsabilidades de seguridad operacional, G.23.2 “Comunicación de seguridad operacional”).

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

Alcanzar un nivel de madurez para el SMS general no significa que cada elemento de SMS esté en el mismo nivel de madurez (por ejemplo, algunos elementos de SMS pueden estar en el nivel "Presente", otros en nivel “Adecuado”, otros en el nivel "Operativo" y algunos en el nivel " Nivel Eficaz”. En este estado, la madurez general del SMS se puede considerar en el nivel “Operativo”). Una persona que utilice este método debe estar familiarizada con lo siguiente:

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

4. Herramienta de la evaluación del SMS

Referirse al procedimiento del MIA, Parte I, Capítulo 14, Apéndice B – Herramienta para la evaluación del SMS.

Apéndice 3

Ejemplo del manual o documento de SMS

Este apéndice debe considerarse junto con el literal G.20.1.7 - Documentación SMS.

Cuando la documentación de SMS está sujeta a un documento independiente (Manual de SMS), que suele ser el caso de una organización mediana y grande, se podría estructurar como el ejemplo propuesto a continuación (reconociendo que cada organización puede adaptar su documentación a sus propias necesidades).

1. Objeto del documento

El manual describe cómo se implementa el sistema de gestión de seguridad operacional (SMS) dentro de la OMA, para cumplir con los requisitos de SMS externos e internos.

2. Control de documentos

Preparación manual:

El Responsable de seguridad operacional prepara este manual con la asistencia personal clave y organizaciones internas de la OMA que tienen interacción son el trabajo que realiza la organización.

Aprobaciones:

El manual está aprobado por el gerente de seguridad operacional y el Gerente responsable de la seguridad operacional.

Al firmar, el Gerente responsable valida el cumplimiento de este manual con todos los requisitos y asegura que la organización está en línea con su contenido.

Cambios en el manual:

Se recomienda que el manual se revise como mínimo una vez al año para mantenerse actualizado en caso de cambios en los requisitos o en los SMS de la OMA.

El Responsable de seguridad operacional está a cargo de revisar el manual.

El circuito de aprobación de cambios es el mismo que el de la aprobación inicial.

Publicación, registro y archivo:

Después de la aprobación, el manual se entrega a todo el personal cubierto por SMS y permanece disponible mientras sea aplicable.

Se registra en un archivo seguro y se archivan todas las versiones.

3. Requisitos de SMS

Los siguientes requisitos de SMS son aplicables a la organización:

Consulte todos los documentos de requisitos y las secciones que requieren un SMS o un elemento (s) de SMS (de la DGAC, clientes, empresas y OMA).

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

Las siguientes actividades están cubiertas por el SMS de la OMA:

- Enumere las actividades de la OMA que tienen un impacto en la seguridad operacional de los servicios o productos suministrados por la organización.

Las siguientes funciones están cubiertas por el SMS de la organización:

- Enumere los servicios, departamentos, direcciones que tienen un impacto en la seguridad operacional de los servicios o productos suministrados por la organización.

La interfaz de SMS de la organización con los siguientes SMS externos:

- Enumere los SMS externos (clientes, proveedores, socios, entre otros) con referencia a la documentación de la interfaz que describe las actividades de la interfaz SMS (contrato, especificación, plan, documento de interfaz, entre otros).

5. Política de seguridad operacional

La seguridad operacional es una prioridad absoluta para la OMA.

Nuestro objetivo de seguridad operacional es que nuestros trabajos de mantenimiento de acuerdo a nuestra lista de capacidades no provoquen accidentes aéreos o incidentes graves.

Todos deberán ser conscientes de los posibles peligros para la seguridad operacional asociados a nuestra actividad.

Se deberán implementar todos los medios para alcanzar el nivel de seguridad operacional más alto posible en los trabajos de mantenimiento y servicios que brindamos.

En este aspecto, es nuestra responsabilidad individual notificar voluntariamente y sin demora toda la información sobre sucesos de tal naturaleza que afecten la seguridad operacional de los servicios que ofrece la OMA.

Con el fin de favorecer la comunicación sin miedo, la OMA se compromete a no tomar ninguna medida disciplinaria contra quien, de forma espontánea y sin demora, haya denunciado algún incumplimiento de las requisitos y procedimientos que haya cometido que pueda tener un impacto en materia de seguridad operacional.

La OMA se compromete a investigar y tomar las acciones apropiadas sobre cualquier suceso notificado internamente.

Cualquiera que sea nuestra función dentro de la OMA, cada uno de nosotros debe comprometerse con este proceso de investigación continua del más alto nivel de seguridad operacional.

Firmado

(insertar nombre)
(insertar la fecha)

6. Objetivos de seguridad operacional

Teniendo en cuenta la política de seguridad operacional descrita en el capítulo 4 del manual, los siguientes objetivos de seguridad operacional son metas que debemos alcanzar:

Enumere los principales objetivos definidos por la OMA para mejorar la seguridad operacional del servicio que ofrece.

7. Rendición de cuentas de seguridad operacional y personal clave

La responsabilidad de SMS se asigna a….

La gestión de SMS está asignada a….

Los informes por SMS se logran mediante….

8. Identificación del peligro y gestión del riesgo de seguridad operacional

- Todos los sucesos, problemas o peligros de seguridad operacional deberán informarse a (insertar nombre o función) por correo electrónico (insertar dirección de correo electrónico), teléfono (insertar número de teléfono) o verbalmente.
- Él o ella documenta todos en el Registro de peligros (archivo de registro de referencia) y los evalúa para determinar cuál es el problema, qué podría suceder como resultado, qué acciones deben tomarse (si corresponde) y quién debe administrar el riesgo.
- Este registro de peligros se revisa y actualiza mensualmente y se comparte con la gerencia de la organización.
- Cuando se identifica o detecta un problema o falla, (insertar nombre o función) documenta un análisis de riesgo basado en el siguiente método de evaluación de riesgos de manera oportuna (para completar, Riesgo = criticidad X probabilidad de suceso, FMEA, PFMEA, escalera de Ishikawa ...).
- Cuando se confirma el riesgo de seguridad operacional, la organización implementa un plan de resolución proponiendo soluciones paliativas/correctivas de manera oportuna.

9. Plan de respuesta ante emergencias y acciones correctivas

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

(ERP) es un componente integral del proceso de gestión de riesgos de seguridad operacional (SRM) de una organización de mantenimiento para abordar emergencias, crisis o eventos relacionados en donde la organización tenga que participar. Cuando existe la posibilidad de que las operaciones o actividades de aviación de un explotador aéreo, al cual la organización de mantenimiento le brinda sus servicios, se vean comprometidas por emergencias como una emergencia de salud pública / pandemia, estos escenarios también deben abordarse en el ERP, según corresponda. El ERP debe abordar las emergencias previsibles identificadas a través del SMS e incluir acciones, procesos y controles atenuantes para gestionar de manera efectiva las emergencias relacionadas con la aviación.

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

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

El siguiente es un ejemplo que la OMA podría utilizar y modificar.

ERP que es: (a completar por la OMA).

Anticipándose a tal situación: las reglas por las cuales la organización ingresa en una gestión de emergencia son las siguientes: (a completar por la OMA).

En tal situación, el proceso a aplicar es el siguiente: (a completar por la OMA)

1. Equipo ERP para reunirse en poco tiempo (lugar, medios, tiempo de respuesta, etc.).
2. Equipo ERP para evaluar la emergencia de la situación.
3. Defina acciones inmediatas:
    a) Considera un refuerzo del equipo del ERP, según corresponda.
4. Prepare la comunicación (explotador, aeródromo…) según corresponda:
    a) Designar al responsable de comunicación de la OMA.
    b) Definir las reglas para las comunicaciones.
5. Preparar siguiendo planes, acciones y medios a corto, mediano y largo plazo dimensionados al problema para recuperar la situación normal.

10. Monitoreo y medición del rendimiento de seguridad operacional

La medición y el monitoreo del rendimiento de seguridad operacional revisará cómo se gestionan todos los sucesos, problemas o peligros de seguridad operacional recopilados. Para esto (insertar nombre o función) define los indicadores clave de seguridad operacional apropiados (por ejemplo, tiempo de resolución de riesgos, número de recomendaciones implementadas, acciones de promoción realizadas, devoluciones de capacitaciones, revisión de cambio de proceso o producto ...). La medición y revisión de los parámetros clave de seguridad operacional se organizan cada seis meses (para escalar de acuerdo con las actividades de la OMA y la naturaleza del servicio de mantenimiento que se proporciona).

11. Gestión de los cambios

Los cambios (en la lista de capacidades, proceso u organización) son revisados por (insertar nombre o función) teniendo en cuenta el impacto del cambio en la seguridad operacional. La evaluación de riesgos de seguridad operacional (consulte literal G.21.2.1 podría ser la herramienta adecuada para evaluar el impacto de dicho cambio en la seguridad operacional.

12. Promoción, instrucción y comunicación de la seguridad operacional

Cada dos años se proporciona capacitación o concientización sobre seguridad operacional y SMS a todas las partes interesadas en la gestión de la seguridad operacional.

Cualquier información crítica para la seguridad operacional que deba distribuirse se enviará por correo electrónico a todas nuestras partes interesadas y se publicará en los paneles de visualización de la empresa. Se espera que todo el personal revise los paneles y lea cualquier artículo de seguridad operacional nuevo.

13. Mejora continua y auditoria de SMS

Cada año, el Gerente Responsable y el Responsable de seguridad operacional se reúnen para revisar el rendimiento del SMS de la OMA. Se implementan las acciones necesarias para garantizar la mejora continua del sistema.

El SMS se audita al menos una vez cada 3 años.

La agenda genérica de revisiones de SMS cubre:

- Revisión de los resultados del rendimiento en seguridad operacional (dashboard de rendimiento en seguridad operacional).
- Principales cambios en el SMS impulsados por requerimientos internos o externos.
- Estado del SRM para riesgos de alto nivel identificados.
- Efectividad de los controles de riesgos de seguridad operacional.
- Nuevos peligros y riesgos identificados por el SRM desde la última revisión.
- Buenas prácticas identificadas y registradas.

- Plan de acción para la mejora del rendimiento en seguridad operacional, incluida la asignación de recursos y la identificación de líderes de acción.
- Revisión de políticas y objetivos; actualizar según sea necesario.

14. Gestión de los archivos del SMS

(Insertar nombre o función) conserva los registros de todos los documentos mencionados en este manual.

Apéndice 4

indicadores de rendimiento en materia de seguridad operacional (SPI) del SMS

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

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

3. Por este motivo las OMA deben desarrollar los SPI del SMS con el asesoramiento de la DGAC. Sus SPI propuestos **deberán ser coherentes** con los indicadores de seguridad operacional de SSP del Estado; por lo tanto, se debe obtener un **acuerdo / aceptación** necesaria con la DGAC.

Ejemplos de indicadores de rendimiento de seguridad operacional (SSP) e indicadores de rendimiento de seguridad operacional (SMS)												
Indicadores de rendimiento en materia de seguridad operacional del SSP (Estado Colectivo)						Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedores de servicios individual)					
Indicadores de alta gravedad/baja probabilidad (basados en sucesos/resultados)			Indicadores de baja gravedad/alta probabilidad (basados en sucesos/resultados)			Indicadores de alta gravedad/baja probabilidad (basados en sucesos/resultados)			Indicadores de baja gravedad/alta probabilidad (basados en sucesos/resultados)		
Indicador de rendimiento en materia de seguridad operacional	Criterios de nivel de alerta	Criterios del nivel de objetivos	Indicador de rendimiento en materia de seguridad operacional	Criterios de nivel de alerta	Criterios del nivel de objetivos	Indicador de rendimiento en materia de seguridad operacional	Criterios de nivel de alerta	Criterios del nivel de objetivos	Indicador de rendimiento en materia de seguridad operacional	Criterios de nivel de alerta	Criterios del nivel de objetivos
Organizaciones de DOA/POA/MRO											
Informes obligatorios de defectos (MDR) trimestrales de la MRO colectiva de la DGAC recibidos	Promedio + 1/2/3 SD (restable-cimientos anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual.	Tasa de % o hallazgos de LEI anual de la auditoria de vigilancia de MRO/POA/DOA colectivas de la DGAC (hallazgos por auditoria)	Consideración	Consideración	Tasa trimestral de MRO/POA de reclamos de la garantía técnica de los componentes	Promedio + 17273 SD (restablecimi ento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual.	Tasa de % o hallazgos de LEI anual de la auditoria de QMS/SMS interna de MRO/POA/DO A (hallazgos por auditoria)	Consideración	Consideración
Tasa trimestral de POA/DOA colectiva de la DGAC de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración				Tasa trimestral de POA/DOA de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración	Tasa de averías/rechazo s trimestrales de la inspección final/pruebas de MRO/POA/DOA (debido a problemas de calidad interna)	Consideración	Consideración

						Tasa trimestral de MRO/POA de los informes obligatorios/importantes de defectos de componentes emitidos (debido a problemas de calidad interna)	Consideración	Consideración	Tasa de informes de peligros voluntarios de MRO/POA/DOA (por personal de operaciones por trimestre)	Consideración	Consideración
ETC											

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

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

5. En este caso, pueden representar la tasa de devoluciones de componentes por garantías a una OMA de componentes, en relación a la hora / hombre empleada en el programa anual de mantenimiento realizado, o la cantidad de constataciones establecidas en el programa de auditorías de SMS y calidad anual de la OMA o la cantidad de observaciones encontradas en las pruebas finales realizadas a las aeronaves después de efectuar su mantenimiento mayor, en relación a estas mismas H/H de trabajo anual, etc., siendo evidenciadas con una notificación / obligatoria durante sus procesos de ejecución (control de H/H/; informe de auditorías e inspección final).

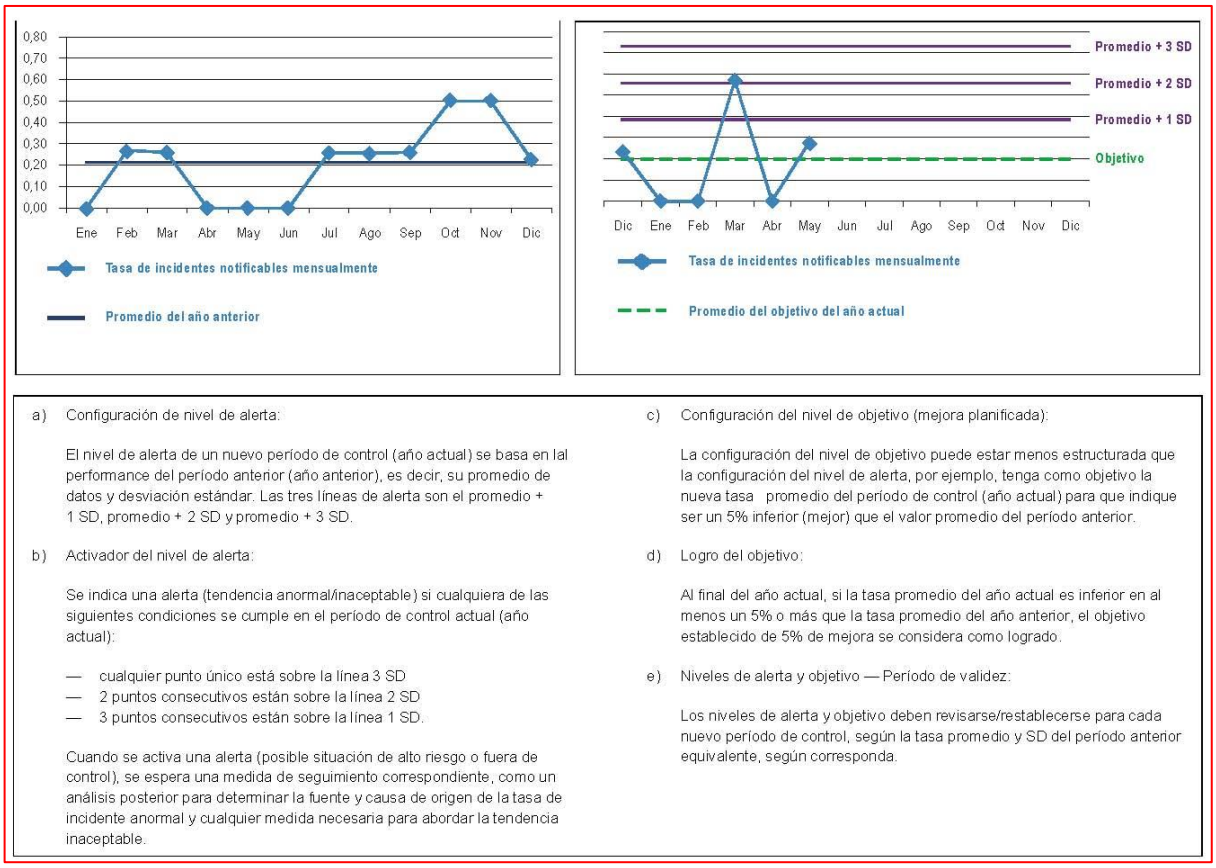


Figura 2. Diagrama de indicador de rendimiento en seguridad operacional de una OMA (con configuración de nivel de alerta y objetivo)

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

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

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

9. La fórmula siguiente permitirá calcular la desviación estándar (σ), considerando que “X” es el valor de cada punto de datos; “N” es el número de puntos de datos y “μ” es el valor promedio de todos los puntos de datos.

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

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

Hoja de datos de muestra usada para generar un diagrama de alto impacto del indicador de seguridad operacional del SMS (con criterios de la configuración de alerta y objetivo)

Año anterior				
Mes	H/H total de la OMA	Cantidad de incidentes de notificación obligatoria	Tasa de incidentes*	Promedio
Enero	3 992	—	0,00	0,21
Febrero	3 727	1,00	0,27	0,21
Marzo	3 900	1,00	0,26	0,21
Abril	3 870	—	0,00	0,21
Mayo	3 976	—	0,00	0,21
Junio	3 809	—	0,00	0,21
Julio	3 870	1,00	0,26	0,21
Agosto	3 904	1,00	0,26	0,21
Septiembre	3 864	1,00	0,26	0,21
Octubre	3 973	2,00	0,50	0,21
Noviembre	3 955	2,00	0,51	0,21
Diciembre	4 369	1,00	0,23	0,21
		Promedio	0,21	
		SD	0,18	

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

Los criterios de configuración del nivel de alerta del año actual se basan en el año anterior (Promedio + 1/2/3 SD).

Año actual							
Mes	H/H total de la OMA	Cantidad de incidentes de notificación obligatoria	Tasa de incidentes*	Promedio del año anterior + 1 SD	Promedio del año anterior + 2 SD	Promedio del año anterior + 3 SD	Promedio del objetivo del año actual
Diciembre	4 369	1,00	0,23	0,39	0,56	0,73	0,21
Enero	4 090	0,00	0,00	0,39	0,56	0,73	0,20
Febrero	3 316	0,00	0,00	0,39	0,56	0,73	0,20
Marzo	3 482	2,00	0,57	0,39	0,56	0,73	0,20
Abril	3 549	0,00	0,00	0,39	0,56	0,73	0,20
Mayo	3 633	1,00	0,28	0,39	0,56	0,73	0,20
Junio				0,39	0,56	0,73	0,20
Julio				0,39	0,56	0,73	0,20
Agosto				0,39	0,56	0,73	0,20
Septiembre				0,39	0,56	0,73	0,20
Octubre				0,39	0,56	0,73	0,20
Noviembre				0,39	0,56	0,73	0,20
Diciembre				0,39	0,56	0,73	0,20
		Promedio					
		SD					

El objetivo del año actual indica una tasa de mejora promedio del 5% sobre la tasa promedio del año anterior, la que es:	0,20

* Cálculo de la tasa (cada 1 000 H/H).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    ✓ los objetivos deberán soportar el objetivo de seguridad operacional primario y los ALosP de la DGAC

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

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

Tabla 4. INDICADORES DE CUESTIONES SISTEMICAS

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
CONFORMIDAD	Monitoreo de auditorías/cumplimiento internas: todos los incumplimientos	Reducción del ____% de los incumplimientos analizados por su importancia para la seguridad operacional en comparación con los del año anterior.
CONFORMIDAD	Monitoreo de auditorías/cumplimiento 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.
CONFORMIDAD	Monitoreo de auditorías / cumplimiento internas: la capacidad de respuesta a las solicitudes de acción correctiva	Reducción en un _____ % del tiempo de espera promedio para completar las acciones correctivas por ciclo de planificación de supervisión – tendencia en comparación con las del año anterior.
CONFORMIDAD	Monitoreo de auditorías/cumplimiento externas: todos los incumplimientos	Reducción del ____% de los incumplimientos analizados por su importancia para la seguridad operacional en comparación con los del año anterior.
CONFORMIDAD	Auditorías externas: incumplimientos importantes	Reducción del ____% de incumplimientos significativos en comparación con el número total de incumplimientos significativos del año anterior.

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
CONFORMIDAD	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.
CONFORMIDAD	Consistencia de los resultados entre auditorías internas y externas / control del cumplimiento	Reducción en un ____% de los incumplimientos significativos descubiertos solamente a través de las auditorías externas en comparación con las del año anterior.
EFECTIVIDAD DEL SMS	Gestión estratégica	Incremento en un ____% de la frecuencia con la que los planes oficiales de la organización y los documentos de estrategia son revisados con respecto a la seguridad operacional en relación al año anterior.
EFECTIVIDAD DEL SMS	Compromiso de la dirección	Número de reuniones de gestión dedicadas a la seguridad operacional al trimestre en relación al número total de reuniones planificadas a realizarse en dicho año.
EFECTIVIDAD DEL SMS	Tasa de rotación del personal clave de seguridad operacional	Duración del personal en el cargo, desde el momento es que asume el cargo hasta su retiro, en relación con los últimos dos años. Número de casos en los que se han analizado las razones de la salida del personal clave en relación a la salida de personal en los últimos dos años.
EFECTIVIDAD DEL SMS	Supervisión	Incremento en un ____% del número de casos en que los responsables de la supervisión expresaron seguimiento positivo sobre el comportamiento consciente en materia de seguridad operacional de su personal al año en comparación con el año anterior.
EFECTIVIDAD DEL SMS	Notificación	Incremento en un ____% del número de notificaciones recibidas al año y la tendencia en comparación con la del año anterior. Incremento en ____% de las notificaciones a las que se proporcionó información al notificante dentro de los 10 días hábiles, en comparación con las del año anterior. Incremento en ____% de las notificaciones seguidas de una revisión independiente de la seguridad operacional, en comparación con las del año anterior.
EFECTIVIDAD DEL SMS	Identificación de los peligros	Reducción del ____% del número de escenarios de accidentes/incidentes graves analizados para apoyar la Gestión de Riesgos de Seguridad operacional (SRM) en relación al año anterior. Número de nuevos peligros identificados a través del sistema de notificación interno al año y la tendencia por cada 10 peligros identificados. Reducción de un ____% de los incumplimientos de las auditorías externas relacionados con peligros que no habían sido percibidos por el personal / gestión previamente en comparación con el año anterior.

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
		Incremento del ____% del número de notificaciones de seguridad operacional recibidas del personal al año y la tendencia en relación al año anterior.
EFECTIVIDAD DEL SMS	Controles de riesgo	Número de nuevos controles de riesgo validados por año en los últimos dos años. Incremento en un ____% del presupuesto total asignado a nuevos controles de riesgo en relación al año anterior.
EFECTIVIDAD DEL SMS	Gestión y desarrollo de las competencias de recursos humanos	Incremento en un ____% de la plantilla para la que se ha establecido una evaluación de competencias en los últimos dos años. Incremento en un ____% de personal que ha tenido formación en gestión de la seguridad operacional en los últimos dos años (instrucción continua). Incremento en un ____% la frecuencia de revisión de los perfiles de competencias en los últimos dos años. Incremento en un ____% la frecuencia de revisión del alcance, contenido y calidad de los programas de formación en comparación con el año anterior. Número de cambios realizados en los programas de capacitación a raíz de la retroalimentación del personal al año en relación a las 10 últimas revisiones efectuadas. Numero de cambios realizados en los programas de formación a raíz del análisis de las notificaciones de seguridad operacional internas por año en relación a los 10 últimos cambios.
EFECTIVIDAD DEL SMS	Gestión del cambio	Número de cambios organizacionales en los que se ha realizado una evaluación formal de riesgos de seguridad operacional al mes / trimestre / año y la tendencia en relación a los 10 últimos cambios. Número de cambios en los procedimientos para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al mes/trimestre/año y la tendencia en relación a los 10 últimos cambios. Número de cambios técnicos (por ejemplo: nuevos equipos, nuevas instalaciones, nuevo hardware) para los que se ha realizado una evaluación formal de riesgos de seguridad operacional al mes/trimestre/año y tendencia en relación a los 10 últimos cambios. Número de controles de riesgo implementados por los cambios al mes/trimestre/año y tendencia en relación a los 10 últimos cambios. % de cambios (organizacionales/procedimientos/técnicos, etc.) que han sido objeto de evaluación de riesgos en relación a los 10 últimos cambios.
EFECTIVIDAD DEL SMS	Gestión de contratistas	Incremento del ____% de contratistas cuyo rendimiento en materia de seguridad operacional se ha evaluado en relación a la cantidad de contratistas que se tuvo el año anterior. Reducción del ____% de la frecuencia con la que se determina el rendimiento en materia de seguridad operacional de los contratistas en relación a la del año anterior.

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
		Reducción en un ____% del tiempo de demora para impartir capacitación (formación) de los contratistas en seguridad operacional en relación al año anterior. Incremento de un ____% de los contratistas que han implementado procedimientos de control de la formación en temas de seguridad operacional en relación al año anterior. Incremento en un ____% de los contratistas que tienen establecido un sistema de información (o seguimiento) sobre cuestiones de seguridad operacional con sus clientes en relación al año anterior. Número de notificaciones de seguridad operacional recibidas de los contratistas por año y tendencia en relación a la cantidad de contratistas que tiene la OMA. Número de acciones de seguridad operacional iniciadas debido a la evaluación del rendimiento en materia de seguridad operacional o de las notificaciones de seguridad operacional recibidas al año y tendencia en relación a la cantidad de contratistas que tiene la OMA.
EFECTIVIDAD DEL SMS	Planificación de respuesta ante emergencia	Número de simulacros de emergencia cumplidos por año en relación a la cantidad planificada. Frecuencia de la revisión del ERP en relación a la cantidad simulacros de ERP realizadas. Número de cursos de formación en ERP realizados por mes / trimestre / año en relación a los cursos programados. % de personal formado en el ERP dentro de un cuarto de año en relación al total del personal de la OMA. Número de reuniones con los socios principales y contratistas para coordinar el ERP al mes / trimestre / año en relación a todas las reuniones planificadas al año.
EFECTIVIDAD DEL SMS	Promoción de la seguridad operacional	Incremento en un ____% del grado en que el personal considera la seguridad operacional como un valor que guía su trabajo diario, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un ____% del grado en que el personal considera que la seguridad operacional es muy valorada por sus gestores, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un ____% del grado en que se aplican los principios de actuación humana, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un ____% del grado en que toma iniciativas el personal para mejorar las prácticas organizacionales o notificar u problema a la gestión, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior.

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
		Incremento en un ____% del grado en el que el comportamiento consciente de la seguridad operacional es apoyado, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior. Incremento en un ____% del grado en el que el personal y la gestión son conscientes de los riesgos de sus operaciones y lo que implican para ellos mismos y para los demás, considerando obtener el valor más alto de una encuesta que se efectúe en relación a todo el personal que trabaja en la OMA (por ejemplo: en una escala de 1 = bajo a 5 = alto) en comparación al año anterior.

L. CONTACTOS PARA MAYOR INFORMACIÓN

Para cualquier consulta técnica con relación a la presente circular de asesoramiento dirigirla a la Coordinación Técnica de Aeronavegabilidad, al siguiente correo electrónico: dgac_aeronavegabilidad@mtc.gob.pe

---

INTENCIONALMENTE DEJADA EN BLANCO