**REPUBLICA DEL PARAGUAY**

**DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL**

# *CIRCULAR DE ASESORAMIENTO*

# CA Nº: 145-002

## Implementación de un Sistema de Gestión de la Seguridad Operacional (SMS) en una Organización Aprobada DINAC R 145

**Aprobado por Resolución Nº: 143 /2013**

**Primera Edición 2013**

## REGISTRO DE ENMIENDAS Y CORRECCIONES

| ENMIENDAS | | | |
|---|---|---|---|
| Num. | Fecha de aplicación | Fecha de anotación | Anotada por |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| CORRECCIONES | | | |
|---|---|---|---|
| Num. | Fecha de aplicación | Fecha de anotación | Anotada por |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# INDICE

## CIRCULAR DE ASESORAMIENTO

## IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN UNA ORGANIZACIÓN APROBADA DINAC R 145

**Apéndices**

# CIRCULAR DE ASESORAMIENTO Nº 002-145

**ASUNTO:** **IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN UNA ORGANIZACIÓN APROBADA DINAC R 145**

## Sección A - Propósito

La presente circular de asesoramiento sobre Implementación de un Sistema de Gestión de la Seguridad Operacional (SMS) en una Organización aprobada DINAC R 145 constituye un documento cuyos textos contienen métodos, e interpretaciones con la intención de aclarar y de servir de guía a las organizaciones de mantenimiento de los Estados miembros del SRVSOP y para el cumplimiento de los requisitos establecidos en el DINAC R 145.510.

## Sección B - Alcance

El alcance está orientado a los siguientes aspectos:

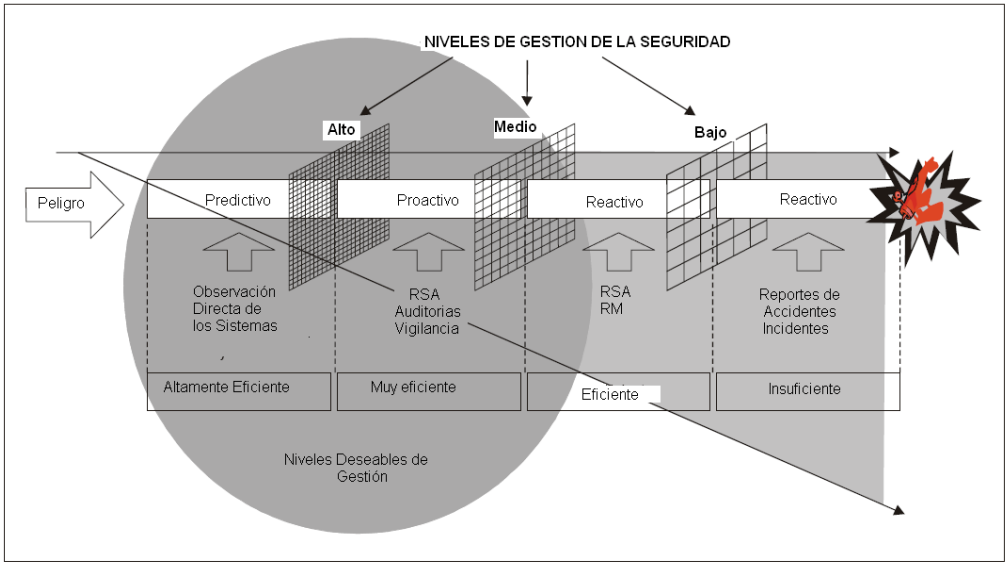
a. Proporcionar una ayuda a las organizaciones de mantenimiento, que soliciten o estén aprobadas bajo DINAC R 145, para la correcta interpretación del requisito DINAC R 145.510.

b. Proporcionar lineamientos de como cumplir de una manera aceptable con los requisitos antes listados.

## Sección C - Introducción

a. Aunque la implementación de un SMS es un proceso simple; dependiendo de un determinado número de factores tales como: disponibilidad de material de orientación publicado por la autoridad, conocimiento de SMS dentro de la organización y recursos disponibles para la implementación; este proceso simple puede convertirse en una tarea sumamente complicada.

b. Para la administración de proyectos es indudable que proyectos complejos son ejecutados de mejor manera dividiendo la tarea en partes más manejables que son componentes de la tarea total. Esto también permite que la asignación de recursos para la implementación sea menor para concluir un determinado subconjunto de actividades. Por otra parte la implementación de este sistema requiere un cambio cultural en las organizaciones y establecer un sistema de recolección de datos que incluya métodos reactivos, proactivos y predictivos, esto permite que se establezcan objetivos en fases que permitan que se desarrolle el sistema de forma gradual hasta alcanzar un sistema muy eficiente para la gestión de la seguridad operacional.



***Nota:*** *RSA: Reporte de seguridad aérea.*

*RM: Reporte mandatario.*

**Figura 1**

c. Esta razón justifica el planteamiento en fases de la implementación del SMS que en resumen está dirigido a:

1. Proporcionar una serie de pasos a seguir, de fácil de administración, para la implementación del SMS; incluyendo la asignación de recursos;
2. Administración efectiva de la carga de trabajo asociada a la implementación del SMS;
3. Evitar demandas absurdas en los requisitos de implementación y el consecuente "cumplimiento cosmético".

d. Una división en cuatro fases es propuesta para la implementación del SMS. Cada fase está asociada con un componente del SMS establecido en el marco de trabajo de OACI. La implementación de cada fase está basada en la introducción de elementos específicos de cada componente durante la fase en cuestión.

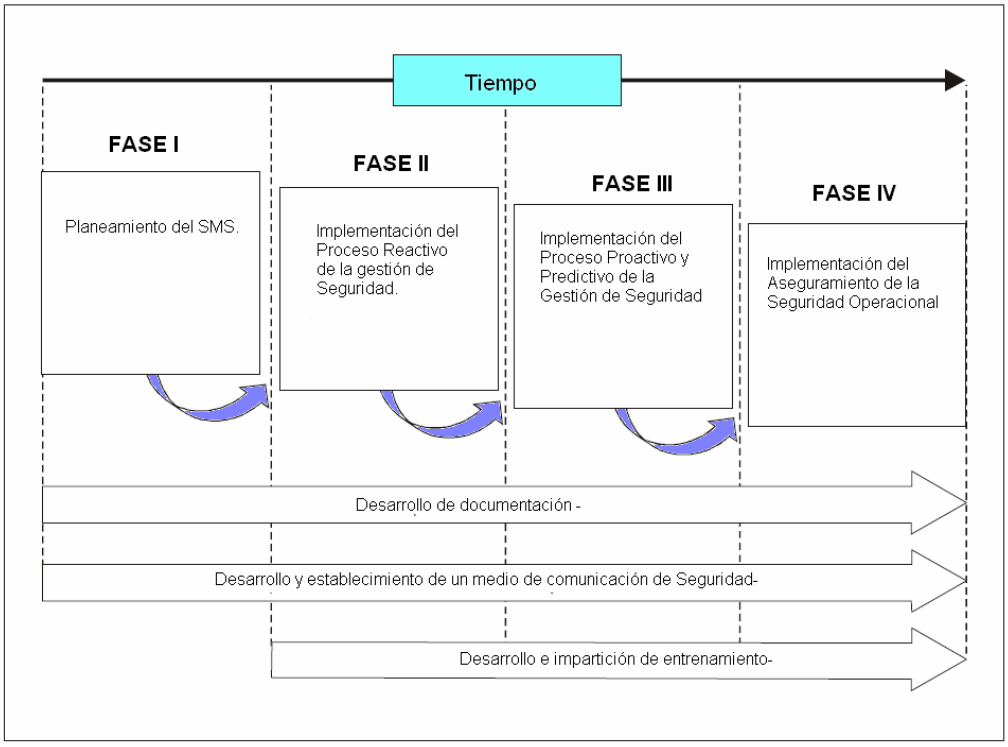



**Figura 2**

e. Esta circular de asesoramiento está vinculada al cumplimiento del requisito DINAC R 145.510; que involucra a las 4 Fases de implementación del SMS.

f. Para uso de esta CA las expresiones "debe", "es necesario que" y "tiene que" en el MAC quieren expresar que es altamente recomendable la utilización del método presentado y no así considerarse como un requisito adicional de la DINAC R 145.

**Sección D - Implementación del Sistema de Gestión de Seguridad operacional**

**a) <u>Fase 1 Planeamiento</u>** (Ver párrafo 145.510(a) del DINAC R 145)

**1.** El objetivo de la fase 1 de implementación del Sistema de Gestión de la Seguridad Operacional (SMS) es proporcionar un esquema de cómo los requerimientos de SMS serán cumplidos e integrados a las actividades de la organización y un marco de responsabilidad para la implementación del SMS.

**2.** Para concluir esta fase las siguientes actividades deben haber sido concluidas de forma satisfactoria para la autoridad, de conformidad con los requerimientos establecidos en la regulación DINAC R 145:

i. Identificar el Gerente Responsable y las responsabilidades de los gerentes.

ii. Identificar la persona o el grupo de personas dentro de la organización responsable por la implementación del SMS.

iii. Descripción del SMS.

iv. Conducción de un análisis del faltante entre los recursos existentes en la organización y los requisitos del DINAC R 145.

v. Desarrollo de un plan de implementación que explique como la organización implementará el SMS en base a los requerimientos, la descripción de su sistema y los resultados del análisis del faltante.

vi. Desarrollo de documentación relativa a los objetivos y políticas de seguridad operacional.

vii. Desarrollo y establecimiento de un medio para la comunicación de seguridad operacional

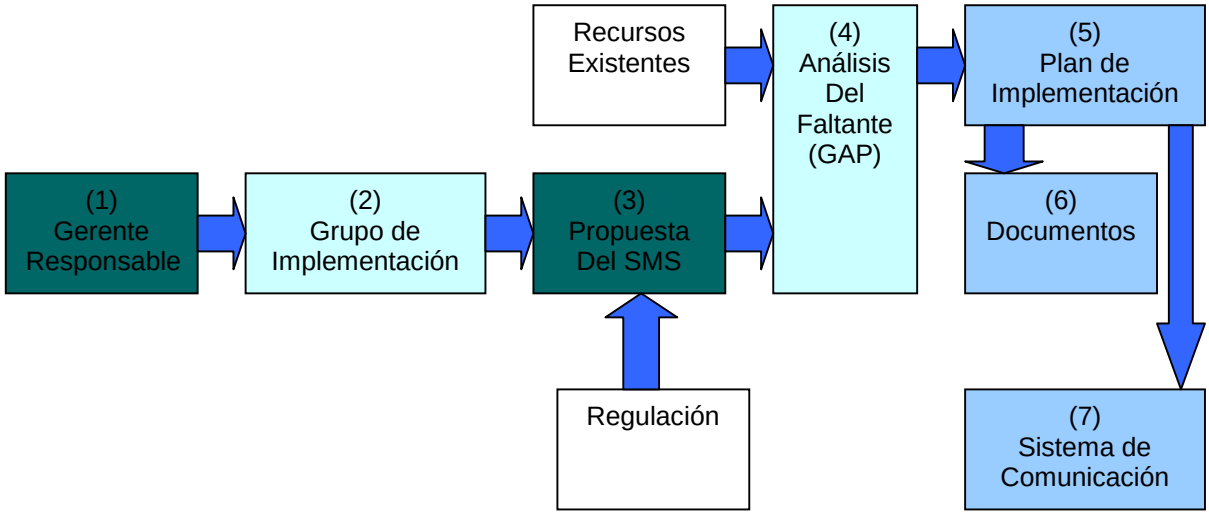



**Figura 3**

**3.** **Identificar el gerente responsable y las responsabilidades de los gerentes.** (Ver párrafo 145.510 (a)(1) del DINAC R 145)

i. **Identificar al Gerente Responsable (DINAC R 145.260)**

A. La organización tiene que identificar el Gerente responsable, que debe ser una única persona que tenga la responsabilidad final por el funcionamiento efectivo y eficiente del SMS de la organización. Dependiendo del tamaño y complejidad de la organización, el Gerente Responsable puede ser:

I. El Oficial Ejecutivo en Jefe;

II. El Presidente de la Junta de Directores;

III. Un socio o

IV. El propietario

B. Más importante que determinar quién es el Gerente Responsable desde la perspectiva de su función dentro de la Organización, deben ser la autoridad y responsabilidades que él debe tener para responder apropiadamente por la operación SMS, incluyendo:

I. Autoridad total por los asuntos de Recursos Humanos;

II. Autoridad sobre los principales asuntos financieros;

III. Responsabilidad Directa por la conducción de los asuntos de la organización;

IV. Autoridad final sobre las operaciones bajo certificado; y

V. Responsabilidad final sobre todos los asuntos de seguridad operacional.

C. El Gerente Responsable puede asignar la administración del SMS a otra persona, siempre que tal asignación esté apropiadamente documentada y descrita en el manual de la organización, sin embargo, esto no afecta la responsabilidad final del Gerente Responsable sobre el funcionamiento del SMS.

D. El Gerente Responsable debe tener la capacidad de garantizar la aplicación del sistema de seguridad definido por la OMA y que existan los recursos necesarios para la ejecución del mantenimiento (materiales, herramientas, personal suficiente), de tal modo no hayan motivos (de carácter estratégico o económico) que degraden la seguridad del trabajo efectuado en cumplimiento fiel a lo establecido por los DINAC Rs. Para garantizar que los recursos estén disponibles no siempre significa que se los deba adquirir, sino que éstos deben estar presentes en un tiempo razonable cuando sean requeridos y de forma tal que puedan ser utilizados.

E. Con respecto al Gerente Responsable es quien en virtud de su posición tiene la responsabilidad global (incluyendo en particular la financiera) de hacer funcionar la organización. El Gerente Responsable puede ocupar en más de una organización ese cargo siempre y cuando demuestre cumplimiento satisfactorio de sus deberes prescritos en el DINAC R 145.260 en cada una de las OMs a su cargo; y en el aspecto técnico, se requiere que al menos tenga conocimiento básico del DINAC R 145. El Gerente Responsable debe tener la capacidad y autoridad en cuanto a la asignación de recursos financieros para cumplir con la responsabilidad en el mantenimiento de las aeronaves y componentes de las aeronaves.

F. Por otra parte, dicha autoridad tiene una garantía de que la responsabilidad relativa a las medidas correctivas respecto a toda no conformidad que se haya observado incumbe al más elevado nivel de la estructura orgánica de la OM, asegurándole así de que se cuente con la autoridad ejecutiva necesaria (incluyendo los aspectos financieros cuando corresponda).

ii. **Identificar la responsabilidad de los Gerentes sobre la Seguridad Operacional (DINAC R 145.255)**

A. Es responsabilidad del gerente o los gerentes definir una estructura del SMS que se ajuste al tamaño y complejidad de la organización y a los riesgos y peligrosos asociados con el desarrollo de las actividades necesarias para brindar el servicio.

B. Es responsabilidad del gerente o los gerentes establecer las responsabilidades del personal clave (jefes de departamento y/o responsables de unidades funcionales) incluyendo en la descripción del trabajo de éstos las responsabilidades sobre el SMS.

C. Las responsabilidades sobre la seguridad operacional de todos los jefes de departamento y/o responsables de unidades funcionales y en particular gerentes de línea deben ser descritas en el manual de la organización. Las responsabilidades sobre la seguridad operacional deberían ser presentadas en un organigrama funcional que muestre la interacción y la relación en términos de administración de la seguridad operacional entre diferentes sectores de la organización.

D. La efectividad del SMS requiere una clara definición de las líneas de autoridad dentro de la organización. Debe ser claramente entendida la responsabilidad y la autoridad de todos los individuos involucrados en el sistema.

E. La persona, o las personas, nominadas para representar la estructura gerencial de la organización de mantenimiento son responsables del cumplimiento de todas las funciones especificadas en el DINAC R 145.

F. La persona o personas designadas estarán en condiciones de demostrar ante la DINAC que poseen conocimientos relevantes, formación y experiencia apropiadas en el mantenimiento de aeronaves o componentes y demostrarán un conocimiento práctico del DINAC R 145.

G. Dependiendo del tamaño de la OM, las funciones de las personas que son partes de la estructura gerencial pueden ser subdivididas en un gerente para cada área o en una combinación de diferentes formas, de manera que se permita acumulación de funciones.

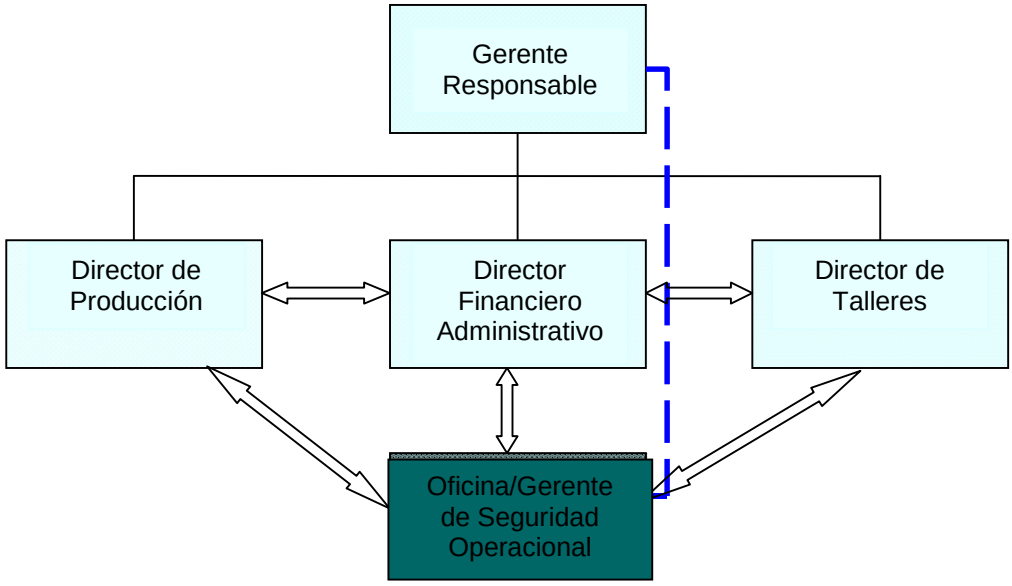



**Figura 3**

H. Cuando la complejidad de la organización lo permita, los Gerentes/Jefes de Departamento y/o los responsables de áreas funcionales, constituirán una Junta de Control de Seguridad Operacional y un Grupo Ejecutivo de Seguridad Operacional que asumirán parte de las funciones en el SMS conforme se establece en la regulación DINAC R 145.

I. En estos casos los gerentes, jefes o encargados de áreas funcionales conformarán la Junta de Control Operacional y participarán en el Grupo Ejecutivo de Seguridad con el personal operativo. El esquema funcional del SMS sería como se ilustra en la siguiente figura.

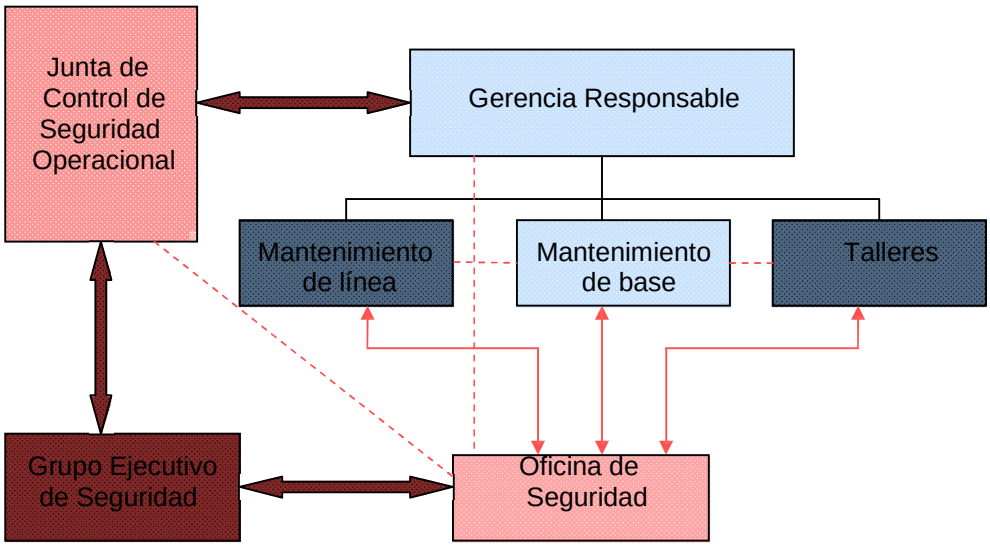



**Figura 4**

**4. <u>Identificar responsable de implementación SMS (Ver párrafo DINAC R 145.510 (a) (2) y DINAC R 145.260 (d)</u>**

i. El nombramiento de la persona a cargo de la operación diaria de la Oficina de Seguridad Operacional es clave para el funcionamiento del SMS. Esta persona puede ser identificada por diferentes nombres en diferentes organizaciones pero en términos generales se conoce como Gerente de Seguridad Operacional.

ii. El Gerente de Seguridad Operacional será la persona designada por el Gerente Responsable para administrar las funciones diarias del SMS. El Gerente de Seguridad operacional es el punto de enlace y el responsable de desarrollar y mantener la efectividad del SMS.

iii. El Gerente de Seguridad Operacional también debe orientar al Gerente responsable y a los demás gerentes/jefes y/o responsables de áreas funcionales respecto de la administración de la seguridad operacional y es responsable por la coordinación y comunicación de los asuntos de seguridad operacional dentro de la organización, con entidades externas, contratistas y otros interesados según corresponda.

iv. Dentro de sus funciones se incluye:

- Administración del plan de implementación del SMS en representación del Gerente Responsable,
- Realizar/propiciar la identificación de peligros y el análisis de riesgo,
- Supervisar las acciones correctivas y evaluar sus resultados,
- Proporcionar reportes periódicos sobre el desempeño de la seguridad operacional de la organización.
- Mantener los registros y la documentación de Seguridad Operacional,
- Planificar y organizar el entrenamiento del personal de Seguridad operacional.

- Proporcionar orientación en asuntos de Seguridad Operacional,
- Vigilar los asuntos relevantes de Seguridad Operacional en la Industria de la Aviación y el impacto percibido en las operaciones y la organización.
- Asegurar la promoción de la seguridad operacional dentro de la organización.
- Coordinar y comunicar sobre asuntos relativos a seguridad operacional con la autoridad a cargo de la vigilancia y otras agencias estatales como sea necesario y
- Coordinar y comunicar sobre asuntos relativos a la Seguridad Operacional con agencias internacionales.

v. Dependiendo del tamaño de la organización y la naturaleza y complejidad de las operaciones, el Gerente de Seguridad Operacional puede ser una sola persona a cargo de la oficina o puede contar con personal adicional.

vi. La selección del Gerente de Seguridad es de especial significado y debería, entre otros, considerar los siguientes aspectos:

- Experiencia en la administración operacional,
- Antecedentes técnicos que le permitan entender los sistemas que soportan las operaciones;
- Habilidad para relacionarse con la gente,
- Habilidad para analizar y resolver problemas,
- Habilidad para administrar proyectos y
- Habilidad para la comunicación oral y escrita.

## 5. Descripción del SMS

i. El explotador en esta fase inicial debe definir como intenta implementar su Sistema de Gestión de Seguridad Operacional, el cual deberá incluir los cuatro componentes conforme se ha establecido en el marco reglamentario:

- Objetivos y política de Seguridad Operacional.
- Gestión de los riesgos.
- Aseguramiento de la Seguridad Operacional.
- Promoción de la Seguridad Operacional.

ii. Objetivos y Política de Seguridad Operacional

A. Al definir las políticas y objetivos del sistema los operadores deben considerar los requerimientos establecidos en la regulación DINAC R 145 y cualquier estándar de seguridad que afecte su operación; adicionalmente el sistema debe establecer la interacción con otros sistemas, ya sea de clientes o proveedores.

B. La organización de mantenimiento debe definir su política de Seguridad Operacional la cual debería cumplir con los requerimientos nacionales e internacionales, según corresponda y esta política debe ser firmada por el Gerente Responsable de la organización. La política debe reflejar los compromisos de la organización respecto a la Seguridad, incluyendo una declaración sobre la provisión de los recursos humanos y financieros necesarios para la implementación del SMS. La política debe ser revisada periódicamente para garantizar que mantiene relevancia y es apropiada para la organización.

C. Los objetivos de SMS son punto de arranque de la política SMS de la

organización de mantenimiento. Estos objetivos deben ser claros y medibles para que se pueda determinar del desempeño del sistema.

D. Teniendo en cuenta que el objetivo del SMS es mantener un nivel de seguridad aceptable mediante el análisis continuo y la implementación de medidas correctivas o de mitigación de riesgo. También es importante recordar que debe existir un balance entre los procesos productivos de la organización y la protección que ofrece el SMS a los mismos, puesto que la producción de servicios es la razón primordial de la existencia de las organizaciones de mantenimiento.

| Objetivos de la Organización | Indicadores de Desempeño |
|---|---|
| Objetivo financiero: *Reducir Costos* | *Reducción de las primas de Seguro* |
| Objetivo de Seguridad:<br><br>*Disminuir el número de incidentes serios en el hangar a un máximo de 20 por año* | *Número de incidentes al año. Severidad de los incidentes del año. N° de Acciones correctivas desarrolladas e implementadas.* |

E. Conforme lo requerido por la regulación se debe establecer la responsabilidad del Gerente Responsable y los demás gerentes, jefes de departamento o encargados de áreas funcionales dentro del SMS. Se deben establecer los procedimientos usados para la integración y operación de la Junta de Control de Seguridad Operacional y el Grupo Ejecutivo de Seguridad.

F. Dentro de la descripción del sistema se debe incluir el Gerente de Seguridad nominado por el Gerente Responsable así como las funciones y responsabilidades sobre el sistema y el plan de implementación del SMS.

G. El requisito de que se documente el plan de trabajo no es propiamente una parte del sistema sino más bien parte de la documentación requerida del SMS. El plan puede estar compuesto por uno o varios documentos.

H. El plan de implementación del SMS debe describir como se iniciarán las actividades del SMS y como se cumplirán las funciones del sistema. El plan de implementación SMS es una definición de cómo la organización intentará adoptar la gestión de la Seguridad. Entonces este será la estrategia para la implementación del SMS que cumple las necesidades de Seguridad de la organización mientras brinda servicios de manera efectiva y eficiente. El plan de implementación detalla las acciones que serán tomadas, los responsables y la duración.

I. Dependiendo del tamaño y la complejidad de las operaciones, el plan de implementación del SMS puede ser desarrollado por una persona o por un grupo de planificación.

J. Un plan de implementación del SMS incluye:

- Objetivos y metas del plan
- Política de Seguridad
- Tareas y responsabilidades en Seguridad
- Política de reportes de Seguridad
- Descripción del sistema
- Análisis del faltante
- Proceso de identificación de peligros

- Procesos de gestión de riesgos
- Medición del desempeño de Seguridad
- Entrenamiento de Seguridad
- Comunicación de Seguridad
- Medios para involucrar a los empleados
- Coordinación con terceras partes
- Gestión de la revisión de desempeño de la seguridad

K. El plan de respuesta ante emergencias debe describir las acciones que serán tomadas después de un accidente y quien es responsable por cada acción. El propósito del plan es garantizar que existan:

- Una transición ordenada y eficiente de operaciones normales a operaciones en emergencia,
- Delegación de autoridad en emergencia
- Asignación de responsabilidades en emergencia.
- Autorización del personal gerencial para la toma de acciones en emergencia
- Coordinación de esfuerzos para enfrentar la emergencia
- Coordinación con planes de respuesta ante emergencia de aquellas organizaciones con las que exista relación durante la prestación de servicios.

El plan de respuesta a la emergencia no solamente responderá a los accidentes e incidentes de las aeronaves sino también a acontecimientos que afecten el funcionamiento de la organización de mantenimiento, tal como eventos graves, catástrofes naturales y epidemias. El plan debe incluir acciones que se deben tomar para comunicar la condición existente a las diferentes entidades involucradas y las personas interesadas. Por otra parte el plan debe estar diseñado para responder de forma adecuada cuando sea requerido por otro SMS. La siguiente ilustración es un ejemplo del proceso del PRE.

**PLAN DE RESPUESTA A LA EMERGENCIA**

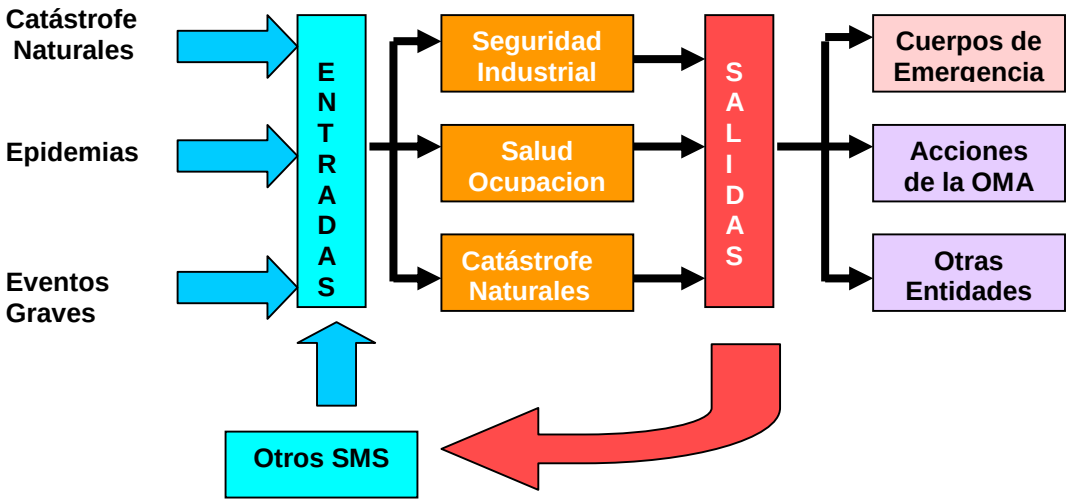



**Figura 5**

L. Una característica muy importante del SMS es que debe ser explícito, como tal todas las actividades deben estar documentadas y a la vista es por eso que la documentación es un elemento esencial del SMS.

M. La documentación debe hacer referencia a todas las regulaciones nacionales e internacionales que le apliquen, incluyendo documentación y registros tales como:

- Formularios de reporte de peligros.
- Líneas de responsabilidad y autoridad en el SMS
- La estructura de la Gestión de la Seguridad de la organización

N. Pero sin duda, la pieza más importante de un SMS es el manual del sistema de gestión de la seguridad. Este Manual es el instrumento clave para comunicarle a toda la organización como la empresa iniciará la gestión de la Seguridad. El manual documenta todos los aspectos del SMS, incluyendo políticas y objetivos de seguridad, procedimientos y responsabilidades individuales sobre la seguridad.

O. En el manual de la organización, en cuanto al sistema SMS, contendría lo siguiente:

- Alcance del SMS.
- Política y objetivos de seguridad.
- Responsabilidades de seguridad.
- Personal clave de seguridad.
- Documentación del SMS y procedimientos de control de la misma.
- Esquemas de identificación de peligros y gestión del riesgo.
- Supervisión del desempeño del SMS.
- Planificación de respuesta ante emergencia.
- Manejo del cambio.
- Auditoria de seguridad.
- Promoción de la seguridad.
- Control de actividades sub-contratadas.

P. En las organizaciones de mantenimiento aprobadas en el MOM se integrarían los puntos enunciados en el párrafo XV, cumpliendo con lo establecido en 145.275. Una OMA, dependiendo de la complejidad de su operación, puede optar por tener diferentes manuales para las actividades de gestión, operación o temas específicos de la misma.

iii. Gestión de Riesgos

A. *Proceso de Identificación de Peligros*. La Organización de Mantenimiento Aprobada DINAC R 145 debe desarrollar y mantener un proceso formal y efectivo para recolectar, registrar, actuar y retroalimentar sobre los peligros en las operaciones basados en una combinación de métodos de recolección de información de seguridad reactivos, proactivos y predictivos.

B. Algunas de las fuentes que se usarán en este proceso de identificación de los peligros:

- Información estadística de sistemas similares que documenten los peligros durante la ejecución de mantenimiento.
- Recomendaciones de investigación de accidentes.

- Sistema de reportes de Seguridad.
- La experiencia operacional.

C. Es por esto que dentro de las políticas que establezca la organización debe propiciar un sistema voluntario de reportes no punitivo, esto permitirá la anuencia de los empleados para reportar peligros y cooperar en la investigación de reportes de seguridad. Es esencial que se desarrolle en la organización un ambiente de trabajo con un sistema efectivo de reportes de seguridad por parte del personal operativo.

D. En este mismo sentido, todos los reportes deberán ser investigados y una retroalimentación debe brindarse al personal.

E. *Proceso de evaluación de riesgos y acciones de mitigación*. La Organización de Mantenimiento Aprobada DINAC R 145 debe desarrollar y mantener un proceso formal de gestión de riesgos que garantice el análisis (en términos de probabilidad y severidad de los sucesos) evaluación (en términos de tolerancia) y control (en términos de mitigación) de los riesgos a un nivel aceptable. La organización también debe definir conjuntamente con la autoridad cuales son los niveles aceptables en que se manejarán los riesgos.

iv. Aseguramiento de la seguridad operacional

A. La Organización de Mantenimiento Aprobada DINAC R 145 debe desarrollar y mantener un medio para verificar el desempeño de su SMS y validar la efectividad del control de riesgos. El desempeño del SMS de la organización debe ser verificado en referencia a los indicadores de desempeño y las metas de desempeño del sistema.

B. Como se señaló anteriormente los indicadores tendrán una correspondencia directa con los objetivos del sistema. El desempeño del sistema debe ser vigilado de forma reactiva y proactiva para comprobar que las metas propuestas se continúan alcanzando. La vigilancia por medio de auditorías es un elemento clave del sistema y deben incluir evaluaciones cualitativas y cuantitativas. Los resultados de la supervisión deben ser documentados y usados como retroalimentación para mejorar el sistema.

C. Usar el índice de accidentes e incidentes no es una medida efectiva de la seguridad y es puramente reactivo. Esto podría crear una falsa impresión, bajo la presunción de que cero accidentes indican que una organización es segura, mientras pueden existir condiciones latentes dentro del sistema que, si no son controladas, pueden llevar a un accidente.

D. Una manera más efectiva de medir la seguridad podría ser una evaluación de las mejoras implementadas en los procesos de trabajo y como estas han mitigado o eliminado los peligros.

E. La Organización de Mantenimiento Aprobada DINAC R 145 debe desarrollar y mantener un proceso formal para identificar los cambios dentro de la organización que puedan afectar los procesos y servicios establecidos, que permitan:

- Describir las disposiciones para garantizar el desempeño de seguridad antes de la implementación del cambio.
- Eliminar o modificar los controles de riesgo que ya no son requeridos o efectivos en virtud de los cambios en el ambiente operacional.

F. La organización debe desarrollar y mantener un proceso formal para identificar las causas de un desempeño por debajo de los estándares del

SMS, determinar las implicaciones en su operación y eliminar o mitigar tales causas.

G. Cuando se da inicio a la implementación de este tipo de sistemas, en donde se requiere un cambio en la cultura de la organización, es recomendable fijarse metas e indicadores que refleje la implantación de este cambio cultural. En este sentido, se podría establecer como un indicador el número de reportes de seguridad. Por ejemplo, una organización cuyo indicador durante el segundo año sea el número de reportes, puede establecerse como meta que en el año se obtengan 20 reportes de seguridad.

v. Promoción de la Seguridad Operacional

A. *Entrenamiento y Educación*. La Organización de Mantenimiento Aprobada DINAC R 145 debe desarrollar y mantener un programa de entrenamiento de seguridad que garantice que el personal está entrenado y competente para realizar las labores del SMS, la amplitud del entrenamiento debe ser apropiada según la participación particular en el SMS.

B. La Organización de Mantenimiento aprobada DINAC R 145 debe desarrollar y mantener un medio formal para las comunicaciones de seguridad, que garantice que todo el personal tiene un conocimiento total del SMS, se transmite información crítica de seguridad y se explica porque se toman acciones particulares de seguridad y porque se introducen o modifican procedimientos de seguridad.

**6. Conducción de análisis del faltante**

i. La mayoría de las Organizaciones de Mantenimiento tienen implementado y en funcionamiento varias actividades relativas al SMS, por eso es importante conocer la estructura existente en la organización y como puede ésta servir de base para el desarrollo del SMS.

ii. El análisis de faltante revelará los recursos, estructuras y disposiciones de Seguridad existentes en el sistema para atender las vulnerabilidades de seguridad que se produzcan por la interacción del personal. También revelará a la organización los recursos, estructuras y disposiciones de Seguridad adicionales que serán necesarios para implementar el SMS según su propuesta.

iii. Una vez concluido y documentado un análisis del faltante, este servirá de base para establecer el plan de implementación del SMS.

iv. El análisis de faltante es simplemente una comparación entre los requisitos del SMS y el sistema de la Organización de Mantenimiento en particular, es entonces factible hacer este análisis mediante una lista de chequeo donde se incluyan los requisitos del SMS y donde el registro de un “no” en la lista revela el faltante.

v. En el apéndice 1 se muestra un pequeño ejemplo de cómo puede documentar el análisis de faltante por medio de lista de chequeo.

**7. Desarrollo del plan de implementación**

i. Como se mencionó con anterioridad el análisis de faltante revelará los recursos, estructuras y disposiciones de seguridad adicionales que son necesarias para la implementación del SMS de la organización. De ese análisis se derivaran entonces una serie de actividades necesarias para la implementación del sistema y según lo que se estableció en el párrafo 5.ii. H, el plan consiste en asignar responsables para cada actividad y tiempos para desarrollo, ahora también debe considerarse el hecho de que la implementación del sistema ha sido dividida en cuatro fases a fin de facilitar la asignación de recursos, de manera que se asignen prioridades dentro del plan de

implementación (Ver tabla 1).

| Actividad | Responsable | Prioridad (Fase) | Tiempo Estimado | Fecha Entrega |
|---|---|---|---|---|
| Nominar al Gerente del SMS | Gerente responsable | 1 | | |
| Establecer la Política de Seguridad | Gerente responsable | 1 | | |
| Establecer la estructura del SMS | Organización | 1 | | |
| Desarrollar el Manual SMS | Gerente SMS | 1 | | |
| Desarrollar los documentos de reporte | Gerente SMS | 1 | | |
| Establecer el sistema de comunicación SMS | Gerente SMS | 1 | | |
| Implementación de la identificación de peligros (método reactivo) | Gerente SMS | 2 | | |
| Implementación de gestión de riesgos (método reactivo) | Gerente SMS | 2 | | |
| Instrucción sobre los procesos reactivos | Gerente SMS | 2 | | |
| Desarrollar la documentación referente a los procesos reactivos | Gerente SMS | 2 | | |
| Implementación de la identificación de peligros (método proactivo) | Gerente SMS | 3 | | |
| Implementación de gestión de riesgos (método proactivo) | Gerente SMS | 3 | | |
| Instrucción sobre los procesos proactivos | Gerente SMS | 3 | | |
| Desarrollar la documentación referente a los procesos reactivos | Gerente SMS | 3 | | |
| Implementar el sistema de garantía de la Seguridad | Gerente SMS | 4 | | |

**Tabla 1**

## 8. Desarrollo de documentación de objetivos y políticas de seguridad

Conforme se mencionó anteriormente, en la primera fase se desarrollarían los documentos que definan el SMS, incluyendo el desarrollo o adecuación del MOM para la inclusión de los aspectos de SMS es uno de los primeros pasos a seguir en este proceso. Es muy importante la participación de toda la empresa en estos procesos por lo que deberá establecerse un medio para recoger las opiniones y recomendaciones del personal.

## 9. Implementación de un medio de comunicación de seguridad

Durante la fase inicial la organización debería implementar un sistema formal de comunicación de la seguridad que cumpla los requerimientos del sistema.

**b) Fase 2 Implementación de proceso reactivo.** (Ver párrafo 145.510(b) del DINAC R 145)

En la segunda fase se deben desarrollar los procesos de gestión de riesgo reactivos, según definió la organización en la descripción del sistema en a.5.iii. La identificación de un peligro y la gestión de riesgo mediante un proceso reactivo pueden realizarse a través de los informes de inspecciones y de auditorías, por el análisis de los informes de investigación de accidentes o incidentes, y por los informes de los empleados.

**1. Identificación del peligro y gestión de riesgo.** El control de la seguridad es un proceso fundamental que permite obtener la información necesaria para el manejo de los riesgos en la organización. Los Gerentes de la OMA deben tener la capacidad de poder acceder y utilizar esta información para realizar una revisión crítica de los procesos que se están desarrollando, los cambios y agregados o los reemplazos propuestos para estos procesos. En esta fase la OMA tiene que establecer un sistema de recolección de informes reactivos sobre peligros potenciales provenientes de fuentes internas y externas a la OMA.

i. Un proceso reactivo responde a hechos que ya ocurrieron o informes de un peligro potencial a través del programa de reportes de la OMA, mientras que los procesos proactivos incluyen procedimientos para identificarlos, técnicas de supervisión activo y creación de perfiles de riesgos que afectan la seguridad.

ii. Una vez que se reporta un hecho, o identifica un peligro, los procedimientos son similares. El método para investigar y tratar el hecho puede variar, sin embargo, el mecanismo para archivar, determinar acciones correctivas y monitorear puede ser el mismo.

**2. Reporte de hechos y peligros**

i. La constatación de un hecho constituye una oportunidad de mejora continua en materia de seguridad que debe ser analizada de manera que todos los empleados, inclusive la gerencia, entiendan no solo qué sucedió, sino también por qué. Esto implica ver más allá del hecho e investigar los factores que contribuyeron a que se produzca.

ii. Para lograr este objetivo, la OMA debe desarrollar los procedimientos para recolectar reportes internos y registrar los hechos, peligros y otros temas relacionados en materia de seguridad. La reunión de datos oportunos, adecuados y precisos permite que la OMA reaccione ante la información recibida y aplique las acciones correctivas necesarias para impedir que el hecho se repita.

iii. La clave para alcanzar este objetivo es contar con un sistema de información que cubra las necesidades de quienes van a utilizarlo. Como tal, la información ingresada por los empleados es vital para el desarrollo del sistema. Un sistema de información sobre seguridad carece de valor si nadie lo usa: por lo tanto, no debe minimizarse la importancia del empleado en todo el proceso. Una política conjunta de información sobre seguridad y el compromiso real y demostrado de la gerencia para alcanzar los objetivos en materia de seguridad, ayudarán a impulsar el desarrollo de la cultura del reporte dentro de la organización.

iv. El sistema de reportes de una OMA debe estar formado por los siguientes elementos fundamentales:

A. Sistemas para reportar peligros, hechos o problemas relacionados con la seguridad.

B. Sistemas para analizar datos, informes y cualquier otra información relacionada con la seguridad.

C. Métodos para reunir, archivar y distribuir datos.

D. Acción correctiva y estrategias de mitigación de riesgos.

E. Sistema de supervisión.

F. Medición de la efectividad de la acción correctiva.

**3. Sistema de reporte de hechos y peligros**

i. Los empleados deben contar con un medio para reportar al gerente correspondiente, identificado en el manual, todos los hechos y peligros emergentes. El gerente envía después el reporte al banco de datos para su procesamiento.

ii. El sistema de reportes debe ser simple, confidencial, fácil de utilizar y complementarse mediante una política de reportes sobre seguridad. Estos atributos, junto con mecanismos eficaces de seguimiento para acusar recibo del reporte ante la persona que lo preparó e informar que se investigó y se actuó en consecuencia, alientan el desarrollo de la cultura del reporte. Los resultados deben distribuirse entre los individuos involucrados y la población en general, cuando corresponda.

iii. Existen numerosos programas de reportes que funcionan para todos los tipos de organizaciones. Es importante establecer un sistema que se adapte al tamaño y nivel tecnológico de la organización. En las organizaciones más pequeñas, la información puede obtenerse mediante un simple formulario escrito depositado en un buzón ubicado en un lugar seguro, y de fácil acceso, en la OMA. Las organizaciones más grandes pueden emplear un sistema de información más sofisticado online. En ciertas circunstancias es más expeditivo presentar un informe verbal; sin embargo, sin excepción, este informe debe ser complementado mediante un informe escrito.

iv. Como mínimo, los formularios para emitir reportes deben tener suficiente espacio como para hacer una descripción completa del hecho y para que la persona que prepara el reporte haga sugerencias acerca de posibles soluciones al problema que reporta. En los reportes hay que emplear una taxonomía común y clara para clasificar los hechos. Dicho de manera simple, se trata de la división de los tipos de hechos en grupos o categorías ordenadas. Es importante que quienes presentan reportes y los investigadores compartan un lenguaje familiar para explicar y comprender los tipos de errores que contribuyen a que se produzcan los hechos. De esta forma se facilitará el ingreso de datos más precisos y el análisis de la tendencia que presentan todos los hechos. No importa qué sistema de información se utiliza, su efectividad dependerá de cuatro hechos:

A. Los empleados entienden perfectamente que hechos deben reportar.

B. Todos los reportes son confidenciales.

C. Los individuos reciben retroalimentación de sus reportes de manera oportuna.

D. La organización tiene vigente una política disciplinaria que promueva el libre flujo de información sobre peligros.

v. El sistema de reportes de seguridad de una OMA debe estar formado por los siguientes elementos fundamentales:

A. Sistemas para reportar peligros, hechos o problemas relacionados con la seguridad.

B. Sistemas para analizar datos, reportes y cualquier otra información relacionada con la seguridad.

C. Métodos para reunir, archivar y distribuir datos.

D. Acción correctiva y estrategias de mitigación de riesgos.

E. Supervisión en curso.

F. Conformación de la efectividad de la acción correctiva.

vi. Para un programa de reportes activos, es fundamental saber que hay que

reportar. Por regla general, deben reportarse todos los hechos o peligros con potencial de provocar daños o perjuicios. Algunos ejemplos de estos asuntos son:

A. Turnos de trabajo excesivos.

B. Poco personal de mantenimiento para realizar las inspecciones.

C. Herramientas o equipamiento de inspección inadecuados.

D. Falta de herramientas y equipos de mantenimiento.

E. Falta de repuestos.

F. Señalización inadecuada en el hangar.

G. Salidas de emergencia bloqueadas.

H. Procedimientos incorrectos o inadecuados y no adhesión a procedimientos estándar.

I. Comunicación deficiente entre las áreas de trabajo.

J. Falta de manuales técnicos actualizados.

K. Cambios de turnos inadecuados.

L. Falta de una adecuada capacitación inicial y continua.

El objetivo de esta lista no es que abarque todos los problemas. De hecho, tratar de definir todos los peligros puede ir en detrimento de la organización. En lugar de ello, la lista debe ser vista como una guía para instruir a los empleados acerca de los tipos de situaciones que constituyen peligros que afecten la seguridad de las tareas de mantenimiento y la operación de las aeronaves.

vii. Investigación y análisis de los reportes

A. Se deben investigar todos los hechos. El alcance de las investigaciones dependerá de las consecuencias efectivas y potenciales de los hechos o peligros las cuales pueden determinarse valorando los riesgos. Los reportes que revelan un potencial elevado deben investigarse con mayor profundidad que aquellos que muestran un bajo potencial.

B. El proceso de investigación debe ser general y ocuparse de los factores que contribuyen a que se produzca el hecho, en lugar de centrarse simplemente en el hecho en sí (falla activa). Las fallas activas son acciones que se produjeron inmediatamente antes del hecho y afectan directamente la seguridad del sistema, debido a la inmediatez de sus efectos adversos. Sin embargo, no son la causa original del hecho; como tales, si se aplican acciones para corregirlos puede ser que no se trate la causa real del problema. Se requiere un análisis más detallado para establecer que factores dentro de la organización contribuyeron a que se produzca el error.

C. El investigador, o equipo de investigadores deben ser competentes desde el punto de vista técnico y contar con información sobre los antecedentes, o tener acceso a ella, para interpretar los hechos con precisión. El personal debe confiar en el investigador y el proceso de investigación debe ser una búsqueda para comprender como se produjo el error, no una cacería para culpar a alguien.

viii. Investigación de los hechos

Se pueden emplear numerosas herramientas para investigar hechos. La valoración inicial de los riesgos ayuda a determinar qué tipo de investigación hay que conducir, o bien la organización puede emplear un formato predeterminado de investigación independientemente del hecho. Depende de una organización en particular determinar cuál es el método más apropiado.

Independientemente del proceso utilizado, se requiere una metodología rigurosa, que pueda repetirse, para investigar hechos eficazmente.

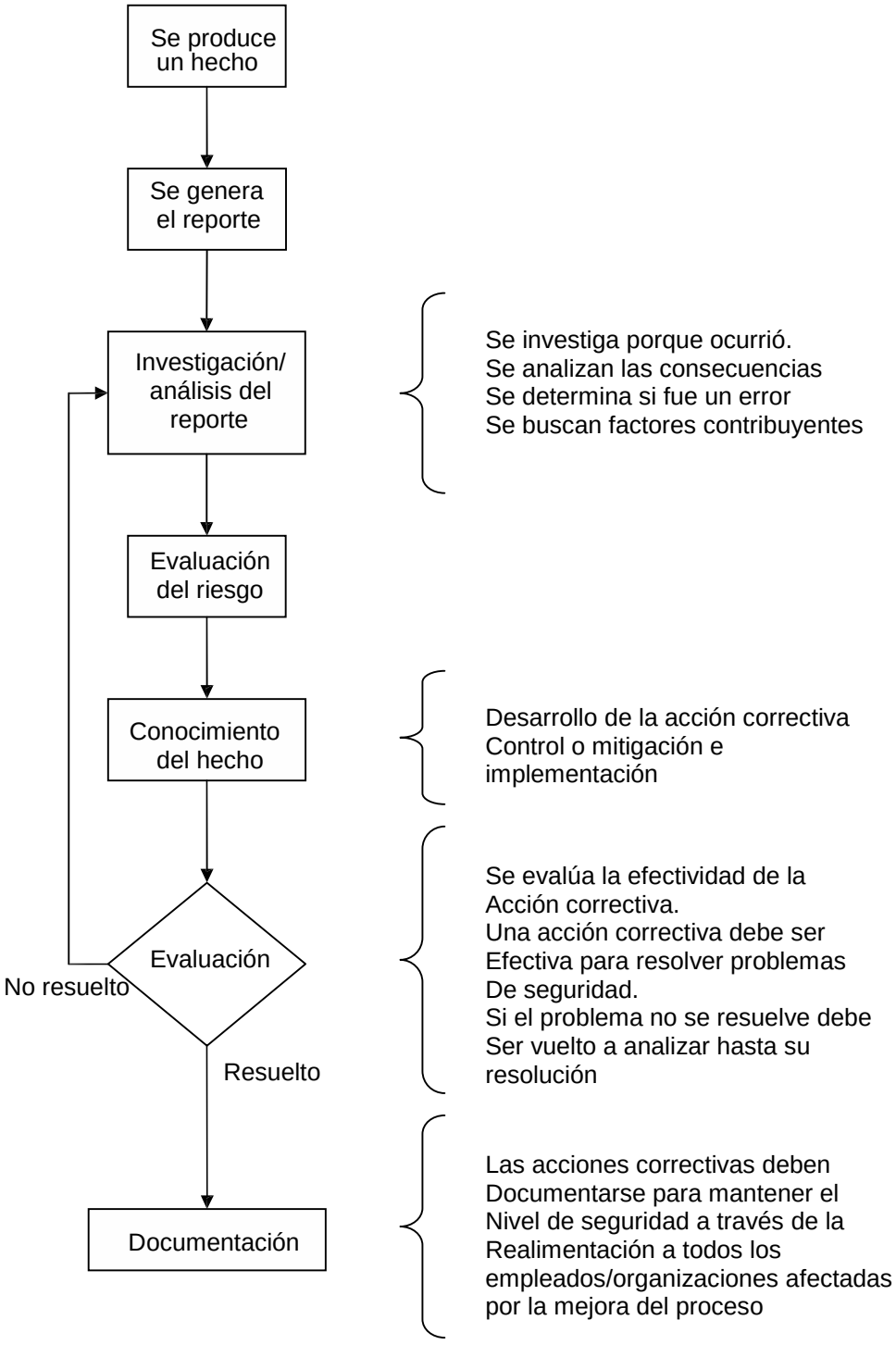



**Figura 6**

## 4. Elementos comunes para los procesos reactivos y proactivos

El reporte sobre hechos y problemas, y su valoración de la seguridad son dos funciones individuales dentro del SMS. Sin embargo, una vez que se presentó un informe, el proceso se desarrolla de la misma forma. Los siguientes son los aspectos comunes de estos elementos que deben tenerse en cuenta al desarrollar un SMS.

i. Procedimientos para reportar hechos

A. El procedimiento para reportar hechos o peligros deben ser tan simple como sea posible. Los procedimientos para presentar los reportes deben ser claros, estar bien documentados e incluir detalles acerca de dónde y a quien deben presentarse esos reportes. De esta manera, se reduce la confusión sobre el destino de los reportes de seguridad y se asegura que todos los hechos se reporten a la persona adecuada.

B. Al diseñar un formulario para reportes de seguridad, es importante tener en cuenta como presentar la información sobre hechos y peligros. El formulario debe estar estructurado de manera tal que permita registrar un tipo de información tanto reactiva como proactiva. Debe tener suficiente espacio como para que quienes presentan el reporte sugieran acciones correctivas relacionadas con el asunto que están informando.

C. Existen numerosas formas posibles de presentar un reporte. El tamaño y la complejidad de la organización determinan si el sistema tiene que ser sofisticado o no. En algunos casos, se necesita un buzón cerrado en el hangar. En otros, es más efectivo presentar los informes directamente en la oficina de seguridad. La OMA debe determinar el método más adecuado a su tipo de organización.

ii. Recopilación de datos

Cuando se prepara un reporte sobre un hecho o un problema, hay que hacer lo posible para asegurar que el formulario pueda entenderse fácilmente y sea de uso sencillo. La organización debe esforzarse para que todos los formularios para reportar sean compatibles con las áreas operativas. De esta forma, se facilita que se compartan los datos, que las tendencias se analicen y también que el proceso de investigación de los hechos y los problemas sea más simple.

Dependiendo del tamaño de la organización los informes pueden ser manuscritos o tomados de datos derivados de informes verbales. Sin embargo, siempre hay que hacer un seguimiento de los informes verbales mediante un informe escrito. También pueden prepararse utilizando un sistema específico de reporte de hechos y peligros a través de un software especifico para elaborar informes predefinidos.

Para la recopilación y archivo electrónico de datos puede utilizarse una simple base de datos preparada en Microsoft ACCESS o un sistema de archivo manual. La opción por un sistema de recopilación de datos se basa en el tamaño y la complejidad de la OMA.

iii. Manejo de riesgos

A. El manejo de riesgos es una actividad proactiva que permite analizar los riesgos asociados con los peligros identificados y ayuda a seleccionar acciones para mantener un nivel adecuado de seguridad al enfrentar esos peligros.

B. Una vez que se identifican los peligros, comienza **el proceso de manejo de riesgos** con la emisión de reportes de hechos/peligros, o la valoración de la seguridad. Se trata de una evaluación de los daños o pérdidas potenciales ocasionados por los peligros y el manejo de ese potencial. Este concepto comprende tanto la probabilidad como la magnitud de la pérdida. Los elementos básicos del proceso de manejo de riesgos son:

I. Análisis de Riesgos

II. Valoración de Riesgos

III. Control de Riesgos

IV. Supervisión

I. Análisis de riesgos. Es el primer elemento del proceso de manejo de riesgos. Comprende la identificación y la estimación de los riesgos. Una vez que se han identificado los peligros, deben identificarse los riesgos asociados con esos peligros y estimarse su magnitud.

II. Valoración de riesgos. Se toma el trabajo completado durante el análisis de los riesgos y se va un paso más adelante realizando una valoración de los riesgos. En ese momento se evalúan la probabilidad y la severidad del peligro para determinar el nivel de riesgo.

| **Probabilidad del riesgo** | **Severidad del riesgo** | | | | |
|---|---|---|---|---|---|
| | **Catastrófico** | **Peligroso** | **Mayor** | **Menor** | **Insignificante** |
| Frecuente | 1 | 2 | 3 | 7 | 8 |
| Ocasional | 4 | 5 | 9 | 14 | 15 |
| Remoto | 6 | 10 | 11 | 16 | 20 |
| Improbable | 12 | 13 | 17 | 21 | 22 |
| Extremadamente Importante | 18 | 19 | 23 | 24 | 25 |

**Ejemplo de matriz de análisis de riesgo**

| **Índice de evaluación Del riesgo** | **Criterio sugerido** |
|---|---|
| 1 a 6 | Inaceptable bajo las circunstancias existentes. |
| 7 a 13 | El control/mitigación del riesgo requiere una decisión de la dirección |
| 14 a 19 | Aceptable después de revisar la operación |
| 20 a 25 | Aceptable |

**Ejemplo de matriz de valoración de riesgos**

Para emplear eficazmente la matriz de valoración de riesgos, es importante que todos interpreten de la misma forma la terminología empleada para evaluar la probabilidad y severidad. Por esta razón, hay que incluir una definición para cada nivel de estos componentes. Corresponde a las OMA´s definir cuando se necesita una intervención. En otras palabras, la organización debe decidir cuál es su nivel de riesgo tolerable.

Una herramienta común para tomar decisiones en relación con un riesgo y su aceptación, es la matriz de riesgo. Esta matriz la debe diseñar la OMA en términos realistas, en relación con el medio en que lleva a cabo sus operaciones. Con esto se asegura que las herramientas de cada organización para la toma de decisiones tengan peso en sus operaciones y su entorno operacional. Un tipo de definición de severidad y probabilidad puede ser la cualitativa, pero en donde sea posible, son preferibles las medidas cuantitativas. La aceptabilidad de los riesgos puede evaluarse empleando una matriz de riesgo, tal como la que ilustra a continuación. La matriz del ejemplo muestra tres áreas de aceptabilidad. Las matrices de riesgo pueden tener códigos de color: inaceptable (rojo), aceptable (verde) y aceptable con mitigación (amarillo).


**Ejemplo de matriz de gestión de la seguridad**

**Figura 7**

III. Control de Riesgos. Se ocupa de todos los riesgos identificados durante el proceso de evaluación que requieren que se emprendan acciones para reducirlos a niveles aceptables. En ese momento se desarrolla un plan de acción correctiva.

IV. Supervisión. Es esencial para asegurar que el plan de acciones correctivas implementado sea efectivo para manejar los asuntos o peligros declarados.

iv. Plan de acciones correctivas

A. Una vez que se investigan y analizan los reportes de hechos relacionados con la seguridad, o se identifican peligros, hay que presentar un reporte de seguridad al gerente correspondiente en el que se describa brevemente el hecho y, si están disponibles, los resultados de la evaluación de los peligros, para determinar qué acciones correctivas o preventivas emprender. El gerente designado debe desarrollar un plan de acciones correctivas en respuesta a las novedades, que describa brevemente como la organización propone corregir las deficiencias documentadas en las novedades. Conforme con las novedades, el plan de acciones correctivas puede incluir acciones a corto plazo y a largo plazo.

I. Acción correctiva a corto plazo: Esta acción permite corregir un asunto particular especificado en la novedad de auditoría y es anterior a la acción a largo plazo que impide que el problema se repita. La acción correctiva a corto plazo debe completarse en la fecha/tiempo especificados en el plan de acciones correctivas.

II. Acción correctiva a largo plazo: La acción correctiva a largo plazo consta de dos componentes. El primer componente consiste en determinar qué factores contribuyen a que se produzca el problema e indicar las medidas que debe tomar el Gerente Responsable para impedir que se repita. Estas medidas deben concentrarse en un cambio de sistema. El segundo componente a un cronograma para la implementación de las acciones correctivas a largo plazo. Estas acciones deben incluir la fecha propuesta de finalización.

B. Las acciones correctivas a corto plazo pueden llegar a insumir períodos que exceden los del cronograma aceptable establecido por la organización; por ejemplo cuando sea necesario realizar compras grandes de equipamiento. Cuando corresponda, la organización debe incluir los puntos destacados o los puntos de revisión de la evolución, que no superen el cronograma establecido que permite la finalización en la fecha propuesta. Cuando las acciones correctivas a corto plazo encaradas reúnan requerimientos de acciones correctivas a largo plazo, se debe dejar constancia en la sección correspondiente a las acciones correctivas a largo plazo del formulario para acciones correctivas.

v. Supervisión en curso

Para asegurar la efectividad de las medidas reparadoras, las acciones correctivas deben monitorearse y evaluarse regularmente. Las actividades de seguimiento deben llevarse a cabo a través del proceso de auditoría interna, el cual tiene que incluir documentación general sobre novedades de auditoría, acciones correctivas y procedimientos de seguimiento.

vi. Difusión de la información

A. La totalidad de la información relacionada con la seguridad debe difundirse en toda la organización. Si un individuo se mantiene actualizado en materia de seguridad está mejor preparado para comprender los distintos aspectos de las condiciones de seguridad de la organización y desarrollar soluciones novedosas a problemas difíciles Este objetivo se logra adoptando programas relacionados con seguridad, dando a conocer informes relevantes y alentando al personal para que participe en cursos de capacitación, seminarios y talleres de seguridad.

B. Otro aspecto de la difusión de la información es la retroalimentación de los reportes de seguridad presentados. Hay que notificar a los empleados cuando se recibe un reporte de seguridad o cuando se detecta una amenaza potencial a la seguridad y proporcionar más información después de la investigación, análisis y acción correctiva. Los reportes también puede difundirse mediante una publicación de la OMA o la creación de un sitio web. La organización debe esforzarse en comunicar a todos los empleados donde pueden encontrar información relacionada con seguridad. De esta forma, la totalidad de los integrantes de la organización se pone al tanto de temas relacionados con seguridad y entiende que la organización busca activamente ocuparse de estos asuntos.

vii. Instrucción

a) Para que los empleados cumplan con todos los requerimientos en materia de seguridad, es necesario que cuenten con información, conocimientos y capacitación o instrucción adecuados. Para ser eficaz en el logro de este objetivo, la organización debe determinar qué requerimientos de instrucción o capacitación se necesitan en cada área de trabajo. Se debe requerir que todos los empleados tengan un mismo nivel de capacitación en el SMS. El temario de los cursos de capacitación que reciban dependerá de su función en el SMS.

b) Además, los empleados deben recibir cursos de instrucción básica de factores humanos para adquirir conciencia acerca factores individuales que pueden afectar el desempeño de las personas y provocar errores. La instrucción puede cubrir temas como fatiga, comunicaciones, estrés, modelos de desempeño humano y falta de concientización.

c) Los empleados a los que se les asignó una función en el SMS deben recibir una mayor capacitación, la cual debe incluir:

I. Investigación de hechos y técnicas de análisis.

II. Determinación de peligros.

III. Principios de auditoría.

IV. Técnicas de comunicación.

V. Análisis e implementación de sistemas.

VI. Preparación para responder a emergencias.

VII. Factores humanos y de organización.

d) Los ejecutivos de alto nivel y el Gerente Responsable deben adquirir conocimientos generales acerca de todos los aspectos del SMS. El Gerente Responsable tiene la responsabilidad de establecer y actualizar el SMS. Por lo tanto, es aconsejable que tenga conocimientos generales sobre el SMS.

**5. Objetivos que se alcanzan en la FASE II**

Los siguientes objetivos deben ser cumplidos dentro del período de tiempo establecido para la conclusión de esta Fase.

i. Establecimiento de una biblioteca con la información de retroalimentación de los reportes de seguridad y de todos aquellos temas relacionados con la seguridad.

ii. Implementación del proceso de manejo reactivo de la seguridad.

iii. Conclusión de la instrucción relevante sobre los componentes del plan de implementación del SMS y del manejo de riesgos basado en los procesos reactivos.

iv. Distribución en la organización de información crítica de seguridad basada en datos adquiridos por los procesos reactivos.

**c) Fase 3 Implementación de proceso proactivo y predictivo. (Ver párrafo 145.510(c) del LAR 145)**

**1. Procesos proactivos y predictivos**

El objetivo de esta fase es estructurar un proceso progresista de gestión de la seguridad. Los procesos de manejo y de análisis de la información son depurados en esta fase. Al finalizar esta etapa la organización estará lista para realizar un análisis coordinado de seguridad basado en información recolectada por medio de procesos reactivos, proactivos y predictivos.

Dentro de esta fase se deben desarrollar los siguientes puntos de cada elemento:

i. Identificación y análisis de peligros basados en procesos proactivos y predictivos.

A. Identificación de peligros.

I. Identificar las fuentes internas y externas a ser usadas en la recolección de información proactiva y predictiva de peligros.

II. Implementar un inicio estructurado de la identificación proactiva y predictiva de peligros.

ii. Gestión de Riesgos basado en procesos proactivos y predictivos.

A. Evaluación de los riesgos.

I. Desarrollar y adoptar una matriz de riesgos relevante al ambiente operacional de la organización.

II. Desarrollar instrucciones de la matriz de riesgo e incluirlas en el programa de instrucción.

iii. Instrucción.

A. Instrucción al personal de la oficina de seguridad en los medios específicos proactivos y reactivos de recolección de datos relacionados de seguridad.

B. Informar a los supervisores y el personal de primera línea sobre los procesos proactivos y predictivos.

C. Desarrollar un programa de entrenamiento de seguridad para el personal de primera línea, administradores y supervisores sobre:

I. Los componentes relevantes del plan de implementación del SMS.

II. Identificación de peligros y manejo de riesgos basados en los procesos proactivos y predictivos. El personal de primera línea es instruido sobre identificación y reporte de peligros desde eventos desencadenantes menos serios o durante las operaciones en tiempo real y los supervisores son instruidos en el manejo de los peligros y riesgos basados en procesos proactivo y predictivo.

iv. Documentación en los procesos proactivo y predictivo.

A. Almacenar información sobre el manejo de riesgos basado en los procesos proactivos y reactivos en la biblioteca de seguridad.

B. Agregar información sobre los procesos proactivo y predictivo del manejo de riesgos al manual SMS.

C. Desarrollar los indicadores de desempeño de la seguridad y las metas de desempeño de la seguridad.

D. Escribir los requerimientos para la identificación de peligros y manejo de riesgos basados en los procesos proactivo y predictivo en la documentación de oferta para los contratistas, si es necesario y notificar por escrito a los contratistas y subcontratistas.

v. Promoción de la seguridad - Comunicación de la seguridad.

A. Establecer un medio para transmitir la información organizacional sobre la Fase III.

I. Cartas, noticias y boletines de seguridad.

II. Sitios internet

III. Correos electrónicos

## 2. Valoración de la seguridad

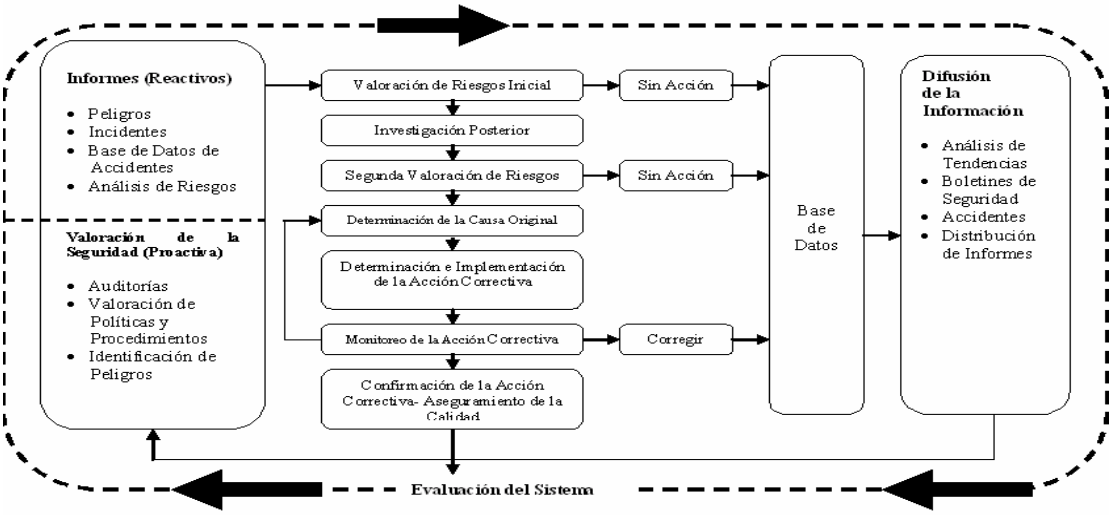


**Figura 8**

Como se puede apreciar en la figura anterior la diferencia entre los procesos reactivos y proactivos radica en el método utilizado para recolectar los datos de identificación de los peligros. En tanto que los procesos reactivos identifican los peligros por medio de informes que se dan de forma posterior a que ocurre un accidente o incidente, los procesos proactivo y predictiva identifica los peligros de forma proactiva mediante las valoraciones de seguridad en vigilancias, auditorias y como resultado de la observación directa de las operaciones de la organización.

i. Para que se produzca la transición del SMS de sistema reactivo a proactivo, el sistema tiene que seleccionar activamente peligros potenciales que afectan la seguridad y evaluar los riesgos asociados con ellos. Este objetivo puede lograrse aplicando métodos de valoración de la seguridad. La valoración de la seguridad permite que se identifiquen peligros potenciales y se apliquen luego técnicas de manejo de riesgo para tratar eficazmente los peligros.

ii. Al realizar la valoración de la seguridad se determina qué condiciones pueden verse afectadas por el personal, el equipamiento o los materiales, llevando a cabo una evaluación sistémica de los procedimientos, procesos, funciones y sistemas de la organización, que incluye el impacto financiero y otros asuntos que no son técnicos.

iii. El sistema de valoración de la seguridad del titular de un certificado debe constar de los siguientes elementos básicos:

A. Sistemas para identificar peligros potenciales

B. Técnicas de manejo de riesgos

C. Supervisión en curso / aseguramiento de la calidad

**3. <u>Frecuencia de la valoración</u>**

La valoración de la seguridad debe emprenderse como mínimo:

i. Durante la implementación del SMS y a intervalos regulares a partir de ese momento.

ii. Cuando se planean cambios mayores en las operaciones

iii. Cuando la organización experimenta cambios rápidos, como crecimiento y expansión, oferta de nuevos servicios, eliminación de servicios existentes o introducción de equipos o procedimientos nuevos.

iv. Cuando cambia el personal clave.

**4. <u>Identificación de peligros</u>**

i. La identificación de los peligros es el acto de determinar las condiciones que potencialmente pueden provocar daños al personal, los equipos o estructuras, pérdida de material, o reducción de la capacidad para desempeñar determinadas funciones. En particular, se incluyen condiciones que podrían contribuir a la liberación de una aeronave que no es aeronavegable, la operación de aeronaves de manera insegura o métodos inseguros empleados en los aeropuertos. Este objetivo puede alcanzarse mediante:

A. La valoración de la seguridad de todos los procesos que aplica una organización para llevar a cabo una operación específica, la cual implica valorar constante las funciones y sistemas y todos los cambios que los afecten y el desarrollo de casos de seguridad para manejar la seguridad de manera proactiva. La valoración de la seguridad es un proceso central en la construcción del manejo de la seguridad y constituye una función vital en la evaluación y mantenimiento de la confianza en la seguridad del sistema;

B. Análisis de Tendencias y Patrones;

C. Sistema de información interna: información ingresada por empleados, proveedores de servicios, clientes, socios industriales;

D. Auditorías de seguridad de todos los aspectos de la operación, inclusive de terceros, entidades no reguladas y contratistas;

E. Supervisión de datos: supervisión de mantenimiento, datos de confiabilidad, estadísticas de incidentes;

F. Revisión de datos de incidentes / accidentes;

G. Inspecciones en sitio: hangar, talleres, línea de vuelo;

H. Revisiones de control de calidad;

I. Supervisión activo de comportamiento: se observa a las personas mientras desempeñan su trabajo;

J. Experiencia corporativa, opiniones obtenidas en el lugar de trabajo;

K. Gerencia de Línea, opinión sobre el entorno operativo;

L. Registro de peligros genéricos que afectan a la industria: listados de Asociaciones e Información de la OACI;

ii. Comprender los peligros y riesgos inherentes asociados con las actividades diarias permite que la organización minimice los actos que ocasionan inseguridad y responda proactivamente, mejorando procesos, condiciones y otros aspectos sistémicos que provocan inseguridad (incluyen capacitación, presupuestos, procedimientos, planificación, mercadeo y otros factores relacionados con la organización que, como se sabe, desempeñan un rol en numerosos accidentes relacionados con sistemas). De esa forma, el manejo de la seguridad pasa a ser una función central de la organización y no simplemente una tarea secundaria de la dirección. Este es un paso vital en la transición desde una cultura reactiva, en la cual la organización reacciona ante un hecho, a una cultura proactiva, en la cual la organización busca activamente ocuparse de asuntos sistémicos relacionados con la seguridad, antes de que provoquen una falla activa.

**5. Construcción de un perfil de riesgos que afectan la seguridad y un registro de peligros**

El perfil de riesgos que afectan la seguridad es un listado con prioridades respecto de los riesgos conocidos dentro de la organización. Para desarrollar este perfil se debe crear un registro de peligros que afectan a la organización, que requieren una supervisión activa y continúa para determinar cuáles son peligros y los riesgos consecuentes. Algunas técnicas para identificar peligros se detallan en la sección 4 anterior.

**6. Creación del perfil de los riesgos que afectan la seguridad**

i. La determinación de los riesgos potenciales es útil para comprender cabalmente su impacto si no se controlan. Para ello, hay que realizar una evaluación completa de los riesgos.

ii. Para preparar el perfil de los riesgos que afectan la seguridad hay que analizar toda la organización y determinar niveles de riesgo dentro de la misma. A continuación se presentan algunos ejemplos de áreas que deben tenerse en cuenta:

A. Factores relacionados con las operaciones, como informaciones sobre el clima y tiempos de entrega.

B. Factores técnicos, como la capacidad de intercambio de partes y capacidad en diversos tipos de aeronave.

C. Factores humanos, tales como disponibilidad de equipamiento, ambiente de trabajo y recursos humanos.

iii. La valoración general de los riesgos permite determinar el rango de los peligros, amenazas o riesgos que afectaron o pueden afectar a la entidad, el área circundante o la infraestructura crítica que le sirve de sustento. El impacto potencial de todo peligro, amenaza o riesgo está determinado por su severidad y la vulnerabilidad de los individuos, la propiedad, las operaciones, el medio ambiente y la entidad ante las amenazas, peligros y/o riesgos.

iv. Al realizar la valoración de los riesgos hay que categorizar amenazas, peligros o riesgos, tanto por su frecuencia como por su severidad relativa, teniendo en cuenta que existen numerosas combinaciones posibles de frecuencia y severidad para cada uno. El titular del certificado debe tratar de atenuar esas amenazas, peligros y riesgos, mitigarlos, prepararse para hacerles frente, responder a ellos y recuperarse de situaciones que pueden afectar a individuos, propiedades, operaciones y medio ambiente, etc.

v. Existen numerosas metodologías y técnicas para valorar riesgos, que van desde simples hasta complejas. Estas técnicas y la información adicional asociada con ellas incluyen las siguientes, pero no se limitan a ellas:

A. "¿Qué pasaría si...?": El propósito del análisis "¿qué pasaría si....?" es identificar peligros o situaciones peligrosas específicas que podrían producir consecuencias no deseadas. Esta técnica tiene una estructura limitada pero descansa en individuos capacitados que están familiarizados con las áreas/operaciones/procesos. El valor del resultado final depende del equipo y de la naturaleza exhaustiva de las preguntas que se formulan acerca de los peligros.

B. Lista de verificación: Lista específica de artículos que se emplea para identificar peligros y situaciones peligrosas comparando las situaciones corrientes o las proyectadas con estándares aceptados. El valor del resultado final depende de la calidad de la lista de verificación y la experiencia/antecedentes del usuario.

C. ¿Qué pasaría si...? / lista de verificación: Se trata de una combinación de la técnica ¿qué pasaría si...? y la lista de verificación. Se emplean ambas técnicas para completar la valoración de los riesgos. Se desarrollan preguntas del tipo ¿qué pasaría si...? y se emplea una(s) lista(s) de verificación para alentar la creatividad del proceso ¿qué pasaría si...? y para cubrir cualquier falta en el proceso de desarrollo de preguntas. El valor del resultado final depende del equipo y de la naturaleza exhaustiva de las preguntas que formula en relación con los peligros.

D. Estudio de peligros y operatividad: Esta técnica requiere haya un equipo interdisciplinario con un conocimiento completo de las áreas/operaciones /procesos a ser valorados. Este enfoque es minucioso, demanda mucho tiempo y es costoso. El valor del resultado depende de la capacitación/ experiencia del equipo, la calidad del material de referencia, la capacidad del grupo para funcionar en equipo y de un liderazgo fuerte y positivo.

E. Modo de falla y análisis de sus efectos: Se examinan los elementos del sistema de manera individual y colectiva para determinar el efecto en caso de que fallen uno o más elementos. Este es un enfoque que va desde abajo hacia arriba, es decir, se examinan los elementos y se predice el efecto de la falla en el sistema general. Se requiere un pequeño grupo interdisciplinario. Esta técnica es la más adecuada para evaluar fallas potenciales de los equipos. El valor del resultado final depende de los antecedentes del equipo y del alcance del sistema a examinar.

F. Análisis del árbol de fallas: Este es un enfoque que va de arriba hacia abajo, mediante el cual se identifica un hecho no deseado y el rango de causas potenciales que pueden contribuir a que se produzca ese hecho. El valor del resultado final depende de la aptitud en el empleo del proceso de análisis del árbol de fallas, de los antecedentes del equipo y de su profundidad.

vi. El análisis del impacto es la descripción extensiva y la cuantificación de un hecho potencial que puede afectar al titular del certificado. Mediante este análisis se obtiene una idea precisa acerca de qué peligros son más probables, qué instalaciones, funciones o servicios se verán afectados por su vulnerabilidad ante el peligro, qué acciones los protegerán de manera más efectiva y el impacto potencial sobre la entidad en términos cuantificables.

vii. La identificación de peligros en una actividad constante. Con frecuencia, los peligros surgen y evolucionan como resultado de cambios en el entorno de las operaciones. Como tal, no se puede suponer que todos los peligros pueden percibirse, aunque la mayoría son predecibles. Por ejemplo, la mayor parte de los peligros que afectan la aviación no son tan obvios como un charco de agua en el piso. Hay que tratar activamente de conocerlos, entenderlos y manejarlos.

viii. Al realizar el perfil de los riesgos que afectan la seguridad se pueden priorizar los que afectan la seguridad y hacer una asignación eficaz de recursos para las áreas sujetas a mayores riesgos.

ix. En el Perfil de los Riesgos que Afectan la Seguridad hay que identificar los 10-12 riesgos más importantes para la seguridad, ya que es imposible ocuparse de todos los riesgos detectados en el sistema. Esta metodología permite que la dirección realice una asignación efectiva de recursos en donde más se necesitan.

x. El perfil de los riesgos que afectan la seguridad debe estar conectado con los objetivos y metas de la organización. Por ejemplo:

| | |
|---|---|
| **Riesgo número 1** | Daños que sufre la aeronave por equipo no protegidos |
| **Objetivo** | Reducir incidentes en los que se producen daños a las aeronaves por equipos no protegidos |
| **Meta 1** | Reducir los daños que sufren las aeronaves un 50% en un periodo de 6 meses |
| **Control (CAP)** | Introducir un nuevo procedimiento para sujetar los equipos |
| **Medida** | Por la cantidad de los incidentes en los que se producen daños a las aeronaves por equipos no protegidos |

xi. El desarrollo y actualización del perfil de riesgos que afectan la seguridad debe tener lugar conforme a ciclos establecidos de informes de gestión. Sin embargo, cuando se detecta un peligro y se evalúa que es crítico, la dirección debe revisarlo y ajustar el perfil del riesgo, cuando sea necesario.

## 7. Desarrollo de Caso de Seguridad

i. Un caso de seguridad se desarrolla casi de la misma forma que un caso de negocios de la organización. Permite que la organización anticipe peligros que pueden producir cambios en las operaciones. Como mínimo, hay que emplearlo:

A. Cuando se planee un cambio mayor en las operaciones.

B. Cuando se planee un cambio mayor en la organización.

C. Cuando cambie el personal clave.

D. Cuando se incorpore una nueva aeronave a las habilitaciones de la OMA.

E. Cuando se considere una nueva base de operaciones.

ii. El desarrollo de un caso de seguridad implica identificar peligros asociados con cambios mayores. Hay que tener en cuenta los peligros generados por cambios en la dirección, instalaciones o equipamiento operativo. Una vez identificados los peligros, hay que realizar la valoración de los riesgos relacionados y elaborar un plan para manejarlos.

iii. El caso de seguridad se desarrolla por necesidad. Cuando se producen cambios en la organización, es necesario desarrollar un caso de seguridad. De esta forma, la organización puede demostrar a todas las partes interesadas que manejó los riesgos asociados con ese cambio.

**8. Fuentes de Información para Determinar Peligros Potenciales**

A menudo se percibe que la identificación de los peligros es una tarea que insume recursos y es indebidamente onerosa. No tiene por qué serlo. Existen numerosas fuentes de información de fácil acceso que pueden utilizarse para comprender mejor los riesgos potenciales dentro de una organización. En la lista siguiente se detallan algunos de estos posibles recursos:

i. Experiencia de la corporación: Informes de seguridad existentes y hechos durante los cuales casi se produce una falla. En las minutas de las reuniones y en los comités de seguridad también se pueden revelar áreas potencialmente problemáticas.

ii. Opinión de la dirección de línea: Todos los directores tienen ideas acerca de donde están los riesgos más grandes dentro de su área de responsabilidad.

iii. Opiniones obtenidas en el lugar de trabajo: Hay que buscar activamente información entre los integrantes del plantel de trabajadores. Este objetivo puede lograrse a través de grupos focales, consultando a representantes de los empleados y realizando análisis de vulnerabilidad estructurado con gerentes de menor nivel y supervisores.

iv. Informes de auditoría: El sistema de auditoría interna de la organización debe contar con un registro estructurado de las áreas a controlar, que tenga un formato en el cual se establezcan prioridades. Hay que revisar los informes de auditoría y los planes de acciones correctivas (incluyendo una evaluación de las acciones de seguimiento que se completaron). A menudo, la memoria de las corporaciones es mucho más frágil de lo que perciben sus directivos en funciones, por lo que las investigaciones que abarquen períodos de más de 5/10 años podrían revelar información importante.

v. Análisis corporativo de los peligros: Los registros de los análisis formales de peligros conducidos con anterioridad permiten detectar la posible exposición a un riesgo, que un determinado momento no parecía muy significativa, pero en la actualidad esta condición ha cambiado, a la luz de la nueva situación.

vi. Registro de peligros genéricos de la industria: Los peligros/riesgos identificados por otras organizaciones pueden generar preocupaciones que deberían ser tratadas por la organización.

**9. Técnicas de supervisión activa**

Para evaluar la seguridad pueden emplearse diversos métodos de supervisión activa, entre los que se incluyen:

i. Inspecciones: Se determina si se cumplen los requerimientos, planes y procedimientos inspeccionando los predios, plantas y equipamiento o controlando las actividades. Generalmente, este objetivo se logra realizando una inspección exhaustiva de las actividades del área específica que se investiga comparándola con los métodos o procedimientos planeados. Tiende a concentrarse a nivel de las tareas.

ii. Inspecciones de seguridad de la dirección: Se determina la eficacia de los sistemas y la demostración del compromiso de la línea. Generalmente se lleva a cabo mediante exámenes practicados a directores o equipos centrados en las actividades que realizan y los sistemas que usan.

iii. Auditorías: Se verifica la conformidad con guías y estándares establecidos. Generalmente se lleva a cabo mediante una revisión sistemática e independiente del personal, instalaciones, etc. y de los sistemas de una organización cuya cobertura tiene un alcance predeterminado. Tiende a centrarse a nivel del proceso.

iv. Supervisión de procesos y métodos: Se determina si el procedimiento empleado es relevante, si se aplica activamente y si los métodos utilizados cumplen con requerimientos documentados. La supervisión puede realizarse a través de la observación del comportamiento: se controla a las personas en tiempo real mientras llevan a cabo sus funciones, lo cual puede ser muy eficaz para determinar donde se producen desviaciones respecto de procedimientos y comportamientos acordes con las normas y se toman atajos. El objetivo de la observación es analizar las causas que determinan los comportamientos, en lugar de señalar con el dedo a alguien.

v. Revisión: Se revisan los procesos para determinar si son adecuados y eficaces. A menudo, el objetivo de esta revisión es la asignación de recursos

**10. Empleo de listas de verificación**

En la mayoría de los sistemas de aseguramiento de la calidad las listas de verificación de auditoría se emplean para reunir datos relacionados con el sistema. Debe utilizarse un mismo tipo de lista de verificación para evaluar la seguridad de la organización. De esta forma, la organización puede desarrollar un caso de seguridad y analizar temas de seguridad que ilustren adecuadamente el nivel de seguridad de la organización.

**11. Objetivos que se alcanzan en la FASE III**

Los siguientes objetivos deben ser cumplidos dentro del período de tiempo establecido para la conclusión de esta Fase.

i. Establecimiento de un período de prueba inicial para el medio proactivo y predictivo de recolectar la identificación de peligros.

ii. Implementación del proceso de manejo proactivo y predictivo de la seguridad.

iii. Conclusión de la instrucción relevante sobre los componentes del plan de implementación del SMS y del manejo de riesgos basado en los procesos proactivo y predictivo.

iv. Desarrollados los indicadores de desempeño de seguridad y las metas de desempeño de la seguridad.

v. Distribución en la organización de información crítica de seguridad basada en datos adquiridos por los procesos reactivo, proactivo y predictivo.

**d) Fase 4 Garantía de seguridad operacional (Ver párrafo DINAC R 145.510(d) del DINAC R 145)**

**1. La Fase 4** es la fase final del proceso de implementación del SMS. En esta fase la garantía de Seguridad Operacional es evaluada por medio de vigilancia periódica, retroalimentación y acciones correctivas continuas para mantener la efectividad de los controles de riesgo bajo las demandas de cambios operacionales. En la fase 4, el manejo de la información de seguridad y los procesos analíticos garantizan la sostenibilidad de los procesos organizacionales de seguridad en el tiempo y durante períodos.

Al finalizar la Fase 4, las siguientes actividades deben estar finalizadas de manera que cumplan las expectativas de la autoridad de aviación civil que ejerce la vigilancia, según se ha establecido:

a. Desarrollar y concertar sobre los indicadores de desempeño de seguridad, las metas de desempeño de seguridad y la mejora continua del SMS.

b. Desarrollar el entrenamiento sobre la garantía de la Seguridad Operacional.

c. Desarrollar la documentación sobre la garantía de Seguridad Operacional.

d. Desarrollar y mantener un medio formal para comunicación de seguridad.

La gestión de los riesgos de seguridad requiera una retroalimentación sobre el desempeño de Seguridad para completar el ciclo de gestión. Por medio de la supervisión y la retroalimentación, se puede evaluar el desempeño del SMS y efectuar cualquier cambio necesario en el sistema. Adicionalmente, la garantía de la Seguridad proporciona a los interesados una indicación del nivel de desempeño de Seguridad del sistema.

El proceso de gestión de riesgos de Seguridad inicia con el buen entendimiento de la organización de sus procesos operacionales y el ambiente en el cual opera; continuando con la identificación de peligros, la evaluación de los riesgos de Seguridad y la mitigación de los mismos, para culminar con el desarrollo e implementación de los controles apropiados de estos riesgos de Seguridad. Una vez que, se han diseñado los controles de los riesgos de Seguridad asociados a los peligros identificados; se ha considerado a estos capaz de controlar los riesgos y se les ha puesto en operación; la garantía de Seguridad toma el control de la gestión de los riesgos de Seguridad.

Una vez que los controles de riesgos de Seguridad han sido desarrollados e implementados, es responsabilidad de la organización garantizar que estos continúen en uso y que trabajen según fue ideado. La garantía consiste, entonces, de las actividades y procesos asumidos por la organización para proporcionar “confiabilidad” en el desempeño y efectividad de los controles. La organización debe vigilar continuamente sus operaciones y el ambiente para garantizar que su sistema reconoce cambios en el ambiente laboral que podrían indicar la aparición de nuevos peligros o peligros no mitigados y la degradación de los procesos operacionales, instalaciones, condiciones de los equipos o desempeño humano que podría reducir la efectividad de los controles de riesgo existentes. Esto indicará la necesidad de regresar al proceso de gestión de riesgo para revisarlo y, si es necesario, revisar los controles de riesgo existentes o desarrollar nuevos controles.

Un proceso permanente de evaluación, análisis y valoración de estos controles debe continuar a través de la operación diaria del sistema. El proceso de garantía de la Seguridad se asemeja al proceso actual de aseguramiento de la Calidad, que tienen implementado algunas OMAs, en cuanto a los requisitos de análisis, documentación, auditorías y revisiones de la administración de la efectividad de los controles de riesgo. La diferencia es que el énfasis en la Garantía de Seguridad está en asegurar que los controles de riesgo se han desarrollados, son practicados y mantienen su efectividad. El énfasis tradicional en el aseguramiento de la calidad típicamente se basa en satisfacción del cliente, el cual, puede o no satisfacer totalmente de forma paralela los requisitos de Seguridad.

En relación a lo anterior, debe quedar claro que las OMAs actualmente cuenta con un proceso de evaluación, análisis y mejora continua del cumplimiento de los requisitos de la norma y procedimientos establecidos de la organización; a este proceso que se le reconoce como Aseguramiento de la Calidad; ahora a este proceso se le debe sumar un proceso para verificar y asegurar la efectividad del desempeño del sistema de seguridad del operacional implementado en la OM.

## 2. Supervisión y medición del desempeño de Seguridad

El concepto de desempeño de la seguridad es un ingrediente esencial en la operación efectiva de un SMS así como el avance progresivo hacia un ambiente regulatorio basado en desempeño. Es necesario para un SMS definir un conjunto de resultados

ponderables en razón de determinar que el sistema está operando realmente de acuerdo con las expectativas que fue diseñado o identificar cuando se requieren acciones para llevar el desempeño del SMS al nivel de estas expectativas. Estos resultados permiten que el desempeño real en actividades críticas para la Seguridad sea evaluado contra los controles organizacionales existentes para que sean tomadas las acciones correctivas necesarias y los riesgos sean mantenidos al más bajo nivel posible. Además el establecimiento y medición de los resultados específicos de desempeño de la seguridad permiten que se alcance la mejora continua en la gestión de la seguridad.

El desempeño de seguridad de un SMS se refiere a la cuantificación de procesos de baja consecuencia que expresa los objetivos de seguridad de una organización de mantenimiento, en forma de resultados ponderables de procesos específicos de bajo nivel. Desde la perspectiva de la relación entre el Estado y la organización de mantenimiento, el desempeño de Seguridad proporciona evidencia objetiva al Estado para ayudar a determinar la efectividad y eficiencia que el SMS de la organización de mantenimiento debe alcanzar mientras conduce sus operaciones. Este desempeño de Seguridad debe ser acordado entre el Estado y la OMA, como el mínimo aceptable que la OMA debe lograr cuando brinda sus servicios.

## 3. Gestión del cambio

Las organizaciones de mantenimiento experimentan cambios de forma frecuente debido a expansión; contratación; cambios de los sistemas, equipos, programas, productos y servicios existentes; y la introducción de nuevos equipos o procedimientos. Algunos peligros pueden ser inadvertidamente introducidos en una operación cuando ocurre un cambio. Las prácticas de gestión de la Seguridad requieren que los peligros producto de estos cambios sean identificados de forma sistemáticamente y proactiva, y que las estrategias de gestión de los riesgos de Seguridad sean desarrolladas, implementadas y subsecuentemente evaluadas.

Un proceso formal de gestión del cambio debe tomar en cuenta las siguientes consideraciones:

i. Sistemas y actividades críticas. Estos tienen una relación cercana con los riesgos de Seguridad. La condición crítica de estos sistemas se relaciona a la consecuencia potencial de un equipo siendo operado inapropiadamente o una actividad siendo incorrectamente ejecutada esencialmente respondiendo a la pregunta ¿Qué tan importante es este equipo/actividad para la operación segura del sistema? Aunque esta es una consideración que debe hacerse durante el proceso de diseño toma relevancia durante una situación de cambio. Siempre existen algunas actividades que son más esenciales que otras. Los equipos y actividades que son considerados más críticos deben ser revisados después de un cambio para asegurar que acciones correctivas puedan ser tomadas para controlar los riesgos potenciales que emerjan.

ii. Estabilidad de los sistemas y ambientes operacionales. Los cambios pueden ser el resultado de una planificación tales como crecimiento, cambios en las habilitaciones, cambios en los servicios contratados y otros cambios bajo el control de la organización. Los cambios en el ambiente organizacional son también importantes, tales como el estatus económico o financiero, malestar laboral, cambios en el ambiente político o regulatorio, o cambios en el ambiente físico tal como cambios en los patrones de clima. Aunque estos factores no están bajo el control de la organización, esta debe tomar acciones para responder a ellos. Frecuentes cambios en los sistemas y ambiente operacional indicaran que los administradores necesitan actualizar la información clave de forma más frecuente que en situaciones más estables.

iii. Desempeño en el pasado. El desempeño en el pasado es un indicador probado de desempeño futuro. Es aquí donde el ciclo natural de aseguramiento de la seguridad entra en juego. Análisis de tendencias en el proceso de aseguramiento de la seguridad debe ser empleado para seguir las medidas de

desempeño de seguridad en el tiempo y para tener en cuenta esta información en la planificación de futuras actividades bajo situaciones de cambio. Más aún, donde se han encontrado y corregido deficiencias como resultado de auditorías, evaluaciones, investigaciones o respuestas pasadas, es esencial que esta información sea considerada para garantizar la efectividad de las acciones correctivas.

Un proceso formal de gestión del cambio debe identificar cambios dentro de la organización que pueden afectar los procesos, procedimientos, productos y servicios establecidos. Antes de implementar los cambios, un proceso formal de gestión del cambio debe describir las disposiciones para garantizar el desempeño de seguridad. El resultado de este proceso es la reducción de los riesgos producidos por los cambios en la provisión de servicios por la organización a los niveles más bajos como sea posible.

**4. <u>Mejora continua del SMS</u>**

i. El aseguramiento radica en el principio del ciclo de mejora continua. En un modo muy similar, en el que el aseguramiento de la calidad facilita el continuo mejoramiento en la calidad, el aseguramiento de la seguridad asegura el control del desempeño de seguridad, incluyendo cumplimiento regulatorio, por medio de la verificación y actualización constante del sistema operacional. Estos objetivos son alcanzados a través de la aplicación de herramientas similares como son: evaluaciones internas y auditorías independientes (internas y externas), estricto control de documentos y supervisión en curso de los controles de seguridad y las acciones de mitigación.

**A.** ***Evaluaciones Internas*** incluye la evaluación de actividades operacionales de la organización así como las funciones específicas del SMS. Las evaluaciones conducidas para el propósito de este requerimiento deben ser conducidas por personas u organizaciones que son funcionalmente independientes del proceso técnico que está siendo evaluado. La función de evaluación interna también requiere evaluar y auditar las funciones de gestión de la seguridad, la formulación de políticas, gestión de riesgo, aseguramiento de la seguridad y promoción de la seguridad

**B.** ***Auditorías Internas*** son una herramienta importante para los administradores usada para obtener información con la cual puede tomar decisiones y mantener las actividades operacionales en el curso correcto. La responsabilidad primaria de la gestión de la seguridad está en aquellos en quienes son “dueños” de las actividades técnicas de la organización que soportan la provisión del servicio. Es aquí donde los peligros son más directamente descubiertos, donde las deficiencias en las actividades contribuyen a los riesgos y donde la supervisión directa sobre el control y asignación de los recursos puede mitigar el riesgo al nivel más bajo posible. Aunque las auditorías internas son frecuentemente ideadas como una prueba o calificación de las actividades de una organización, son una herramienta esencial para la garantía de la seguridad, para ayudar a los administradores a cargo de las actividades a mantener control sobre estas actividades, una vez que los controles de riesgo han sido implementados, continúan trabajando y son efectivos para mantener la seguridad operacional continua. Se debe conducir una auditoria inicial que cubra actividades técnicas, seguida de un ciclo de auditorías internas periódicas y llevar un registro detallado de las novedades de auditoría, que incluya temas relacionados con cumplimiento y no cumplimiento, acciones correctivas e inspecciones de seguimiento. El ciclo de auditorías periódicas no es fijo. Los resultados de la auditoría deben comunicarse a toda la organización.

ii. Implementación de un Programa de Auditoría Interna

El primer paso para establecer el programa de auditoría (evaluación) interna es desarrollar las políticas y guías conforme a las cuales operará el programa. Estas políticas (que deben incluirse en un manual aprobado, o, si se desarrolló, en el Manual de Políticas del SMS, al que se hagan referencias cruzadas en el manual aprobado) son la guía de "más alto nivel" que describe el programa de garantía de seguridad en términos generales y se relacionan normalmente con los requerimientos de las regulaciones. Por lo general, los ítems que se incluyen comprenden el compromiso de contar con un programa de garantía de la seguridad, la descripción general del programa con su objetivo, el detalle de los puestos, con antecedentes y capacitación, las responsabilidades en cuanto a la preparación de reportes, la declaración emitida en virtud del ciclo de auditoría periódica y referencias a documentos con procedimientos que no forman parte del manual aprobado. Esto se debe a que los procedimientos de auditoría son dinámicos y probablemente se modifiquen a medida que el programa atraviese el ciclo de mejora continua.

**C.** ***Auditorías Externas*** del SMS pueden ser conducidas por la autoridad responsable de la vigilancia, organizaciones clientes u otras organizaciones terceras. Estas auditorías no solo proporcionan un fuerte enlace con la supervisión del sistema sino que son un sistema secundario de garantía.

iii. La mejora continua del SMS aspira así a determinar las causas inmediatas de un desempeño inferior al estándar y sus implicaciones en la operación del SMS y rectificar las situaciones identificadas como causantes a través de las actividades de garantía de seguridad. La mejora continua es alcanzada por medio de evaluaciones internas, auditorías externas e internas aplicadas a:

A. Evaluación proactiva de instalaciones, equipos, documentación y procedimientos, por ejemplo en las evaluaciones internas.

B. Evaluación proactiva de un desempeño individual, para verificar el total cumplimiento de las responsabilidades de seguridad individuales, por ejemplo, por medio de chequeos periódicos de competencia (auditoria/evaluación) y

C. Evaluaciones reactivas en razón de verificar la efectividad del sistema para el control y mitigación de riesgos, por ejemplo, por medio de auditorías internas y externas.

## 5. Relación entre la gestión del riesgo y la garantía de seguridad

i. La función de gestión del riesgo de un SMS proporciona la identificación de peligros y las evaluaciones de los riesgos iniciales. Los controles de riesgo organizacionales son desarrollados y una vez que se determina que estos son capaces de llevar el riesgo al nivel más bajo posible, son implementados en las operaciones diarias. La garantía de la seguridad toma control a esta altura para asegurar que los controles de riesgo están siendo practicados según se planeó y que continúan alcanzando los objetivos. La función de la garantía de la calidad también proporciona identificación de necesidades de nuevos controles de riesgo debido a los cambios en el ambiente operacional.

ii. En un SMS, los requerimientos de seguridad del sistema son desarrollados con base a una evaluación objetiva de los riesgos en las actividades de la organización que soportan el servicio brindado. La parte de garantía del sistema se centra en la organización probando que estos requerimientos han sido cumplidos, por medio de la colección y análisis de evidencia objetiva.

iii. Es importante reiterar los papeles de estas dos funciones dentro del proceso integrado de SMS: la gestión de riesgos (GR) y la garantía de seguridad (GS).

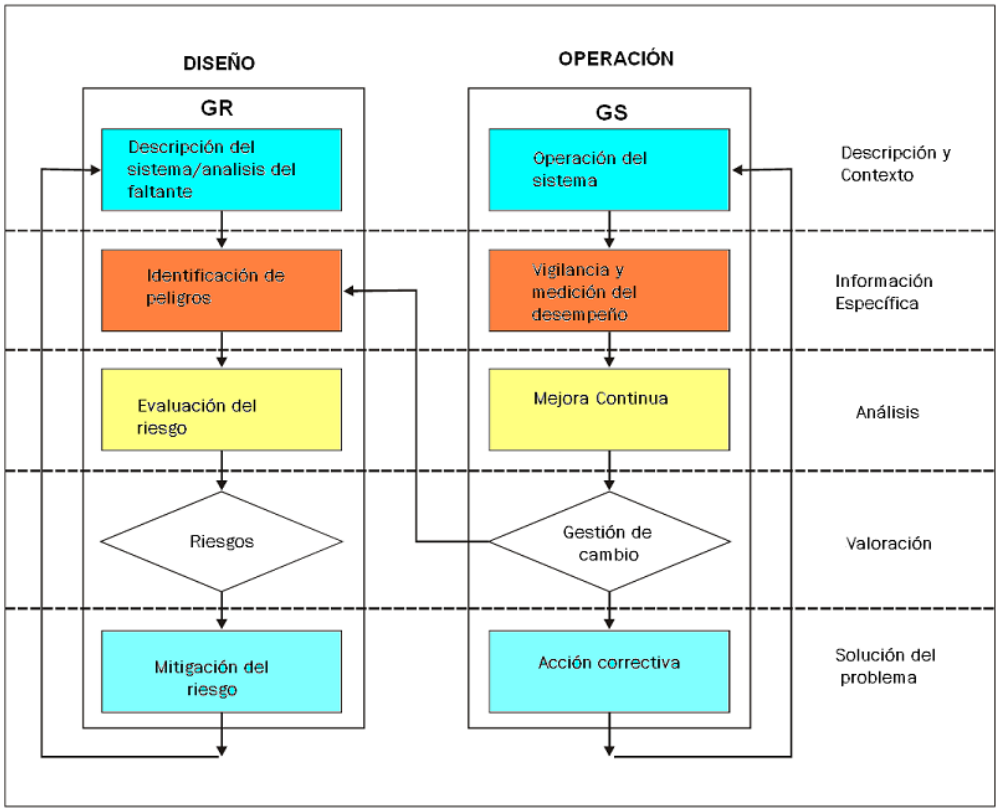



**Figura 9**

## 6. El SMS y el sistema de gestión de la calidad

i. La gestión de la calidad ha sido establecida en las organizaciones de mantenimiento aeronáutico desde hace varios años. Estas organizaciones han implementado y operado un sistema de control de Calidad y/o un sistema de aseguramiento por mucho tiempo.

ii. El programa de aseguramiento de la calidad define y establece las políticas y objetivos de calidad de la organización. Este asegura que la organización tiene en uso los elementos necesarios para mejorar la eficiencia y reducir los riesgos relacionados al servicio. Si está apropiadamente implementado, un sistema de aseguramiento de la calidad asegura que los procedimientos son llevados a cabo de forma consistente y en cumplimiento con los requerimientos aplicables; que los problemas son identificados y resueltos y que la organización revisa y mejora continuamente sus procedimientos, productos y servicios. El aseguramiento de la calidad debe identificar los problemas y mejorar los procedimientos en razón de cumplir los objetivos corporativos.

iii. La aplicación de los principios de aseguramiento de la calidad a los procesos de gestión de la seguridad ayudan a garantizar que el requisito de medidas de seguridad del sistema han sido usados para apoyar a la organización en el logro de sus objetivos de seguridad. Sin embargo el aseguramiento de la calidad no puede por sí mismo, como se ha propuesto en calidad, cumplir como garantía de seguridad. Es la integración de los principios y conceptos de aseguramiento de la calidad dentro de un SMS bajo el componente de garantía de la seguridad que permiten a una organización garantizar la estandarización necesaria de los procesos para alcanzar todos los objetivos de seguridad.

iv. Se pueden establecer entonces aspectos comunes de ambos sistemas:

A. Son planificados y administrados.

B. Dependen de mediciones y supervisión.

C. Involucran cada función, proceso y persona de la organización y

D. Buscan la mejora continua.

v. Por otra parte los sistemas difieren en:

A. El SMS se enfoca en aspectos de seguridad, humanos y organizacionales buscando satisfacer la seguridad.

B. La gestión de la calidad está enfocada en los productos y servicios de una organización buscando la satisfacción del cliente.

vi. Es por eso que resulta posible la integración de ambos sistemas teniendo en cuenta las diferencias que han sido establecidas. La integración de ambos sistemas permite un acometida estructurada para vigilar que los procesos y procedimientos de identificación de los peligros y sus posibles consecuencias; manteniendo los riesgos asociados a las operaciones bajo el control de la organización, funcionando según lo planeado y cuando esto no suceda, mejorarlos.

vii. Así, las auditorías entonces pueden ser denominadas como de “seguridad” o de “calidad” o simplemente de aseguramiento, lo importante es que los aspectos de seguridad y calidad sean considerados y cumplidos.

**PAGINA DEJADA INTENCIONALMENTE EN BLANCO**

# Apéndice 1

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| Componente 1 - POLITICA Y OBJETIVOS DE SEGURIDAD | | | |
| Elemento1.1- Compromiso y responsabilidad Gerencial | | | |
| | ¿Tiene establecido la organización de mantenimiento un sistema de gestión de la Seguridad con componentes definidos, el cual es mantenido y respetado? | | |
| | ¿Es el sistema de gestión de la seguridad apropiado al tamaño y la complejidad de la organización? | | |
| | ¿Existe una política de seguridad aplicada? | | |
| | ¿Está basado el sistema de gestión de la seguridad en la política de seguridad? | | |
| | ¿Está la política de seguridad, aprobada y promovida por el Gerente Responsable? | | |
| | ¿Es la política de seguridad revisada periódicamente? | | |
| | ¿Existe un proceso formal para desarrollar un adecuado conjunto de objetivos de seguridad? | | |
| | ¿Existen objetivos de seguridad que corresponden a los indicadores de desempeño, metas de desempeño y requisitos de seguridad? | | |
| | ¿Están los objetivos de seguridad publicados y distribuidos? | | |
| | ¿Existe en práctica una política que garantiza un efectivo sistema de reporte de deficiencias de seguridad, peligros y sucesos incluyendo las condiciones bajo las cuales aplica una protección sobre acciones disciplinarias y/o administrativas? | | |
| Elemento1.2 – Responsabilidades de los Gerentes sobre la seguridad | | | |
| | ¿Tiene la organización identificado un gerente responsable quien será el último responsable para en su representación implementar y mantener el SMS? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| | ¿Tiene el Gerente Responsable el control total de los recursos financieros requeridos para que sean conducidas las operaciones autorizadas bajo el certificado de operación? | | |
| | ¿Tiene el Gerente Responsable control total de los recursos humanos requeridos para que sean conducidas las operaciones autorizadas bajo el certificado de operación? | | |
| | ¿Tiene el Gerente Responsable autoridad final sobre las operaciones autorizadas a ser conducidas bajo el certificado de operación? | | |
| Elemento 1.3- Nominación de personal clave de Seguridad | | | |
| | ¿Ha nominado la organización a una persona calificada para administrar y vigilar diariamente la operación del SMS? | | |
| | ¿Cumple la persona que vigila la operación del SMS con las funciones de trabajo y las responsabilidades requeridas? | | |
| | ¿Se encuentran definidas y documentadas las responsabilidades y funciones de seguridad del personal a todos los niveles de la organización? | | |
| Elemento 1.5 –Coordinación de Respuesta ante Emergencia. | | | |
| | ¿Tiene la organización un plan de contingencia o respuesta ante emergencia apropiado a su naturaleza, tamaño y complejidad? | | |
| | ¿Tiene el plan de emergencia o contingencia procedimientos documentados, implementados y con responsables asignados? | | |
| | ¿Tiene la organización procedimientos para comunicar el contenido de los procedimientos de contingencia o plan de emergencia a todo el personal? | | |
| | ¿Conduce la organización prácticas y ejercicios con todo el personal clave a intervalos específicos? | | |
| Elemento 1.6 –Documentación. | | | |
| | ¿Ha desarrollado y mantenido la organizació documentación SMS, en papel o electrónica? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| | ¿La documentación ha sido desarrollada de manera que describe el SMS y la relación entre los componentes? | | |
| | ¿Ha desarrollado la organización los requisitos del SMS en el MOM como un instrumento para comunicar el planteamiento de seguridad de la organización a todo el personal? | | |
| | ¿Documenta el manual todos los aspectos del SMS, incluyendo política de seguridad, objetivos, procedimientos y responsabilidades individuales sobre la seguridad? | | |
| | ¿Tiene el manual claramente expresado el papel de la gestión de riesgo como la actividad de inicio y el de aseguramiento de seguridad como la actividad continua? | | |
| | ¿Tiene la organización un sistema de registros que asegure la generación y retención de todos los registros necesarios para documentar y soportar los requisitos de operación? | | |
| | ¿Está el sistema de registros de la organización de conformidad con los requisitos de la regulación aplicable y con las mejores prácticas de la industria? | | |
| | ¿Proporciona el sistema de registros de la organización el control necesario para garantizar la apropiada identificación, legibilidad, almacenaje, protección, archivo, tiempo de retención y disposición de los registros? | | |
| Componente 2 – GESTION DE RIESGOS | | | |
| Elemento 2.1 –Proceso de identificación de peligros. | | | |
| | ¿Tiene la organización un sistema formal para la recolección y análisis de la información de seguridad que recoge de manera efectiva información sobre los peligros en las operaciones? | | |
| | ¿Incluye este sistema una combinación de métodos reactivos, proactivos y predictivos de recolección de información de seguridad? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| | ¿Tiene la organización procesos reactivos que permitan la obtención de información referente a la gestión de riesgos? | | |
| | ¿Tiene la organización desarrollado entrenamiento respecto al método reactivo de recolección de información de seguridad? | | |
| | ¿Tiene la organización desarrollado comunicación sobre al método reactivo de recolección de información de seguridad? | | |
| | ¿El sistema de reportes reactivo es simple, accesible y acorde al tamaño de la organización? | | |
| | ¿Son los reportes reactivos revisados en un nivel apropiado de la administración? | | |
| | ¿Existe un proceso de retroalimentación para notificar a los empleados que su reporte ha sido recibido y para compartir los resultados del análisis? | | |
| | ¿Cuenta la organización con un proceso proactivo que busca activamente identificar los peligros por medio del análisis de las actividades de la organización? | | |
| | ¿Tiene la organización desarrollado entrenamiento respecto al método proactivo de recolección de información de seguridad? | | |
| | ¿Tiene la organización desarrollado comunicación sobre al método proactivo de recolección de información de seguridad? | | |
| | ¿El sistema de reportes proactivo es simple, accesible y acorde al tamaño de la organización? | | |
| Elemento 2.2 –Proceso de evaluación y mitigación de riesgos | | | |
| | ¿Tiene la organización documentación de SMS que exprese claramente la relación entre peligros, consecuencias y riesgos? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| | ¿Existe un proceso estructurado para el análisis de riesgos asociados a las consecuencias de peligros identificados, expresados en términos de probabilidad y severidad de los sucesos? | | |
| | ¿Existe un criterio para evaluar los riesgos y establecer la tolerabilidad de los riesgos? | | |
| | ¿Existe una estrategia para la mitigación de riesgos que incluye planes de acciones correctivas y preventivas para prevenir la recurrencia de sucesos o deficiencias reportadas? | | |
| | ¿Son generadas acciones correctivas y preventivas como respuesta al análisis de un evento? | | |
| Componente 3 – ASEGURAMIENTO DE LA SEGURIDAD | | | |
| Elemento 3.1 –Supervisión y medición del desempeño del SMS. | | | |
| | Se realizan revisiones planeadas regulares y periódicas respecto: | | |
| | Desempeño del SMS | | |
| | Revision de auditorías internas | | |
| | Identificación de peligros e investigación de sucesos | | |
| | Resultados de análisis de riesgos y sucesos | | |
| | Retroalimentación externa de análisis y resultados | | |
| | Estado de las acciones correctivas | | |
| | Acciones de seguimiento de revisiones previas | | |
| | Cambios que pueden afectar la seguridad | | |
| | Recomendaciones de mejora | | |
| | Compartir las mejores prácticas a través de la organización | | |
| | ¿Existe un proceso para evaluar la efectividad de las acciones correctivas? | | |
| | ¿Son los reportes de seguridad revisados en un nivel apropiado de la administración? | | |
| | ¿Existe un proceso de retroalimentación para notificar a los empleados que su reporte ha sido recibido y para compartir los resultados del análisis? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| | ¿Existe un proceso establecido para vigilar y analizar tendencias? | | |
| | ¿Cuenta la organización con un proceso implementado de auto evaluación, tal como revisiones regulares, evaluaciones vigilancias y auditorías? | | |
| | ¿Son generadas acciones correctivas y preventivas como respuesta a la identificación de un peligro? | | |
| | ¿Existen procedimientos establecidos para la conducción de investigaciones internas? | | |
| | ¿Existen medidas para asegurar que todos los sucesos y deficiencias reportadas son investigados? | | |
| | ¿Existe un proceso para asegurar que los sucesos y deficiencias reportadas son analizados para identificar todos los riesgos asociados? | | |
| | ¿Son generadas acciones preventivas y correctivas como respuesta a una investigación de accidente y análisis de riesgo? | | |
| | ¿Tiene la organización un proceso para evaluar la efectividad de las medidas correctivas/preventivas que se han desarrollado? | | |
| | ¿Tiene la organización un sistema para vigilar el proceso interno de reportes y las acciones correctivas asociadas? | | |
| | ¿Existe la función de auditoría con la independencia y autoridad requerida para realizar evaluaciones internas de mane efectiva? | | |
| | ¿Cubre el sistema de auditoría todas las funciones, actividades y organismos dentro de la organización? | | |
| | ¿Existen alcances, criterios, frecuencias y métodos bien definidos para las auditorias? | | |
| | ¿Existen procesos de selección y entrenamiento para asegurar la objetividad y la competencia de los auditores así como la imparcialidad del proceso? | | |
| | ¿Existe un procedimiento para reportar los resultados de la auditoria y mantener los registros de estos? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| | ¿Existe un procedimiento que describe los requisitos para que las acciones correctivas y preventivas en respuesta a los resultados de una auditoria sean ejecutadas de manera oportuna? | | |
| | ¿Existe un procedimiento para registrar la verificación de acciones tomadas y reportar los resultados de la verificación? | | |
| | Realiza la organización revisiones periódicas de la administración de funciones criticas de seguridad y reportes relevantes de seguridad resultado de evaluaciones internas | | |
| Elemento 3.2 – Gestión del cambio. | | | |
| | ¿Ha desarrollado y mantenido la organización un proceso formal para la gestión de cambios? | | |
| | ¿Este proceso analiza los cambios en operaciones o personal clave por riesgos? | | |
| | ¿Se identifican los cambios dentro de la organización que pueden afectar los procesos y servicios establecidos? | | |
| | ¿Tiene la organización disposiciones asegurar que se mantiene el desempeño de seguridad antes de la implementación del cambio? | | |
| | ¿Tiene la organización un proceso establecido para eliminar o modificar controles de riesgo que no son más requerido debido a los cambios en el ambiente operacional? | | |
| Elemento 3.3 – Mejora continúa del SMS. | | | |
| | ¿Tiene la organización un proceso para la evaluación proactiva de instalaciones, equipos, documentación y procedimientos por medio de auditorías y vigilancias? | | |
| | ¿Tiene la organización un proceso para la evaluación proactiva de desempeño individual, para verificar cumplimiento de las responsabilidades sobre seguridad? | | |
| | ¿Tiene la organización un proceso reactivo para verificar la efectividad del sistema de control y mitigación de riesgos? | | |

| ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA DINAC R 145 | | | |
|---|---|---|---|
| Referencia | Aspecto Evaluado o interrogante sobre requisito | Respuesta | |
| | | Si | No |
| Componente 4 – PROMOCION DE LA SEGURIDAD | | | |
| Elemento 4.1 – Entrenamiento y Educación. | | | |
| | ¿Existe un procedimiento documentado para identificar los requisitos de entrenamiento para que el personal este entrenado y competente para realizar las labores del SMS? | | |
| | ¿El entrenamiento de Seguridad es el apropiado para la participación individual en el SMS? | | |
| | ¿Está el entrenamiento de seguridad incorporado en el entrenamiento de inducción del empleado? | | |
| | ¿Existe entrenamiento en plan de respuesta de emergencia o plan de contingencia para el personal afectado? | | |
| | ¿Existe un proceso para medir la efectividad del entrenamiento? | | |
| Elemento 4.2 – Comunicación de Seguridad. | | | |
| | ¿Existe un proceso establecido dentro de la organización que permite que el SMS funcione efectivamente? | | |
| | ¿Los procesos de comunicación (escrita, reuniones, electrónica, etc.) están acorde con el tamaño y alcance de la organización? | | |
| | ¿La información es establecida y mantenida en un medio disponible que permite canalizar documentos relevantes de Seguridad? | | |
| | ¿Existe un proceso de diseminación de la información de seguridad a través de la organización y un medio de vigilar la efectividad de este proceso? | | |