Manual de Aviación Civil

Manual de Gestión de la Seguridad Operacional SSP / SMS

PROGRAMA DE SEGURIDAD OPERACIONAL DEL ESTADO (SSP)
&
SISTEMAS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

SISTEMA DE EDICIÓN Y ENMIENDAS

LAS ENMIENDAS AL PRESENTE MANUAL, SERAN INDICADAS MEDIANTE UNA BARRA VERTICAL EN EL MARGEN IZQUIERDO, ENFRENTE DEL RENGLÓN, SECCIÓN O FIGURA QUE ESTE SIENDO AFECTADA POR EL MISMO.

LA EDICIÓN SERÁ EL REEMPLAZO DEL DOCUMENTO COMPLETO POR OTRO.

ESTAS SE DEBEN ANOTAR EN EL REGISTRO DE EDICIONES Y ENMIENDAS, INDICANDO EL NÚMERO CORRESPONDIENTE, FECHA DE EFECTIVIDAD Y LA FECHA DE INSERCIÓN.

Registro de Ediciones y Enmiendas

Edi./Enm. #	Fecha de emisión	Fecha de inserción	Insertada por:

Preámbulo

En cumplimiento e implementación del sistema RAC que fue aprobado mediante Resolución No. 02 – 2006 (COMITRAN XXVI), de fecha 02 de junio del 2006, y de acuerdo al RAC 11:

- El borrador inicial del PCI-SSP/SMS fue emitido el 20 de mayo del 2009 y fue desarrollado en base al documento 9859 de la OACI, primera edición – 2006; y al Programa de Seguridad Operacional desarrollado por el Estado de Costa Rica.

- El mismo fue revisado por el grupo de expertos de seguridad operacional de la región en la ciudad de Guatemala en Noviembre del 2009.

- En junio del 2010, la asesoría legal de ACSA recomendó que dicho documento no se enviara a los Estados como MRAC sino como un PCI; ya que la base o sustento legal aun no era el adecuado, pudiendo llegar a ser un MRAC en otro momento.

- En julio del 2010 se enmendó este documento de acuerdo a la segunda edición 2009 del Doc. 9859 de la OACI.

Lista de Páginas Efectivas

Página #	Edición/ Enmienda	Fecha
Portada	Inicial	20 enero 2011
SEE - 1	Inicial	20 enero 2011
REE - 1	Inicial	20 enero 2011
P - 1	Inicial	20 enero 2011
LPE - 1	Inicial	20 enero 2011
LPE - 2	Inicial	20 enero 2011
TC - 1	Inicial	20 enero 2011
TC - 2	Inicial	20 enero 2011
PIG-1	Inicial	20 enero 2011
Sección 1		
1 - 1	Inicial	20 enero 2011
1 - 2	Inicial	20 enero 2011
1 - 3	Inicial	20 enero 2011
1 - 4	Inicial	20 enero 2011
1 - 5	Inicial	20 enero 2011
1 - 6	Inicial	20 enero 2011
1 - 7	Inicial	20 enero 2011
1 - 8	Inicial	20 enero 2011
1 - 9	Inicial	20 enero 2011
1 - 10	Inicial	20 enero 2011
1 - 11	Inicial	20 enero 2011
1 - 12	Inicial	20 enero 2011
1 - 13	Inicial	20 enero 2011
1 - 14	Inicial	20 enero 2011
1 - 15	Inicial	20 enero 2011
1 - 16	Inicial	20 enero 2011
1 - 17	Inicial	20 enero 2011
Sección 2		
2 – 1	Inicial	20 enero 2011
2 – 2	Inicial	20 enero 2011
2 – 3	Inicial	20 enero 2011
2 – 4	Inicial	20 enero 2011
2 – 5	Inicial	20 enero 2011
2 – 6	Inicial	20 enero 2011
2 – 7	Inicial	20 enero 2011
2 – 8	Inicial	20 enero 2011
2 – 9	Inicial	20 enero 2011
2 – 10	Inicial	20 enero 2011
2 – 11	Inicial	20 enero 2011
2 – 12	Inicial	20 enero 2011

Página #	Edición/ Enmienda	Fecha
2 – 13	Inicial	20 enero 2011
2 – 14	Inicial	20 enero 2011
2 – 15	Inicial	20 enero 2011
2 – 16	Inicial	20 enero 2011
2 – 17	Inicial	20 enero 2011
2 – 18	Inicial	20 enero 2011
2 – 19	Inicial	20 enero 2011
2 – 20	Inicial	20 enero 2011
2 – 21	Inicial	20 enero 2011
Apéndices		
3-1	Inicial	20 enero 2011
3-Ap1-1	Inicial	20 enero 2011
3-Ap1-2	Inicial	20 enero 2011
3-Ap1- 3	Inicial	20 enero 2011
3-Ap1- 4	Inicial	20 enero 2011
3-Ap2- 1	Inicial	20 enero 2011
3-Ap2- 2	Inicial	20 enero 2011
3-Ap2- 3	Inicial	20 enero 2011
3-Ap2- 4	Inicial	20 enero 2011
3-Ap2- 5	Inicial	20 enero 2011
3-Ap2- 6	Inicial	20 enero 2011
3-Ap2- 7	Inicial	20 enero 2011
3-Ap2- 8	Inicial	20 enero 2011
3-Ap3- 1	Inicial	20 enero 2011
3-Ap3- 2	Inicial	20 enero 2011
3-Ap3- 3	Inicial	20 enero 2011
3-Ap3- 4	Inicial	20 enero 2011
3-Ap3- 5	Inicial	20 enero 2011
3-Ap3- 6	Inicial	20 enero 2011
3-Ap3- 7	Inicial	20 enero 2011
3-Ap3- 8	Inicial	20 enero 2011
3-Ap3- 9	Inicial	20 enero 2011
3-Ap4- 1	Inicial	20 enero 2011
3-Ap4- 2	Inicial	20 enero 2011
3-Ap4- 3	Inicial	20 enero 2011
3-Ap5- 1	Inicial	20 enero 2011
3-Ap5- 2	Inicial	20 enero 2011
3-Ap5- 3	Inicial	20 enero 2011
3-Ap5- 4	Inicial	20 enero 2011
3-Ap5- 5	Inicial	20 enero 2011

Página #	Edición/ Enmienda	Fecha
3-Ap5- 6	Inicial	20 enero 2011
3-Ap6- 1	Inicial	20 enero 2011
3-Ap6- 2	Inicial	20 enero 2011
3-Ap6- 3	Inicial	20 enero 2011
3-Ap6- 4	Inicial	20 enero 2011
3-Ap6- 5	Inicial	20 enero 2011
3-Ap6- 6	Inicial	20 enero 2011
3-Ap7- 1	Inicial	20 enero 2011
3-Ap7- 2	Inicial	20 enero 2011
3-Ap7- 3	Inicial	20 enero 2011
3-Ap7- 4	Inicial	20 enero 2011
3-Ap7- 5	Inicial	20 enero 2011
3-Ap7- 6	Inicial	20 enero 2011
3-Ap7- 7	Inicial	20 enero 2011
3-Ap7- 8	Inicial	20 enero 2011
3-Ap7- 9	Inicial	20 enero 2011
3-Ap7- 10	Inicial	20 enero 2011
3-Ap7- 11	Inicial	20 enero 2011
3-Ap7- 12	Inicial	20 enero 2011
3-Ap7- 13	Inicial	20 enero 2011
3-Ap7- 14	Inicial	20 enero 2011
3-Ap7- 15	Inicial	20 enero 2011
3-Ap7- 16	Inicial	20 enero 2011

Página #	Edición/ Enmienda	Fecha
3-Ap7- 17	Inicial	20 enero 2011
3-Ap7- 18	Inicial	20 enero 2011
3-Ap7- 19	Inicial	20 enero 2011
3-Ap7- 20	Inicial	20 enero 2011
3-Ap7- 21	Inicial	20 enero 2011
3-Ap7- 22	Inicial	20 enero 2011
3-Ap7- 23	Inicial	20 enero 2011
3-Ap7- 24	Inicial	20 enero 2011
3-Ap7- 25	Inicial	20 enero 2011
3-Ap7- 26	Inicial	20 enero 2011
3-Ap7- 27	Inicial	20 enero 2011
3-Ap7- 28	Inicial	20 enero 2011
3-Ap7- 29	Inicial	20 enero 2011
3-Ap7- 30	Inicial	20 enero 2011
3-Ap7- 31	Inicial	20 enero 2011
3-Ap7- 32	Inicial	20 enero 2011
3-Ap7- 33	Inicial	20 enero 2011
3-Ap7- 34	Inicial	20 enero 2011
3-Ap7- 35	Inicial	20 enero 2011
3-Ap7- 36	Inicial	20 enero 2011
3-Ap7- 37	Inicial	20 enero 2011
3-Ap7- 38	Inicial	20 enero 2011
3-Ap7- 39	Inicial	20 enero 2011

Tabla de Contenidos

PRESENTACIÓN E INTRODUCCION GENERAL

1 Presentación

Este Manual SSP/SMS, se presenta en páginas sueltas y se divide en tres secciones. Cada página se identifica mediante la fecha de la edición o enmienda mediante la cual se incorporó.

El texto de las secciones está escrito en arial 10. Las notas explicativas no se consideran requisitos y cuando existan, están escritas en letra arial 8.

Los apéndices no siguen un formato estandarizado.

2 Introducción General

La Sección 1 contiene los requisitos de la OACI que corresponden a las actividades SSP que deberían implementar los Estados asociados al Sistema RAC y como los Estados pueden llevar a cabo la implementación por fases.

La Sección 2 contiene los requisitos del SMS que deberían cumplir los prestadores de servicios o usuarios finales, para garantizar la Seguridad Operacional a todo nivel y de qué forma estos pueden llevar a cabo la implementación por fases del sistema.

La Sección 3 anexa 7 Apéndices que tratan temas fundamentales relacionados con el SSP y el SMS; así como también con la implementación de un Sistema de Gestión de la Seguridad Operacional (SMS) en una organización de mantenimiento aprobada (MRAC 145).

Estos requisitos se basan en la normativa internacional que la Organización de Aviación Civil Internacional, ha puesto en vigencia para los Anexos 1, 6, 8, 11, 13 y 14, en materia de Seguridad Operacional.

El presente Manual está basado, principalmente en el texto del Documento 9859 de la OACI, segunda edición de 2009, y aplicable desde el 19 de noviembre del 2009.

Se ha utilizado la terminología “debería” y deberían”, pensando en que todavía los Estados de la región no han hecho las modificaciones necesarias dentro de sus leyes para que los requisitos de la OACI tengan cabida. Como esto es un Manual y a pesar de que el RAC 11 nos permite utilizar los conceptos de obligatoriedad, se han dejado por ahora de esta manera, (a pesar de ser muchos de ellos, requisitos) para que este documento no entre en conflicto con lo establecido en los Estados.

SECCION

1

PCI – SSP/SMS

PROGRAMA DE SEGURIDAD OPERACIONAL DEL ESTADO (SSP) &
SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

SUBPARTE A.
GENERALIDADES.

PCI SSP/SMS 1.001 Acrónimos

ALARP: Del inglés "As low as reasonable practicable", traducido como "tan bajo como sea razonablemente posible

SMM: Del inglés Safety Managment Manual, traducido como Manual de Gestión de la Seguridad Operacional,

SA: Safety Assurance del inglés, ver definiciones.

SMS: Sistema de gestión de la Seguridad Operacional

SSP: Programa de Seguridad Operacional del Estado

SDCPS Sistemas de recopilación y procesamiento de datos sobre seguridad operacional

PCI SSP/SMS 1.002 Definiciones

Los términos y expresiones que se definen en el presente PCI para lo concerniente a la Seguridad Operacional tienen los siguientes significados:

Accidente: Todo suceso, relacionado con la utilización de una aeronave, que ocurre dentro del período comprendido entre el momento en que una persona entra a bordo de la aeronave, con intención de realizar un vuelo, y el momento en que todas las personas han desembarcado, durante el cual:

1) Cualquier persona sufre lesiones mortales o graves a consecuencia de:

   a) Hallarse en la aeronave, o

   b) Por contacto directo con cualquier parte de la aeronave, incluso las partes que se hayan desprendido de la aeronave, o

   c) Por exposición directa al chorro de un reactor, excepto cuando las lesiones obedezcan a causas naturales, se las haya causado una persona a sí misma o hayan sido causadas por otras personas o se trate de lesiones sufridas por pasajeros clandestinos escondidos fuera de las áreas destinadas normalmente a los pasajeros y la tripulación; o

2) la aeronave sufre daños o roturas estructurales que:

   a) afecten adversamente sus resistencia estructural, su performance o sus características de vuelo, y

   b) normalmente exigen una reparación importante o el recambio del componente afectado, excepto por falla o daños del motor, cuando el daño se limita al motor, su capó o sus accesorios, o por daños limitados en las hélices, extremos del ala, antenas, neumáticos, frenos o laminas, pequeñas abolladuras o perforaciones en el revestimiento de la aeronave;

   c) la aeronave desaparece o es totalmente inaccesible.

Análisis de carencias (Gap analysis): Un análisis de las estructuras de seguridad existentes dentro de la organización en comparación con las estructuras que deberían de existir.

Análisis de Seguridad Operacional: Es el proceso de organizar hechos empleando técnicas, métodos, o instrumentos específicos para:

1) ayudar a decidir qué datos adicionales se necesitan;

2) determinar los factores causales y los que contribuyen, y

3) ayudar a llegar a conclusiones válidas

Aseguramiento de la Seguridad Operacional: Es lo que llevan a cabo los proveedores de servicios con relación al monitoreo y medición del desempeño de la Seguridad Operacional.

Auditoría de Seguridad Operacional: Proceso sistemático, independiente y documentado para obtener las evidencias de la auditoría y evaluarlas de manera objetiva para determinar el grado en que se cumplen los criterios de Seguridad Operacional.

Descripción del sistema: La mayoría de los peligros son generados por interacciones operacionales entre los diferentes componentes de un sistema. Es por lo tanto esencial describir el sistema en términos de sus componentes como una de las primeras actividades cuando se planifica el SSP/SMS.

El Ejecutivo o Gerente Responsable: Dueño o autoridad máxima de una organización o empresa, dependiendo del tamaño y complejidad de una organización, esta persona podría ser el:

1) Director

2) Gerente General (Chief Executive Officer/CEO);

3) Presidente de la Junta Directiva;

4) Socio mayoritario

5) Dueño

Gestión de la Seguridad Operacional: Un conjunto organizado de procesos y procedimientos en el que el riesgo de provocar daños a las personas o a la propiedad es reducido a, o mantenido por debajo de un nivel aceptable por medio de un proceso continuo e identificación de los peligros, gestión de los riesgos y la asignación de recursos.

Incidente: Todo suceso relacionado con la utilización de una aeronave, equipo, diseño o instrucción que no llegue a ser un accidente, que afecte o pueda afectar la seguridad de las Operaciones.

Indicadores de Seguridad Operacional: Objetivos de corto y mediano plazo del programa de Seguridad Operacional de un Estado asociado al Sistema RAC, o del SMS de un proveedor de servicios**.**

Manual de gestión de Seguridad Operacional Documentación para desarrollar y mantener un sistema de gestión de la Seguridad Operacional

Medición de la seguridad operacional:

1) La medición de la seguridad operacional comprende la cuantificación de los resultados de sucesos de alto nivel, consecuencias graves o funciones estatales de alto nivel, tales como proporciones de accidentes, proporciones de incidentes graves y cumplimiento de los reglamentos.

2) La medición de la eficacia de la seguridad operacional comprende la cuantificación de los resultados de procesos de bajo nivel y consecuencias leves que proporciona una medida de la implantación realista de cada SSP más allá de las proporciones de accidentes o cumplimiento de los reglamentos.

Metas de Seguridad Operacional: Objetivos de largo plazo del SSP del Estado, o del SMS de un proveedor de servicios. Balance entre lo que es deseable y lo que es realista para un proveedor de servicios individual**.**

1) Objetivos de alto nivel de gestión de Seguridad Operacional de un SSP conocido como la Medición de la Seguridad Operacional;

2) Desempeño mínimo de la Seguridad Operacional que los Estados Asociados al Sistema RAC debería alcanzar a través de la implementación de su SSP conocido como la Medición del desempeño de la Seguridad Operacional;

3) Una referencia indirecta para medir el desempeño de la Seguridad Operacional de los proveedores de servicios.

Mitigación – Medidas que eliminan el peligro potencial o que reducen la probabilidad o severidad del riesgo**.**

Monitoreo continuo: Es el proceso por el cual el desempeño de la seguridad de una organización se verifica en comparación con las políticas y objetivos de seguridad aprobados**.**

Nivel aceptable de Seguridad Operacional (ALoS): es el grado mínimo de seguridad operacional que debería ser garantizado por parte de la autoridad de supervisión o vigilancia. Los ALoS de un SSP serán establecidos por los Estados asociados al Sistema RAC y se deberían expresar en términos prácticos por dos medidas o métricas:

1. Indicadores de desempeño de seguridad, y

2. Metas de desempeño de seguridad

Peligro o Amenaza de Seguridad Operacional: Condición, objeto o actividad que potencialmente puede causar lesiones al personal, daños al equipamiento o estructuras, pérdida de personal, o reducción de la habilidad de desempeñar una función determinada.

Probabilidad – La posibilidad que una situación de peligro pueda ocurrir.

Programa de Seguridad Operacional del Estado: (SSP) Un conjunto integrado de reglamentos y actividades encaminados a mejorar la Seguridad Operacional.

Proveedor de servicios: Desde del contexto de este documento se refiere a aquellas organizaciones que prestan o proporciona servicios de aviación. Este término incluye a aquellas organizaciones de instrucción reconocidas que están expuestas a riesgos operacionales durante la entrega de sus productos o servicios, proveedor de servicioses de aeronaves, organizaciones aprobadas de mantenimiento, organizaciones responsables por el diseño de un tipo y / o fabricantes de aeronaves, proveedores de los servicios de tránsito aéreo y aeródromos certificados según aplique.

Requisitos de Seguridad Operacional: Es una evaluación objetiva de los riesgos de la seguridad operacional en las actividades de la organización, tales como: procedimientos operacionales, tecnologías y sistemas, programas, planes de contingencias, etc. Pueden añadirse medidas de confiabilidad, disponibilidad o precisión.

Riesgo – La posibilidad de pérdida o daño, medida en términos de severidad y probabilidad. La posibilidad que algo pueda ocurrir y sus consecuencias si ocurre**.**

Seguridad: Un estado en el que el riesgo de lesiones a las personas o daños a la propiedad es reducido a, o mantenido por debajo de un nivel aceptable por medio de un proceso continuo de identificación de los peligros y gestión del riesgo**.**

Seguridad Operacional Predictiva: Basada en la noción que la gestión de la seguridad se optimiza saliendo a buscar los problemas y no esperando que se produzcan. Búsqueda agresiva de la información de diferentes fuentes que puede revelar riesgos a la seguridad emergentes.

Seguridad Operacional Proactiva: Basada en la noción que las fallas del sistema pueden ser minimizadas: identificando los riesgos de seguridad existentes en el sistema antes que el sistema falle; y tomando las acciones necesarias para reducir los riesgos que afectan la seguridad**.**

Seguridad Operacional Reactiva: Método reactivo que responde a los sucesos que ya ocurrieron, como incidentes y accidentes. Es el nivel más bajo de los sistemas, estrategias y métodos de captura de datos de seguridad operacional, la investigación de accidentes e incidentes graves se realiza con carácter de reparación de daños, apropiada para: situaciones que involucran fallas de tecnología, eventos inusuales

Severidad: Las posibles consecuencias de una situación de peligro, tomando como referencia la peor condición previsible.

Sistema de gestión de la Seguridad Operacional (SMS): Enfoque sistemático para la gestión de la seguridad operacional, que incluye la estructura orgánica, líneas de responsabilidad, políticas y procedimientos necesarios para el proveedor de servicios.

Supervisión de la seguridad Son las actividades que lleva a cabo una Autoridad Aeronáutica de los Estados miembros de COCESNA con relación al SMS de los proveedores de servicios.

INTENCIONALMENTE EN BLANCO

PCI SSP/SMS 1.005 Aplicabilidad.

1) Este Manual determina los requisitos que debería cumplir un Estado asociado al Sistema RAC en relación con su Programa de la Seguridad Operacional (SSP).

2) Asimismo los requisitos del funcionamiento de un sistema de Gestión de la Seguridad Operacional (SMS) para los proveedores de servicios.

3) Estos requisitos están en acuerdo con los siguientes Anexos:

   a) Anexo1— Licencias al Personal Técnico Aeronáutico: organizaciones aprobadas de entrenamiento que están expuestas a riesgos operacionales durante la entrega de sus productos o servicios,

   b) Anexo 6 — Operación de Aeronaves, Parte I — Transporte Aéreo Comercial Internacional - Aviones— y Parte III — Operaciones Internacionales — Helicópteros: proveedor de servicioses de aeronaves.

   c) Anexo 8 — Aeronavegabilidad de las Aeronaves: organizaciones aprobadas de mantenimiento, organizaciones responsables por el diseño de un tipo y / o fabricantes de aeronaves.

   d) Anexo 11 — Servicios de Tránsito Aéreo;

   e) Anexo 13 (aplicable solo a los Estados) – Investigación de incidentes y accidentes de aeronaves, y

   f) Anexo 14 — Aeródromos, Volumen I — Aeródromo Diseño y Operación: aeródromos certificados.

4) Este PCI se ocupa de la Seguridad Operacional en la aviación, sus procesos, procedimientos y actividades relacionados, tales como: la seguridad ocupacional, protección ambiental o servicio al cliente o calidad del producto.

5) El proveedor de servicios es el responsable directo de las acciones relacionadas con la Seguridad Operacional de los servicios o productos contratados a terceros.

6) Este PCI establece los requisitos mínimos aceptables, el proveedor de servicios podrá establecer requisitos más estrictos.

PCI SSP/SMS 1.010 Efectividad.

1) Este PCI SSP/SMS entra en vigencia:

   a) A partir de su publicación oficial, sin embargo, los tiempos de implementación para el SSP y el SMS se harán de acuerdo a las diferentes fases propuestas mas adelante y se establecen de la siguiente manera, 12 meses para la primera fase, veinticuatro meses para la segunda fase, treinta y seis meses para la tercera fase y cuarenta y ocho meses para la cuarta y última fase (para un total de 4 años)

2) Disposiciones transitorias.

   a) Hasta la fecha de entrada en vigencia establecida en el párrafo (a) anterior, los Estados asociados al Sistema RAC se regirán de acuerdo a las regulaciones nacionales vigentes en la materia.

   b) Sin prejuicio del párrafo (1) anterior, cualquier Estado asociado al Sistema RAC puede implementar su SSP o SMS antes de las fechas propuestas por las fases.

PCI SSP/SMS 1.015 Aceptación.

1) Doce meses posteriores a la aprobación oficial de este PCI SSP/SMS, los Estados asociados al Sistema RAC deberían exigir, como parte de su Programa de Seguridad Operacional (SSP), que un proveedor de servicios implemente un sistema de gestión de la Seguridad Operacional (SMS) aceptable para el Estado, que como mínimo:

   a) identifique los peligros de Seguridad Operacional;

b) asegure que se aplican las medidas correctivas necesarias para que se mantenga el desempeño de Seguridad Operacional;

c) prevea la supervisión permanente y evaluación periódica del desempeño de Seguridad Operacional; y

d) tenga como meta mejorar continuamente el desempeño global del SMS

2) Para que un SMS sea aceptable para los Estados asociados al Sistema RAC, el proveedor de servicios deberá cumplir con los requisitos establecidos en esta PCI.

PCI SSP/SMS 1.020 Alcance.

Este documento describe los requisitos para la operación de un Programa de Seguridad Operacional (SSP) por parte de los Estados asociados al Sistema RAC y de un Sistema de Gestión de la Seguridad Operacional (SMS) de los proveedores de servicios a la aviación civil, de conformidad a las Regulaciones pertinentes de las MRAC LPTA, MRAC OPS 1, MRAC OPS 3, MRAC 139, MRAC ATS, MRAC 13, y MRAC 14.

INTENCIONALMENTE EN BLANCO

SUBPARTE B

PROGRAMA DE SEGURIDAD OPERACIONAL DEL ESTADO (SSP)

PCI SSP/SMS 1.025 Estructura del SSP.

La estructura OACI del programa de seguridad Operacional del Estado (SSP), la cual se encuentra integrada por 4 componentes y 11 elementos es la siguiente:

1. Política y objetivos de Seguridad Operacional del Estado
   - 1.1 Marco legislativo Estatal de la seguridad operacional.
   - 1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional.
   - 1.3 Investigación de accidentes e incidentes.
   - 1.4 Política de cumplimiento.

2. Gestión de riesgos de Seguridad Operacional del Estado.
   - 2.1 Requisitos de seguridad operacional para el SMS de los proveedores de servicios
   - 2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional.

3. Garantía de la Seguridad Operacional del Estado
   - 3.1 Vigilancia de la seguridad operacional
   - 3.2 Recopilación, análisis e intercambio de datos de seguridad operacional
   - 3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención

4. Promoción de la Seguridad Operacional del Estado
   - 4.1 Instrucción, comunicación y divulgación interna de información sobre seguridad operacional
   - 4.2 Instrucción, comunicación y divulgación externa de información sobre seguridad operacional.

Nota: En el apéndice 1 se encuentra una breve explicación de cada uno de los elementos de la estructura del SSP.

INTENCIONALMENTE EN BLANCO

SUBPARTE C

1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL DEL ESTADO

PCI SSP/SMS 1.030 Marco legislativo Estatal de la seguridad operacional

El Estado asociado al Sistema RAC debería:

1. Examinar, elaborar y promulgar un marco legislativo nacional y Regulaciones específicas en cumplimiento con los estándares internacionales y nacionales, los cuales definirán el cómo se debería conducir la gestión de la Seguridad Operacional en el Estado asociado al Sistema RAC.

2. Participar junto con las organizaciones que tengan actividades específicas en aviación en el establecimiento de las funciones, responsabilidades y las diferentes interacciones entre dichas organizaciones.

3. Revisar periódicamente el marco legislativo para asegurar que se mantiene conforme a las necesidades del Estado asociado al Sistema RAC.

PCI SSP/SMS 1.035 Responsabilidad y rendición de cuentas del Estado respecto de la seguridad operacional

El Estado asociado al Sistema RAC debería:

1. Identificar, definir y documentar los requisitos, las responsabilidades y la rendición de cuentas relativas a la creación y el mantenimiento del SSP. Esto incluye las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar permanentemente el SSP, el cual debería cumplir los objetivos de seguridad operacional del Estado. Incluir, además, una declaración clara sobre la provisión de los recursos necesarios para la implantación del SSP.

2. Identificar y designar al Ejecutivo responsable del SSP del Estado quien debería de tener:

   a) la responsabilidad final y la obligación administrativa de rendir cuentas en nombre del Estado para la implantación y mantenimiento del SSP;

   b) plena autoridad sobre asuntos de recursos humanos relativos a la organización de aviación del Estado que ha sido designada como depositaria del SSP;

   c) plena autoridad sobre los aspectos financieros de la organización de aviación del Estado que ha sido designada como depositaria del SSP;

   d) autoridad final sobre los aspectos de gestión de los certificados del proveedor de servicios; y

   e) responsabilidad final en la resolución de todos los asuntos de seguridad operacional de la aviación en el Estado.

3. El Estado debería de establecer el equipo de implantación del SSP

4. El Estado debería de asignar el tiempo necesario para cada tarea relacionada con la implantación del SSP entre los diferentes niveles de gestión de las organizaciones de aviación del Estado.

5. El Estado debería de presentar a todo el personal los conceptos del SSP a un nivel de acuerdo con su participación individual en el SSP.

6. Elaborar e implantar una política de seguridad operacional del Estado que debería incluir, pero sin limitarse necesariamente a ellos, los puntos siguientes:

   a) el compromiso de elaborar e implantar estrategias y procesos para asegurar que todas las actividades de aviación bajo vigilancia alcanzarán el nivel más elevado de eficacia de la seguridad operacional;

b) la elaboración y promulgación de un marco legislativo nacional de seguridad operacional y reglamentos de funcionamiento aplicables para la gestión de la seguridad operacional en el Estado;

c) el compromiso de asignar los recursos necesarios a las organizaciones de aviación del Estado tales como los servicios de tránsito aéreo para permitir que su personal cumpla sus responsabilidades, tanto relacionadas con la seguridad operacional como de otro tipo;

d) el apoyo a la gestión de la seguridad operacional en el Estado mediante un sistema efectivo de notificación y comunicación de peligros;

e) el establecimiento de disposiciones para la protección de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS);

f) el compromiso de una interacción efectiva con los proveedores de servicios en la resolución de los problemas de seguridad operacional;

g) el compromiso de comunicar, con la firma visible, la política de seguridad operacional del Estado a todo el personal; y

h) una política de cumplimiento adecuada a las operaciones del proveedor de servicios en un entorno SMS.

7. Establecer los medios necesarios para asegurar que la política de seguridad operacional del Estado es comprendida, implantada y observada en todos los niveles dentro de las organizaciones de aviación del Estado.

Nota: Ver Apéndice 3, en este se encuentran responsabilidades y funciones de seguridad operacional del Director de Aviación Civil, de gerentes, personal clave, comité de seguridad operacional, departamento de seguridad operacional.

PCI SSP/SMS 1.040 Investigación de accidentes e incidentes

El Estado asociado al Sistema RAC debería:

1. Elaborar y establecer los mecanismos para asegurar un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo sea la prevención de accidentes e incidentes, en apoyo de la gestión de la seguridad operacional en el Estado, y no la asignación de culpa o responsabilidad.
   Nota: para mejor referencia ver MRAC 13)

2. Las investigaciones de los Estados asociados al Sistema RAC, en este esquema están encaminadas en darle soporte al Programa de Seguridad Operacional del Estado.

3. Para un buen funcionamiento del SSP, los Estados asociados al Sistema RAC deberían mantener una independencia del organismo investigador de accidentes e incidentes.

PCI SSP/SMS 1.045 Política de cumplimiento (sanciones)

El Estado asociado al Sistema RAC debería:

1. Cada Estado asociado al Sistema RAC debería promulgar una política de sanciones que establezca las condiciones y circunstancias bajo la cual los proveedores de servicios se les permita tratar y resolver, internamente algunos eventos relacionados con ciertas desviaciones de Seguridad Operacional, siempre dentro del contexto del SMS aceptado de este proveedor de servicios y a satisfacción de la Autoridad.

2. Cada Estado asociado al Sistema RAC debería desarrollar una política de sanciones que le permita establecer las condiciones y circunstancias bajo las cuales pueden establecer o no procedimientos punitivos para tratar con aquellas desviaciones de la Seguridad Operacional.

3. La política de sanciones de cada Estado asociado al Sistema RAC debería asegurar que bajo ninguna circunstancia, una información derivada de un proceso voluntario interno de reporte establecido o un dato

obtenido de un sistema de monitoreo de información de vuelo (FDM), todo bajo un SMS, puede ser usado como evidencia para una acción legal punible.

4. El Estado debería desarrollar medidas de salvaguardia que permitan proteger aquella información que se obtenga de un proceso voluntario interno de reporte establecido o un dato obtenido de un sistema de monitoreo de información de vuelo (FDM),

   a) elaborar y promulgar una política de cumplimiento que establezca las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, y a satisfacción de la autoridad estatal competente.

   b) establecer las condiciones y circunstancias en las cuales las desviaciones respecto de la seguridad operacional deberían abordarse mediante procedimientos establecidos en cuanto a cumplimiento.

   c) asegurar que ninguna información obtenida de un sistema de notificación interna de peligros o un sistema de vigilancia de datos de vuelo establecidos en el marco del SMS se utilice para la aplicación de medidas disciplinarias.

PCI SSP/SMS 1.050 Documentación del SSP

Nota: este literal no forma parte de la estructura del SSP

El Estado debería de elaborar y establecer una biblioteca de seguridad operacional del Estado que documente los requisitos, responsabilidades y líneas de rendición de cuentas relativas al establecimiento y mantenimiento del SSP. Esta biblioteca de seguridad operacional debería de mantenerse y actualizarse, según sea necesario y debería contener como mínimo la siguiente documentación del SSP:

1. Marco legislativo Estatal de seguridad operacional promulgado.

2. Responsabilidades y rendición de cuentas establecidas, documentadas y publicadas del Estado respecto de la seguridad operacional.

3. Políticas de seguridad operacional y de cumplimiento del Estado firmadas por el Ejecutivo responsable.

4. Políticas de seguridad operacional y de cumplimiento del Estado distribuidas dentro de las organizaciones de aviación del Estado y entre los proveedores de servicio bajo vigilancia.

5. Los requisitos del SSP

6. Los procedimientos y procesos del SSP

7. El nivel aceptable de seguridad operacional (ALoS) del Estado relacionados con el SSP

8. Procesos independientes de investigación de accidentes e incidentes establecidos.

9. Estructura de organización del SSP implantada

INTENCIONALMENTE EN BLANCO

SUBPARTE D

2. Gestión de riesgos de seguridad operacional del Estado

PCI SSP/SMS 1.055 Requisitos de seguridad operacional para los SMS de los proveedores de servicios

El Estado asociado al Sistema RAC debería:

1. Establecer los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para el SMS del proveedor de servicios (marco normativo para SMS, circular de asesoramiento, etc.) como controles que rigen la forma en que los proveedores de servicios identificarán los peligros y gestionarán y controlarán los riesgos de seguridad operacional.

2. Establecer un cronograma para consulta con los proveedores de servicios sobre estos requisitos.

3. Establecer un cronograma para examinar periódicamente los requisitos y reglamentos específicos de funcionamiento a efectos de asegurar que siguen siendo pertinentes y apropiados para los proveedores de servicios.

PCI SSP/SMS 1.060 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

El Estado asociado al Sistema RAC debería:

1. Elaborar y establecer un procedimiento para acordar con cada proveedor de servicios la eficacia de la seguridad operacional de sus SMS sobre la base de:

   a) valores de indicador de la eficacia de la seguridad operacional;

   b) valores de objetivo de la eficacia de la seguridad operacional; y

   c) planes de acción.

2. Incluir en el procedimiento acordado que la eficacia de la seguridad operacional del proveedor de servicios debería ser proporcional a:

   a) la complejidad de los contextos operacionales y específicos de cada proveedor de servicios; y

   b) la disponibilidad de recursos en cada proveedor de servicios para enfrentar los riesgos de seguridad operacional.

3. Medir la eficacia de la seguridad operacional del SMS del proveedor de servicios mediante exámenes periódicos de la eficacia de seguridad del SMS acordada para asegurar que los indicadores de eficacia de la seguridad y objetivos de eficacia de la seguridad siguen siendo pertinentes y apropiados para los proveedores de servicios.

4. Elaborar un medio para evaluar resultados de bajo nivel y procesos más frecuentes entre diferentes proveedores de servicios.

5. Determinar resultados de eficacia medibles dentro de los diferentes SMS.

6. Siendo los resultados:

   a) Reglamentos sobre SMS promulgados.

   b) Textos de orientación sobre implantación del SMS distribuidos a los proveedores de servicios.

   c) Primer examen anual de la eficacia de la seguridad operacional de los proveedores de servicios acordada completado.

SUBPARTE E

3. Garantía de la seguridad operacional del Estado

PCI SSP/SMS 1.065 Vigilancia de la seguridad operacional

El Estado asociado al Sistema RAC debería:

1. Los Estados asociados al Sistema RAC deberían establecer mecanismos que aseguren que tiene un monitoreo efectivo de sus funciones con respecto a los ocho elementos críticos en que se basa la vigilancia de la Seguridad Operacional.

2. Los Estados asociados al Sistema RAC deberían establecer mecanismos para asegurar que la identificación de peligros y la gestión de los riesgos de la Seguridad Operacional de los proveedores de servicios sigan los controles regulatorios establecidos tales como los requisitos, regulaciones de operación específicas y políticas de implementación.

3. Los mecanismos deberían incluir inspecciones, auditorías y encuestas para asegurar que los controles para mitigar los riesgos regulatorios de Seguridad Operacional están adecuadamente integrados dentro del SMS del proveedor de servicios, que se practican según fueron diseñados, y que estos controles regulatorios tengan el efecto deseado sobre los mismos.

4. Desarrollar una auditoría interna del SSP.

PCI SSP/SMS 1.070 Colección, análisis e intercambio de datos sobre seguridad operacional

El Estado asociado al Sistema RAC debería:

1. Elaborar y establecer un medio para recopilar, analizar y almacenar datos sobre peligros y riesgos de seguridad operacional a nivel del Estado:

   a) establecer un sistema de notificación obligatoria de peligros;

   b) establecer un sistema de notificación voluntaria de peligros

   c) establecer un sistema de notificación confidencial de peligros;

   d) elaborar una base de datos estatal sobre peligros;

   e) establecer un mecanismo para elaborar información a partir de los datos almacenados;

   f) establecer un medio para recopilar datos sobre peligros a nivel global del Estado y a nivel de cada proveedor de servicios; y

   g) establecer un medio para implantar planes de medidas correctivas.

2. Asegurar que los procesos de identificación de peligros y de gestión de riesgos de seguridad operacional del proveedor de servicios se ajustan a los requisitos normativos establecidos y que los controles de riesgos de seguridad operacional están adecuadamente integrados en el SMS del proveedor de servicios, incluyendo, entre otros:

   a) inspecciones;

   b) auditorías; y

   c) encuestas.

3. Observar la secuencia siguiente para la implantación:

a) controles normativos de riesgos de seguridad operacional integrados en el SMS del proveedor de servicios;

b) actividades de vigilancia para asegurar que los procesos de identificación de peligros y gestión de riesgos de seguridad operacional del proveedor de servicios se ajustan a los requisitos normativos establecidos; y

c) actividades de vigilancia para verificar que los proveedores de servicios aplican los controles de riesgos de seguridad operacional

4. Establecer el nivel aceptable de seguridad (ALoS) relativo al SSP, comprendiendo una combinación de medición de la seguridad operacional y medición de la eficacia de la seguridad operacional:

a) la medición de la seguridad operacional comprende la cuantificación de los resultados de sucesos de alto nivel, consecuencias graves o funciones estatales de alto nivel, tales como proporciones de accidentes, proporciones de incidentes graves y cumplimiento de los reglamentos.

b) la medición de la eficacia de la seguridad operacional comprende la cuantificación de los resultados de procesos de bajo nivel y consecuencias leves que proporciona una medida de la implantación realista de cada SSP más allá de las proporciones de accidentes o cumplimiento de los reglamentos.

PCI SSP/SMS 1.075 Sobre la base de datos de seguridad operacional, concentración de la vigilancia operacional en las áreas de mayor prioridad o necesidad

El Estado asociado al Sistema RAC debería:

1. Establecer procedimientos para priorizar las inspecciones, auditorías y encuestas, basadas en análisis de peligros y riesgos de seguridad operacional y los resultados obtenidos deberían de ser:

a) sistemas Estatales de notificación obligatoria y confidencial de peligros implantados.

b) primer examen anual de la política y objetivos de seguridad operacional realizado.

c) primer examen anual de la política de cumplimiento realizado.

d) ALoS establecido.

INTENCIONALMENTE EN BLANCO

SUBPARTE F

4. Promoción de la seguridad operacional del Estado

PCI SSP/SMS 1.080 Capacitación, comunicación y diseminación de información sobre seguridad operacional en forma interna

El Estado asociado al Sistema RAC debería:

1. Desarrollar y mantener un programa de capacitación apropiado a cada individuo de acuerdo a su competencia dentro de la Seguridad Operacional y estar establecido de forma recurrente para varios niveles, que permita asegurar que el personal está entrenado y de esa forma mantener las competencias para llevar a cabo las tareas y responsabilidades del SSP/SMS.

2. Identificar requisitos de instrucción internos.

3. Elaborar y proporcionar instrucción genérica en seguridad operacional a todo el personal.

4. Elaborar un programa de instrucción sobre componentes clave del SSP y el SMS para el personal que debería incluir:

   a) adoctrinamiento o instrucción inicial en seguridad operacional;

   b) instrucción en seguridad operacional en el puesto de trabajo (OJT);

   c) instrucción periódica en seguridad operacional.

5. Establecer un medio para medir la efectividad de la instrucción.

6. Elaborar un medio para comunicar internamente cuestiones relacionadas con la seguridad operacional, debería incluir:

   a) políticas y procedimientos de seguridad operacional;

   b) boletines de noticias;

   c) avisos; y

   d) un sitio web.

PCI SSP/SMS 1.085 Capacitación, comunicación y diseminación de información sobre seguridad operacional en forma externa

El Estado asociado al Sistema RAC debería:

1. Establecer los medios para proporcionar intercambio de información relacionada con la seguridad operacional para apoyar la implantación del SMS entre proveedores de servicios, incluyendo los proveedores de servicios menores.

2. Proveer instrucción y elaborar textos de orientación sobre implantación del SMS para proveedores de servicios.

3. Establecer los medios para comunicar externamente asuntos relacionados con la seguridad operacional incluyendo:

   a) políticas y procedimientos de la seguridad operacional;

   b) boletines de noticias;

c) avisos; y

d) un sitio web.

4. Los resultados del cuarto componente como mínimo deberían de ser:

a) Primer ciclo de instrucción genérica en seguridad operacional para el personal completado.

b) Programa de instrucción sobre componentes clave de un SSP y SMS para personal técnico y de apoyo completado.

c) Texto de orientación sobre SMS distribuido a los proveedores de servicios, incluyendo los explotadores menores.

d) Primer ciclo de instrucción para proveedores de servicios sobre implantación de SMS completado.

e) Medios para comunicar interna y externamente la información relacionada con la seguridad operacional establecidos.

INTENCIONALMENTE EN BLANCO

SUBPARTE G

IMPLEMENTACIÓN DEL SSP

PCI SSP/SMS 1.090 Plan de implementación del SSP.

El plan de implementación del Programa de Seguridad Operacional del Estado debería contener los puntos que se detallan a continuación y debería ser aprobado por el Director de Aviación Civil o la Autoridad competente:

1. Política de la Seguridad Operacional del Estado.
2. Planificación de la Seguridad Operacional, objetivos y metas del Estado.
3. Descripción del sistema de Aviación del Estado.
4. Análisis de carencias en el sistema de Aviación del Estado.
5. Componentes del SSP.
6. Roles y responsabilidades de Seguridad Operacional del Estado.
7. Política de reportes de Seguridad Operacional del Estado.
8. Medición del desempeño de la Seguridad Operacional del Estado.
9. Medios para la participación de los empleados.
10. Comunicación de la Seguridad Operacional (interna y externa).
11. Entrenamiento en Seguridad Operacional.
12. Revisión por parte de la dirección del desempeño de la seguridad.

Nota: para una mejor orientación ver Apéndice 2

PCI SSP/SMS 1.095 Documentación del SSP.

1. La documentación debería definir, evidenciar y respaldar la política de Seguridad Operacional confirmando los objetivos identificados durante la fase de planificación, incluyendo un compromiso para:

   a) Cumplir los más altos estándares de seguridad operacional;

   b) Observar todos los reglamentos aplicables, así como las normas internacionales y las mejores prácticas;

   c) Proveer los recursos adecuados;

   d) Cumplir con la seguridad como responsabilidad primaria de todos los directores;

   e) Asegurar que la política es comprendida, implementada y mantenida en todos los niveles.

SECCION

2

SUBPARTE H

SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

PCI SSP/SMS 1.100 Estructura del SMS

Los proveedores de servicios deberían de contar con un SMS que por lo menos contenga los componentes y elementos recomendados por la OACI, el proveedor de servicios podrá agregar más requisitos.

1. Política y objetivos de Seguridad Operacional

1.1 Responsabilidad y compromiso de la dirección

1.2 Responsabilidades de seguridad operacional

1.3 Designación del personal clave de seguridad

1.4 Coordinación de la planificación de respuesta a la emergencia

1.5 Documentación del SMS

2. Gestión del riesgo de Seguridad Operacional

2.1 Identificación de peligros

2.2 Evaluación y mitigación del riesgo

3. Garantía de la Seguridad Operacional

3.1 Monitoreo y medición de la performance de la seguridad

3.2 Gestión del cambio

3.3 Mejora continua del SMS

4. Promoción de la Seguridad Operacional

4.1 Entrenamiento y educación

4.2 Comunicación de seguridad

SUBPARTE I

1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

PCI SSP/SMS 1.105 Responsabilidad y compromiso de la dirección

1. El proveedor de servicios debería definir una política de Seguridad Operacional de su organización que será firmada por el Ejecutivo Responsable de dicha organización.

2. El proveedor de servicios definirá la política de seguridad operacional de la organización que debería:

   a) Estar de acuerdo con los requisitos nacionales e internacionales y de la organización

   b) Reflejar el compromiso de la organización con respecto a la seguridad operacional;

   c) Asegurarse que la política de seguridad operacional sea constante y apoye al cumplimiento de todas las actividades de la organización.

   d) Se debería comunicar y transmitir a través de toda la organización.

   e) Incluir una declaración clara sobre la disposición de los recursos necesarios para la puesta en práctica de la política de seguridad operacional;

   f) Reflejar el compromiso relativo a la Seguridad Operacional

   g) Incluir una clara declaración de la dotación de los recursos humanos y financieros para su implementación.

   h) Ser comunicada, con visible endoso, a través de toda la organización;

   i) Incluir los procedimientos de informes de seguridad operacional;

   j) Indicar claramente qué tipos de comportamientos operacionales son aceptables y cuáles no, por lo tanto,

   k) Incluir las condiciones bajo las cuales una acción disciplinaria no sería aplicable;

   l) Si la empresa u organización tiene un sistema de calidad establecido, el proveedor de servicios debería asegurar que la política de calidad de la organización es consistente con y apoya totalmente las actividades del SMS.

3. La política de Seguridad Operacional debería incluir los siguientes objetivos y compromisos:

   a) El compromiso de la alta gerencia para implementar el SMS.
   b) El compromiso de un mejoramiento continúo del nivel de Seguridad Operacional.
   c) El compromiso de gestionar los riesgos de Seguridad Operacional.
   d) El establecimiento y mantenimiento de un SMS eficaz y eficiente;
   e) El compromiso de cumplir los estándares de seguridad operacional y los requisitos reglamentarios;
   f) El compromiso de mantener los niveles más altos de seguridad operacional;
   g) El compromiso para identificar, gestionar y mitigar los riesgos de seguridad operacional;
   h) El compromiso de alentar a todo el personal del proveedor de servicios a reportar los problemas de seguridad operacional que permitan llevar a cabo acciones correctivas en lugar de acciones punitivas;
   i) El compromiso de que todos los niveles de la administración estarán dedicados a la seguridad operacional;
   j) El compromiso de mantener comunicación abierta con todo el personal sobre la seguridad operacional;

k) El compromiso de que todo personal relevante participará en el proceso de toma de decisiones;

l) El compromiso de proveer instrucción necesaria para crear y mantener habilidades de liderazgo relacionadas con la seguridad operacional; y

m) El compromiso de que la seguridad de los empleados, pasajeros y proveedores será parte de la estrategia del proveedor de servicios.

n) Establecer las pautas claras del proceder aceptable; así como, el establecimiento de reglas e informes claros y disponibles que permitan a todo el personal involucrarse en los asuntos de seguridad operacional;

o) Identificar las responsabilidades de la administración y de los empleados con respecto a la eficiencia de la Seguridad Operacional.

4. La política de Seguridad Operacional debería también:

a) Ser revisada periódicamente para asegurar que permanece relevante y adecuada a la organización.

b) Asegurar la puesta en marcha de las acciones correctivas necesarias para mantener el desempeño de seguridad operacional acordado;

c) Prever el control continuo y la evaluación regular del desempeño de Seguridad Operacional;

d) Tener como objetivo la mejora continua del desempeño del SMS en su totalidad.

e) Tener una declaración sobre los objetivos de seguridad y normas de desempeño de la seguridad operacional, en relación a:

i) Los indicadores de desempeño de seguridad;

ii) Las metas de desempeño de seguridad y

iii) Los requisitos de seguridad.

5. El proveedor de servicios deber establecer los objetivos de Seguridad Operacional; estos objetivos deberían de estar relacionados con los indicadores de eficiencia, las metas y los requisitos de Seguridad Operacional establecidos por y con el Estado.

PCI SSP/SMS 1.110 Responsabilidades de seguridad operacional

1. El proveedor de servicios debería identificar y notificar al Estado el nombre del Ejecutivo Responsable, garante de dar cuentas a nombre del proveedor de servicios de las obligaciones estipuladas en las leyes del país y en este PCI

2. El Ejecutivo Responsable es solo una persona, identificable que, con independencia de otras funciones, debería tener la responsabilidad final por la implementación y el mantenimiento del SMS.

3. El Ejecutivo Responsable deber tener:

a) Total control de los recursos humanos requeridos para las operaciones, funciones o deberes autorizados para ser llevadas a cabo bajo el certificado de operación, permiso, aprobación dado o emitido por la Autoridad de Aviación Civil.

b) Total control de los recursos financieros necesarios para las operaciones autorizadas bajo el certificado de operación, permiso u otro tipo de aprobación emitida por el Estado

c) Total autoridad sobre las operaciones o funciones autorizadas para ser conducidas bajo el certificado de operación, permiso, aprobación dado o emitido por la Autoridad de Aviación Civil.

d) Responsabilidad directa para conducir los asuntos de la organización y

e) Responsabilidad final en los asuntos de Seguridad Operacional.

f) Asegurarse de que todo el personal cumpla con la política del SMS sobre la base de acciones correctivas y no punitivas;

g) Asegurarse de que la política de seguridad operacional sea comprendida, implementada y mantenida en todos los niveles de la organización;

h) Tener un conocimiento apropiado respecto al SMS y a los reglamentos de operación;

i) Asegurarse que los objetivos y las metas sean medibles y realizables;

j) La responsabilidad final sobre todos los aspectos de seguridad operacional de la organización.

k) Identificar las responsabilidades de seguridad operacional de todos los miembros del personal directivo, que serán independientes de sus funciones principales.

l) Documentar y comunicar las responsabilidades y atribuciones del personal directivo respecto a la seguridad operacional a toda la organización.

4. Las responsabilidades, la obligación de rendición de cuentas y las facultades deberían:

a) Estar documentadas;

b) Ser comunicadas a través de la organización;

c) Incluir una definición de los niveles de gestión con autoridad para tomar decisiones con respecto a la tolerabilidad de los riesgos de seguridad operacional

PCI SSP/SMS 1.115 Designación del personal clave de seguridad operacional

1. La organización debería identificar las responsabilidades de todos los miembros de la dirección, con independencia de otras funciones; así como, de los empleados con respecto al desempeño de la seguridad operacional del SMS.

2. El proveedor de servicios debería determinar al gerente (coordinador) de Seguridad Operacional, que debería ser un miembro de la administración, aceptable para la Autoridad de Aviación Civil con suficiente experiencia, competencia y calificación adecuada, quién en nombre del Ejecutivo responsable será el responsable individual y punto focal para la implantación y mantenimiento de un SMS efectivo.

3. El gerente (coordinador) de Seguridad Operacional puede ser la única persona que maneja la Oficina de servicios de seguridad o puede estar apoyado por personal adicional, principalmente analistas de datos de seguridad. Esto dependerá del tamaño de la organización y del carácter y complejidad de las operaciones que apoyan la prestación de servicios. Independientemente del tamaño de la Oficina de servicios de seguridad y el nivel de su personal,

a) Algunas de las funciones y responsabilidades del gerente de seguridad operacional deberían ser:

i) asegurar que los procesos necesarios para el funcionamiento efectivo del SMS, estén establecidos, implementados y que sean mantenidos por el proveedor de servicios;

ii) asegurar que la documentación de seguridad operacional refleje con precisión la situación actual del proveedor de servicios;

iii) proporcionar orientación y dirección para el funcionamiento efectivo del SMS del proveedor de servicios;

iv) fomentar el SMS a través de la organización;

v) presentar informes periódicos al ejecutivo responsable sobre la eficacia de la seguridad operacional y de cualquier oportunidad de mejora; y

vi) proveer asesoramiento independiente al ejecutivo responsable, a los ejecutivos de alto nivel, y a otros miembros del personal sobre cuestiones relacionadas con la seguridad operacional del

proveedor de servicios.

vii) realizar y facilitar la identificación de peligros y el análisis de gestión de riesgos;

viii) supervisar las medidas correctivas y evaluar sus resultados;

ix) mantener registros y documentación de seguridad

x) planificar y organizar la instrucción del personal en seguridad;

xi) proporcionar asesoramiento independiente sobre asuntos de seguridad

xii) Supervisar problemas de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones de la organización dirigidas a la prestación de servicios;

xiii) Coordinar y comunicarse (en nombre del Ejecutivo responsable) con la autoridad de vigilancia del Estado y otras agencias estatales según corresponda sobre problemas relacionados con la seguridad operacional; y

xiv) Coordinar y comunicarse (en nombre del Ejecutivo responsable) con agencias internacionales sobre cuestiones relativas a la seguridad operacional.

xv) acceso directo al directivo responsable y al personal directivo que corresponda;

xvi) realizar auditorías de seguridad operacional sobre cualquier aspecto de las actividades del proveedor de servicios; e

xvii) iniciar la investigación pertinente sobre cualquier accidente o incidente de conformidad con los procedimientos especificados en el manual de gestión de la seguridad operacional del proveedor de servicios.

b) Comité de seguridad operacional

i) Para proveer apoyo al gerente de seguridad operacional y asegurar que el SMS funcione correctamente, el proveedor de servicios designará un comité de seguridad operacional que se encuentre al más alto nivel de la función empresarial y esté conformado por:

(1) el directivo responsable que lo presidirá;

(2) el gerente de seguridad operacional que actuará como secretario;

(3) los gerentes de la organización; y

(4) personal de los departamentos claves de la organización.

ii) El comité de seguridad operacional debería tener las siguientes funciones y responsabilidades:

(1) asegurar que los objetivos y las acciones especificadas en el plan de seguridad operacional son alcanzadas en los plazos previstos.

(2) supervisar el desempeño de la seguridad operacional en relación a la política y objetivos planteados;

(3) monitorear la eficacia del plan de implantación del SMS en la organización;

(4) conocer y asesorar sobre cuestiones de seguridad operacional al directivo responsable;

(5) examinar el progreso de la organización respecto a los peligros identificados y medidas adoptadas a raíz de accidentes e incidentes;

(6) monitorear que cualquier acción correctiva necesaria, sea realizada de manera oportuna;

(7) formular recomendaciones para tomar acciones y eliminar los peligros identificados de la seguridad operacional;

(8) examinar los informes de auditorías internas de seguridad operacional;

(9) examinar y aprobar las respuestas a las auditorías y medidas adoptadas;

(10) ayudar a identificar peligros y defensas;

(11) preparar y examinar informes sobre seguridad operacional para el directivo responsable;

(12) asegurar que los recursos apropiados sean asignados para la ejecución de las acciones acordadas;

(13) monitorear la eficacia de la vigilancia operacional de las operaciones subcontratadas por la organización; y

(14) proveer dirección y orientación estratégica al grupo de acción de seguridad operacional.

c) Grupo de acción de seguridad operacional (SAG)

i) Para apoyar en la evaluación de los riesgos que enfrente la organización y sugerir los métodos para mitigarlos, el directivo responsable designará un grupo de acción de seguridad operacional, el que estará conformado por:

(1) los gerentes;

(2) los supervisores; y

(3) el personal del área funcional apropiada.

ii) El grupo de acción de seguridad operacional debería de tener como mínimo las siguientes responsabilidades:

(1) supervisar la seguridad operacional dentro de las áreas funcionales;

(2) asegurar que cualquier acción correctiva sea realizada de forma oportuna;

(3) resolver los peligros identificados;

(4) llevar a cabo evaluaciones de seguridad operacional antes que el proveedor de servicios implemente cambios operacionales, a fin de determinar el impacto que pueden tener estos cambios en la seguridad operacional;

(5) implantar los planes de acciones correctivas;

(6) asegurar la eficacia de las recomendaciones previas de seguridad;

(7) promover la participación de todo el personal en la seguridad operacional; e

(8) informar y aceptar dirección estratégica del comité de seguridad operacional de la organización

4. El proveedor de servicios debería determinar las responsabilidades en Seguridad Operacional de todos los miembros de las gerencias, sin importar otras responsabilidades.

5. El proveedor de servicios debería establecer la estructura organizacional necesaria para la implementación y mantenimiento del SMS. Las posiciones, responsabilidades y autoridad deberían ser definidas, documentadas y comunicadas a lo largo de la organización.

PCI SSP/SMS 1.120 Coordinación de la planificación de respuesta a la emergencia

El proveedor de servicios debería desarrollar, mantener y coordinar apropiadamente, un plan de respuesta ante emergencias (ERP), detallando por escrito las acciones que deberían adoptarse después de un accidente y designa los responsables de cada acción, que asegure:

1. Una transición ordenada y eficiente de las operaciones normales a las operaciones de emergencia.

2. Delegación de la autoridad durante una emergencia.

3. Asignación de las responsabilidades en la emergencia.

4. Autorización para el personal clave para las acciones contenidas en el plan.

5. Coordinación de los esfuerzos para enfrentar la emergencia (interno y externo).

6. Continuación segura de las operaciones, o retorno a las operaciones normales tan pronto sea posible.

PCI SSP/SMS 1.125 Documentación del SMS

1. El proveedor de servicios debería desarrollar y mantener la documentación del SMS en forma electrónica o en papel, en donde todas las actividades de la gestión de seguridad operacional deberían estar documentadas y ser visibles, convirtiendo la documentación en un principio esencial del SMS. La documentación SMS debería incluir al menos lo siguiente:

   a) Formularios de notificación de peligros

   b) Líneas de rendición de cuentas

   c) Responsabilidad y facultad relativas a la gestión de la seguridad operacional

   d) Estructura de la organización de gestión de la seguridad operacional, y

   e) El enfoque de la organización, mediante el manual de gestión de la seguridad operacional

2. El proveedor de servicios debería como parte de la documentación:

   a) Desarrollar y mantener un Manual de Gestión de la Seguridad Operacional (SMSM), el cual debería ser para uso de todo el personal involucrado con la Seguridad Operacional, comunicar la aproximación de la organización a la Seguridad Operacional a lo largo de la organización y también para que la Autoridad de Aviación Civil conozca de primera mano como el proveedor de servicios gestiona la seguridad operacional.

   b) El Manual debería contener los aspectos relevantes del SSP/SMS, incluyendo la política de seguridad, objetivos, procedimientos y responsabilidades individuales en materia de seguridad operacional del proveedor de servicios.

   c) El Manual también documentará todos los aspectos del SMS y su contenido debería por lo menos contener lo siguiente:

      i) Alcance del sistema de gestión de la seguridad operacional;

      ii) Política y objetivos de seguridad operacional;

      iii) Responsabilidades (rendición de cuentas) de seguridad operacional;

      iv) Personal clave de seguridad operacional;

      v) Procedimientos de control de la documentación;

      vi) Coordinación de la planificación de respuestas ante emergencias;

      vii) Planes de identificación de peligros y gestión de riesgos de seguridad operacional;

      viii) Supervisión de la eficacia (garantía) de la seguridad operacional;

      ix) Auditoría (monitoreo) de la seguridad operacional;

      x) Procedimientos para la gestión del cambio;

      xi) Promoción de la seguridad operacional; y

      xii) Control de las actividades contratadas.

d) El proveedor de servicios establecerá y mantendrá en el manual de gestión de la seguridad operacional:

i. los procedimientos de reporte de seguridad operacional relacionados con el desempeño de la seguridad operacional y monitoreo; y

ii. claramente indicará qué tipos de comportamientos operacionales son aceptables o inaceptables, incluyendo las condiciones bajo las cuales se considerará la inmunidad respecto a las medidas disciplinarias.

INTENCIONALMENE EN BLANCO

SUBPARTE J

2. GESTIÓN DEL RIESGO DE SEGURIDAD OPERACIONAL

PCI SSP/SMS 1.130 Identificación de peligros

1. La gestión de los riesgos de seguridad operacional inicia con la descripción del sistema como base para la identificación de peligros, convirtiéndose en la primera fase de un protocolo de recoger, registrar, adoptar medidas y generar retroalimentación sobre peligros y riesgos de seguridad en las operaciones.

2. La organización debería desarrollar y mantener un proceso formal que asegure que las amenazas en las operaciones sean identificadas. La identificación de peligros se debería basar en una combinación de métodos reactivos, proactivos y predictivos.

    a) Ejemplo de técnicas de enfoque estructurado en la identificación de peligros

        i) Listas de verificación: Examen de la experiencia y datos disponibles del sistema similares y establecimiento de una lista de verificación de peligros. Los sectores potencialmente peligrosos exigirán mayor evaluación.

        ii) Examen de grupo**:** Pueden utilizarse sesiones de grupos para examinar la lista de verificación de peligros, estudiar más ampliamente dichos peligros o llevar a cabo un detallado análisis del escenario.

3. Para los peligros identificados, el proveedor de servicios debería desarrollar y mantener un sistema de recolección y procesamiento de datos para el almacenamiento de peligros, su análisis y respectiva evaluación y mitigación del riesgo.

4. Cada peligro identificado a través del proceso de identificación de peligros descrito en el punto (2) anterior debería ser evaluado por su tolerabilidad a riesgo en términos de probabilidad y severidad de ocurrencia que asegure la eliminación y o mitigación a un nivel aceptable.

    a) Ejemplo de cómo funcionaria una identificación de peligros en una organización:

        i) Las sesiones de identificación de peligros exigen una gama de personal operacional y técnico experimentado y normalmente se realizan en forma de debates de grupo dirigidos. Un facilitador familiarizado con las técnicas de generar ideas en forma grupal (brainstorming) debería dirigir las sesiones del grupo. El gerente de seguridad, si está designado, normalmente cumpliría esta función. Si bien el uso de sesiones de grupo se trata aquí en el contexto de la identificación de peligros, el mismo grupo trataría también la evaluación de la probabilidad y gravedad de los riesgos de seguridad operacional de las consecuencias de los peligros que ha identificado.

        ii) En la evaluación de peligros se deberían tener en cuenta todas las posibilidades, desde la más pequeña hasta la más probable. Hay que prever adecuadamente las “peores” condiciones, pero también es importante que los peligros que se incluyan en el análisis final sean peligros “creíbles”.

        iii) Los procesos de identificación de peligros deberían incluir los siguientes pasos:

            (1) Reportar los peligros, eventos o preocupaciones de Seguridad Operacional;

            (2) Recolección y archivo de datos de Seguridad Operacional;

            (3) Análisis de datos de Seguridad Operacional;

            (4) Distribución de la información proveniente de los datos de Seguridad Operacional.

5. La organización debería definir los niveles de tolerabilidad y tener la autoridad para tomar decisiones de mitigación de riesgos.

6. Un proveedor de servicios, como parte del SMS, debería desarrollar y mantener un proceso formal para la investigación de sucesos que no requieren ser investigados por el Estado o reportados a la autoridad de vigilancia.

PCI SSP/SMS 1.135 Evaluación y mitigación de riesgos

1. El proveedor de servicios debería desarrollar y mantener un proceso formal que asegure el análisis (probabilidad y severidad del evento), la evaluación (tolerabilidad) y la mitigación de los riesgos de seguridad operacional de los peligros en las operaciones evaluadas.

    a) Cuando se tienen identificados los peligros, se deberían evaluar (analizar) los riesgos de las posibles consecuencias de esos peligros que se ha determinado que amenazan la capacidad de la organización, tomando en cuenta dos factores importantes, tales como:

        i) la probabilidad de que el suceso o condición perjudicial ocurra, y

        ii) la gravedad o severidad del suceso o condición, en caso de que ocurra

2. Cuando ya han sido evaluados los riesgos de seguridad operacional, se debería realizar la eliminación o mitigación a nivel ALARP.

    a) El proveedor de servicios debería definir los niveles de gestión, para tomar las decisiones sobre la tolerabilidad de los riesgos de seguridad operacional.

    b) El proveedor de servicios debería definir los controles de seguridad operacional para cada riesgo determinado como tolerable.

    c) Ejemplos de controles de riesgo de seguridad operacional, tomando en cuenta las tres defensas tradicionales en la aviación (tecnología, reglamentación y entrenamiento):

        i) Procedimientos adicionales o modificados,

        ii) Nuevos controles de supervisión,

        iii) Cambios en la instrucción, y

        iv) Equipo adicional o modificado

3. Después de diseñado los controles de los riesgos de seguridad operacional, pero antes de que el sistema se coloque “en línea”, debería realizarse una evaluación para ver si los controles no introducen nuevos peligros al sistema.

4. Ahora, el sistema debería de estar listo para la introducción o reintroducción operacional, suponiendo que los controles de los riesgos de seguridad operacional se consideran aceptables.

INTENCIONALMENTE EN BLANCO

SUBPARTE K

3. GARANTÍA DE LA SEGURIDAD OPERACIONAL

PCI SSP/SMS 1.140 Monitoreo y medición de la performance de la seguridad

Los requisitos de la OACI introducen el concepto de los Niveles Aceptables de Seguridad Operacional (ALoS) como una manera de medir el rendimiento de la Seguridad Operacional de un SSP y el concepto del rendimiento de la Seguridad Operacional como una manera de medir el resultado de Seguridad Operacional de un proveedor de servicios.

1. Un proveedor de servicios debería desarrollar y mantener un proceso que asegure que el control de riesgos a la Seguridad Operacional desarrollado como consecuencia de las actividades de identificación de peligros y gestión del riesgo alcancen los objetivos pretendidos.

2. La información para la eficacia y la supervisión de la seguridad operacional podría proceder de varias fuentes incluyendo auditorías formales y evaluación, investigaciones de sucesos relacionados con la seguridad, supervisión continua de las actividades cotidianas relacionadas con la prestación de servicios y aportes de los empleados a través de los sistemas de notificación de peligros.

    a) Fuentes de información para la supervisión y medición de la eficacia de la seguridad operacional podrían comprender:

        i) Informes sobre peligros

        ii) estudios de seguridad operacional;

        iii) revisiones de seguridad operacional;

        iv) reportes de seguridad operacional

        v) investigaciones internas de seguridad operacional, que incluyan eventos que no requieren ser reportados a la Autoridad de Aviación Civil.

        vi) auditorías de seguridad; (podrán también ser independientes)

            (1) El proveedor de servicios podrá contratar a otra organización o a una persona con conocimiento técnico aeronáutico apropiado y con experiencia demostrada en auditorias, que sean aceptables a la AAC, para realizar las auditorias independientes de seguridad operacional requeridas en el párrafo (iv) de esta sección.

            (2) El proveedor de servicios establecerá, como parte del sistema de supervisión y medición del desempeño de la seguridad operacional, un sistema de retroalimentación que asegure que el personal de gestión del SMS tome las medidas preventivas y correctivas apropiadas y oportunas en respuesta a los informes resultantes de las auditorias independientes.

            (3) Los objetivos de estas auditorías es asegurarse de que los procedimientos para las auditorias tanto propias como independientes cumplan con lo siguiente:

                (a) niveles apropiados de personal,

                (b) monitorear el cumplimiento de los procedimientos, instrucciones y requisitos reglamentarios,

                (c) determinar si los procedimientos de operación son adecuados;

                (d) nivel de competencia, entrenamiento y mantenimiento satisfactorio para:

                    (i) operar el equipamiento y las facilidades

(ii) mantenimiento de su nivel de performance

vii) encuestas de seguridad; y

examinar áreas particulares o procesos de una operación especifica, tales como:

(1) Áreas con problemas o cuellos de botella en operaciones diarias

(2) Percepciones y opiniones del personal operativo

(3) Áreas de desacuerdo, discordia o confusión

Ejemplos de encuestas de seguridad:

(1) Listas de verificación

(2) Cuestionarios

(3) Entrevistas confidenciales informales

viii) investigaciones internas de seguridad

estas incluyen eventos que no requieren ser investigados o reportados al Estado, por ejemplo:

(1) Turbulencia en vuelo (operaciones de vuelo)

(2) Congestión de la frecuencia (ATC)

(3) Falla de material (mantenimiento)

(4) Operaciones de vehículos en la rampa (aeródromo)

b) Tipos de sistemas de notificación:

i) notificación obligatoria;

ii) notificación voluntaria; y

iii) notificación confidencial

3. El proceso de seguimiento de la Seguridad Operacional se debería aplicar a un SMS si las actividades y/o operaciones son cumplidas o incumplidas.

4. El proveedor de servicios, como parte de las actividades de seguimiento de la Seguridad Operacional, debería desarrollar y mantener los medios necesarios para verificar la eficacia de la Seguridad Operacional de la organización en comparación con las políticas y objetivos de Seguridad Operacional establecidos por el Estado y validar la efectividad de los controles de riesgos implementados.(medición del rendimiento de la Seguridad Operacional del proveedor de servicios)

5. El procedimiento de reportes de Seguridad Operacional debería sentar aquellas condiciones bajo las cuales se pueden considerar la inmunidad de la acción disciplinaria.

6. El proveedor de servicios debería, como parte de las actividades de aseguramiento del SMS, para identificar las causas de baja eficiencia del SMS, determinar las implicaciones en sus operaciones, y eliminar tales causas.

PCI SSP/SMS 1.145 Gestión del cambio

1. El proveedor de servicios, debería como parte de las actividades del aseguramiento de la Seguridad Operacional del SMS, desarrollar y mantener un proceso formal para gestionar el cambio.

2. El proceso formal de gestión del cambio debería:

   a) Identificar cambios dentro de la organización que puedan afectar los procesos y servicios establecidos.

   b) Describir los arreglos para asegurar la eficiencia de la Seguridad Operacional antes de implementar los cambios.

   c) Eliminar o modificar los controles del riesgo de la Seguridad Operacional que ya no se necesiten debido a cambios en el ambiente operacional.

3. Toda organizaciones de la aviación experimenta cambios permanentes debido a expansión, introducción de nuevos equipos o procedimientos,

   a) Los cambios pueden:

      i) Introducir nuevos peligros,

      ii) Impactar la utilidad de la mitigación del riesgo, y

      iii) Afectar la eficacia de la mitigación del riesgo.

4. Se podría tener dos tipos de cambios:

   a) Externos, e

   b) Internos

      i) Ejemplos de cambios externos:

         (1) Cambios de los requisitos,

         (2) Seguridad aeroportuaria,

         (3) Reorganización del control de tránsito aéreo,

      ii) Ejemplos de cambios internos:

         (1) Cambios de administración,

         (2) Equipamiento nuevo,

         (3) Nuevos procedimientos.

PCI SSP/SMS 1.150 Mejora continua

1. El proveedor de servicios debería como parte de las actividades del aseguramiento de la Seguridad Operacional del SMS, desarrollar y mantener procesos formales para alcanzar el mejoramiento continuo del SMS, identificando las causas de la baja eficiencia del SMS, determinar las implicaciones en sus operaciones, y mitigar o eliminar tales causas.

2. El mejoramiento continuo del SMS de un proveedor de servicios debería incluir:

   a) Evaluaciones proactivas de las facilidades, equipo, documentación y procedimientos, para verificar la efectividad de las estrategias para el control y mitigación de los riesgos de la Seguridad Operacional. y

   b) Evaluación proactiva de la performance individual para verificar el cumplimiento de las responsabilidades de Seguridad Operacional.

3. El proveedor de servicios alcanzará la mejora continua a través de una evaluación reactiva para verificar la eficacia de los sistemas de control y mitigación de los riesgos, por ejemplo, a través de información obtenida de investigación de accidentes, incidentes y eventos significativos.

INTENCIONALMENTE EN BLANCO

SUBPARTE L

4. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

PCI SSP/SMS 1.155 Entrenamiento de la seguridad operacional

1. El proveedor de servicios debería desarrollar y mantener un programa de entrenamiento de seguridad operacional que asegure que el personal está entrenado y es competente para llevar a cabo los deberes del SMS.

2. El alcance del la capacitación de Seguridad Operacional debería ser apropiado de acuerdo al nivel de involucramiento de cada individuo dentro del SMS.

3. El gerente (coordinador) de seguridad operacional debería, conjuntamente con el departamento de personal, revisar las descripciones de las funciones de todo el personal, e identificar aquellas posiciones que tengan responsabilidades de seguridad operacional, tales como:

   a) Personal operativo,

   b) Gerentes y supervisores,

   c) Directores,

   d) Ejecutivo responsable.

4. Instrucción y educación

   a) El Ejecutivo Responsable debería recibir entrenamiento (concientización) respecto a:

      i) Política y objetivos de Seguridad operacional,

      ii) Responsabilidades y funciones del SMS

      iii) Gestión de riesgo de seguridad operacional

      iv) Garantía de la Seguridad Operacional.

Nota: este entrenamiento no debería de exceder de cuatro horas.

   b) Considerando que es esencial que el personal directivo comprenda el SMS, el proveedor de servicios debería proveer capacitación a este personal en lo siguiente:

      i) principios del SMS;

      ii) sus obligaciones y responsabilidades; y

      iii) aspectos legales pertinentes, por ejemplo: sus respectivas responsabilidades ante la ley.

   c) El proveedor de servicios proveerá instrucción al gerente de seguridad operacional, por lo menos en los siguientes ítems:

      i) familiarización con las diferentes flotas, tipos de operación, rutas, etc.;

      ii) comprensión de la función de la actuación humana en las causas de accidentes y la prevención de los mismos;

      iii) funcionamiento de los SMS;

      iv) investigación de accidentes e incidentes;

      v) gestión de crisis y planificación de la respuesta ante emergencias;

vi) promoción de la seguridad operacional;

vii) técnicas de comunicación;

viii) gestión de la base de datos de seguridad operacional;

ix) instrucción o familiarización especializada en gestión de recursos de la tripulación (CRM), FDA, LOSA y NOSS.

d) El currículo de instrucción inicial de seguridad operacional para todo el personal del proveedor de servicios cubrirá por lo menos los siguientes ítems:

i) principios básicos de gestión de la seguridad operacional;

ii) filosofía, políticas y normas de seguridad operacional de la organización (incluido el enfoque de la organización con respecto a las medidas disciplinarias y a los problemas de seguridad operacional, la naturaleza integral de la gestión de la seguridad operacional, la toma de decisiones sobre gestión de riesgos, la cultura de seguridad operacional, etc.);

iii) importancia de observar la política de seguridad operacional y los procedimientos que forman parte del SMS;

iv) organización, funciones y responsabilidades del personal con relación a la seguridad operacional;

v) antecedentes de seguridad operacional de la organización, incluidas las debilidades sistemáticas;

vi) metas y objetivos de seguridad operacional de la organización;

vii) procesos de identificación de peligros;

viii) procesos de evaluación y mitigación de riesgos;

ix) monitoreo y medición del desempeño de la seguridad operacional;

x) gestión del cambio;

xi) mejora continua del sistema de gestión de la seguridad operacional;

xii) programas de gestión de la seguridad operacional de la organización (p. ej., sistemas de notificación de incidentes, auditoría de la seguridad de las operaciones de ruta (LOSA), estudios sobre seguridad operacional en las operaciones normales (NOSS));

xiii) requisito de evaluación interna continua del desempeño de la seguridad operacional en la organización (p. ej., encuestas a empleados, auditorías y evaluaciones de seguridad operacional);

xiv) notificación de accidentes, incidentes y peligros percibidos;

xv) líneas de comunicación para los aspectos de seguridad operacional;

xvi) retorno de la información y métodos de comunicación para la difusión de la información de seguridad operacional;

xvii) auditorías de la seguridad operacional;

xviii) plan de respuesta ante emergencias; y

xix) promoción de la seguridad operacional y difusión de la información.

e) Además del currículo de instrucción inicial, el proveedor de servicios proveerá instrucción al personal operativo en los siguientes temas:

i) procedimientos para notificar accidentes e incidentes;

ii) peligros particulares que enfrenta el personal de operaciones;

iii) procedimientos para la notificación de peligros;

iv) iniciativas específicas de seguridad operacional, tales como:

(1) programa de análisis de datos de vuelo (FDA);

(2) programa LOSA;

(3) programa NOSS. y

(4) otros.

5. La instrucción y educación en seguridad operacional debería comprender lo siguiente:

   a) Un proceso documentado para identificar requisitos de instrucción;

   b) Un proceso de validación que mida la efectividad de la instrucción;

   c) Instrucción inicial (seguridad general) específica de la tarea;

   d) Adoctrinamiento/instrucción inicial que incorpora el SMS, incluyendo factores humanos y factores de organización; e

   e) Instrucción periódica en seguridad operacional.

6. El proveedor de servicios debería documentar los requisitos y actividades de instrucción para cada área de actividad dentro de la organización.

7. El proveedor de servicio debería elaborar un archivo de instrucción para cada empleado, incluyendo los administradores, para ayudar a identificar y hacer el seguimiento de los requisitos de instrucción del empleado y verificar que el personal ha recibido la instrucción prevista.

PCI SSP/SMS 1.160 Comunicación de la seguridad operacional

1. El proveedor de servicios debería desarrollar y mantener medios formales de recolección, grabación, actuación y generación de retroalimentación sobre los peligros de las operaciones, que combinen métodos reactivos, proactivos y predictivos de datos de Seguridad Operacional.

2. El proveedor de servicios debería desarrollar y mantener actividades de comunicación para crear un ambiente donde los objetivos de Seguridad Operacional puedan ser alcanzados.

3. El proveedor de servicios, como parte de sus actividades de promoción de la Seguridad Operacional, debería desarrollar y mantener medios formales para la comunicación de Seguridad Operacional con el objetivo de:

   a) Asegurar que el personal tiene los conocimientos necesarios del SMS

   b) Transmitir información crítica de Seguridad Operacional.

   c) Explicar el porqué fueron tomadas acciones particulares de Seguridad Operacional.

   d) Explicar el porqué procedimientos de Seguridad Operacional se introdujeron o cambiaron.

   e) Transmitir cualquier información que pueda ser útil,

   f) Asegurar el desarrollo y el mantenimiento de una cultura positiva de seguridad operacional en la organización;

4. En virtud de que la comunicación es un pilar esencial para el desarrollo y el mantenimiento de un SMS, algunos ejemplos de comunicación de Seguridad Operacional en la organización podrían ser:

   a) Manual de sistemas de gestión de la seguridad operacional (SMSM),

   b) Procesos y procedimientos de Seguridad Operacional,

   c) Boletines informativos, avisos y anuncios,

   d) Sitio web o correo electrónico.

SUBPARTE M

PLAN DE IMPLEMENTACION

PCI SSP/SMS 1.165 Plan de implementación del SMS

El plan de implementación del SMS, debería definir el enfoque de la organización respecto de la gestión de la seguridad operacional, en el cual se debería describir de qué forma la organización logrará sus objetivos de seguridad operacional y cómo va a satisfacer cualquier requisito reglamentario o de otro tipo; ya sea nuevo o revisado de seguridad operacional. El plan de implantación del SMS, puede consistir en más de un documento, detallando las medidas que han de adoptarse, por quienes y según que cronogramas.

1. Dependiendo del tamaño de la organización y la complejidad de sus operaciones, el plan de implantación del SMS puede ser elaborado por una persona, o por un grupo de planificación que comprenda una base de experiencia apropiada.

2. Este grupo (o persona) de planificación debería reunirse regularmente con la administración superior para evaluar el progreso del plan de implantación y para que se le asignen recursos (incluyendo el tiempo para las reuniones), conmensurables con la tarea que debe realizar.

3. Generalmente, el contenido del plan de implementación del SMS comprende:

   a) Políticas y objetivos de seguridad operacional,

   b) descripción del sistema;

   c) análisis de las carencias;

   d) componentes del SMS;

   e) funciones y responsabilidades de seguridad operacional;

   f) política de notificación de peligros;

   g) medios para la participación de los empleados;

   h) medición de la eficacia de la seguridad;

   i) comunicación de seguridad;

   j) instrucción de seguridad; y

   k) revisión por la administración de la eficacia de la seguridad operacional

4. El plan de implementación del SMS, al estar completado debería ser endosado por la administración superior (ejecutivo responsable).

5. El proveedor de servicios debería de implementar el plan en cuatro fases y podría tener una duración para la implementación de uno a cuatro años. Las fases en mención deberían de ser las siguientes:

   a) Fase I – Planificación de la implementación del SMS,

   b) Fase II – Procesos reactivos de gestión de la seguridad operacional,

   c) Fase III – Procesos proactivos y predictivos de gestión de la seguridad operacional, y

   d) Fase IV – Garantía de la seguridad operacional.

PCI SSP/SMS 1.170 Fases de implementación del sistema de gestión de la seguridad operacional (SMS)

Los proveedores de servicios deberían utilizar cuatro fases (como lo recomienda OACI) para la implementación del sistema de gestión de la seguridad operacional (SMS). Cada fase debería tener una duración no mayor a un año.

A continuación se detallan las actividades que deberían de ser cumplidas en cada una de las fases:

PCI SSP/SMS 1.175 Fase I - Planificación de la implementación del SMS

En esta fase el proveedor de servicios presentará una propuesta de cómo los requisitos del SMS serán logrados e integrados a las actividades diarias de su organización, y un marco de responsabilidades para la implementación del SMS.

Además en esta fase, el proveedor de servicios debería:

1. Identificar al ejecutivo responsable y determinar las responsabilidades de seguridad operacional de los gerentes (elementos 1.1 y 1.2 de la estructura SMS recomendada por OACI);
2. Identificar dentro de la organización a la persona o al grupo de planificación que será responsable de implementar el SMS (elemento 1.5 de la estructura SMS recomendada por OACI);
3. Describir el sistema de la organización (elemento 1.5 de la estructura SMS recomendada por OACI);
4. Realizar un análisis de carencias de los recursos existentes en la organización en relación con los requisitos nacionales e internacionales para el establecimiento del SMS (elemento 1.5 de la estructura SMS recomendada por OACI);
5. Elaborar un plan de implementación del SMS que explique cómo la organización implementará el SMS sobre la base de los requisitos nacionales y las normas y métodos recomendados internacionales, la descripción del sistema y los resultados del análisis de carencias (elemento 1.5 de la estructura SMS recomendada por OACI);
6. Coordinar el plan de respuesta de emergencias con las organizaciones con las que existe relación durante la prestación de los servicios (elemento 1.4 de la estructura recomendada por OACI);
7. Elaborar documentación relativa a la política y a los objetivos de seguridad operacional (elemento 1.5 de la estructura SMS recomendada por OACI); y
8. Elaborar y establecer los medios de comunicación de seguridad operacional (elemento 4.2 de la estructura SMS recomendada por OACI).

PCI SSP/SMS 1.180 Fase II - Procesos reactivos de gestión de la seguridad operacional

Finalizando la fase I, la organización debería de estar en condiciones de realizar análisis coordinados de la seguridad operacional, basados en la información obtenida mediante métodos reactivos de recolección de datos de seguridad operacional.

En esta fase el proveedor de servicios debería de realizar las siguientes actividades y de esa forma podría satisfacer las expectativas de la Autoridad de Aviación Civil:

1. Poner en práctica aspectos esenciales que involucren la gestión de riesgos de seguridad operacional basadas en procesos reactivos (elementos 2.1 y 2.2 de la estructura SMS recomendada por OACI);
2. Proporcionar instrucción pertinente a los componentes del plan de implementación del SMS y a la gestión de riesgos de seguridad operacional basándose en procesos reactivos. (elemento 4.1 de la estructura SMS recomendada por OACI);
3. Elaborar documentación relativa a los componentes del plan de implementación del SMS y a la gestión de riesgos de seguridad operacional basándose en procesos reactivos (elemento 1.5 de la estructura SMS recomendada por OACI);
4. Desarrollar y mantener medios formales para las comunicaciones de seguridad operacional (elemento 4.2 de la estructura SMS recomendada por OACI);

PCI SSP/SMS 1.185 Fase III – Procesos proactivos y predictivos de gestión de la seguridad operacional

En esta fase se debería estructurar los procesos de gestión de la seguridad operacional orientados al futuro y de esta forma estar en condiciones de realizar análisis de seguridad operacional coordinados sobre la base la información obtenida a través de métodos reactivos, proactivos y predictivos de recolección de datos:

1. implementar procesos proactivos y predictivos de la gestión de riesgos de seguridad operacional, (elementos 2.1 y 2.2 de la estructura SMS recomendada por OACI);
2. Proveer entrenamiento relativo a los procesos proactivos y predictivos de la gestión de riesgos de seguridad operacional (elemento 4.1 de la estructura SMS recomendada por OACI);
3. Elaborar la documentación relacionada con los procesos proactivos y predictivos de la gestión de riesgos de seguridad operacional (elemento 1.5 de la estructura SMS recomendada por OACI);
4. Desarrollar y mantener medios formales para las comunicaciones de seguridad operacional (elemento 4.2 de la estructura SMS recomendada por OACI);

PCI SSP/SMS 1.190 Fase IV – Garantía de la seguridad operacional

En esta fase se debería evaluar la garantía de la seguridad operacional mediante la implementación de supervisión periódica, retroalimentación y medidas correctivas continuas para mantener la efectividad de los controles de riesgos de seguridad en situaciones operacionales cambiantes y de esta forma que los procesos de gestión y análisis de la información de seguridad operacional garanticen la sostenibilidad de los procesos de organización seguros, a lo largo del tiempo y durante períodos de cambio en el entorno operacional.

El proveedor de servicios debería:

1. Desarrollar y ponerse de acuerdo sobre:
   a) Los indicadores de desempeño de seguridad operacional,
   b) Las metas de desempeño de seguridad operacional, y
   c) La mejora continua del SMS.

   (Elementos 1.1, 3.1 y 3.3 de la estructura SMS recomendada por OACI)
2. Proveer entrenamiento relacionado con la garantía de la seguridad operacional (elemento 4.1 de la estructura SMS recomendada por OACI);
3. Desarrollar la documentación relativa a la garantía de la seguridad operacional (elemento 4.1 de la estructura SMS recomendada por OACI); y
4. Desarrollar y mantener medios formales para las comunicaciones de seguridad operacional (elemento 4.2 de la estructura SMS recomendada por OACI);

INTENCIONALMENTE EN BLANCO

SECCION 3

APENDICES

Apéndice 1

MARCO ESTRUCTURAL PARA EL PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

En este apéndice se presenta un marco estructural del programa Estatal de seguridad operacional (SSP). El marco está compuesto por los siguientes cuatro componentes y once elementos:

1. Política y objetivos de seguridad operacional de los Estados

1.1 Marco legislativo estatal de la seguridad operacional
1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
1.3 Investigación de accidentes e incidentes
1.4 Política de cumplimiento

2. Gestión de riesgos de seguridad operacional por los Estados

2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

3. Garantía de la seguridad operacional por los Estados

3.1 Vigilancia de la seguridad operacional
3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención

4. Promoción de la seguridad operacional por los Estados

4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

A continuación se encuentra una breve descripción de cada elemento.

1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL DE LOS ESTADOS

1.1 Marco legislativo estatal de la seguridad operacional

El Estado ha promulgado un marco legislativo nacional de seguridad operacional y reglamentos específicos de conformidad con normas nacionales e internacionales, que definen la forma en que el Estado llevará a cabo la gestión de la seguridad operacional en el Estado. Esto incluye la participación de las organizaciones de aviación estatales en actividades específicas relacionadas con la gestión de la seguridad operacional en el Estado, y la creación de los roles, las responsabilidades y las relaciones de dichas organizaciones. El marco legislativo de la seguridad operacional y la reglamentación específica se examinan periódicamente para asegurar que sigan siendo pertinentes y apropiados para el Estado.

1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional

El Estado ha identificado, definido y documentado los requisitos, las responsabilidades y la rendición de cuentas relativas a la creación y el mantenimiento del SSP. Esto incluye las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional del Estado. Incluye además una declaración clara sobre la provisión de los recursos necesarios para la implantación del SSP.

1.3 Investigación de accidentes e incidentes

El Estado ha establecido un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes, y no la asignación de culpa o responsabilidad. Estas investigaciones respaldan la gestión de la seguridad operacional en el Estado. En el marco del SSP, el Estado mantiene la independencia de la organización de investigación de accidentes e incidentes respecto de otras organizaciones estatales de aviación.

1.4 Política de cumplimiento

El Estado ha promulgado una política de cumplimiento que establece las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional, y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, a satisfacción de la autoridad estatal competente. La política de cumplimiento establece además las condiciones y circunstancias en las cuales las desviaciones con respecto de la seguridad operacional deberían abordarse mediante procedimientos establecidos en cuanto a cumplimiento.

2. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL POR LOS ESTADOS

2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios

El Estado ha establecido los controles que rigen la forma en que los proveedores de servicios detectarán los peligros y gestionarán los riesgos de seguridad operacional. Esto incluye los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para los SMS de los proveedores de servicios. Los requisitos, reglamentos específicos de funcionamiento y políticas de implantación se examinan periódicamente para asegurar que sigan siendo pertinentes y apropiados para los proveedores de servicios.

2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

El Estado ha acordado con cada proveedor de servicios la actuación de sus SMS respecto de la seguridad operacional. La eficacia de la seguridad operacional acordada de los SMS de cada proveedor de servicios se examina periódicamente para asegurar que siga siendo pertinente y apropiada para los proveedores de servicios.

3. GARANTÍA DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS

3.1 Vigilancia de la seguridad operacional

El Estado ha establecido mecanismos para asegurar la supervisión eficaz de los ocho elementos críticos de la función de vigilancia de la seguridad operacional. El Estado ha creado además mecanismos para garantizar que la detección de peligros y la gestión de riesgos de seguridad operacional por los proveedores de servicios se ajusten a los controles reguladores establecidos (requisitos, reglamentos de funcionamiento específicos y políticas de implantación). Estos mecanismos incluyen inspecciones, auditorías y encuestas para asegurar que los controles reguladores de los riesgos de seguridad operacional se integren apropiadamente en los SMS de los proveedores de servicios, que se lleven a la práctica conforme a su diseño, y que tengan el efecto previsto en los riesgos de seguridad operacional.

3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional

El Estado ha establecido mecanismos para asegurar la captura y almacenamiento de datos sobre peligros y riesgos de seguridad operacional a nivel tanto individual como global. El Estado ha establecido además mecanismos para preparar información a partir de los datos almacenados y para intercambiar activamente información sobre seguridad operacional con los proveedores de servicios y otros Estados, según corresponda.

3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención

El Estado ha establecido procedimientos para priorizar las inspecciones, auditorías y encuestas relacionadas con los elementos que plantean más preocupación o que requieren mayor atención, según lo detectado en el análisis de los datos sobre peligros, sus consecuencias en las operaciones y los riesgos de seguridad operacional evaluados.

4. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS

4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional

El Estado proporciona instrucción y fomenta el conocimiento y el intercambio de información relacionada con la seguridad operacional para respaldar, en las organizaciones estatales de aviación, el desarrollo de una cultura organizativa que promueva SSP eficaces.

4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional

El Estado proporciona educación y promueve el conocimiento con respecto a los riesgos de seguridad operacional y el intercambio de información relativa a la seguridad operacional para respaldar, entre los proveedores de servicios, el desarrollo de una cultura organizativa que promueva SMS eficaces.

— — — — — — — — — —

INTENCIONALMENTE EN BLANCO

Apéndice 2

ORIENTACIÓN SOBRE LA ELABORACIÓN DE UN PLAN DE IMPLEMENTACION DEL SSP

1. ANTECEDENTES

a) En el presente apéndice se proporciona orientación para ayudar a los Estados a elaborar un plan de implantación del SSP. El plan de implantación del SSP describe la forma en que el Estado pondrá en práctica, en forma secuencial y basada en principios, los procesos, procedimientos y medios que le permitirán cumplir sus responsabilidades relacionadas con la gestión de la seguridad operacional en la aviación civil.

b) La implantación de un SSP debería ser proporcional al tamaño y complejidad del sistema de aviación del Estado, y puede requerir la coordinación entre las múltiples autoridades responsables de cada elemento de las funciones de aviación civil en el Estado. Esta orientación está concebida como referencia y puede tener que adaptarse para satisfacer las necesidades particulares de los Estados.

c) La elaboración de un plan implantación del SSP permitirá a los Estados:

i) formular una estrategia general para la gestión de la seguridad operacional en el Estado;
ii) coordinar los procesos ejecutados por las diferentes organizaciones de aviación del Estado en el marco del SSP;
iii) establecer los controles que gobiernan la forma en que funcionará el sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios;
iv) asegurar que el funcionamiento del SMS del proveedor de servicios se ajusta a los controles establecidos; y
v) apoyar la interacción entre el SSP y el funcionamiento del SMS del proveedor de servicios.

d) Cuando el Estado es responsable de la provisión de servicios específicos (p. ej., servicios de aeródromo, servicios de navegación aérea) la organización que proporciona estos servicios debería elaborar e implantar un SMS

2. ANÁLISIS DE LAS CARENCIAS DEL SSP

a) Para elaborar un plan de implantación del SSP, debería realizarse un análisis de las carencias, de las estructuras y procesos que existen en el Estado con respecto al marco para SSP de la OACI. Esto permitirá al Estado evaluar la existencia y grado de maduración de los elementos del SSP dentro del propio Estado. Una vez completado y documentado el análisis de las carencias, los componentes/elementos identificados como faltantes o deficientes formarán junto con los que ya existen o son eficaces, la base para el plan de implantación del SSP.

b) Cada componente/elemento debería evaluarse para determinar si el Estado debería crear o modificar reglamentos, políticas o procedimientos para desarrollar los componentes/elementos requeridos del SSP. El marco para SSP de la OACI que constituye la base para la elaboración del plan de implantación del SSP comprende cuatro componentes y once elementos, como sigue:

1. Política y objetivos de seguridad operacional de los Estados

1.1 Marco legislativo estatal de la seguridad operacional
1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
1.3 Investigación de accidentes e incidentes
1.4 Política de cumplimiento

2. Gestión de riesgos de seguridad operacional por los Estados

2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

3. Garantía de la seguridad operacional por los Estados

3.1 Vigilancia de la seguridad operacional
3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención

4. Promoción de la seguridad operacional por los Estados

4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

3. PLAN DE IMPLEMENTACION DEL SSP

a) El plan de implantación del SSP es un plan de trabajo sobre cómo se elaborará e integrará el SSP en las actividades de gestión de la seguridad operacional del Estado. Dada la potencial magnitud de la empresa, es importante gestionar adecuadamente la carga de trabajo relacionada con las actividades en que se basan la elaboración e implantación del SSP. Se propone que los cuatro componentes y once elementos del marco para SSP de la OACI se implanten en forma secuencial que permita lograr los resultados específicos. El orden de esta secuencia dependerá del resultado del análisis de las carencias y de la complejidad y alcance del sistema de aviación dentro de cada Estado.

b) Uno de los objetivos específicos de un SSP es generar un contexto que apoye la implantación del SMS por los proveedores de servicios. Por consiguiente, dentro del alcance de las actividades del SSP, cuatro pasos específicos apoyan la implantación del SMS por los proveedores de servicios.

1. POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL DE LOS ESTADOS

1.1 Marco legislativo estatal de la seguridad operacional

a) Examinar, elaborar y promulgar, según sea necesario, un marco legislativo nacional de la seguridad operacional y reglamentos específicos, en cumplimiento de las normas internacionales y nacionales que definen la forma en que el Estado supervisará la gestión de la seguridad operacional dentro de su jurisdicción.
b) Establecer un grupo a nivel nacional dentro del Estado en forma de junta, comité, etc., para asegurar la participación coordinada de las organizaciones aeronáuticas del Estado en actividades específicas relativas a la gestión de la seguridad operacional en el Estado, y el establecimiento de funciones, responsabilidades y relaciones de tales organizaciones.
c) Establecer un cronograma para examinar periódicamente la legislación de seguridad operacional y los reglamentos de funcionamiento específicos para asegurar que siguen siendo pertinentes y apropiados para el Estado.

1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional

a) Identificar, definir y documentar los requisitos, las responsabilidades y la rendición de cuentas relativas a la creación y el mantenimiento del SSP. Esto incluye las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional del Estado. Incluir, además, una declaración clara sobre la provisión de los recursos necesarios para la implantación del SSP.
b) Identificar y designar al Ejecutivo responsable del SSP del Estado quien tendrá, entre otras cosas:

   i) la responsabilidad final y la obligación administrativa de rendir cuentas en nombre del Estado para la implantación y mantenimiento del SSP;
   ii) plena autoridad sobre asuntos de recursos humanos relativos a la organización de aviación del Estado que ha sido designada como depositaria del SSP;
   iii) plena autoridad sobre los aspectos financieros de la organización de aviación del Estado que ha sido designada como depositaria del SSP;
   iv) autoridad final sobre los aspectos de gestión de los certificados del proveedor de servicios; y
   v) responsabilidad final en la resolución de todos los asuntos de seguridad operacional de la aviación en el Estado.

c) Establecer el equipo de implantación del SSP.

d) Asignar el tiempo necesario para cada tarea relacionada con la implantación del SSP entre los diferentes niveles de gestión de las organizaciones de aviación del Estado.

e) Presentar a todo el personal los conceptos del SSP a un nivel de acuerdo con su participación individual en el SSP.
f) Elaborar e implantar una política de seguridad operacional del Estado que incluya, pero sin limitarse necesariamente a ellos, los puntos siguientes:

   i) el compromiso de elaborar e implantar estrategias y procesos para asegurar que todas las actividades de aviación bajo vigilancia alcanzarán el nivel más elevado de eficacia de la seguridad operacional;
   ii) la elaboración y promulgación de un marco legislativo nacional de seguridad operacional y reglamentos de funcionamiento aplicables para la gestión de la seguridad operacional en el Estado;
   iii) el compromiso de asignar los recursos necesarios a las organizaciones de aviación del Estado para permitir que su personal cumpla sus responsabilidades, tanto relacionadas con la seguridad operacional como de otro tipo;
   iv) el apoyo a la gestión de la seguridad operacional en el Estado mediante un sistema efectivo de notificación y comunicación de peligros;
   v) el establecimiento de disposiciones para la protección de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS);
   vi) el compromiso de una interacción efectiva con los proveedores de servicios en la resolución de los problemas de seguridad operacional;
   vii) el compromiso de comunicar, con visible endoso, la política de seguridad operacional del Estado a todo el personal; y
   viii) una política de cumplimiento adecuada a las operaciones del proveedor de servicios en un entorno SMS.

g) Establecer los medios necesarios para asegurar que la política de seguridad operacional del Estado es comprendida, implantada y observada en todos los niveles dentro de las organizaciones de aviación del Estado.

1.3 Investigación de accidentes e incidentes

a) Elaborar y establecer los mecanismos para asegurar un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes, en apoyo de la gestión de la seguridad operacional en el Estado, y no la asignación de culpa o responsabilidad.

b) Elaborar y establecer los arreglos necesarios para asegurar la independencia de la organización de investigación de accidentes e incidentes respecto de otras organizaciones estatales de aviación.

1.4 Política de cumplimiento

a) Elaborar y promulgar una política de cumplimiento que establezca las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, y a satisfacción de la autoridad estatal competente. La política de cumplimiento establece también las condiciones y circunstancias en las cuales las desviaciones respecto de la seguridad operacional deberían abordarse mediante procedimientos establecidos en cuanto a cumplimiento.

b) La política también debería asegurar que ninguna información obtenida de un sistema de notificación interna de peligros o un sistema de vigilancia de datos de vuelo establecidos en el marco del SMS se utilizará para la aplicación de medidas disciplinarias.

1.5 Documentación del SSP

a) Elaborar y establecer una biblioteca de seguridad operacional del Estado que documente los requisitos, responsabilidades y líneas de rendición de cuentas relativas al establecimiento y mantenimiento del SSP. Esta biblioteca de seguridad operacional mantendrá y actualizará, según sea necesario, la documentación del SSP relativa al marco legislativo nacional de seguridad operacional, las políticas y objetivos de seguridad operacional del Estado, los requisitos del SSP, los procedimientos y procesos del SSP, las líneas de rendición de cuentas, responsabilidades y facultades para procesos y procedimientos, y el nivel aceptable de seguridad operacional (ALoS) del Estado relacionados con el SSP.

Resultados Esperados

a) Marco legislativo estatal de seguridad operacional promulgado.

b) Responsabilidades y rendición de cuentas establecidas, documentadas y publicadas del Estado respecto de la seguridad operacional.

c) Políticas de seguridad operacional y de cumplimiento del Estado firmadas por el Ejecutivo responsable.

d) Políticas de seguridad operacional y de cumplimiento del Estado distribuidas dentro de las organizaciones de aviación del Estado y entre los proveedores de servicio bajo vigilancia.

e) Procesos independientes de investigación de accidentes e incidentes establecidos.

f) Estructura de organización del SSP implantada.

2. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL POR LOS ESTADOS

2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios

a) Establecer los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para el SMS del proveedor de servicios (marco normativo para SMS, circular de asesoramiento, etc.) como controles que rigen la forma en que los proveedores de servicios identificarán los peligros y gestionarán y controlarán los riesgos de seguridad operacional.

b) Establecer un cronograma para consulta con los proveedores de servicios sobre estos requisitos.

c) Establecer un cronograma para examinar periódicamente los requisitos y reglamentos específicos de funcionamiento a efectos de asegurar que siguen siendo pertinentes y apropiados para los proveedores de servicios.

2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

a) Elaborar y establecer un procedimiento para acordar con cada proveedor de servicios la eficacia de la seguridad operacional de sus SMS sobre la base de:

i) valores de indicador de la eficacia de la seguridad operacional;
ii) valores de objetivo de la eficacia de la seguridad operacional; y
iii) planes de acción.

b) Incluir en el procedimiento acordado que la eficacia de la seguridad operacional del proveedor de servicios debería ser proporcional a:

i) la complejidad de los contextos operacionales y específicos de cada proveedor de servicios; y
ii) la disponibilidad de recursos en cada proveedor de servicios para enfrentar los riesgos de seguridad operacional.

c) Medir la eficacia de la seguridad operacional del SMS del proveedor de servicios mediante exámenes periódicos de la eficacia de seguridad del SMS acordada para asegurar que los indicadores de eficacia de la seguridad y objetivos de eficacia de la seguridad siguen siendo pertinentes y apropiados para los proveedores de servicios.

d) Elaborar un medio para evaluar resultados de bajo nivel y procesos más frecuentes entre diferentes proveedores de servicios.

e) Determinar resultados de eficacia medibles dentro de los diferentes SMS.

Resultados Esperados

a) Reglamentos sobre SMS promulgados.

b) Textos de orientación sobre implantación del SMS distribuidos a los proveedores de servicios.

c) Primer examen anual de la eficacia de la seguridad operacional de los proveedores de servicios acordada completado.

3. GARANTÍA DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS

3.1 Vigilancia de la seguridad operacional

a) Establecer mecanismos que garanticen que la identificación de peligros y la gestión de riesgos de seguridad operacional por los proveedores de servicios se ajustan a controles reglamentarios establecidos.

b) Establecer mecanismos que garanticen que los controles de riesgo de seguridad operacional se integran en el SMS del proveedor de servicios.

c) Desarrollar una auditoría interna del SSP.

3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional

a) Elaborar y establecer un medio para recopilar, analizar y almacenar datos sobre peligros y riesgos de seguridad operacional a nivel del Estado:

i) establecer un sistema de notificación obligatoria de peligros;
ii) establecer un sistema de notificación confidencial de peligros;
iii) elaborar una base de datos estatal sobre peligros;
iv) establecer un mecanismo para elaborar información a partir de los datos almacenados;
v) establecer un medio para recopilar datos sobre peligros a nivel global del Estado y a nivel de cada proveedor de servicios; y
vi) establecer un medio para implantar planes de medidas correctivas.

b) Asegurar que los procesos de identificación de peligros y de gestión de riesgos de seguridad operacional del proveedor de servicios se ajustan a los requisitos normativos establecidos y que los controles de riesgos de seguridad operacional están adecuadamente integrados en el SMS del proveedor de servicios, incluyendo, entre otros:

i) inspecciones;
ii) auditorías; y
iii) encuestas.

c) Observar la secuencia siguiente para la implantación:

i) controles normativos de riesgos de seguridad operacional integrados en el SMS del proveedor de servicios;
ii) actividades de vigilancia para asegurar que los procesos de identificación de peligros y gestión de riesgos de seguridad operacional del proveedor de servicios se ajustan a los requisitos normativos establecidos; y
iii) actividades de vigilancia para verificar que los proveedores de servicios aplican los controles de riesgos de seguridad operacional.

d) Establecer el nivel aceptable de seguridad (ALoS) relativo al SSP, comprendiendo una combinación de medición de la seguridad operacional y medición de la eficacia de la seguridad operacional:

i) La medición de la seguridad operacional comprende la cuantificación de los resultados de sucesos de alto nivel, consecuencias graves o funciones estatales de alto nivel, tales como proporciones de accidentes, proporciones de incidentes graves y cumplimiento de los reglamentos.

ii) La medición de la eficacia de la seguridad operacional comprende la cuantificación de los resultados de procesos de bajo nivel y consecuencias leves que proporciona una medida de la implantación realista de cada SSP más allá de las proporciones de accidentes o cumplimiento de los reglamentos.

3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención

a) Establecer procedimientos para priorizar las inspecciones, auditorías y encuestas, basadas en análisis de peligros y riesgos de seguridad operacional.

Resultados Esperados

a) Sistemas estatales de notificación obligatoria y confidencial de peligros implantados.

b) Primer examen anual de la política y objetivos de seguridad operacional realizado.

c) Primer examen anual de la política de cumplimiento realizado.

d) ALoS establecidos.

4. PROMOCION DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS

4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional

a) Identificar requisitos de instrucción internos.

b) Elaborar y proporcionar instrucción genérica en seguridad operacional a todo el personal.

c) Elaborar un programa de instrucción sobre componentes clave del SSP y el SMS para el personal que incluya:

i) adoctrinamiento/instrucción inicial en seguridad operacional;
ii) instrucción en seguridad operacional en el puesto de trabajo (OJT);
iii) instrucción periódica en seguridad operacional.

d) Establecer un medio para medir la efectividad de la instrucción.

e) Elaborar un medio para comunicar internamente cuestiones relacionadas con la seguridad operacional, incluyendo:

i) políticas y procedimientos de seguridad operacional;
ii) boletines de noticias;
iii) avisos; y
iv) un sitio web.

4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional

a) Establecer los medios para proporcionar intercambio de información relacionada con la seguridad operacional para apoyar la implantación del SMS entre proveedores de servicios, incluyendo los proveedor de servicioses menores.

b) Elaborar instrucción y textos de orientación sobre implantación del SMS para proveedores de servicios.

c) Establecer los medios para comunicar externamente asuntos relacionados con la seguridad operacional incluyendo:

i) políticas y procedimientos de la seguridad operacional;
ii) boletines de noticias;
iii) avisos; y

iv) un sitio web.

Resultados Esperados

a) Programa de instrucción sobre componentes clave de un SSP y SMS para personal técnico y de apoyo completado.

b) Primer ciclo de instrucción genérica en seguridad operacional para el personal completado.

c) Texto de orientación sobre SMS distribuido a los proveedores de servicios, incluyendo los explotadores menores.

d) Primer ciclo de instrucción para proveedores de servicios sobre implantación de SMS completado.

e) Medios para comunicar interna y externamente la información relacionada con la seguridad operacional establecidos.

INTENCIONALMENTE EN BLANCO

Apéndice 3

RESPONSABILIDADES DE SEGURIDAD OPERACIONAL

Ejecutivo responsable

(Más información sobre la escogencia del Ejecutivo Responsable en los Apéndices A & B al final de este Apéndice 3)

En los Estados asociados al Sistema RAC, el Director de la AAC o la Autoridad Competente:

1. Es el máximo responsable y el que debería de responder por la implementación y mantenimiento del Programa de Seguridad Operacional del Estado en el tema de Aviación Civil.

2. Debe tener la capacidad de establecer políticas y aprobar los recursos para atender las obligaciones del Estado asociado al Sistema RAC.

3. Si el Director no tiene esta capacidad dentro de sus atribuciones, entonces el Estado asociado al Sistema RAC debería identificar, definir y documentar quién es esta persona.

4. Debe acatar las recomendaciones del Comité de Gestión de la Seguridad y Operacional, que será a su vez, el responsable de realizar estudios, evaluaciones, encuestas, investigaciones, supervisiones y auditorias de Seguridad Operacional tanto en la parte interna de las Autoridades, así como en los Proveedor de servicioses, Explotadores y Proveedores de servicios de la industria de la aviación.

5. Tendrá la autoridad completa y final para proveer los recursos financieros, materiales y humanos necesarios para aprobar los cambios en la política, impulsar la mejora de la actuación y facilitar la gestión y planificación del sistema aeronáutico en materia de la Seguridad Operacional para cumplir con los fines que tiene encomendados.

6. Debe desarrollar y promover una política que permita los reportes de amenazas a la Seguridad Operacional voluntaria y confidencial no punitiva, a fin de que todas las amenazas a la seguridad puedan ser reportados por todos los funcionarios de la Autoridad o por cualquier otra persona que se entere de las mismas.

7. Tendrá la autoridad completa y final sobre los aspectos de certificación de los Proveedores de Servicios; y

8. Tendrá la autoridad completa y final para tomar decisiones sobre la resolución de cuestiones de Seguridad Operacional.

Otros Directores y funcionarios

1. Los Directores / Jefes / Encargados de los diferentes departamentos relacionados con los temas del SSP/SMS son los responsables de que los proveedores de servicios implementen sus Sistemas de Seguridad Operacional y deberían supervisarlos y auditarlos para corroborar que se está cumpliendo con los requerimientos nacionales e internacionales en esa materia: También deberían reportar las no conformidades o hallazgos al Comité de Seguridad Operacional de la Institución a fin de que este recomiende las acciones pertinentes a tomar.

2. Los funcionarios de los departamentos anteriormente mencionados son los responsables de realizar las supervisiones y auditorias y deberían de dar cuentas de sus acciones ante los encargados de dichos departamentos.

3. Los Directores / Jefes / Encargados de los diferentes departamentos que proveen servicios y que pertenezcan a la Autoridad de Aviación Civil deberían implementar, mantener y ser responsables de su propio Sistema de Gestión de Seguridad Operacional del cual deberían rendir cuentas y pueden ser auditados por el Comité de Seguridad Operacional de la Institución quien reporta al Director de Aviación Civil.

4. Los funcionarios de los diferentes departamentos de la Autoridad que proporcionan servicios deberían cumplir con toda la reglamentación y otras disposiciones emanadas por la respectiva Dirección y tener a la Seguridad Operacional y la eficiencia como sus principales prioridades de todas sus actividades,

5. En el ámbito de sus competencias en la gestión de Direcciones, Unidades y Aeropuertos, los Jefes, Directores o Encargados asumen las capacidades para:

a) Proponer al secretario del Comité de Seguridad Operacional para su estudio y aprobación en el Comité, propuestas de mejoras de Seguridad Operacional.

b) Promover la participación de la Dirección, Unidad o Aeropuerto en el programa de Seguridad Operacional.

c) Promover la mejora de la Seguridad Operacional a todos los usuarios.

d) Promover la formación en materia de Seguridad Operacional del personal a su cargo.

e) Promover entre su personal la cultura de Seguridad Operacional, especialmente la cultura del reporte de amenazas a la seguridad.

6. Todos y cada uno de los funcionarios de la Autoridad de de Aviación Civil son responsables de la eficacia de la Seguridad Operacional de acuerdo a sus funciones dentro de la organización, deberían dar cuentas de sus acciones ante sus superiores de acuerdo a sus responsabilidades en Seguridad Operacional.

Personal clave y estructura.

1. Se considera necesario contar con una estructura y órganos calificados para asegurar una mejora constante de la Seguridad Operacional en los diferentes servicios y productos que se facilitan a la sociedad.

2. Los Estados asociados al Sistema RAC deberían establecer un Equipo multidisciplinario para implementar el SSP.

3. Se debería de asignar el tiempo necesario para cada tarea relacionada con la implementación del SSP dentro de los diferentes niveles de gestión de las Autoridades de Aviación Civil de los Estados asociados al Sistema RAC.

4. Se debería dar a conocer a todo el personal del Estado asociado al Sistema RAC, los conceptos del SSP de acuerdo al nivel de involucramiento del mismo.

5. En consecuencia se define la siguiente estructura y órganos competentes en materia de Seguridad Operacional:

a) Comité o Equipo de Seguridad Operacional;

b) Oficina o Unidad de Gestión de la Seguridad Operacional;

c) Responsable del Sistema de Gestión de la Seguridad Operacional;

d) El Director de la Seguridad Operacional.

Comité de Seguridad Operacional.

1. El Comité de Seguridad Operacional es un foro que provee el medio de análisis desde diferentes perspectivas, especialmente cuando los asuntos de Seguridad Operacional requieren de un amplio punto de vista. Debe tener expertos de diferentes disciplinas para evaluar el rendimiento del SMS desde una perspectiva sistémica.

2. El Comité de Seguridad Operacional debería estar conformado por el Sub-Director General Técnico o un Representante de la Dirección, el Director de Seguridad Operacional y por representantes de los diferentes departamentos o unidades técnicas como: el departamento de Licencias, Operaciones, Aeronavegabilidad, Investigación de Accidentes, Aeropuertos y Navegación Aérea y pueden incorporar otros especialistas de los diferentes campos de la aviación cuando así lo requiera. El Comité será presidido por el Sub-Director General Técnico, con el Director de Seguridad Operacional actuando como Secretario.

3. Debe de existir un Libro de Actas del Comité en el que debería constar, como mínimo:

a) Fecha de las reuniones;

b) Asistentes;

c) Decisiones y acuerdos del Comité;

d) Firmas del Presidente y Secretario del Comité.

4. El Director de la Gestión de Seguridad Operacional debería participar en las reuniones del Comité de Seguridad Operacional, con voz y voto.

5. Corresponde al Comité de Seguridad Operacional el ejercicio de las siguientes funciones:

a) Actuar como una fuente de conocimiento y asesoría en materia de Seguridad Operacional para el Director General;

b) Revisar el progreso en la identificación de peligros y acciones tomadas después de incidentes o accidentes;

c) Hacer recomendaciones de Seguridad Operacional para la gestión de errores y amenazas;

d) Revisar los reportes de las auditorías internas de seguridad operacional;

e) Revisar y aprobar las respuestas a las auditorias y las acciones tomadas;

f) Promover el pensamiento uniforme en asuntos de Seguridad Operacional;

g) Ayudar a identificar los peligros y las defensas;

h) Coordinar y realizar por medio de la Unidad de Gestión de la Seguridad Operacional, auditorias a los proveedores de servicios y proveedores de servicios en la aviación civil;

i) Preparar y revisar reportes para el Director General;

j) Aprobar Planes Estratégicos de Seguridad Operacional y normas específicas para el Programa de Seguridad Operacional (SSP);

k) Recomendar al Director General la Aceptación de los Sistemas de Gestión de la Seguridad Operacional de los Proveedores de servicios y Proveedores de Servicios;

l) Solicitar los recursos necesarios para llevar adelante el Programa de Seguridad Operacional;

m) Proponer modificaciones al Reglamento de funcionamiento de los órganos competentes en materia de Seguridad Operacional, así como de su estructura y funcionamiento;

n) Aprobar los Manuales de Seguridad Operacional tanto de la Institución como los de proveedores de servicios, y proveedores de servicios;

o) Aprobar las revisiones de los Manuales de Seguridad Operacional;

p) Aprobar la estructura y funciones de la Unidad de Gestión de la Seguridad Operacional;

q) Definir los objetivos anuales en materia de Seguridad Operacional.

Reuniones del Comité de seguridad operacional.

1. El Comité de Seguridad Operacional debería reunirse, convocado por su Presidente, al menos una vez al mes, lo cual no será un impedimento para que puedan reunirse más veces cuando las condiciones así lo ameriten.

2. Para quedar constituido se precisan, al menos, la mayoría simple de sus miembros.

3. Los siguientes puntos se deberían de llevar a cabo en las reuniones del Comité:

   a) *Agenda*. Todos los miembros del Comité pueden someter puntos de agenda. El Jefe de Seguridad Operacional, como secretario, junto con el Presidente deberían finalizar la agenda proporcionando suficiente retroalimentación para cada asunto. Se debería dar prioridad a los asuntos que requieran decisiones y acciones, sobre aquellos de carácter informativo.

   b) *Las minutas*. El Jefe de Seguridad Operacional como secretario de la reunión debería preparar minutas en borrador inmediatamente después de cada reunión. Una vez que el Presidente haya firmado las minutas, estas se convertirán en un documento de acción. Las minutas deberían ser distribuidas, dentro de los 5 días de trabajo después de la reunión para recordar el compromiso en los asuntos de acción. Copias de las minutas se distribuirán a través de la organización entre los funcionarios y las diferentes jefaturas.

   c) *Seguimiento*. Después de la reunión, otras prioridades pueden capturar la atención de la acción a tomar. El Jefe de Seguridad Operacional debería monitorear discretamente las acciones tomadas y no tomadas y revisar su progreso con aquellos que se han comprometido con la acción.

Departamento de seguridad operacional (SSP/SMS).

1. El Departamento de Seguridad Operacional (SSP/SMS) es el encargado de gestionar todos los asuntos referentes a la Seguridad Operacional tanto de la institución como de la comunidad aeronáutica en general.

2. Las funciones del Departamento del SSP/SMS son:

   a) Asesorar al Director General en materias relacionadas con la Seguridad Operacional tales como:

      (i) Colaborar en desarrollar la política de Seguridad Operacional;

      (ii) Definir las responsabilidades en Seguridad Operacional;

      (iii) Establecer un sistema efectivo de Gestión de la Seguridad Operacional;

      (iv) Recomendar la asignación de recursos en soporte para las iniciativas de Seguridad Operacional;

      (v) Comunicar los asuntos de Seguridad Operacional; y

      (vi) Desarrollar un plan de respuesta ante emergencias.

3. Asesorar para:

   a) Evaluar los riesgos identificados, y

   b) Seleccionar las mejores medidas de mitigación del riesgo.

4. Vigilar el sistema de identificación de peligros a través de:

   a) Investigar los incidentes; y

   b) Mantener el sistema de reporte de incidentes.

5. Gestionar la base de datos de Seguridad Operacional:

   a) Gestionar los programas de análisis de datos.

6. Conducir análisis de Seguridad Operacional:

   a) Monitorear las tendencias;

b) Realizar estudios de Seguridad Operacional.

7. Capacitar en métodos de Seguridad Operacional.

8. Coordinar el Comité de Seguridad Operacional.

9. Promocionar la Seguridad Operacional:

a) Mantener conocimiento y entendimiento del proceso de seguridad operacional de la Institución a través de todas las áreas operativas;

b) Transmitir lecciones internas de Seguridad Operacional;

c) Intercambiar información de Seguridad Operacional con otras Organizaciones similares.

10. Medir el rendimiento de la Seguridad Operacional:

a) Conducir encuestas de Seguridad Operacional;

b) Proveer guía en vigilancia de la Seguridad Operacional;

c) Establecer los índices y metas de Seguridad Operacional.

11. Participar en la investigación de incidentes y accidentes.

12. Reportar para cumplir con los requerimientos de:

a) La administración (revisar las tendencias e identificar los asuntos no resueltos de Seguridad Operacional); y

b) La autoridad de aviación civil.

Jefe del departamento de seguridad operacional (SSP/SMS).

1. El Jefe del Departamento de Seguridad Operacional es el punto focal para el desarrollo y mantenimiento de un sistema efectivo de la Seguridad Operacional; también es el principal punto de contacto con los proveedores de servicios en todos los asuntos relacionados con la Seguridad Operacional, sus responsabilidades incluyen:

a) Informar directamente al Director General, demostrándole que la seguridad está a un nivel de importancia equivalente en el proceso de toma de decisiones como las otras funciones operativas de la Institución;

b) promover el conocimiento sobre seguridad operacional;

c) asegurar que la gestión de la Seguridad Operacional tiene el mismo nivel de prioridad que cualquier otro proceso dentro de la organización.

2. La gestión de la Seguridad Operacional es una responsabilidad compartida con Jefe o Encargado de Departamento o Unidad dentro de la Autoridad y asesorada por el Jefe de Seguridad Operacional, las actividades específicas de Seguridad Operacional son responsabilidad de los Jefes de Departamentos.

3. El Director General no debería hacer al Jefe de Seguridad Operacional responsable por competencias de otros Jefes de Departamentos, más bien el Jefe de Seguridad Operacional deber prestar ayuda efectiva a todos éstos asegurar el éxito del sistema de gestión de la Seguridad Operacional. El Jefe de Seguridad Operacional es responsable de cualquier deficiencia en el SSP/SMS. El Jefe de Seguridad Operacional no es responsable del rendimiento de la Seguridad Operacional de la Institución.

4. El Jefe de Seguridad Operacional no debería de tener otra responsabilidad que la Seguridad Operacional. Sus funciones deberían ser el manejar todos los aspectos de operación del SSP/SMS. Esto debería asegurar que la documentación refleje exactamente el ambiente, el monitoreo efectivo de las acciones correctivas, el

rendimiento por medio de reportes periódicos y el asesoramiento independiente al Director General, jefaturas y cualquier otro personal en lo relacionado con materias de Seguridad Operacional.

5. El Jefe de Seguridad Operacional y su oficina deberían coordinar actividades y proveer asistencia al Comité de Seguridad Operacional.

Relaciones del responsable de departamento de seguridad operacional (SSP/SMS).

1. En el SSP/SMS las áreas de interés son muy amplias, incluyendo relaciones externas con proveedores de servicios, contratistas, suplidores, fabricantes y oficiales de la autoridad reguladora. Ellos deberían adaptar un efectivo trabajo de relaciones a través de todo el espectro de aquellos que influyen en la Seguridad Operacional, estas relaciones deberían estar marcadas por:

   a) Competencia y profesionalismo;

   b) Cordialidad y cortesía;

   c) Honradez e integridad; y

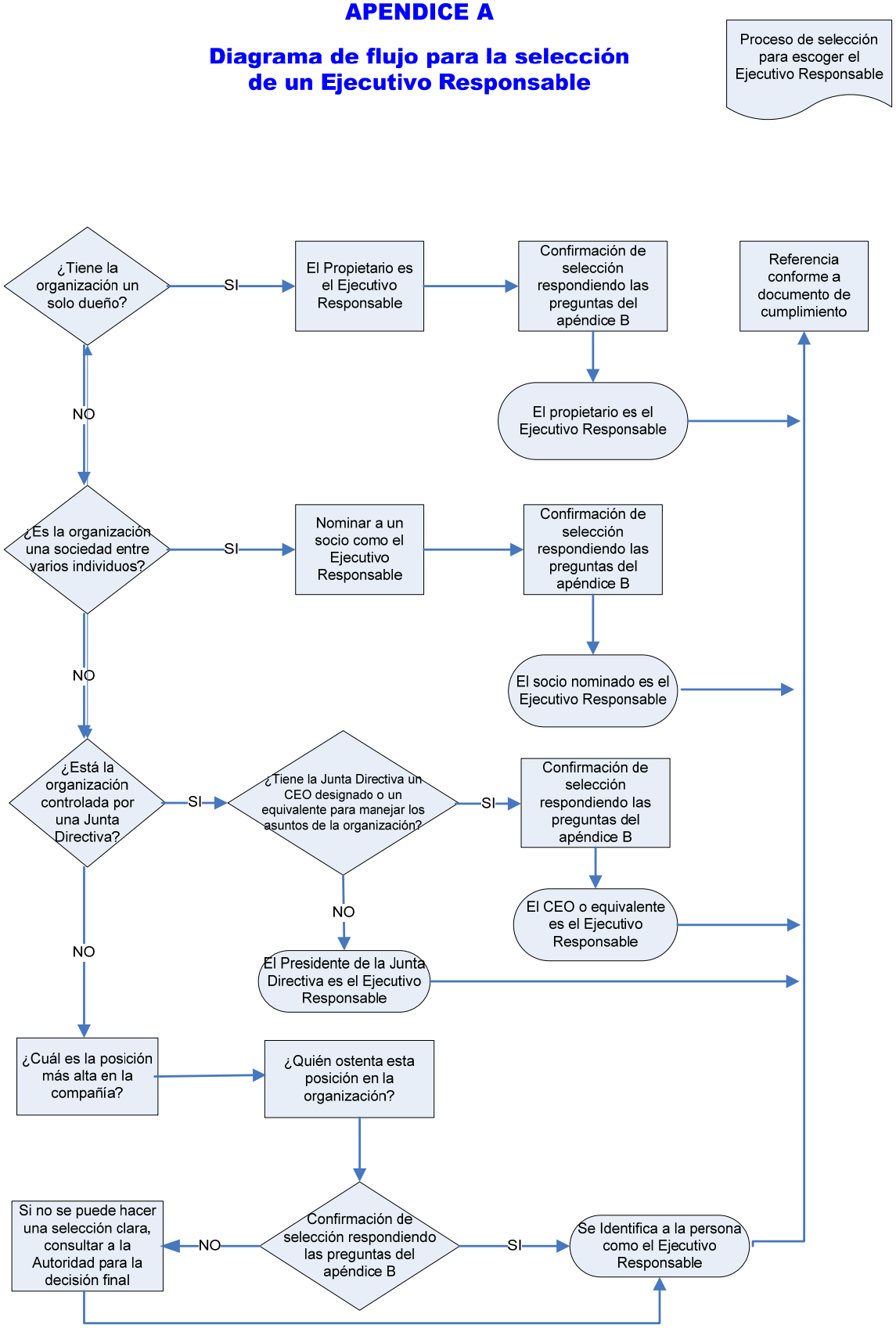
   d) Apertura.

El Jefe de Seguridad Operacional debería estar disponible para razonar los asuntos de Seguridad Operacional con cualquier persona. La llamada política de “puertas abiertas” no es suficiente. El Jefe de Seguridad Operacional debería ser visible y accesible cuando él se mueve por todas las áreas de operaciones, mantenimiento, licencias, ATS, aeropuertos, con los proveedores de servicios y con los suplidores externos de servicios.

INTENCIONALMENTE EN BLANCO

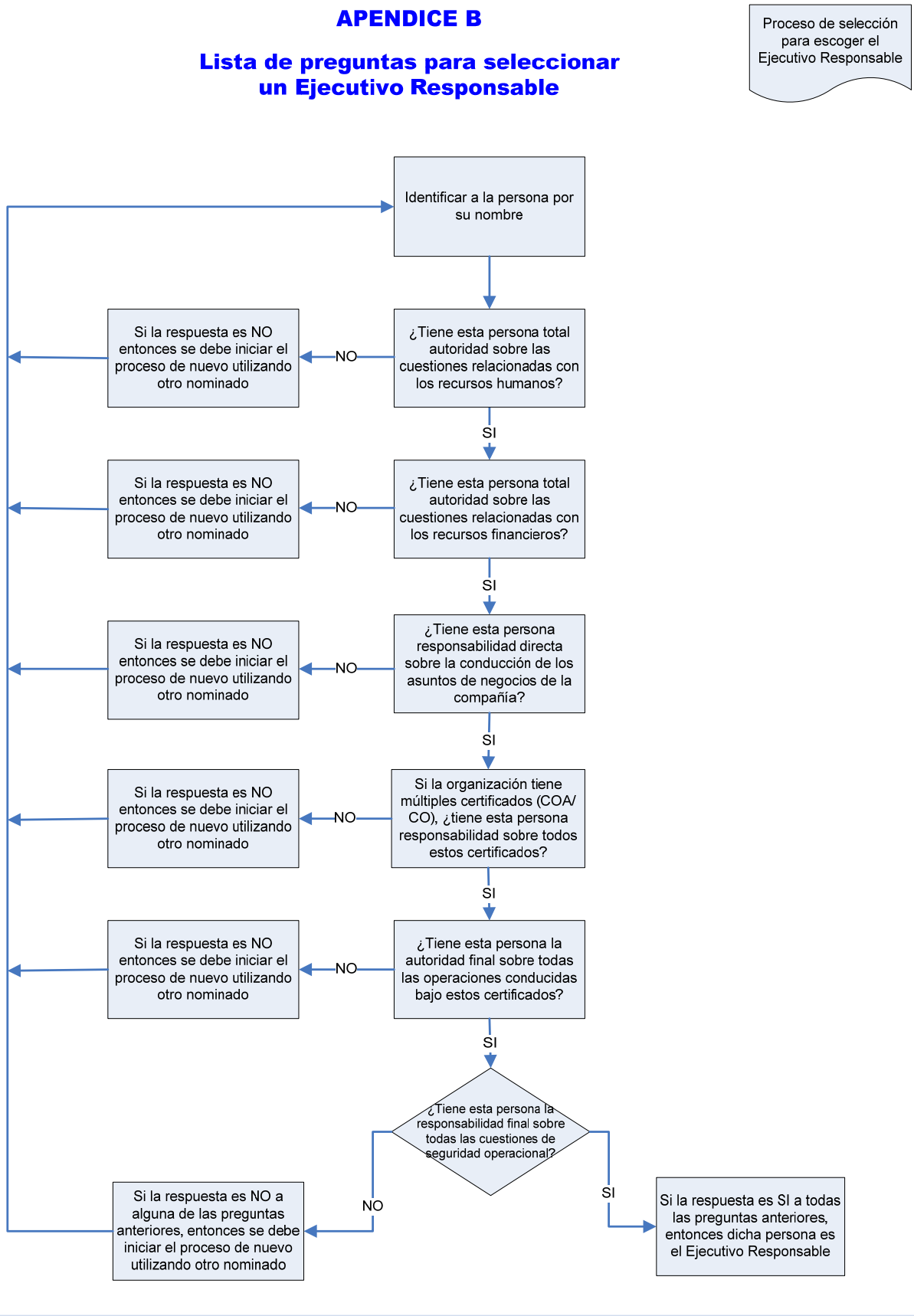
APENDICE A

Diagrama de flujo para la selección de un Ejecutivo Responsable



APENDICE B

Lista de preguntas para seleccionar un Ejecutivo Responsable



Apéndice 4

EJEMPLO DE UNA DECLARACIÓN ESTATAL DE POLÍTICA DE SEGURIDAD OPERACIONAL

La gestión de la seguridad operacional de la aviación civil es una de las principales responsabilidades de [Estado]. [Estado] se compromete a elaborar, implantar, mantener y mejorar constantemente estrategias y procesos para asegurar que todas las actividades de aviación que tienen lugar bajo su supervisión lograrán el mayor nivel de eficacia de seguridad operacional, satisfaciendo al mismo tiempo las normas nacionales e internacionales.

Los titulares de certificados de aviación de [Estado] deberán demostrar que sus sistemas de gestión reflejan adecuadamente un enfoque de SMS. El resultado previsto de este enfoque es una gestión de la seguridad operacional y prácticas de seguridad operacional mejoradas, incluyendo la notificación de seguridad dentro de la industria de aviación civil.

En [Estado], todos los niveles de administración son responsables por el logro del más alto nivel de eficacia de la seguridad operacional dentro de [Estado], comenzando por el Ejecutivo responsable [según corresponda a la organización]. [Estado] se compromete a:

a) elaborar la formulación de reglas generales y políticas operacionales específicas, fundadas en principios de gestión de la seguridad operacional, sobre la base de un análisis completo del sistema de aviación del Estado;

b) consultar a todos los sectores de la industria de la aviación sobre aspectos relativos a la elaboración de reglamentos;

c) apoyar la gestión de la seguridad operacional en el Estado mediante un sistema efectivo de notificación y comunicación de la seguridad operacional;

d) interactuar eficazmente con los proveedores de servicios para la resolución de problemas de seguridad operacional;

e) asegurar que dentro de [la administración estatal supervisora de la seguridad operacional], se asignan suficientes recursos y que el personal cuenta con las competencias y la instrucción adecuadas para realizar sus tareas, tanto relacionadas con la seguridad operacional como de otro tipo;

f) realizar actividades de supervisión tanto basadas en la eficacia como en el cumplimiento, apoyadas por análisis y asignación priorizada de recursos basada en los riesgos de seguridad operacional;

g) cumplir y, cuando sea posible, superar, los requisitos y normas internacionales de seguridad operacional;

h) promover conceptos y principios de gestión de la seguridad operacional y educar a la industria de la aviación al respecto;

i) supervisar la implantación de SMS dentro de las organizaciones de aviación;

j) asegurar que todas las actividades bajo supervisión logran las más altas normas de seguridad operacional;

k) establecer disposiciones para la protección de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS), de modo que se aliente a las personas a proporcionar información esencial relacionada con la seguridad operacional sobre peligros, y que existe una corriente e intercambio continuos de datos de gestión de la seguridad operacional entre [Estado] y los proveedores de servicios;

l) establecer y medir la implantación realista de nuestro SSP con respecto a los indicadores de seguridad operacional y a los objetivos de seguridad operacional que están claramente identificados; y

m) promulgar una política de cumplimiento que asegure que ninguna información obtenida de SDCPS establecidos en el marco del SSP o el SMS se utilizará como base para la imposición de sanciones, excepto en caso de negligencia grave o desviaciones intencionales.

Esta política debería ser comprendida, implantada y observada por todo el personal que participa en actividades relacionadas con [administración estatal de supervisión de la seguridad operacional].

(Firma) _____

Ejecutivo responsable

— — — — — — — — — —

INTENCIONALMENTE EN BLANCO

Apéndice 5

ORIENTACIÓN SOBRE LA ELABORACIÓN DE UN ANÁLISIS DE LAS CARENCIAS DEL PROGRAMA DE SEGURIDAD OPERACIONAL DEL ESTADO (SSP)

1. ANÁLISIS DE LAS CARENCIAS

a) La implantación de un SSP requiere que el Estado realice un análisis de su sistema de seguridad operacional para determinar cuáles son los componentes y elementos del SSP que están actualmente implantados y cuáles deberían añadirse o modificarse para satisfacer los requisitos de implantación. Este análisis se conoce como análisis de las carencias y entraña la comparación de los requisitos del SSP respecto de los recursos existentes en un Estado.

b) El análisis de las carencias proporciona, en forma de lista de verificación, información para ayudar en la evaluación de los componentes y elementos que integran el marco de la OACI para SSP e identificar los componentes y elementos que deberían elaborarse. Una vez completado y documentado el análisis de carencias, constituye una de las bases del plan de implantación del SSP.

2. MARCO DE LA OACI PARA SSP

El marco de la OACI para SSP consta de cuatro componentes y once elementos, a saber:

1. Política y objetivos de seguridad operacional de los Estados

   1.1 Marco legislativo estatal de la seguridad operacional
   1.2 Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional
   1.3 Investigación de accidentes e incidentes
   1.4 Política de cumplimiento

2. Gestión de riesgos de seguridad operacional por los Estados

   2.1 Requisitos de seguridad operacional para los SMS de los proveedores de servicios
   2.2 Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional

3. Garantía de la seguridad operacional por los Estados

   3.1 Vigilancia de la seguridad operacional
   3.2 Recopilación, análisis e intercambio de datos sobre seguridad operacional
   3.3 Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención

4. Promoción de la seguridad operacional por los Estados

   4.1 Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional
   4.2 Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional.

3. ANÁLISIS DE LAS CARENCIAS DEL PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

La siguiente lista para análisis de las carencias puede utilizarse como modelo para realizar un análisis de ese tipo. Cada pregunta está concebida para obtener una respuesta “sí” o “no”. Una respuesta “sí” indica que el Estado ya ha incorporado a su sistema de seguridad operacional el componente o elemento del marco de la OACI para SSP en cuestión y que cumple o supera el requisito. Una respuesta “no” indica que existe una brecha (carencia) entre el componente/elemento del marco de la OACI para SSP y el sistema de seguridad operacional en el Estado.

Referencia OACI (Doc. 9859	*Aspecto para analizar*	*Respuesta*	*Estado de implementación*
Componente 1 — POLÍTICAS Y OBJETIVOS DE SEGURIDAD OPERACIONAL DE LOS ESTADOS			
Elemento 1.1 — Marco legislativo estatal de seguridad operacional			
Cap. 11	¿Ha promulgado [Estado] un marco legislativo nacional de seguridad operacional y las reglamentaciones específicas que definen la gestión de la seguridad operacional en el Estado?	☐ SI ☐ NO	
Cap. 11	¿Ha definido [Estado] las actividades específicas relacionadas con la gestión de la seguridad operacional en el Estado en las cuales cada organización de aviación de [Estado] debería participar?	☐ SI ☐ NO	
Cap. 11	¿Ha establecido [Estado] los requisitos, las responsabilidades y las obligaciones de rendir cuentas con respecto a la gestión de la seguridad operacional en todas las organizaciones de aviación de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Se examinan periódicamente el marco legislativo y la reglamentación específica para asegurar que sigan siendo pertinentes y apropiadas para el Estado?	☐ SI ☐ NO	
Cap. 11	¿Se examinan periódicamente el marco legislativo y la reglamentación específica de [Estado] para asegurar que están actualizados con respecto a las normas internacionales?	☐ SI ☐ NO	
Cap. 11	¿Ha establecido [Estado] una política de seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿La política de seguridad operacional de [Estado] está firmada por el Ejecutivo responsable del SSP de [Estado] o una autoridad superior dentro de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Se examina periódicamente la política de seguridad operacional de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿La política de seguridad operacional de [Estado] se comunica con visible endoso a todos los empleados de todas las organizaciones de aviación de [Estado] para que tomen conciencia de sus responsabilidades individuales de seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Ha elaborado [Estado] documentación que describa el SSP, incluyendo las interrelaciones entre sus componentes y elementos?	☐ SI ☐ NO	
Cap. 11	¿Cuenta [Estado] con un sistema de registro que asegure que la generación y conservación de todos los registros necesarios para documentar y apoyar las actividades del SSP?	☐ SI ☐ NO	
Cap. 11	¿Proporciona el sistema de registro los procesos de control necesarios para asegurar la apropiada identificación, legibilidad, almacenamiento, protección, archivo, recuperación, tiempo de conservación y disposición de los registros?	☐ SI ☐ NO	
Elemento 1.2 — Responsabilidades y rendición de cuentas del Estado respecto de la seguridad operacional			
Cap. 11	¿Ha identificado y definido [Estado] los requisitos, las responsabilidades y la rendición de cuentas estatales relativos a la creación y mantenimiento del SSP?	☐ SI ☐ NO	
Cap. 11	¿Incluyen los requisitos directrices y actividades para planificar, organizar, desarrollar, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Incluyen los requisitos una declaración clara sobre la provisión de los recursos necesarios para la implantación y mantenimiento del SSP?	☐ SI ☐ NO	
Cap. 11	¿Ha identificado y designado [Estado] un Ejecutivo responsable como persona cualificada con responsabilidad directa por la implantación, funcionamiento y supervisión del SSP?	☐ SI ☐ NO	
Cap. 11	¿Cumple el Ejecutivo responsable del SSP de [Estado] las funciones y responsabilidades requeridas de su tarea?	☐ SI ☐ NO	
Cap. 11	¿Coordina el Ejecutivo responsable de SSP de [Estado], según corresponda, las actividades de las diferentes organizaciones de aviación del Estado en el marco del SSP?	☐ SI ☐ NO	
Cap. 11	¿Tiene el Ejecutivo responsable del SSP de [Estado] control sobre los recursos necesarios requeridos para la ejecución adecuada del SSP?	☐ SI ☐ NO	

Cap. 11	¿Verifica el Ejecutivo responsable del SSP de [Estado] que todo el personal de las organizaciones de aviación de [Estado] comprenden sus facultades, responsabilidades y obligaciones de rendir cuentas con respecto al SSP y todos los procesos, decisiones y medidas de gestión de la seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Están definidas y documentadas, en todos los niveles, las responsabilidades y obligaciones de rendición de cuentas de seguridad operacional?	☐ SI ☐ NO	
Elemento 1.3 — Investigación de accidentes e incidentes			
Cap. 11	¿Ha establecido [Estado], como parte de la gestión de la seguridad operacional, un proceso independiente de investigación de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes, cuyo único objetivo es la prevención de accidentes e incidentes y no la asignación de culpa o responsabilidad	☐ SI ☐ NO	
Cap. 11	¿Mantiene [Estado] la independencia de la organización de investigación de accidentes e incidentes respecto de otras organizaciones estatales de aviación?	☐ SI ☐ NO	
Elemento 1.4 — Política de cumplimiento			
Cap. 11	¿Ha promulgado [Estado] una política de cumplimiento?	☐ SI ☐ NO	
Cap. 11	¿Establece la política de cumplimiento las condiciones y circunstancias en las cuales los proveedores de servicios pueden encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional, y resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios, a satisfacción de la autoridad estatal competente?	☐ SI ☐ NO	
Cap. 11	¿Establece la política de cumplimiento las condiciones y circunstancias en las cuales las desviaciones respecto de la seguridad operacional deberían abordarse mediante procedimientos establecidos en cuanto a cumplimiento?	☐ SI ☐ NO	
Componente 2 — GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL POR LOS ESTADOS			
Elemento 2.1 — Requisitos de seguridad operacional para los SMS de los proveedores de servicios			
Cap. 11	¿Ha establecido [Estado] los controles que rigen la forma en que los proveedores de servicios detectarán los peligros y gestionarán los riesgos de seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Incluyen esos controles los requisitos, reglamentos específicos de funcionamiento y políticas de implantación para los SMS de los proveedores de servicios?	☐ SI ☐ NO	
Cap. 11	¿Se basan todos los requisitos, reglamentos operacionales específicos y políticas de implantación en los peligros identificados y en el análisis de los riesgos de seguridad operacional que se corren a consecuencia de los peligros?	☐ SI ☐ NO	
Cap. 11	¿Se examinan periódicamente los requisitos, reglamentos específicos del funcionamiento y políticas de implantación para asegurar que siguen siendo pertinentes y apropiados para los proveedores de servicios?	☐ SI ☐ NO	
Cap. 11	¿Existe un proceso estructurado dentro de [Estado] para evaluar cómo los proveedores de servicios gestionarán los riesgos de seguridad operacional relacionados con peligros identificados, expresados en términos de probabilidad y gravedad de ocurrencia?	☐ SI ☐ NO	
Cap. 11	¿Existe una política de [Estado] que asegure la notificación efectiva de las deficiencias, peligros u ocurrencias de seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Incluye la política de [Estado] sobre notificación de deficiencias, peligros u ocurrencias de seguridad operacional las condiciones en las cuales se aplica la protección con respecto a medidas disciplinarias o administrativas?	☐ SI ☐ NO	
Elemento 2.2 — Acuerdo sobre la actuación de los proveedores de servicios en cuanto a seguridad operacional			
Cap. 11	¿Ha acordado [Estado] con cada proveedor de servicios la eficacia de la seguridad operacional de sus SMS?	☐ SI ☐ NO	
Cap. 11	¿Es la eficacia de la seguridad operacional acordada proporcional a la complejidad del contexto operacional específico de cada proveedor de servicios?	☐ SI ☐ NO	

Cap. 11	¿Considera la eficacia de la seguridad operacional acordada los recursos de cada proveedor de servicios para tratar los riesgos de seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Se expresa la eficacia de la seguridad operacional acordada mediante múltiples indicadores de seguridad operacional y objetivos de seguridad operacional, en vez de uno solo, así como mediante planes de acción?	☐ SI ☐ NO	
Cap. 11	¿Se examina periódicamente la eficacia de la seguridad operacional acordada para asegurar que siga siendo pertinente y apropiada para los proveedores de servicios?	☐ SI ☐ NO	
Componente 3 — GARANTÍA DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS			
Elemento 3.1 — Vigilancia de la seguridad operacional			
Cap. 11	¿Ha establecido [Estado] mecanismos para asegurar que la identificación de peligros y la gestión de riesgos de seguridad operacional por los proveedores de servicios se ajusten a los controles reguladores establecidos?	☐ SI ☐ NO	
Cap. 11	¿Incluyen los mecanismos establecidos inspecciones, auditorías y encuestas para asegurar que los controles reguladores de los riesgos de seguridad operacional se integran apropiadamente en los SMS de los proveedores de servicios?	☐ SI ☐ NO	
Cap. 11	¿Aseguran los mecanismos establecidos que los controles regulares de los riesgos de seguridad operacional se llevan a la práctica conforme a su diseño?	☐ SI ☐ NO	
Cap. 11	¿Aseguran los mecanismos establecidos que los controles regulares de los riesgos de seguridad operacional tienen el efecto previsto en dichos riesgos?	☐ SI ☐ NO	
Cap. 11	¿Se realizan exámenes regulares y periódicos respecto del ALoS de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Consideran los exámenes cambios que puedan afectar al SSP de [Estado] y su ALoS, recomendaciones de mejoras y mejores prácticas compartidas en todo el Estado?	☐ SI ☐ NO	
Cap. 11	¿Se realizan exámenes regulares y periódicos para evaluar si el SSP de [Estado] y su ALoS siguen siendo apropiados al alcance y complejidad de las operaciones de aviación en el Estado?	☐ SI ☐ NO	
Cap. 11	¿Existe un proceso para evaluar la efectividad de los cambios relacionados con el SSP?	☐ SI ☐ NO	
Elemento 3.2 — Recopilación, análisis e intercambio de datos sobre seguridad operacional			
Cap. 11	¿Ha establecido [Estado] mecanismos para asegurar la captura y almacenamiento de datos sobre peligros y riesgos de seguridad operacional a nivel tanto individual como global en el Estado?	☐ SI ☐ NO	
Cap. 11	¿Ha establecido [Estado] mecanismos para preparar información a partir de los datos almacenados y promover el intercambio de información de seguridad operacional con los proveedores de servicios u otros Estados, según corresponda?	☐ SI ☐ NO	
Cap. 11	¿Ha establecido [Estado] un nivel aceptable de seguridad operacional (ALoS) relativo a su SSP?	☐ SI ☐ NO	
Cap. 11	¿Combina el ALoS relativo al SSP de [Estado] elementos de medición de la seguridad operacional y medición de la eficacia de la seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Es el ALoS de [Estado] proporcional a la complejidad de las actividades de aviación dentro de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Existe dentro de [Estado] un protocolo para elaborar y mantener un conjunto de parámetros para medir la implantación realista del SSP?	☐ SI ☐ NO	
Elemento 3.3 — Fijación de objetivos en función de los datos de seguridad operacional para la vigilancia de los elementos más preocupantes o que requieren mayor atención			
Cap. 11	¿Ha elaborado [Estado] procedimientos para priorizar las inspecciones, auditorías y encuestas relacionadas con los elementos que plantean más preocupación o que requieren mayor atención en materia de seguridad operacional?	☐ SI ☐ NO	
Cap. 11	¿Es la priorización de inspecciones y auditorías resultado del análisis de datos sobre peligros, sus consecuencias en las operaciones y los riesgos de seguridad operacional evaluados?	☐ SI ☐ NO	

Componente 4 — PROMOCIÓN DE LA SEGURIDAD OPERACIONAL POR LOS ESTADOS			
Elemento 4.1 — Instrucción, comunicación y divulgación internas de la información sobre seguridad operacional			
Cap. 11	¿Proporciona [Estado] instrucción interna, conocimiento e intercambio de información relacionada con la seguridad operacional dentro de las organizaciones de aviación de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Existen procesos de comunicación dentro de [Estado] para asegurar que la información sobre las funciones y productos del SSP se dan a conocer a las organizaciones de aviación de [Estado] en forma oportuna?	☐ SI ☐ NO	
Cap. 11	¿Existe un proceso para la difusión de información de seguridad operacional en todas las organizaciones de aviación de [Estado] y un medio para supervisar la efectividad de este proceso?	☐ SI ☐ NO	
Cap. 11	¿Son los procesos de comunicación (escritos, reuniones, electrónicos, etc.) proporcionales al tamaño y alcance de las organizaciones de aviación de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Se mantienen en un medio adecuado la información de seguridad y la información sobre funciones y productos del SSP?	☐ SI ☐ NO	
Elemento 4.2 — Instrucción, comunicación y divulgación externas de la información sobre seguridad operacional			
Cap. 11	¿Proporciona [Estado] educación, conocimiento de los riesgos de seguridad operacional e intercambio de información relacionada con la seguridad operacional externos?	☐ SI ☐ NO	
Cap. 11	¿Existen procesos de comunicación dentro de [Estado] que permitan promover el SSP tanto nacional como internacionalmente?	☐ SI ☐ NO	
Cap. 11	¿Existe un protocolo para la divulgación externa de información de seguridad operacional a los proveedores de servicios de [Estado] y medios para supervisar la efectividad de dicho proceso?	☐ SI ☐ NO	
Cap. 11	¿Existen en [Estado] procesos de comunicación para asegurar que la información sobre funciones y productos del SSP se ponen en conocimiento de los proveedores de servicios de [Estado] en forma oportuna?	☐ SI ☐ NO	
Cap. 11	¿Existen procesos de comunicación (escrita, reuniones, electrónico, etc.) proporcionales al tamaño y alcance de los proveedores de servicios de [Estado]?	☐ SI ☐ NO	
Cap. 11	¿Se establecen y mantienen en un medio adecuado la información de seguridad operacional y la información sobre funciones y productos del SSP?	☐ SI ☐ NO	

— — — — — — — — — —

INTENCIONALMENTE EN BLANCO

Apéndice 6

ORIENTACIÓN PARA LA ELABORACIÓN DE UNA POLÍTICA DE CUMPLIMIENTO Y PROCEDIMIENTOS DE CUMPLIMIENTO DEL ESTADO EN UN ENTORNO SMS

POLÍTICA DE CUMPLIMIENTO

1. INTRODUCCIÓN

La presente política de cumplimiento se promulga bajo responsabilidad legal en [reglamentos de aviación civil aplicables del Estado, órdenes de navegación aérea o normas regulatorias].

2. PRINCIPIOS

a) Esta política de cumplimiento es la culminación de un examen completo por [AAC del Estado] de su capacidad y reglamentos para evaluar las actividades de seguridad operacional de los proveedores de servicios.

b) La implantación de sistemas de gestión de la seguridad operacional (SMS) exige que [AAC del Estado] elabore un enfoque flexible del cumplimiento en este marco de seguridad operacional en evolución realizando, al mismo tiempo, funciones de cumplimiento en forma equitativa, práctica y coherente. Un enfoque flexible del cumplimiento en un entorno SMS debería basarse en dos principios generales.

c) El primer principio general es elaborar procedimientos de cumplimiento que permita a los proveedores de servicios encargarse de sucesos que suponen algunas desviaciones respecto de la seguridad operacional, y

d) resolverlos, internamente, en el contexto del sistema de gestión de la seguridad operacional (SMS) del proveedor de servicios y a satisfacción de la autoridad competente. Las transgresiones intencionales de [Ley de aviación civil del Estado] y [Reglamentos de aviación civil del Estado] se investigarán y pueden ser objeto de medidas disciplinarias convencionales, si corresponde.

e) El segundo principio general es que ninguna información obtenida de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) establecidos en el marco del SMS se utilizará como base para la adopción de medidas disciplinarias.

3. ALCANCE

a) Los principios subyacentes de esta declaración de política de cumplimiento procedimientos de cumplimiento conexos se aplican a los proveedores de servicio que funcionan con arreglo a los siguientes documentos de la OACI: Anexo 1 — *Licencias al personal;* Anexo 6 — *Operación de aeronaves*, Parte I — *Transporte aéreo comercial internacional — Aviones*, y Parte III — *Operaciones internacionales — Helicópteros;* Anexo 8 — *Aeronavegabilidad;* Anexo 11 — *Servicios de tránsito aéreo;* y Anexo 14 — *Aeródromos*, Volumen I — *Diseño y operaciones de aeródromos*.

b) En el contexto de esta orientación, el término “proveedor de servicios” se refiere a toda organización que proporciona servicios de aviación. El término incluye además a las organizaciones de instrucción reconocidas que están expuestas a riesgos de seguridad operacional mientras prestan servicios, los explotadores de aeronaves, los organismos de mantenimiento reconocidos, las organizaciones responsables del diseño de tipo o los fabricantes de aeronaves, los proveedores de servicios de tránsito aéreo y los aeródromos certificados, según corresponda.

4. GENERALIDADES

a) [Proveedor de servicios] establecerá, mantendrá y cumplirá un SMS proporcional al tamaño, carácter y complejidad de las operaciones cuya realización se autoriza en su certificado de operaciones y a los peligros y riesgo de seguridad operacional relacionados con esas operaciones.

b) Para elaborar una política de cumplimiento que apoye la implantación del SMS, inspectores de [AAC del Estado] mantendrán una comunicación abierta con los proveedores de servicios.

c) Cuando un proveedor de servicios que opera en el marco de un SMS transgrede involuntariamente [Ley de aviación civil o reglamentos de aviación civil], se aplicarán procedimientos de examen específicos. Estos procedimientos permitirán al inspector de [AAC del Estado] responsable de la vigilancia del proveedor de servicios la oportunidad de entablar un diálogo con la organización regida por el SMS. El objetivo de este

diálogo es convenir medidas correctivas propuestas y un plan de acción que trate adecuadamente las deficiencias que llevaron a la transgresión y brindar al proveedor de servicios tiempo razonable para implantarlas. Este enfoque se dirige a nutrir y mantener una efectiva notificación de seguridad operacional, por la cual los empleados del proveedor de servicios pueden notificar deficiencias y peligros de seguridad operacional sin temor a medidas punitivas. Por consiguiente, el proveedor de servicios puede, sin asignar culpas y sin temor de medidas disciplinarias, analizar el suceso y los factores de la organización o individuales que puedan haber conducido al mismo, a efectos de incorporar medidas correctivas que mejor contribuyan a prevenir repeticiones.

5. **MEDIDAS CORRECTIVAS**

[AAC del Estado], mediante el inspector responsable de la vigilancia del proveedor de servicios, evaluará las medidas correctivas propuestas por el proveedor de servicios o los sistemas actualmente implantados para tratar el suceso que llevó a la transgresión. Si las medidas correctivas se consideran apropiadas y que podrían prevenir repeticiones y fomentar el futuro cumplimiento, el examen de la violación se dará por concluido sin medidas disciplinarias. En los casos en que las medidas correctivas o los sistemas implantados se consideren inapropiados, [AAC del Estado] continuará interactuando con el proveedor de servicios para encontrar una solución satisfactoria a efectos de prevenir la adopción de medidas disciplinarias. No obstante, en casos en que el proveedor de servicios se niegue a tratar el suceso y proporcionar medidas correctivas efectivas, [AAC del Estado] considerará la adopción de medidas disciplinarias u otras medidas administrativas con respecto al certificado.

6. **PROCEDIMIENTOS DE CUMPLIMIENTO**

Las transgresiones de los reglamentos de aviación pueden ocurrir por muchas razones diferentes, desde una genuina mala interpretación de los reglamentos a la desconsideración total por la seguridad operacional. [AAC del Estado] cuenta con una gama de procedimientos de cumplimiento para tratar efectivamente las obligaciones de seguridad operacional en el marco de [Ley estatal aplicable] a la luz de circunstancias diferentes. Estos procedimientos pueden resultar en una variedad de medidas, a saber:

a) asesoramiento profesional;

b) instrucción correctiva; o

c) variación, suspensión y cancelación de autorizaciones.

7. IMPARCIALIDAD DE LAS MEDIDAS DE CUMPLIMIENTO

Las decisiones en materia de cumplimiento no deberían estar influidas por:

a) conflictos personales;

b) consideraciones de género, raza, religión, opiniones o afiliación política; o

c) el poder personal, político o financiero de los involucrados.

8. PROPORCIONALIDAD DE LAS RESPUESTAS

Las decisiones de cumplimiento deberían ser proporcionales a las transgresiones identificadas y a los riesgos de seguridad operacional que ellas provocarían, sobre la base de dos principios:

a) [AAC del Estado] adoptará medidas contra aquellos que en forma continua y deliberada operan sin respetar los reglamentos de aviación civil; y

b) [AAC del Estado] procurará educar y promover la instrucción o supervisión de aquellos que demuestren compromiso a resolver deficiencias de seguridad operacional.

9. JUSTICIA NATURAL Y RENDICIÓN DE CUENTAS

Las decisiones de cumplimiento deberían:

a) ser justas y ajustarse al debido proceso;

b) ser transparentes para todos los involucrados;

c) tener en cuenta las circunstancias del caso y la actitud/acciones del proveedor de servicios cuando se considere la aplicación de medidas;

d) ser medidas o decisiones coherentes con circunstancias iguales o similares; y

e) estar sujetas a exámenes internos y externos apropiados.

10. EXCEPCIONES

a) Esta política no se aplica si hay pruebas de intentos deliberados de ocultar el incumplimiento.

b) Esta política no se aplica si el proveedor de servicios no está en condiciones de proporcionar confianza en sus medios de identificación de peligros y de gestión de riesgo de seguridad operacional.

c) Esta política no se aplica si el proveedor de servicios es un violador reiterado. Un violador reiterado es un violador que, en el [período], pasado, ha ejecutado las mismas violaciones o violaciones muy similares.

d) En tales circunstancias, se aplicará la matriz de sanciones (o medición aplicable) de los procedimientos de cumplimiento establecidos.

(Firma) _____

Ejecutivo responsable del Estado

— — — — — — — — — —

INTENCIONALMENTE EN BLANCO

Procedimientos de cumplimiento en un entorno SMS

1. GENERALIDADES

En el marco del programa estatal de seguridad operacional (SSP) de [Estado], [AAC del Estado] es responsable de la vigilancia de los titulares de certificados que operan en un entorno SMS. Los procedimientos de cumplimiento proporcionan orientación para los responsables de la vigilancia de los proveedores de servicios que operan en un entorno SMS asesorándoles sobre la repuesta apropiada a acciones u omisiones para garantizar que si se adoptan medidas de cumplimiento éstas tendrán éxito. Los procedimientos de cumplimiento desempeñan una función de apoyo en el proceso, y la decisión final sobre cualquier aspecto de cumplimiento es responsabilidad del Ejecutivo responsable.

2. APLICACIÓN

a) Estos procedimientos se aplican a transgresiones que pueden haber sido cometidas por personas o proveedores de servicios que realizan actividades en el marco de un SMS.

b) Estos procedimientos entran en vigor el [fecha]. Remplazan y sustituyen procedimientos anteriores indicados en [Reglamentos de aviación civil del Estado].

c) Cuando los proveedores de servicios han demostrado su disposición a realizar sus operaciones en el marco de un SMS, pueden aplicarse procedimientos de cumplimiento de SMS con respecto a aquellos proveedores de servicios que, aunque no cuentan con un SMS aceptado, han implantado algunos componentes básicos esenciales de un SMS y están tramitando la plena implantación.

d) [AAC del Estado] no aplicará procedimientos de cumplimiento SMS a los proveedores de servicios que, después de iniciarse una investigación de una transgresión, aducen arbitrariamente que están elaborando un SMS. Estos procedimientos se aplicarán a los proveedores de servicios que han participado diligentemente en el desarrollo de un SMS que en última instancia satisfaría los requisitos de los reglamentos SMS pertinentes, y están aplicando un “enfoque en fases” similar al indicado en los textos de asesoramiento publicados [AM-xxx] de [AAC del Estado] — Guía de procedimientos de implantación para SMS.

e) Cuando los proveedores de servicios no han demostrado estar funcionando en un entorno SMS, las medidas de cumplimiento pueden aplicarse sin las ventajas de los procedimientos que se mencionan en el punto 3.

3. PROCEDIMIENTOS

a) Para fines de determinar si debería realizarse una investigación aplicando procedimientos de cumplimiento SMS, será necesario que los investigadores disciplinarios de la aviación determinen la condición de implantación del SMS del proveedor de servicios específico. Esta determinación podría efectuarse inicialmente mediante comunicación entre los investigadores y el inspector principal responsable de la vigilancia y aceptación del proveedor de servicios que se está investigando.

b) El inspector principal determinará si el proveedor de servicios satisface los criterios mencionados anteriormente para los procedimientos de cumplimiento SMS. Para facilitar la evaluación inicial, [AAC del Estado] puede preparar una lista de proveedores de servicios que han iniciado el proceso de elaboración e implantación de un SMS. Si esta lista se pone en conocimiento de los encargados del cumplimiento, ello ayudará a los investigadores en la adopción de decisiones respecto de la aplicación de procedimientos de cumplimiento SMS.

c) Durante el “enfoque en fases” del SMS del proveedor de servicios, [AAC del Estado] aplicará los procedimientos de cumplimiento del SMS a los proveedores de servicios que no han implantado plenamente el SMS, siempre que se satisfagan ciertas condiciones.

d) [AAC del Estado] exigirá, como mínimo, que se satisfagan las tres condiciones siguientes antes de poder aplicar los procedimientos de cumplimiento SMS:

i) el proveedor de servicios cuenta con un programa efectivo de notificación interna de peligros apoyado por la administración superior;
ii) el proveedor de servicios cuenta con un proceso proactivo de análisis de sucesos proporcional al tamaño y complejidad de sus operaciones y adecuado para determinar factores causales y elaborar medidas correctivas;
iii) la información obtenida del proceso a que se hace referencia en el párrafo 3, adecuadamente protegida para no poner en peligro el SDCPS, se comunica, a petición, al inspector principal asignado al proveedor de servicios específicos.

3.1 Informe inicial de violación

Los inspectores de cumplimiento de la aviación deberían realizar un análisis preliminar en todos los casos en que se detecte una transgresión o cuando se recibe información sobre una posible transgresión.

3.2 Análisis preliminar

a) Las preguntas siguientes deberían considerarse sobre la base de la información recibida:

i) ¿Hay motivo razonable para creer que una persona u organización que realiza actividades en el marco de un SMS puede haber cometido una transgresión?
ii) ¿Es el carácter del suceso tan grave que sería necesario considerar medidas disciplinarias?
iii) ¿Existen pruebas perecederas que deberían protegerse para las acciones disciplinarias?

3.3 Provisión de apoyo efectivo

a) Cuando las tres preguntas tienen respuesta afirmativa, deberá notificarse al inspector principal identificando el suceso y la transgresión.

b) Cuando se solicite, los investigadores de cumplimiento en aviación proporcionarán apoyo efectivo al Ejecutivo responsable brindando asesoramiento sobre la respuesta apropiada a la transgresión, para asegurar que si se adoptan medidas disciplinarias, éstas tendrán éxito. El apoyo al Ejecutivo responsable comprende recoger y asegurar pruebas perecederas.

3.4 Iniciación de una investigación de cumplimiento

Una investigación de cumplimiento se iniciará solamente a petición del inspector principal, no de los investigadores de cumplimiento.

3.5 Inmunidad

Ninguna información obtenida de un SDCPS establecido en el marco de un SMS se utilizará como base para la adopción de medidas disciplinarias.

Nota.— La política de cumplimiento de SMS y procedimientos conexos también pueden aplicarse a explotadores extranjeros de servicios aéreos que funcionan en el marco de los reglamentos SMS, se ajustan a los requisitos y orientación establecidos por la Organización de Aviación Civil Internacional (OACI) y satisfacen las condiciones expresadas en este apartado 3

— — — — — — — — — —

INTENCIONALMENTE EN BLANCO

Apéndice 7

IMPLEMENTACION DEL SMS EN LAS ORGANIZACIONES DE MANTENIMIENTO APROBADAS (MRAC 145)

ASUNTO: IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS) EN UNA ORGANIZACIÓN APROBADA MRAC 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 MRAC 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 Sistema RAC y para el cumplimiento de los requisitos establecidos en el MRAC 145.66.

Sección B – Alcance

El alcance está orientado a los siguientes aspectos:

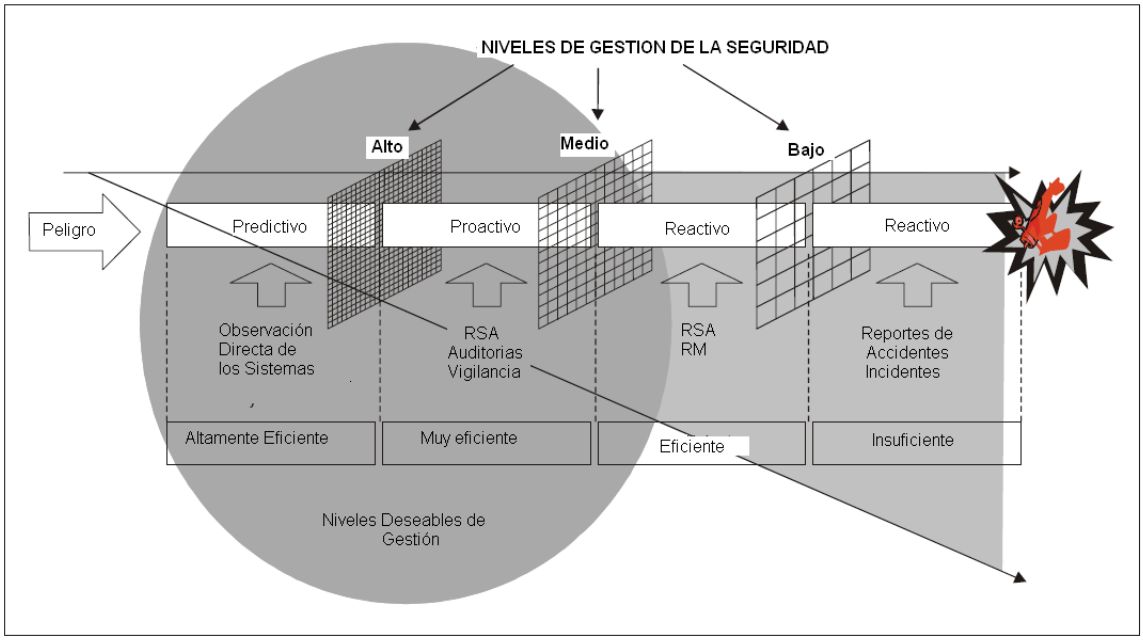
a. Proporcionar una ayuda a las organizaciones de mantenimiento, que soliciten o estén aprobadas bajo MRAC 145, para la correcta interpretación del requisito MRAC 145.66.

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 o con un método de gestión del riesgo 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. Se estima que cada una de estas fases tiene una duración de un año.

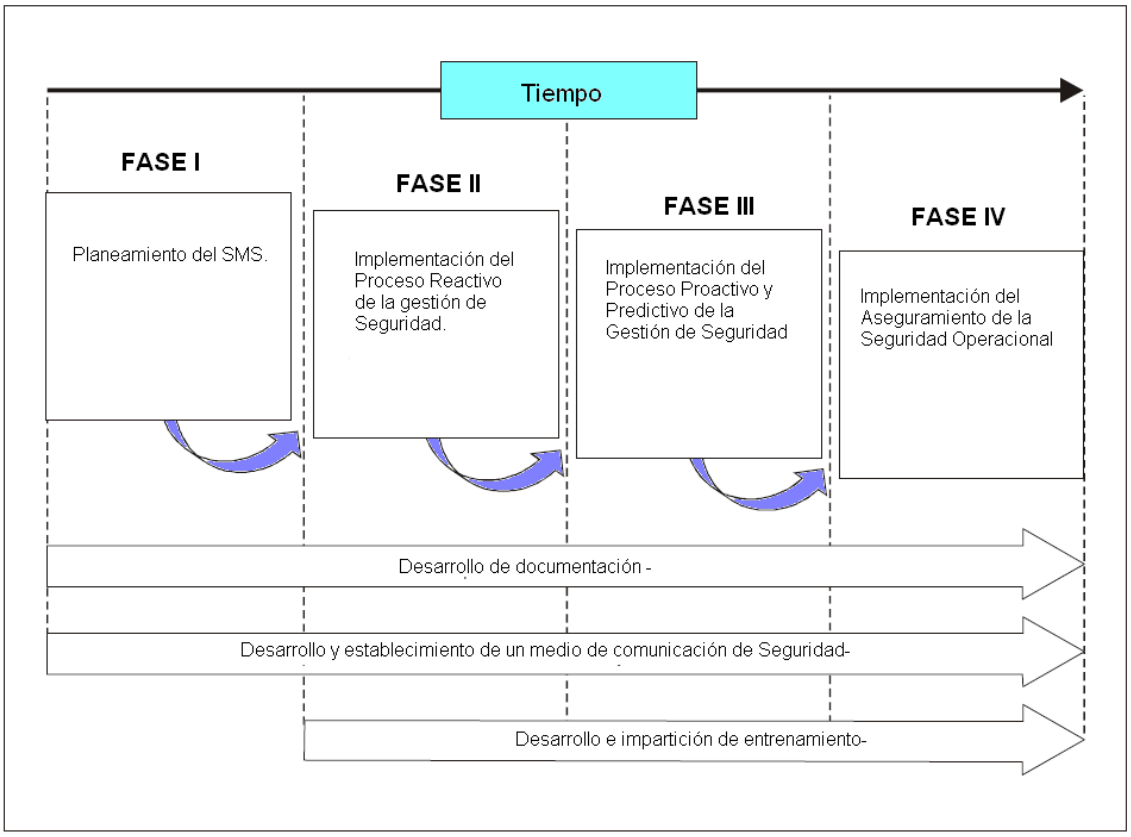


Figura 2

e. Esta circular de asesoramiento está vinculada al cumplimiento del requisito MRAC 145.66; que requiere la implementación del SMS, recomendando el proceso de 4 fases para la implementación.

f. Para uso de esta CA las expresiones “debería”, “es necesario que” y “tiene que” quieren expresar que es altamente recomendable la utilización del método presentado y no son requisitos adicionales de la MRAC 145, sino más bien un desglose y explicación de ese requisito.

Sección D - Implementación del Sistema de Gestión de Seguridad operacional

a) <u>Fase 1 Planeamiento</u>

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 deberían haber sido concluidas de forma satisfactoria para la autoridad, de conformidad con los requerimientos establecidos en la regulación MRAC 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 MRAC 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

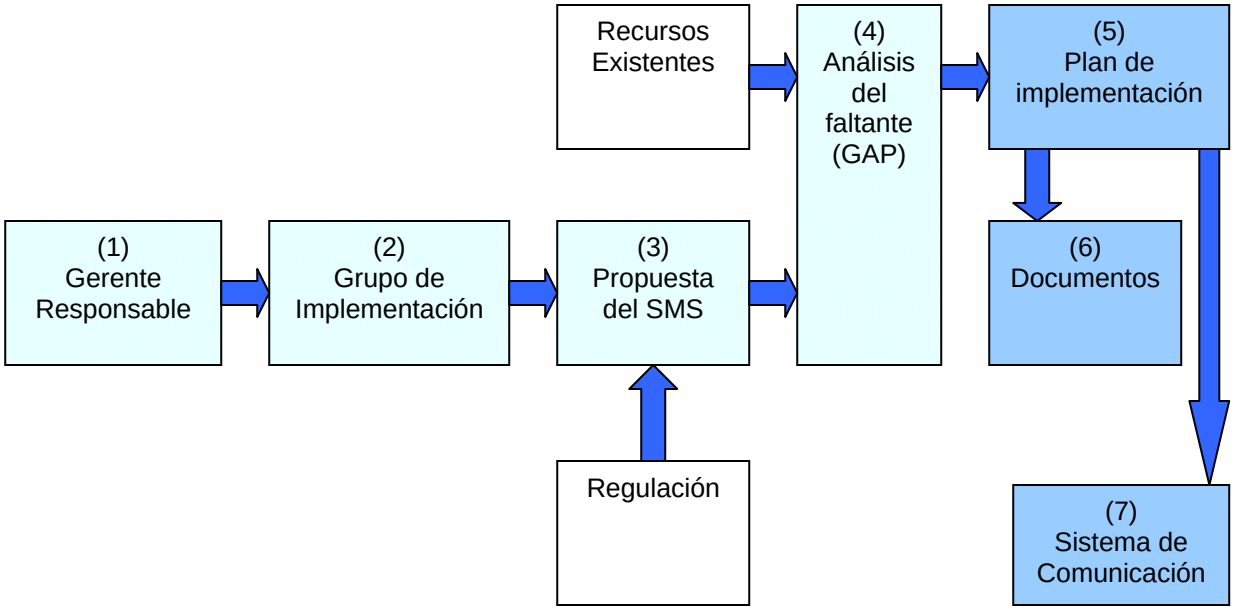


Figura 3

3. <u>Identificar el gerente</u> responsable **<u>y las responsabilidades de los gerentes</u>**.

i. **<u>Identificar al Gerente Responsable.</u>**

A. La organización tiene que identificar el Gerente responsable, que debería 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, deberían ser la autoridad y responsabilidades que él debería 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 debería 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 que no existan motivos (de carácter estratégico o económico) que degraden la seguridad del trabajo efectuado en cumplimiento fiel a lo establecido por las MRACs. Para garantizar que los recursos estén disponibles no siempre significa que se los deba adquirir, sino que éstos deberían 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 MRAC 145 en cada una de las OMs a su cargo; y en el aspecto técnico, se requiere que al menos tenga conocimiento básico del MRAC 145. El Gerente Responsable debería 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. (ver apéndice 6)

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.**

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 deberían 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 MRAC145.

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

G. Dependiendo del tamaño de la OM, las funciones de las personas que son parte 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.

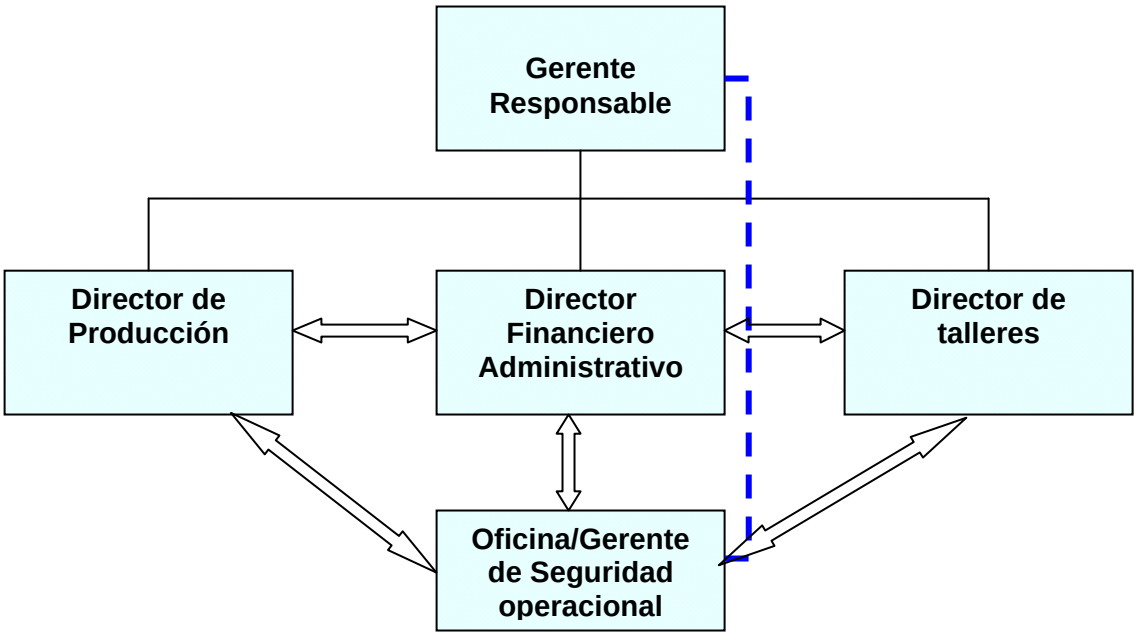


Figura 4

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 y los marcos regulatorios establecidos por OACI.

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.

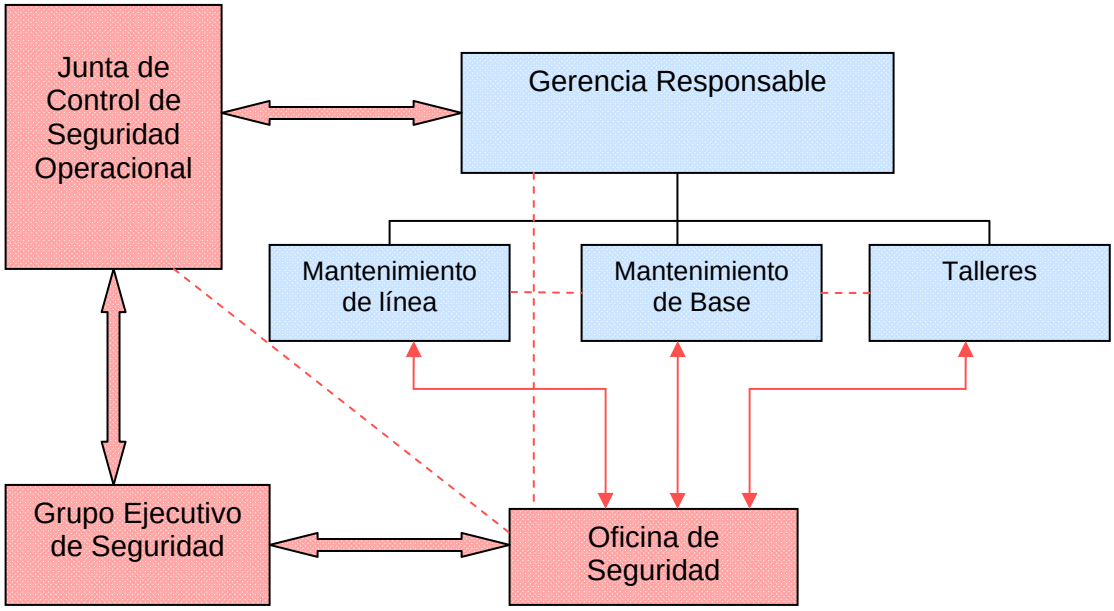


Figura 5

4. Identificar responsable de implementación SMS

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. El Gerente de Seguridad Operacional debería ser nominado ante la Autoridad para su aceptación.

iii. El Gerente de Seguridad Operacional también debería 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 debería 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. <u>Objetivos y Política de Seguridad Operacional</u>

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

B. La organización de mantenimiento debería definir su política de Seguridad Operacional la cual debería cumplir con los requerimientos nacionales e internacionales, según corresponda y esta política debería ser firmada por el Gerente Responsable de la organización. La política debería 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 debería 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 deberían ser claros y medibles para que se pueda determinar del desempeño del sistema.

D. Se debería tener 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 debería 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: *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 debería establecer la responsabilidad del Gerente Responsable y los demás gerentes, jefes de departamento o encargados de áreas funcionales dentro del SMS. Se deberían 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 debería 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 debería 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 debería 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 debería incluir acciones que se deberían tomar para comunicar la condición existente a las diferentes entidades involucradas y las personas interesadas. Por otra parte el plan debería estar diseñado

para responder de forma adecuada cuando sea requerido por otro SMS. La siguiente ilustración es un ejemplo del proceso del PRE.

Figura 6

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

M. La documentación debería 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 la MRAC 145 y los anteriores. 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 MRAC 145 debería 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 debería 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 debería brindarse al personal.

E. *Proceso de evaluación de riesgos y acciones de mitigación*. La Organización de Mantenimiento Aprobada MRAC 145 debería 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 debería 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 MRAC 145 debería 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 debería 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 debería 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 deberían incluir evaluaciones cualitativas y cuantitativas. Los resultados de la supervisión deberían 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 riesgos.

E. La Organización de Mantenimiento Aprobada MRAC 145 debería 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 debería 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 50 reportes de seguridad.

v. Promoción de la Seguridad Operacional

A. *Entrenamiento y Educación*. La Organización de Mantenimiento Aprobada MRAC 145 debería 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 debería ser apropiada según la participación particular en el SMS.

B. La Organización de Mantenimiento aprobada MRAC 145 debería 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 del 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 se 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 derivarán entonces una serie de actividades necesarias para la implementación del sistema y según lo que se estableció el plan consiste en asignar responsables para cada actividad y tiempos para desarrollo; ahora también debería 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.

En la segunda fase se deberían desarrollar los procesos de gestión de riesgo reactivos, según definió la organización en la descripción del sistema. 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 deberían 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 debería 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 debería desarrollar los procedimientos para recolectar reportes internos y registrar los hechos, peligros y otros temas relacionados en materia de seguridad. La reunión oportuna de datos 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 debería 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 debería 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 deberían 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 debería 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 deberían 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 debería ser complementado mediante un informe escrito.

iv. Como mínimo, los formularios para emitir reportes deberían 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 deberían 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 debería 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, deberían 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 debería 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 deberían 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 peligro potencial elevado deberían investigarse con mayor profundidad que aquellos que muestran un peligro potencial bajo.

B. El proceso de investigación debería 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 deberían 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 debería confiar en el investigador y el proceso de investigación debería 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.

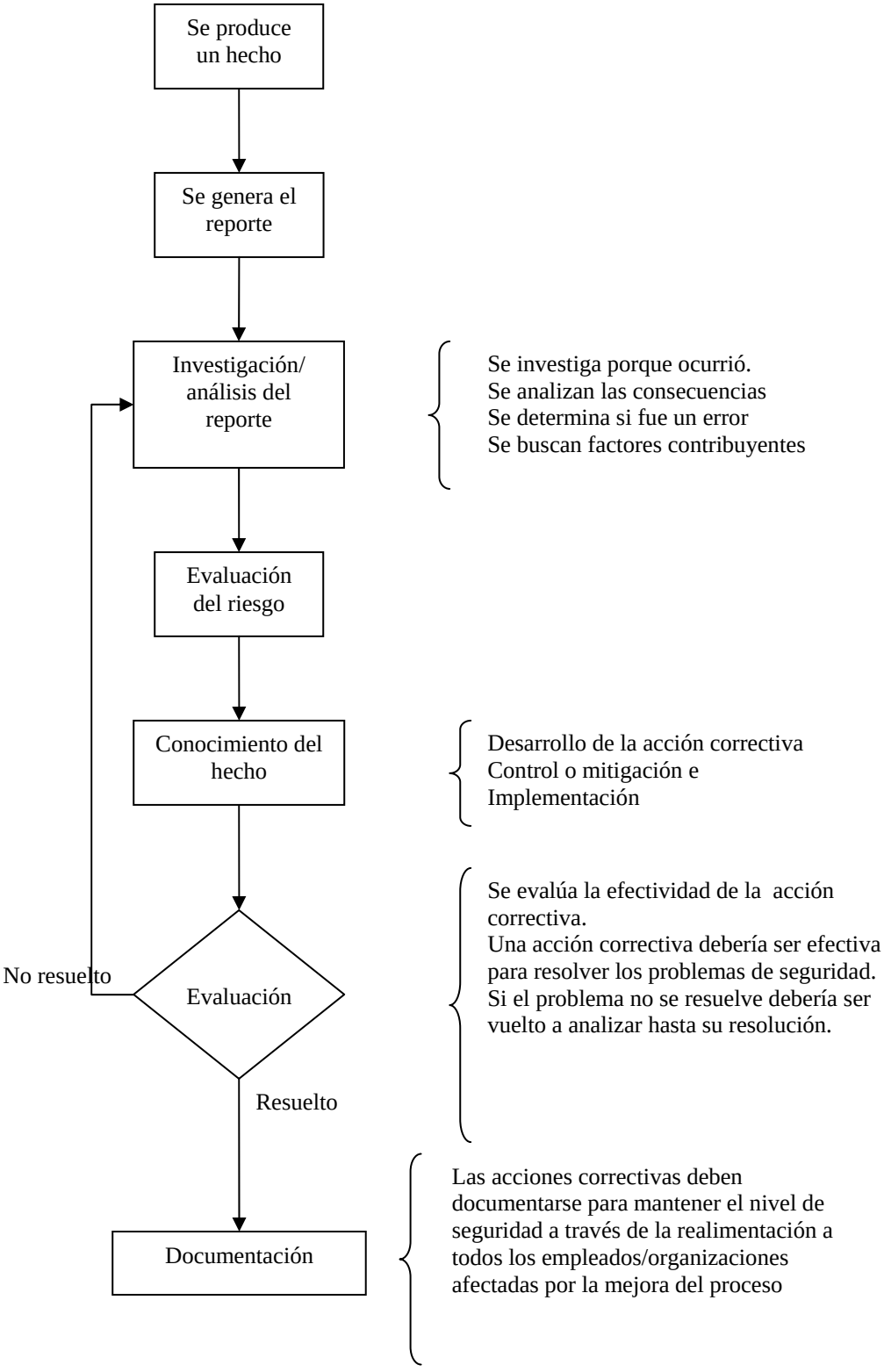

Se produce un hecho
Se genera el reporte
Investigación/ análisis del reporte
Se investiga porque ocurrió.
Se analizan las consecuencias
Se determina si fue un error
Se buscan factores contribuyentes
Evaluación del riesgo
Conocimiento del hecho
Desarrollo de la acción correctiva
Control o mitigación e
Implementación
Evaluación
No resuelto
Se evalúa la efectividad de la acción correctiva.
Una acción correctiva debería ser efectiva para resolver los problemas de seguridad.
Si el problema no se resuelve debería ser vuelto a analizar hasta su resolución.
Resuelto
Documentación
Las acciones correctivas deben documentarse para mantener el nivel de seguridad a través de la realimentación a todos los empleados/organizaciones afectadas por la mejora del proceso

Figura 7

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 deberían tenerse en cuenta al desarrollar un SMS.

i. Procedimientos para reportar hechos

A. El procedimiento para reportar hechos o peligros deberían ser tan simple como sea posible. Los procedimientos para presentar los reportes deberían ser claros, estar bien documentados e incluir detalles acerca de dónde y a quien deberían 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 debería 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 debería 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 debería 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, deberían 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 Improbable	**18**	**19**	**23**	**24**	**25**

Ejemplo de matriz de análisis de riesgos

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 debería 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 debería 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 8

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. <u>Plan de acciones correctivas</u>

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 debería 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 debería 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 debería tomar el Gerente Responsable para impedir que se repita. Estas medidas deberían concentrarse en un cambio de sistema. El segundo componente a un cronograma para la implementación de las acciones correctivas a largo plazo. Estas acciones deberían 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 debería 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 debería 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 deberían monitorearse y evaluarse regularmente. Las actividades de seguimiento deberían 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 debería 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 debería 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 debería determinar qué requerimientos de instrucción o capacitación se necesitan en cada área de trabajo. Se debería 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 deberían 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 deberían recibir una mayor capacitación, la cual debería 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 deberían 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 deberían 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.

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 deberían 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 instruido 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

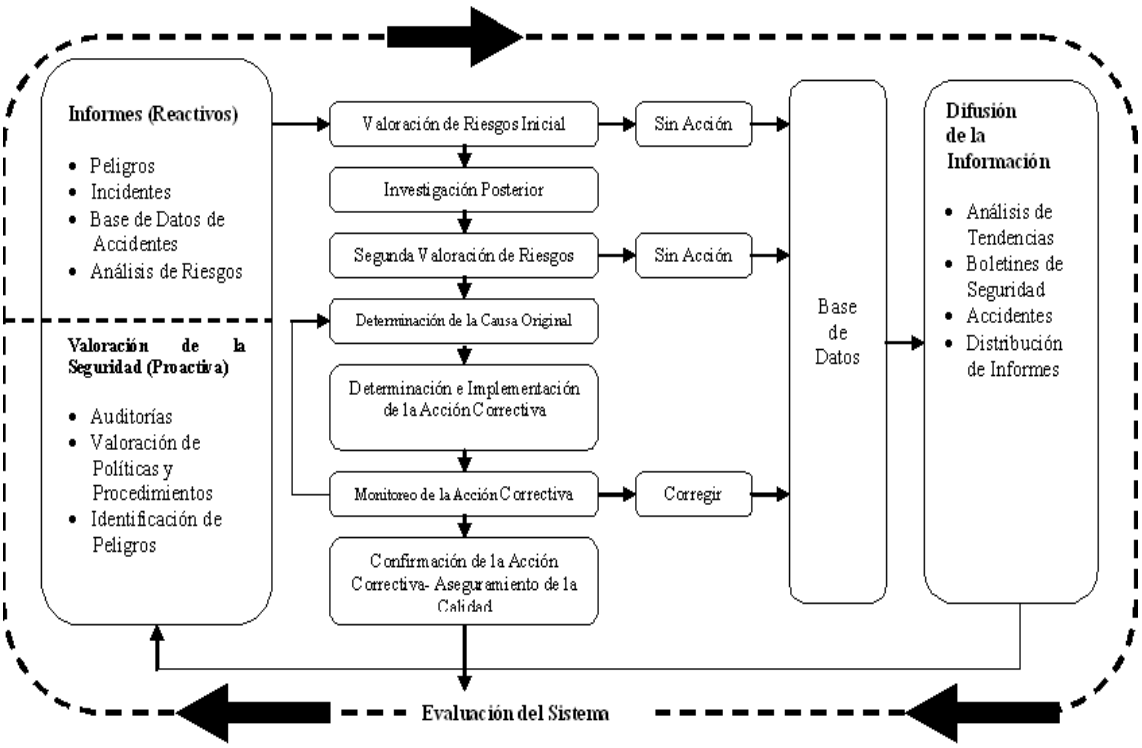


Figura 9

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 identifican 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 debería 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. Frecuencia de la valoración

La valoración de la seguridad debería 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. Identificación de peligros.

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 activa 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 debería crear un registro de peligros que afectan a la organización, que requieren una supervisión activa y continua 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 deberían 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 debería 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 que exista 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 debería estar conectado con los objetivos y metas de la organización. Por ejemplo:

Riesgo número 1	Daños que sufre la aeronave por equipos no protegidos
Objetivo 1	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 período 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 debería 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 debería 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 debería 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 deberían 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**

1. **La Fase 4** es la fase final del proceso de implementación del SMS. En esta fase la garantía de Seguridad Operacional es implementada 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 diferentes períodos.

   Al finalizar la Fase 4, las siguientes actividades deberian 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 requieren 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 continuen 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 deberia 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 deberia 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, deberia quedar claro que las OMAs actualmente cuenta con un proceso de evaluación, analisis 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 deberia 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 debería alcanzar mientras conduce sus operaciones. Este desempeño de Seguridad debería ser acordado entre el Estado y la OMA, como el mínimo aceptable que la OMA debería 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 debería 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 debería hacerse durante el proceso de diseño toma relevancia durante una situación de cambio. Siempre existen algunas actividades que son más importantes que otras. Los equipos y actividades que son considerados más críticos deberían 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 debería 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 debería 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 debería 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 debería 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. Mejora continua del SMS.

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 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 deberían 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 debería 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 deberían comunicarse a toda la organización

I. **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 deberían incluirse en un manual aprobado, o, si se desarrolló, en el Manual de 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 puntos 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 debería 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.

ii. 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).

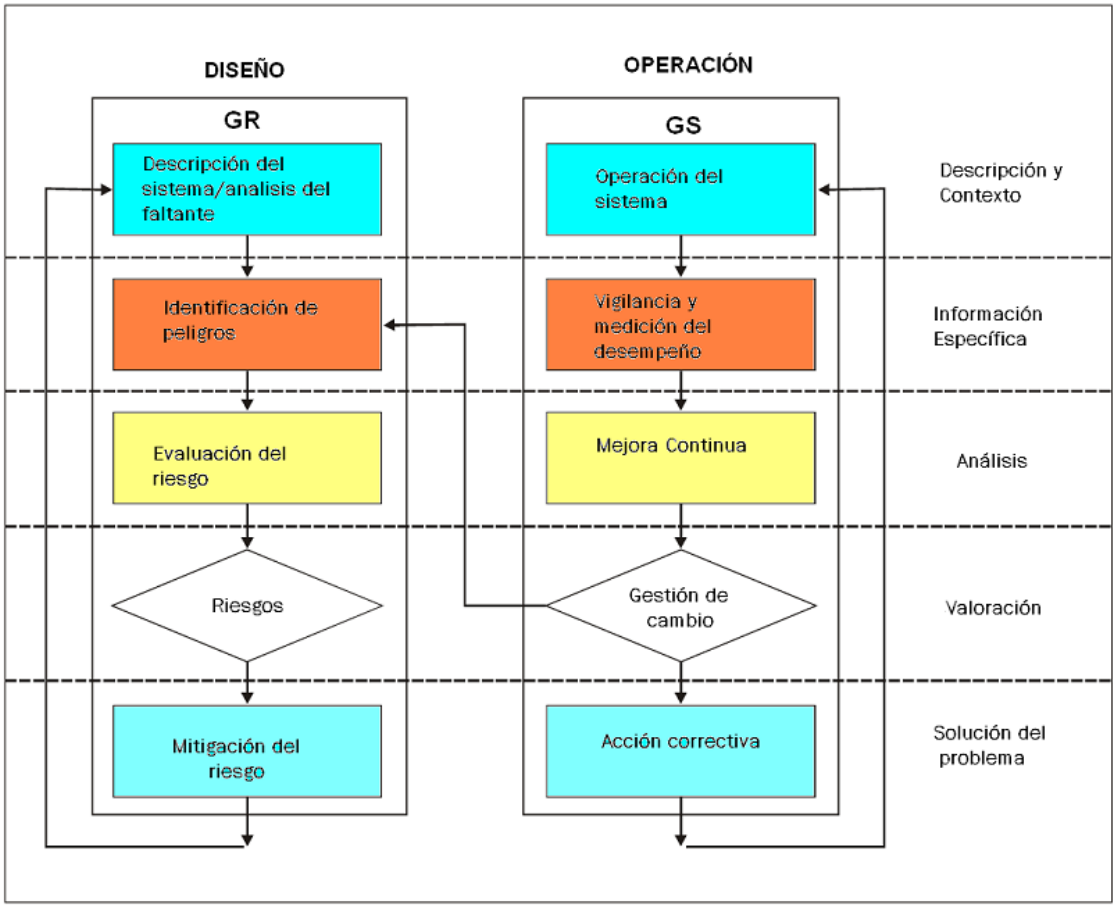


Figura 10

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 debería 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 ambos aspectos de seguridad y calidad sean considerados y cumplidos.

Apéndice 1

ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA MRAC 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 MRAC 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 organización documentación SMS, en papel o electrónica?		

ANALISIS DE FALTANTE SMS DE UNA ORGANIZACIÓN DE MANTENIMIENTO APROBADA MRAC 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 MRAC 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 MRAC 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		
	Revisión 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 MRAC 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 manera 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 MRAC 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 continua 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 MRAC 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?		