REPÚBLICA DEL PARAGUAY

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL

MANUAL DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

SEGUNDA EDICIÓN R00 AÑO 2017

Esta edición fue aprobada por Resolución Nº /2017.-

REGISTROS DE ENMIENDAS Y CORRIGENDOS

REGISTRO DE ENMIENDAS			
NÚM.	FECHA DE APLICACIÓN	FECHA DE ANOTACIÓN	ANOTADA POR
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

REGISTRO DE CORRIGENDOS			
NÚM.	FECHA DE APLICACIÓN	FECHA DE ANOTACIÓN	ANOTADA POR
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

*****

LISTA DE PÁGINAS EFECTIVAS

ÍTEM	TEMAS	EDICIÓN / REVISIÓN	PÁG.
TAPA		*SEGUNDA EDICIÓN - R00*	N/A
REGISTRO	ENMIENDAS Y CORRIGENDOS	*SEGUNDA EDICIÓN - R00*	I
LISTA	PÁGINAS EFECTIVAS	*SEGUNDA EDICIÓN - R00*	II
ÍNDICE		*SEGUNDA EDICIÓN - R00*	III
CAPÍTULO 1	**Definiciones.-**	*SEGUNDA EDICIÓN - R00*	1-4
CAPÍTULO 2	**Generalidades.-**		
2.2	Objetivos.-	*SEGUNDA EDICIÓN - R00*	1-6
2.3	Concepto de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	1-6
2.4	Cultura de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	1-6
2.5	Errores e infracciones.-	*SEGUNDA EDICIÓN - R00*	3-6
2.6	Indicadores de rendimiento en materia de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	5-6
CAPÍTULO 3	**Alcance y aplicabilidad.-**		
3.1	Alcance.-	*SEGUNDA EDICIÓN - R00*	1-3
3.2	Aplicabilidad y aceptación.-	*SEGUNDA EDICIÓN - R00*	1-3
3.3	Requisitos de gestión de la seguridad operacional	*SEGUNDA EDICIÓN - R00*	1-3
3.4	Política de calidad	*SEGUNDA EDICIÓN - R00*	3-3
3.5	Destinatarios.-	*SEGUNDA EDICIÓN - R00*	3-3
CAPÍTULO 4	**Identificación de los peligros y gestión de riesgos.-**		
4.3	Metodologías de identificación de peligros.-	*SEGUNDA EDICIÓN - R00*	1-7
4.4	Riesgos de la seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	1-7
4.5	Proceso de gestión de la seguridad operacional	*SEGUNDA EDICIÓN - R00*	4-7
4.6	Proceso de gestión del riesgo.-	*SEGUNDA EDICIÓN - R00*	4-7
4.7	Tabla de probabilidad del riesgo de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	5-7
4.8	Tabla de gravedad del riesgo de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	5-7
4.9	Matriz de evaluación del riesgo de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	6-7
4.10	Matriz de tolerabilidad del riesgo de seguridad operacional.-	*SEGUNDA EDICIÓN - R00*	6-7
4.11	Tabla de identificación, análisis y evaluación de riesgos.-	*SEGUNDA EDICIÓN - R00*	7-7
CAPÍTULO 5	**Planificación de la implementación del SMS.-**		
5.1	Descripción del sistema.-	*SEGUNDA EDICIÓN - R00*	1-1

****

ÍNDICE

****

CAPÍTULO 1.

DEFINICIONES

Cuando los términos y expresiones indicados a continuación se emplean en las normas y métodos recomendados para la gestión de la seguridad operacional, tienen los significados siguientes:

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

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

— hallarse en la aeronave, o

— por contacto directo con cualquier parte de la aeronave, incluso las partes que se hayan desprendido de la aeronave, o

— por exposición directa al chorro de un reactor,

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

b) La aeronave sufre daños o roturas estructurales que:

— afectan adversamente su resistencia estructural, su performance o sus características de vuelo; y

— que normalmente exigen una reparación importante o el recambio del componente afectado,

excepto por falla o daños del motor, cuando el daño se limita a un solo motor (incluido su capó o sus accesorios); hélices, extremos de ala, antenas, sondas, álabes, neumáticos, frenos, ruedas, carenas, paneles, puertas de tren de aterrizaje, parabrisas, revestimiento de la aeronave (como pequeñas abolladuras o perforaciones), o por daños menores a palas del rotor principal, palas del rotor compensador, tren de aterrizaje y a los que resulten de granizo o choques con aves (incluyendo perforaciones en el radomo); o

c) La aeronave desaparece o es totalmente inaccesible.-

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

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

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

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

AERONAVE. Toda máquina que puede sustentarse en la atmósfera por reacciones del aire que no sean las reacciones del mismo contra la superficie de la tierra.-

AVIÓN (aeroplano). Aerodino propulsado por motor, que debe su sustentación en vuelo principalmente a reacciones aerodinámicas ejercidas sobre superficies que permanecen fijas en determinadas condiciones de vuelo.-

DATOS SOBRE SEGURIDAD OPERACIONAL. Conjunto de hechos definidos o conjunto de valores de seguridad operacional recopilados de diversas fuentes de aviación, que se utiliza para mantener o mejorar la seguridad operacional.-

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

a) Investigaciones de accidentes o incidentes;

b) Notificaciones de seguridad operacional;

c) Notificaciones sobre el mantenimiento de la aeronavegabilidad;

d) Supervisión de la eficiencia operacional;

e) Inspecciones, auditorías, constataciones; o

f) Estudios y exámenes de seguridad operacional.-

ESTADO DE DISEÑO. El Estado que tiene jurisdicción sobre la entidad responsable del diseño de tipo.-

ESTADO DE FABRICACIÓN. El Estado que tiene jurisdicción sobre la entidad responsable del montaje final de la aeronave.-

ESTADO DEL EXPLOTADOR. Estado en el que está ubicada la oficina principal del explotador o, de no haber tal oficina, la residencia permanente del explotador.-

HELICÓPTERO. Aerodino que se mantiene en vuelo principalmente en virtud de la reacción del aire sobre uno o más rotores propulsados por motor que giran alrededor de ejes verticales o casi verticales.-

Nota.- *Algunos Estados emplean el término "giroavión" como alternativa de "helicóptero".-*

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

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

INDICADOR DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL. Parámetro basado en datos que se utiliza para observar y evaluar el rendimiento en materia de seguridad operacional.-

INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL. Datos sobre seguridad operacional procesados, organizados o analizados en un determinado contexto a fin de que sean de utilidad para fines de gestión de la seguridad operacional.-

LESIÓN GRAVE. Cualquier lesión sufrida por una persona en un accidente y que:

a) Requiera hospitalización durante más de 48 horas dentro de los siete días contados a partir de la fecha en que se sufrió la lesión; o

b) Ocasione la fractura de algún hueso (con excepción de las fracturas simples de la nariz o de los dedos de las manos o de los pies); o

c) ocasione laceraciones que den lugar a hemorragias graves, lesiones a nervios, músculos o tendones; o

d) ocasione daños a cualquier órgano interno; o

e) Ocasione quemaduras de segundo o tercer grado u otras quemaduras que afecten más del 5% de la superficie del cuerpo; o

f) Sea imputable al contacto, comprobado, con sustancias infecciosas o a la exposición a radiaciones perjudiciales.-

MEJORES PRÁCTICAS DE LA INDUSTRIA. Textos de orientación preparados por un órgano de la industria, para un sector particular de la industria de la aviación, a fin de que se cumplan los requisitos de las normas y métodos recomendados de la OACI, otros requisitos de seguridad operacional de la aviación y las mejores prácticas que se consideren apropiadas.-

Nota.- *Algunos Estados aceptan las mejores prácticas de la industria y hacen mención a ellas al preparar reglamentos para cumplir los requisitos del Anexo 19 y proporcionan sus fuentes o informan cómo obtenerlas.-*

META DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL. La meta proyectada o prevista del Estado o proveedor de servicios que se desea conseguir, en cuanto a un indicador de rendimiento en materia de seguridad operacional, en un período de tiempo determinado que coincide con los objetivos de seguridad operacional.-

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

PERSONAL DE OPERACIONES. Personal que participa en las actividades de aviación y está en posición de notificar información sobre seguridad operacional.-

Nota.- *Dicho personal comprende, entre otros: tripulaciones de vuelo; controladores de tránsito aéreo; operadores de estaciones aeronáuticas; técnicos de mantenimiento; personal de organizaciones de diseño y fabricación de aeronaves; tripulaciones de cabina; despachadores de vuelo; personal de plataforma y personal de servicios de escala.-*

PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP). Conjunto integrado de reglamentos y actividades destinado a mejorar la seguridad operacional.-

RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL. Logro de un Estado o un proveedor de servicios en lo que respecta a la seguridad operacional, de conformidad con lo definido mediante sus metas e indicadores de rendimiento en materia de seguridad operacional.-

RIESGO DE SEGURIDAD OPERACIONAL. La probabilidad y la severidad previstas de las consecuencias o resultados de un peligro.-

SEGURIDAD OPERACIONAL. Estado en el que los riesgos asociados a las actividades de aviación relativas a la operación de las aeronaves, o que apoyan directamente dicha operación, se reducen y controlan a un nivel aceptable.-

SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS). Enfoque sistemático para la gestión de la seguridad operacional que incluye las estructuras orgánicas, la obligación de rendición de cuentas, las responsabilidades, las políticas y los procedimientos necesarios.-

SUPERVISIÓN DE LA SEGURIDAD OPERACIONAL. Función desempeñada por los Estados para garantizar que las personas y las organizaciones que llevan a cabo una actividad aeronáutica cumplan las leyes y reglamentos nacionales relacionados con la seguridad operacional.-

VIGILANCIA. Actividades estatales mediante las cuales el Estado verifica, de manera preventiva, con inspecciones y auditorías, que los titulares de licencias, certificados, autorizaciones o aprobaciones en el ámbito de la aviación sigan

cumpliendo los requisitos y la función establecidos, al nivel de competencia y seguridad operacional que el Estado requiere.-

*****

CAPÍTULO 2.

GENERALIDADES

2.1 Este manual tiene como fin proporcionar material guía sobre el establecimiento de requisitos así como también, sobre el desarrollo y la implementación del SMS por parte de los proveedores de servicios, de acuerdo con las normas y métodos recomendados (SARPS) de la OACI.-

Nota.- *En el contexto de la gestión de la seguridad operacional, el término "proveedor de servicios" o "proveedor de productos y servicios" hace referencia a cualquier organización que proporcione productos o servicios de aviación. Por tanto, los términos abarcan organizaciones de capacitación reconocidas que están expuestas a riesgos de seguridad operacional durante la entrega de sus servicios, explotadores de aeronaves, organismos de mantenimiento reconocidos, organizaciones responsables del diseño o fabricación de aeronaves, proveedores de servicios de tránsito aéreo y aeródromos certificados.-*

2.2 OBJETIVO

El objetivo de este manual es proporcionar a los proveedores de servicios:

a) Una descripción general de los aspectos básicos de la gestión de la seguridad operacional;

b) Un resumen de los SARPS de la gestión de seguridad operacional de la OACI, incluidos en los Anexos 1, 6, 8, 11, 13 y 14;

c) Una guía sobre cómo desarrollar e implementar un SMS que cumpla con los SARPS pertinentes de la OACI, como un marco de trabajo reglamentario armonizado para la vigilancia del SMS de los proveedores de productos y servicios; y

d) Una guía sobre el desarrollo, la implantación y el mantenimiento del SMS.-

2.3 CONCEPTO DE SEGURIDAD OPERACIONAL

2.3.1 Dentro del contexto de la aviación, la seguridad operacional es "el estado donde la posibilidad de dañar a las personas o las propiedades se reduce y mantiene al mismo nivel o debajo de un nivel aceptable mediante el proceso continuo de identificación de peligros y gestión de riesgos de la seguridad operacional".-

2.3.2 Si bien la eliminación de los accidentes o incidentes graves en aeronaves sigue siendo la meta final, se reconoce que el sistema de aviación no puede estar completamente libre de peligros y riesgos asociados. Las actividades humanas o los sistemas construidos por humanos no pueden garantizar estar completamente libres de errores de operaciones y de sus consecuencias. Por lo tanto, la seguridad es una característica dinámica del sistema de aviación, por el cual los riesgos de seguridad operacional deben mitigarse continuamente. Es importante tener presente que la aceptabilidad del rendimiento en materia de seguridad operacional se ve influenciado comúnmente por las normas y la cultura tanto nacionales como internacionales. Siempre y cuando los riesgos de seguridad operacional se mantengan en un nivel de control adecuado, un sistema tan abierto y dinámico como la aviación podrá seguir gestionándose para mantener el equilibrio correcto de producción y protección.-

2.4 CULTURA DE SEGURIDAD OPERACIONAL

2.4.1 La cultura se caracteriza por tener creencias, valores, tendencias y sus conductas resultantes que se comparten entre miembros de una sociedad, grupo u

organización. Una comprensión de estos componentes culturales, además de la interacción entre sí, es importante para la gestión de la seguridad operacional. Los tres componentes culturales más influyentes son la **cultura institucional, profesional y nacional**. Una **cultura de notificación** es un componente clave de estas diferentes culturas. La mezcla de los componentes culturales puede variar enormemente entre las organizaciones y puede influenciar negativamente la notificación eficaz de peligros, el análisis colaborativo de la causa de origen y la mitigación de riesgos aceptable. La mejora continua del rendimiento en materia de seguridad operacional es posible cuando la seguridad operacional se convierte en un valor dentro de la organización, así como también, una prioridad a nivel nacional o profesional.-

2.4.2 Una cultura de seguridad operacional abarca las percepciones y creencias más comunes de los miembros de una organización en relación con la seguridad operacional del público y puede llegar a ser un comportamiento determinante de los miembros. Una cultura de seguridad operacional saludable depende en un alto grado de confianza y respeto entre el personal y la administración, y debe, por tanto, crearse y respaldarse a nivel de la administración superior.-

2.4.2.1 **La cultura institucional** hace referencia a las características y percepciones de seguridad operacional entre miembros que interactúan dentro de una entidad particular. Los sistemas de valores institucionales incluyen políticas de priorización o equilibrio que abarcan áreas como, por ejemplo, productividad versus calidad, seguridad operacional versus eficiencia, área financiera versus área técnica, profesional versus académico, y cumplimiento versus medida correctiva.-

2.4.2.2 **La cultura profesional** diferencia las características de los grupos profesionales particulares (es decir, el comportamiento característico de los pilotos en relación con aquél de los controladores de tránsito aéreo, el personal de la autoridad de aviación civil o los mecánicos de mantenimiento). Mediante la selección de personal, educación, capacitación, experiencia en el trabajo, presión de pares, etc., los profesionales tienden a adoptar el sistema de valores y desarrollar patrones de conducta coherentes con sus pares o predecesores. Una cultura profesional eficaz refleja la capacidad de los grupos profesionales de diferenciar entre los problemas de rendimiento en materia de seguridad operacional y los problemas contractuales o industriales. Una cultura profesional saludable puede describirse como la capacidad que disponen todos los grupos profesionales dentro de la organización para abordar de forma colaborativa los problemas del rendimiento en materia de seguridad operacional.-

2.4.2.3 **La cultura nacional** diferencia las características de naciones determinadas, como el papel de cada persona dentro de la sociedad, la forma en que se distribuye la autoridad, las prioridades nacionales en relación con los recursos, las responsabilidades, la moralidad, los objetivos y los diferentes sistemas legales. Desde una perspectiva de gestión de la seguridad operacional, la cultura nacional juega un gran papel en la determinación de la naturaleza y el alcance de políticas de cumplimiento reglamentario, como la relación entre el personal de la autoridad reglamentaria y el personal industrial, y el punto hasta donde se protege la información relacionada con la seguridad operacional.-

2.4.2.4 **La cultura de notificación** se origina a partir de las creencias y actitudes del personal acerca de los beneficios y los posibles perjuicios asociados con los sistemas de notificación y el efecto final que tiene en la aceptación o uso de tales sistemas. Las culturas institucional, profesional y nacional son las que más influyen en ella y, además, es un criterio para juzgar la eficacia de un sistema de seguridad operacional. Una cultura de notificación saludable apunta a diferenciar entre las desviaciones intencionales y accidentales, y a determinar el mejor curso de acción para la organización como un todo y para las personas que participan directamente.-

2.4.2.5 El éxito de un sistema de notificación depende del flujo continuo de información

del personal de primera línea. Las políticas que distinguen los actos deliberados de conducta impropia de los errores accidentales, y ofrecen una respuesta punitiva o no punitiva correspondiente, son esenciales para garantizar una notificación eficaz de deficiencias sistemáticas de seguridad operacional. Una cultura “sin culpa en lo absoluto” no solo es poco razonable, sino que no es viable. Mientras la administración obtiene información de seguridad operacional, el sistema será ineficaz si interfiere con las medidas punitivas correspondientes. Por el contrario, una cultura que no puede distinguir errores accidentales / equivocaciones de actos deliberados de conducta impropia inhibirá el proceso de notificación. Si el personal evita notificar por miedo a castigos, la administración no obtiene información de seguridad operacional importante.-

2.5 ERRORES E INFRACCIONES

2.5.1 La implementación eficaz del SMS por parte del proveedor de servicios, así como también, la vigilancia eficaz del SMS por parte del Estado, depende de una clara y mutua comprensión de los errores y las infracciones, además de la diferenciación entre ambos conceptos. La diferencia entre error e infracción yace en la intencionalidad. Mientras que un error es accidental, una infracción es un acto o una omisión deliberada que se lleva a cabo para desviarse de los procedimientos, los protocolos, las normas o las prácticas establecidos.-

2.5.2 Los errores o las infracciones pueden generar una falta de cumplimiento de los reglamentos o los procedimientos operacionales reconocidos. Las medidas punitivas tomadas en respuesta a las acciones de no cumplimiento pueden generar una reducción en la notificación de errores en ausencia de otros procesos. En consecuencia, el Estado y el proveedor de servicios deben considerar si las acciones de no cumplimiento son el resultado de una infracción o error accidental al determinar si corresponde implementar una medida punitiva, siendo los criterios normalmente si el no cumplimiento es resultado de una conducta impropia deliberada o una negligencia grave.-

2.5.3 Errores

2.5.3.1 Como se indicó previamente, un error se define como una "medida tomada o no tomada por un miembro del personal de operaciones que genera un desvío de las intenciones o expectativas del miembro del personal de operaciones o institucional”. En el contexto de un SMS, tanto la DINAC como el proveedor de servicios deben comprender y esperar que los seres humanos cometan errores sin importar el nivel de tecnología usado, el nivel de capacitación o la existencia de reglamentos, procesos y procedimientos. Una meta importante entonces es establecer y mantener defensas para reducir la probabilidad de errores e, igualmente importante, reducir las consecuencias de los errores cuando ocurre. Para lograr eficazmente esta tarea, se debe identificar, informar y analizar los errores para tomar una medida correctiva adecuada. Los errores pueden dividirse en las siguientes dos categorías:

a) **Las confusiones y omisiones** son fallas en la ejecución de una medida determinada. Las confusiones son acciones que no se llevaron a cabo según lo planificado, mientras que las omisiones son fallas de memoria. Por ejemplo, accionar la palanca de flap en lugar de la palanca de engranajes (prevista) es una confusión. Olvidar una lista de verificación es una omisión.-

b) **Las equivocaciones** son fallas en el plan de acción. Incluso si la ejecución del plan fuera correcta, no podría haber sido posible lograr el resultado esperado.-

2.5.3.2 Se deben implementar estrategias de seguridad operacional para controlar o eliminar los errores. Las estrategias para controlar errores aprovechan las defensas básicas dentro del sistema de aviación. Estas incluyen lo siguiente:

a) **Las estrategias de reducción** proporcionan intervención directa para reducir o eliminar los factores que contribuyen con el error. Entre los

ejemplos de estrategias de reducción se incluye la mejora de factores ergonómicos y la reducción de distracciones ambientales.-

b) **Las estrategias de captura** suponen que el error sucederá. La intención es "capturar" el error antes de detectar alguna consecuencia adversa del error. Las estrategias de captura son diferentes de las estrategias de reducción, ya que utilizan listas de verificación y otras intervenciones de procesamientos en lugar de eliminar directamente el error.-

c) **Las estrategias de tolerancia** hacen referencia a la capacidad de un sistema de aceptar que un error se cometerá sin experimentar consecuencias graves. La incorporación de sistemas redundantes o múltiples procesos de inspección son ejemplos de medidas que aumentan la tolerancia a errores del sistema.-

2.5.3.3 Ya que el rendimiento del personal se ve influenciado generalmente por factores institucionales, reglamentarios y ambientales, la gestión de riesgos de seguridad operacional debe incluir la consideración de políticas, procesos y procedimientos institucionales relacionados con la comunicación, la programación de personal, la asignación de recursos y las limitaciones presupuestarias que pueden contribuir con la incidencia de errores.-

2.5.4 Infracciones

2.5.4.1 Una infracción se define como "un acto deliberado de conducta impropia deliberada u omisión que genere una desviación de los reglamentos, los procedimientos, las normas o las prácticas establecidas". Sin embargo, el incumplimiento no es necesariamente el resultado de una infracción, ya que las desviaciones de los requisitos reglamentarios o procedimientos operacionales pueden ser el resultado de un error. Para complicar aún más el problema, aunque las infracciones son actos intencionales, no siempre actúan con intenciones maliciosas. Las personas pueden desviarse conscientemente de las normas, creyendo que la infracción facilita el cumplimiento de la misión sin crear consecuencias adversas. Las infracciones de esta naturaleza son errores de criterio y puede que no generen automáticamente medidas disciplinarias, según las políticas implementadas. Las infracciones de este tipo pueden categorizarse de la siguiente forma:

a) **Las infracciones situacionales** se cometen en respuesta a los factores experimentados en un contexto específico, como presión de tiempo o alta carga de trabajo.-

b) **Las infracciones rutinarias** se vuelven la forma normal de hacer negocios dentro de un grupo de trabajo. Tales infracciones se cometen en respuesta a las situaciones en las cuales el cumplimiento de los procedimientos establecidos dificulta la finalización de la tarea. Esto se puede deber a problemas de funcionalidad/viabilidad de trabajo, deficiencias en el diseño de la interfaz humana – tecnológica y otros problemas que causan que las personas adopten "soluciones", las que finalmente se vuelven rutinarias. Estas modificaciones, conocidas como "desviaciones", pueden continuar sin consecuencias, pero con el paso del tiempo pueden volverse frecuentes y generar consecuencias potencialmente graves. En algunos casos, las infracciones rutinarias tienen buenos fundamentos y pueden incorporarse como procedimientos aceptados luego de realizar una evaluación de seguridad operacional adecuada y que se demuestre que no se compromete la seguridad operacional.-

c) **Las infracciones inducidas por la organización** pueden considerarse una extensión de las infracciones rutinarias. Este tipo de infracción tiende a ocurrir cuando una organización intenta satisfacer demandas de mucha producción ignorando o extendiendo las defensas de seguridad operacional.-

2.6 INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL

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

2.6.2 Los indicadores de rendimiento en materia de seguridad operacional también proporcionan evidencia objetiva para que el regulador evalúe la eficacia del SMS del proveedor de servicios y controle el logro de sus objetivos de seguridad operacional. Los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios consideran factores como la tolerancia de los riesgos de seguridad operacional de la organización, el costo/beneficios que conlleva la implementación de las mejoras al sistema, los requisitos reglamentarios y las expectativas públicas. Se deben seleccionar y desarrollar indicadores de rendimiento en materia de seguridad operacional con el asesoramiento de la autoridad reglamentaria del proveedor de servicios. Este proceso es necesario para facilitar la agregación del regulador y la armonización de los indicadores de rendimiento en materia de seguridad operacional del proveedor de servicios para el mismo sector de aviación.-

2.6.3 Los indicadores de rendimiento en materia de seguridad operacional y los objetivos asociados deben ser aceptados por la DINAC como organismo responsable de la autorización, certificación o designación del proveedor de servicios. Los indicadores de rendimiento en materia de seguridad operacional son complementarios a cualquier requisito legal o reglamentario y no exime a los proveedores de servicios de sus obligaciones reglamentarias.-

2.6.4 El rendimiento en materia de seguridad operacional de un SMS se expresa mediante indicadores de rendimiento en materia de seguridad operacional y sus valores de alertas y objetivos correspondientes. El proveedor de servicios debe controlar el rendimiento de los indicadores actuales en el contexto de tendencias históricas para identificar cambios anormales en el rendimiento en materia de seguridad operacional. De igual forma, la configuración de objetivos y alertas debe considerar el rendimiento histórico reciente para un indicador determinado. Los objetivos de mejora deseados deben ser realistas y alcanzables para el proveedor de servicios y el sector de aviación asociado.-

2.6.5 El establecimiento de un nivel de alerta para un indicador de seguridad operacional es pertinente desde una perspectiva de control de riesgos. Un nivel de alerta es un criterio común para delinear las regiones de rendimiento aceptable de aquellas inaceptables para un indicador de seguridad operacional particular.-

2.6.6 Una gama de indicadores de rendimiento en materia de seguridad operacional de alto y bajo impacto proporcionan una comprensión más integral acerca del rendimiento en materia de seguridad operacional del proveedor de servicios. Esto garantiza que se aborden los resultados de alto impacto (por ejemplo, accidentes e incidentes graves), así como también, los eventos de bajo impacto (por ejemplo, incidentes, informes de no cumplimiento, desviaciones). Los indicadores de rendimiento en materia de seguridad operacional son básicamente diagramas de tendencias de datos que rastrean los sucesos en términos de tasas de eventos (por ejemplo, cantidad de incidentes cada 1 000 horas de vuelo). Los indicadores de alto impacto deben abordarse primero, mientras que los indicadores de bajo impacto pueden desarrollarse en una etapa más madura de la implementación del SMS.-

2.6.7 Luego de definir los indicadores de rendimiento en materia de seguridad operacional y su configuración de objetivos y alertas correspondiente, el resultado del rendimiento de cada indicador debe actualizarse y controlarse de forma regular.

También se puede compilar/agregar un resumen consolidado del resultado de rendimiento general de objetivos y alertas de todo el paquete de indicadores de rendimiento en materia de seguridad operacional para un período de control determinado. Se pueden asignar valores cualitativos (satisfactorio/insatisfactorio) para cada “objetivo logrado” y cada “nivel de alerta no violado”. O bien, se pueden usar valores numéricos (puntos) para proporcionar una medición cuantitativa del rendimiento general del paquete de indicadores.-

*****

CAPITULO 3.

ALCANCE Y APLICABILIDAD

3.1 ALCANCE

3.1.1 Se describen los requerimientos para un sistema de gestión de la seguridad (SMS) de todo proveedor de servicio ATS, operador de aeródromos certificados, organizaciones de mantenimiento y operadores de aeronaves operando en territorio paraguayo de conformidad con los siguientes reglamentos nacionales y Anexos de la OACI:

DINAC R121: Operación de Aeronaves - Certificación y Operación de Transportes Aéreos Internos, Internacionales y Suplementarios.-

DINAC R135: Operación de Aeronaves – Certificación y Operación de Empresas Aéreas, Operación Programada y/o Requerimiento-taxi Aéreo.-

DINAC R145: Aeronavegabilidad – Talleres Aeronáuticos de Reparaciones.-

DINAC R11: Servicios de Tránsito Aéreo.-

DINAC R14: Aeródromos.-

Anexo 1: Licencias al personal.-

Anexo 6: Operación de aeronaves, Parte I — Transporte aéreo internacional — Aeroplanos, y Parte III — Operaciones internacionales — Helicópteros.-

Anexo 8: Aeronavegabilidad.-

Anexo 11: Servicios de tránsito aéreo.-

Anexo 13: Investigación de accidentes e incidentes de aviación.-

Anexo 14: Aeródromos, Volumen I — Diseño y operación de aeródromos.-

3.1.2 El proveedor de servicio es responsable por la seguridad de los servicios o productos contratados o adquiridos de otras organizaciones.-

3.2 APLICABILIDAD Y ACEPTACIÓN

3.2.1 A partir del 5 de marzo de 2013, se ha establecido que todo operador o proveedor de servicio ATS, de aeródromos certificados, organizaciones de mantenimiento y operador de aeronaves, deberán poseer un sistema de gestión de la seguridad operacional (SMS) que sea aceptable para la DINAC, que como mínimo:

a) Identifique los riesgos de seguridad;

b) Asegure la implementación de las acciones necesarias para mantener un nivel aceptable de seguridad;

c) Provea un monitoreo continuo y una regular valoración del nivel de seguridad obtenido; y

d) Establezca una mejora continua en todos los niveles de seguridad.-

3.2.2 A fin de ser aceptable para la DINAC, el SMS del proveedor de servicio debe reunir los requisitos establecidos en este reglamento.-

3.3 REQUISITOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

3.3.1 Los SARPS de la OACI también incluyen requisitos para la implementación de un SMS por parte de proveedores de servicios y explotadores de aviación general como un elemento de cada SSP del Estado. El SMS proporciona los medios para

identificar los peligros de seguridad operacional, implementar medidas para reducir los riesgos de seguridad operacional, controlar el rendimiento en materia de seguridad operacional y lograr una mejora continua en el rendimiento en materia de seguridad operacional.-

3.3.2 Un marco de trabajo del SMS requiere actividades y procesos específicos que deben llevar a cabo los proveedores de servicios de aviación. El marco de trabajo del SMS se compone de los siguientes cuatro componentes:

a) Política y objetivos de seguridad operacional;

b) Gestión de riesgos de seguridad operacional;

c) Aseguramiento de la seguridad operacional; y

d) Promoción de la seguridad operacional.-

3.3.3 Los explotadores de aviación general internacional de aeroplanos grandes o de turborreactor, como se describe en el Anexo 6 (OACI), Parte II, Sección III, deberán establecer y mantener un SMS que sea adecuado para la envergadura y complejidad de la operación y, como mínimo, debe incluir:

a) Un proceso para identificar peligros de seguridad operacional reales y potenciales, y evaluar los riesgos asociados;

b) Un proceso para desarrollar e implementar la medida correctiva necesaria para mantener un nivel de seguridad operacional aceptable; y

c) Disposiciones para el control continuo y evaluación regular de la relevancia y eficacia de las actividades de gestión de la seguridad operacional.-

3.3.4 La siguiente tabla proporciona un resumen de las referencias a los requisitos de gestión de la seguridad operacional para los proveedores de servicios y los explotadores de aviación general, como el marco de trabajo del SMS.

Verificar contenido en los documentos mencionados

Fuente		Tema
Anexo	Disposición	
6, Partes I, y III 11 14, Volumen I	Definiciones	Sistema de gestión de la seguridad operacional
1	Apéndice 2	Requisitos del SMS para organizaciones de capacitación aprobadas
6, Parte I	Capítulo 3, 3.3, Capítulo 8, 8.7.3	Requisitos del SMS para los explotadores de aeronaves y las organizaciones de mantenimiento
6, Parte II	Capítulo 3, 3.3.2	Requisitos del SMS para los aeroplanos que participan en la aviación internacional general
6, Parte III	Sección I, Capítulo 1, 1.3.3	Requisitos del SMS para los explotadores de helicópteros
8	Capítulo 5	Requisitos del SMS para las organizaciones responsables del tipo de diseño y fabricación de la aeronave
11	Capítulo 2, 2.28	Requisitos del SMS para los proveedores de servicios de tránsito aéreo
14, Volumen I	Capítulo 1, 1.4.4	Requisitos del SMS para los explotadores de aeródromos certificados

6 Parte I	Apéndice 5	Marco de trabajo del SMS
6, Parte III	Apéndice 1	

3.4 POLÍTICA DE CALIDAD

Un proveedor de servicio asegurará que la política de calidad de la organización sea coherente y apoye el cumplimiento de las actividades del SMS.-

3.5 DESTINATARIOS

3.5.1 La aplicación de este documento no se limita al personal de operaciones. Más bien, debería ser importante para todo el espectro de interesados en la seguridad operacional, incluido el personal directivo de alto nivel.-

3.5.2 En particular, este documento está dirigido al personal responsable del diseño, aplicación y gestión de actividades de seguridad operacional eficaces, es decir:

a) Funcionarios responsables de la reglamentación del sistema de aviación;

b) Administradores de organizaciones operacionales, tales como explotadores, proveedores ATS, aeródromos y organismos de mantenimiento; y

c) Profesionales de la seguridad operacional, tales como jefes y asesores de los servicios de seguridad operacional.-

3.5.3 Quienes usen este documento deberían encontrar en él información suficiente para la justificación, la creación y el funcionamiento de un SMS viable.-

*****

CAPITULO 4.

IDENTIFICACIÓN DE LOS PELIGROS Y GESTIÓN DE RIESGOS

4.1 La identificación de peligros es un requisito previo para el proceso de gestión de riesgos de seguridad operacional. Cualquier diferenciación incorrecta entre peligros y riesgos de seguridad operacional puede causar confusión. Una comprensión clara de los peligros y sus consecuencias relacionadas es fundamental para la implementación de una sólida gestión de riesgos de seguridad operacional.-

4.2 Los peligros existen en todos los niveles en la organización y son detectables mediante el uso de sistemas de notificación, inspecciones o auditorías. Los contratiempos ocurren cuando los peligros interactúan con ciertos factores activadores. Como resultado, los peligros deben identificarse antes de que produzcan accidentes, incidentes u otros sucesos relacionados con la seguridad operacional. Un mecanismo importante para la identificación proactiva de peligros es un sistema de notificación voluntaria de peligros/incidentes. La información recopilada mediante tales sistemas puede complementarse con las observaciones o los hallazgos registrados durante las inspecciones de rutina en el sitio o las auditorías de la organización.-

4.3 METODOLOGÍAS DE IDENTIFICACIÓN DE PELIGROS

4.3.1 Las tres metodologías para identificar peligros son:

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

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

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

4.4 RIESGOS DE LA SEGURIDAD OPERACIONAL

4.4.1 La gestión de riesgos de seguridad operacional es otro componente clave de un sistema de gestión de la seguridad operacional. El término gestión de riesgos de seguridad operacional fue creado para diferenciar esta función de la gestión de riesgos financieros, legales, económicos, etc. Esta sección presenta los fundamentos del riesgo de seguridad operacional e incluye los siguientes temas:

a) Definición de un riesgo de seguridad operacional;

b) Probabilidad del riesgo de seguridad operacional;

c) Gravedad del riesgo de seguridad operacional;

d) Tolerabilidad del riesgo de seguridad operacional; y

e) Gestión del riesgo de seguridad operacional.

4.4.2 Definición de riesgo de seguridad operacional

4.4.2.1 El riesgo de seguridad operacional es la probabilidad y gravedad proyectada de la consecuencia o el resultado de una situación o peligro existente. Aunque el resultado puede ser un accidente, una "consecuencia / evento intermedio inseguro" puede identificarse como "el resultado más creíble".-

4.4.3 Probabilidad del riesgo de seguridad operacional

4.4.3.1 El proceso de controlar los riesgos de seguridad operacional comienza al evaluar la probabilidad de que las consecuencias de los peligros se materialicen durante las actividades de aviación realizadas por la organización. Ver Tabla **4.7**.-

4.4.3.2 La probabilidad de riesgo de seguridad operacional se define como la probabilidad o frecuencia de que pueda suceder una consecuencia o un resultado de la seguridad operacional. Con las siguientes preguntas se puede ayudar a determinar dicha probabilidad:

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

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

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

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

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

4.4.4 Gravedad del riesgo de seguridad operacional

4.4.41 Luego de completar la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional, considerando las posibles consecuencias relacionadas con el peligro. Ver Tabla **4.8**.-

4.4.4.2 La gravedad del riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La evaluación de la gravedad puede basarse en:

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

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

4.4.4 Tolerabilidad del riesgo de seguridad operacional

4.4.4.1 El proceso de evaluación de la probabilidad y gravedad del riesgo de seguridad operacional puede usarse para derivar un índice de riesgo de seguridad operacional. El índice que se crea mediante la metodología descrita anteriormente consta de un identificador alfanumérico, que indica los resultados combinados de las evaluaciones de probabilidad y gravedad.-

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

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

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

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

c) Cancelar la operación si la mitigación no es posible.-

4.4.5 Gestión de riesgos de la seguridad operacional

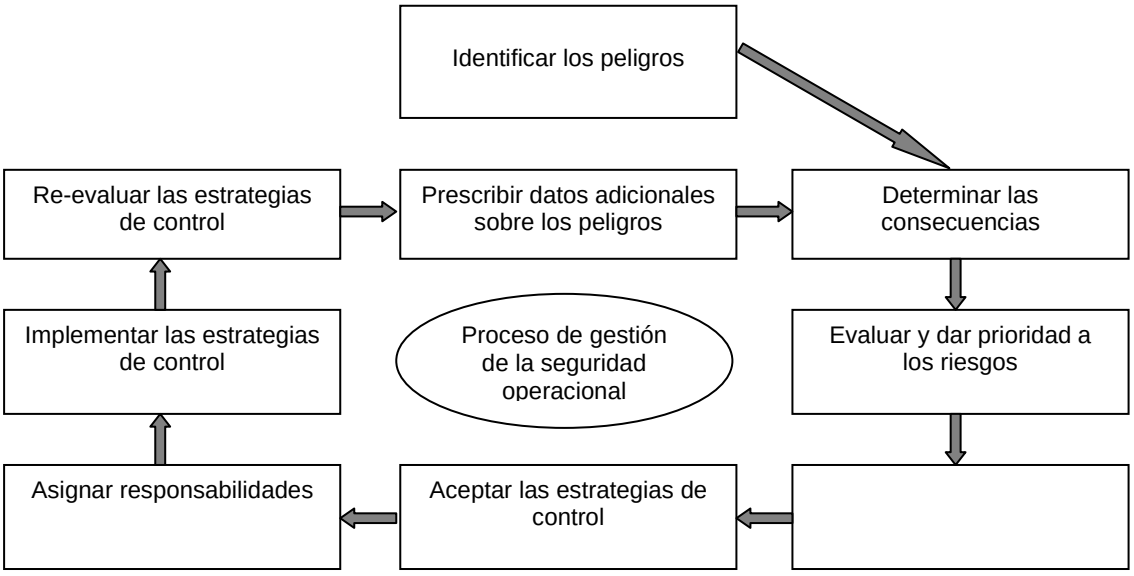
4.4.5.1 La gestión de riesgo de seguridad operacional abarca la evaluación y mitigación de los riesgos de seguridad operacional. El objetivo de la gestión de riesgo de seguridad operacional es evaluar los riesgos asociados con los peligros identificados y desarrollar e implementar mitigaciones eficaces y adecuadas.-

4.4.5.2 Los riesgos de seguridad operacional son evaluados en concepto como aceptables, tolerables o intolerables. Los riesgos evaluados que desde un principio estaban identificados en la región intolerable son inaceptables bajo todo punto de vista. La probabilidad o gravedad de las consecuencias de los peligros tienen tal magnitud, y sus posibles daños representan tal amenaza para la seguridad operacional, que se requiere una medida de mitigación inmediata.-

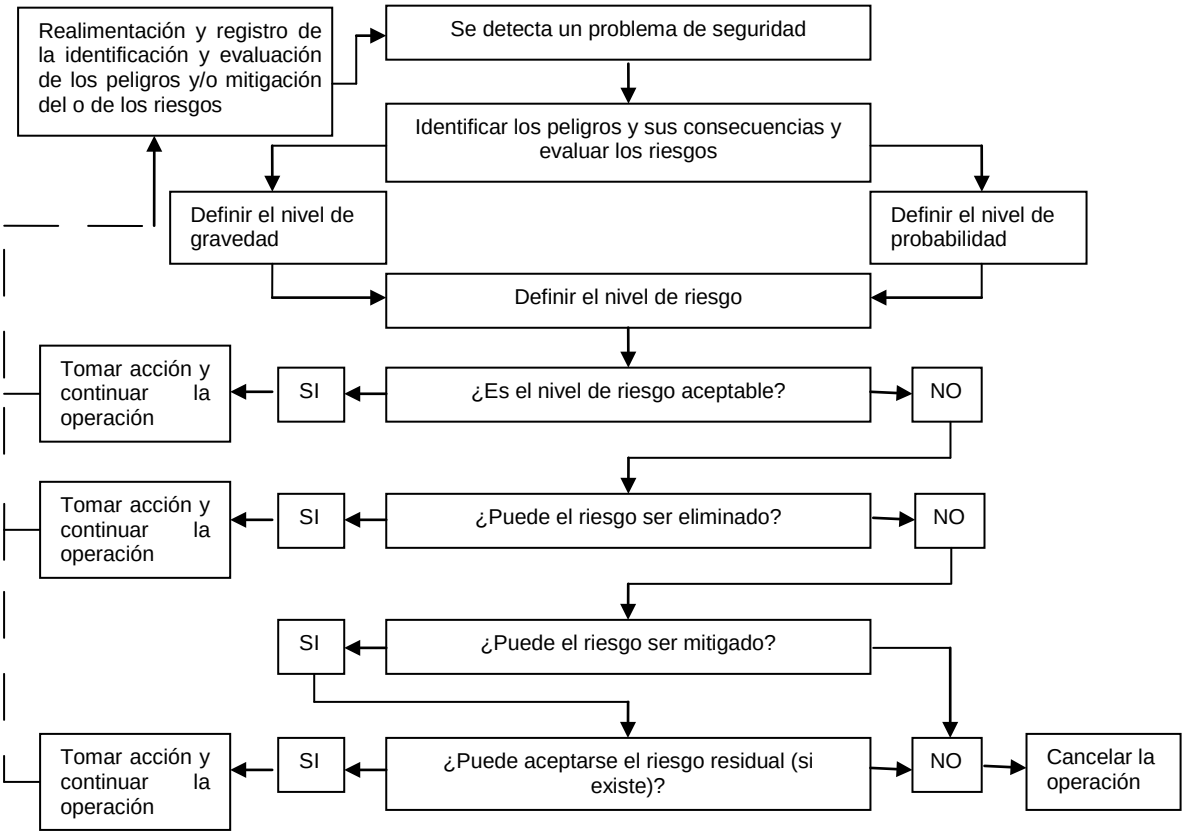
4.4.5.3 Los riesgos de seguridad operacional evaluados en la región tolerable son aceptables, siempre y cuando la organización implemente las estrategias de mitigación correspondientes. Un riesgo de seguridad operacional evaluado inicialmente como intolerable puede mitigarse y, posteriormente, trasladarse a una región tolerable, siempre y cuando dicho riesgo siga bajo el control de estrategias de mitigación adecuadas. En ambos casos, se debe realizar un análisis de costo-beneficios complementario, si se considera adecuado.-

4.4.5.4 Los riesgos de seguridad operacional evaluados que desde un principio estaban identificados en la región aceptable son aceptables tal y como están, y no requieren medidas para llevar o mantener la probabilidad o gravedad de las consecuencias de los peligros bajo control institucional.-

4.5 PROCESO DE GESTIÓN DE LA SEGURIDAD OPERACIONAL



4.6 PROCESO DE GESTIÓN DEL RIESGO



4.7 TABLA DE PROBABILIDAD DEL RIESGO DE SEGURIDAD OPERACIONAL

Descripción	Descripción de la probabilidad	Nivel
Frecuente	Es probable que suceda muchas veces (ha ocurrido frecuentemente) Error cada dos operaciones	5
Ocasional	Es probable que suceda algunas veces (ha ocurrido con poca frecuencia) Error cada 10 operaciones	4
Remoto	Es poco probable que ocurra, pero no imposible (rara vez ha ocurrido) Error cada 100 operaciones	3
Improbable	Es muy poco probable que ocurra (no se sabe si ha ocurrido). Error cada 1000 operaciones	2
Excepcional	Es casi inconcebible que ocurra el evento. Error cada 10.000 operaciones	1

4.8 TABLA DE GRAVEDAD DEL RIESGO DE SEGURIDAD OPERACIONAL

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

4.9 MATRIZ DE EVALUACIÓN DEL RIESGO DE SEGURIDAD OPERACIONAL

Probabilidad del riesgo		Gravedad del riesgo				
		Catastrófico A	Peligroso B	Grave C	Leve D	Insignificante E
Frecuente	5	5A	5B	5C	5D	5E
Ocasional	4	4A	4B	4C	4D	4E
Remoto	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Excepcional	1	1A	1B	1C	1D	1E

4.10 MATRIZ DE TOLERABILIDAD DEL RIESGO DE SEGURIDAD OPERACIONAL

Tolerabilidad	Índice de riesgo	Medida recomendada
Región intolerable	5A, 5B, 5C, 4A, 4B, 3A	Inaceptable según las circunstancias existentes. Cese o disminuya la operación oportunamente si fuera necesario. Realice la mitigación de riesgos de prioridad para garantizar que haya controles preventivos adicionales o mejorados implementados para reducir el índice de riesgos
Región tolerable	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Aceptable según la mitigación de riesgos. Puede necesitar una decisión de gestión.-
Región aceptable	3E, 2D, 2E,1B, 1C, 1D, 1E,	Aceptable. No se necesita una mitigación de riesgos posterior.

4.11 TABLA DE IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

Responsable:												Hoja---- de----
Fecha de elaboración:				Fecha de revisión:				Resultado de acciones				
Proceso / Actividad	Peligro	Riesgo	Probabilidad	Gravedad	N. de riesgo	Acción recomendada	Área Responsable y fecha de terminación	Acciones tomadas	Probabilidad	Gravedad	N. de riesgo	

CAPITULO 5.

PLANIFICACIÓN DE LA IMPLEMENTACIÓN DEL SMS

5.1 Descripción del sistema

Una revisión y descripción del sistema de los elementos de SMS y su interfaz con los sistemas y los procesos existentes es el primer paso en la definición del alcance y aplicabilidad del SMS. Este ejercicio proporciona una oportunidad para identificar cualquier brecha relacionada con los componentes y elementos de SMS del proveedor de servicios. La descripción del sistema incluye las interfaces de SMS dentro de la organización, así como también, las interfaces pertinentes con otras organizaciones externas, como subcontratistas. Una descripción general del sistema y su estructura de responsabilidad y notificación debe incluirse en la documentación del SMS.-

5.2 Plan de implementación del SMS

5.2.1 Un plan de implementación de SMS se desarrolla con el asesoramiento del ejecutivo responsable y los gerentes responsables del suministro de productos y servicios relacionados con la operación segura de la aeronave o en respaldo de esta. Luego de completarse, el ejecutivo responsable apoya el plan. El plan de implementación del SMS incluye cronologías e hitos coherentes con los requisitos identificados en el proceso de análisis de brechas, la envergadura del proveedor de servicios y la complejidad de sus productos o servicios. El plan debe abordar la coordinación con organizaciones o contratistas externos, donde corresponda.-

5.2.2 El plan de implementación del proveedor de servicios puede documentarse de diferentes formas, lo que varía de una simple hoja de cálculos hasta software especializado de gestión de proyectos. El plan de implementación debe abordar brechas mediante la finalización de medidas e hitos específicos de acuerdo con la cronología determinada. La asignación de cada tarea garantiza una responsabilidad en todo el proceso de implementación. El plan debe revisarse y actualizarse regularmente, según sea necesario.-

5.2.3 La completa implementación de todos los componentes y elementos del marco de trabajo del SMS puede demorar hasta cinco años, según la madurez y complejidad de la organización.-

*****

CAPITULO 6.

MARCO DE TRABAJO DEL SMS

6.1 Se establece un marco de trabajo para la implementación de SMS por parte de los proveedores de servicios de aviación pertinentes. Se debe tener presente que la implementación del marco de trabajo debe ser proporcional a la envergadura de la organización y la complejidad de los productos o servicios proporcionados.-

6.2 El marco de trabajo incluye cuatro componentes y doce elementos, los que representan los requisitos mínimos para la implementación del SMS. Los cuatro componentes y los doce elementos de un SMS son:

1 Política y objetivos de seguridad operacional;

1.1 Compromiso y responsabilidad de la gestión,

1.2 Responsabilidades de la seguridad operacional,

1.3 Nombramiento de personal de seguridad operacional clave,

1.4 Coordinación de la planificación de respuesta ante emergencias,

1.5 Documentación del SMS.-

2 Gestión de riesgos de seguridad operacional;

2.1 Identificación de peligros,

2.2 Evaluación y mitigación de riesgos de seguridad operacional.-

3 Aseguramiento de la seguridad operacional;

3.1 Control y medición del rendimiento en materia de la seguridad operacional,

3.2 La gestión de cambio,

3.3 Mejora continua del SMS.-

4 Promoción de la seguridad operacional;

4.1 Capacitación y educación,

4.2 Comunicación de seguridad operacional.-

6.2.1 Las políticas y objetivos de seguridad operacional crean el marco de referencia para el SMS. El objetivo del componente de gestión de riesgos de seguridad operacional es identificar peligros, evaluar los riesgos relacionados y desarrollar mitigaciones adecuadas en el contexto de la entrega de los productos y servicios de la organización. Se logra el aseguramiento de la seguridad operacional mediante procesos constantes que controlan el cumplimiento de las normas internacionales y los reglamentos nacionales. Es más, el proceso de aseguramiento de la seguridad operacional proporciona confianza en que el SMS funciona como fue diseñado y es eficaz. La promoción de la seguridad operacional proporciona la toma de conciencia y capacitación necesarias.-

6.2.2 A continuación se proporciona un resumen de alto nivel de cada uno de los componentes, y le sigue el texto del marco de trabajo del SMS para cada elemento. Luego se presentan estrategias de implementación generales para cada elemento.-

6.3 POLÍTICA Y OBJETIVOS DE LA SEGURIDAD OPERACIONAL

La política establece el compromiso de la administración superior para incorporar y

mejorar continuamente la seguridad operacional en todos los aspectos de sus actividades. La administración superior desarrolla objetivos de seguridad operacional a nivel de la organización medible y asequible que puedan alcanzarse.-

6.3.1 Compromiso y responsabilidad de la gestión

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

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

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

c) Incluir procedimientos de notificación de seguridad operacional;

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

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

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

g) Revisarse periódicamente para garantizar que sigue siendo pertinente y adecuado para el proveedor de servicios; y

h) Garantizar que se entiende, implementa y mantiene la política de seguridad operacional en todos los niveles.-

6.3.1.1 La administración superior desarrolla y apoya la política de seguridad operacional, la cual está firmada por un ejecutivo responsable.-

6.3.1.2 Luego de haber desarrollado una política de seguridad operacional, la administración superior deberá:

a) Respaldar visiblemente la política;

b) Comunicar la política a todo el personal correspondiente;

c) Establecer objetivos de rendimiento en materia de seguridad operacional para el SMS y la organización; y

d) Establecer objetivos de seguridad operacional que identifiquen lo que intenta alcanzar la organización en términos de gestión de la seguridad operacional.-

6.3.2 Responsabilidades de la seguridad operacional

El proveedor de servicios deberá:

a) Identificar al ejecutivo responsable quien, sin importar otras funciones, tiene la responsabilidad final, en nombre de la organización, de implementar y mantener al SMS;

b) Definir claramente líneas de responsabilidad de la seguridad operacional en toda la organización, lo que incluye una responsabilidad directa de la seguridad operacional por parte de la administración superior;

c) Identificar las responsabilidades de todos los miembros de la administración, sin importar otras funciones, así como también, de los empleados, en relación con el rendimiento en materia de seguridad operacional del SMS;

d) Documentar y comunicar las responsabilidades de la seguridad operacional y las autoridades en toda la organización; y

e) Definir los niveles de administración con la autoridad para tomar decisiones acerca de la tolerabilidad de los riesgos de seguridad operacional.-

6.3.2.1 La gestión de la seguridad operacional puede ser una función principal para cualquier proveedor de servicios de la aviación. La definición de las responsabilidades de todo el personal implicado en las tareas relacionadas con la seguridad operacional servirá para garantizar la entrega de productos y operaciones seguras, así como también, una asignación de recursos equilibrada de forma correcta.-

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

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

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

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

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

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

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

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

h) El establecimiento y mantenimiento de la competencia de la organización para aprender del análisis de los datos recopilados mediante su sistema de notificación de seguridad operacional.-

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

6.3.3 Nombramiento del personal de seguridad operacional clave

6.3.3.1 El proveedor de servicios deberá asignar un gerente de seguridad operacional que sea responsable de la implementación y mantenimiento de un SMS eficaz.-

6.3.3.2 El gerente de seguridad operacional es la persona responsable del desarrollo y mantenimiento de un SMS eficaz. El gerente de seguridad operacional también aconseja al ejecutivo responsable y a los gerentes de línea sobre los asuntos de gestión de la seguridad operacional y es responsable de coordinar y comunicar temas de seguridad operacional dentro de la organización, así como también, con accionistas externos. Las funciones del gerente de seguridad operacional incluyen, entre otras:

a) Gestionar el plan de implementación del SMS en nombre del ejecutivo responsable;

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

c) Controlar las medidas correctivas y evaluar sus resultados;

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

e) Mantener registros y documentación de la seguridad operacional;

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

g) Proporcionar consejos independientes sobre asuntos de seguridad operacional;

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

i) Coordinarse y comunicarse (en nombre del ejecutivo responsable) con la autoridad de vigilancia del Estado y otras entidades estatales, según sea necesario, sobre temas relacionados con la seguridad operacional.-

6.3.4 Coordinación de la planificación de respuesta ante emergencias

6.3.4.1 El proveedor de servicios deberá garantizar que un plan de respuesta ante emergencias esté coordinado correctamente con los planes de respuesta ante emergencias de aquellas organizaciones con las que deben establecer una interfaz, durante la entrega de sus servicios.-

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

6.3.4.3 La aplicabilidad de la planificación de respuesta ante emergencias se extiende a los proveedores de productos de aviación que pueden atribuirse al suceso de seguridad operacional de la aviación o verse afectado por él. Por lo general, los procesos del proveedor de productos se conocen como "respaldo de producto de contingencia" e incluyen la medida de aeronavegabilidad de emergencia, los servicios de alerta y el respaldo en terreno para los accidentes de la aeronave.-

6.3.5 Documentación del SMS

6.3.5.1 El proveedor de servicios deberá desarrollar un plan de implementación de SMS, formalmente respaldado por la organización, que defina el enfoque de la organización acerca de la gestión de la seguridad operacional en una forma que cumpla los objetivos de seguridad operacional de la organización.-

6.3.5.2 El proveedor de servicios deberá desarrollar y mantener la documentación de SMS que describa:

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

b) Los requisitos de SMS;

c) Los procesos y procedimientos de SMS;

d) Las responsabilidades y autoridades para los procesos y procedimientos de SMS; y

e) Los resultados de SMS.-

6.3.5.3 El proveedor de servicios deberá desarrollar y mantener un manual de SMS como parte de su documentación de SMS.-

6.3.5.4 La documentación de SMS aborda todos los elementos y procesos del SMS y deberá incluir:

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

1) gestión de documentos y registros;

2) requisitos del SMS reglamentario;

3) marco de trabajo, alcance e integración;

4) política y objetivos de seguridad operacional;

5) responsabilidades de la seguridad operacional y personal clave;

6) sistema de notificación de peligros voluntaria;

7) procedimientos de notificación e investigación de incidentes;

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

9) indicadores de rendimiento en materia de seguridad operacional;

10) capacitación y comunicación de seguridad operacional;

11) mejora continua y auditoría de SMS;

12) gestión de cambio; y

13) planificación de contingencia de emergencia u operaciones;

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

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

2) indicadores de rendimiento en materia de seguridad operacional;

3) registro de evaluaciones de seguridad operacional completadas o en progreso;

4) registros de revisión o auditoría internas de SMS;

5) registros de promoción de seguridad operacional;

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

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

8) plan de implementación del SMS (durante el proceso de implementación).-

6.4 GESTIÓN DE RIESGOS DE LA SEGURIDAD OPERACIONAL

6.4.1 Los proveedores de servicios deben garantizar que los riesgos de seguridad operacional encontrados en las actividades de aviación están bajo control para alcanzar sus objetivos de eficacia de la seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional e incluye la identificación de peligros, la evaluación de riesgos de seguridad operacional y la implementación de medidas de solución adecuadas.-

6.4.1.1 El componente de la gestión de riesgos de seguridad operacional identifica sistemáticamente los peligros que existen dentro del contexto de la entrega de sus productos o servicios. Puede que los peligros sean el resultado de los sistemas que son deficientes en su diseño, función técnica, interfaz humana o interacciones con otros procesos y sistemas. También pueden producirse a partir de una falla de los procesos o sistemas existentes para adaptar los cambios en el entorno de operación del proveedor de servicios. A menudo, un análisis cuidadoso de estos factores durante las etapas de planificación, diseño e implementación puede identificar posibles peligros antes de que el sistema quede operativo.-

6.4.2 Identificación de peligros

6.4.2.1 El proveedor de servicios deberá desarrollar y mantener un proceso formal que garantice que los peligros asociados con sus productos o servicios de aviación están identificados.-

6.4.2.2 La identificación de peligros deberá basarse en una combinación de métodos reactivos, proactivos y predictivos de recopilación de datos de seguridad operacional.-

6.4.2.3 Lo siguiente podrá considerarse mientras se participa en el proceso de identificación de peligros:

a) Factores de diseño, como el diseño del equipo y las tareas;

b) Limitaciones del desempeño humano (por ejemplo, fisiológico, sicológico y cognitivo);

c) Procedimientos y prácticas de operación, como su documentación y las listas de verificación bajo condiciones de operación reales;

d) Factores de comunicación, como medios, terminología e idioma;

e) Factores institucionales, como aquellos relacionados con el reclutamiento, capacitación y retención de personal, la compatibilidad de metas de producción y seguridad operacional, la asignación de los recursos, las presiones de operación y la cultura de seguridad operacional empresarial;

f) Factores relacionados con el entorno operacional del sistema de aviación (por ejemplo, ruido ambiental y vibración, temperatura, iluminación y la disponibilidad de equipo y ropa de protección);

g) Factores de vigilancia reglamentaria, como la aplicabilidad y ejecutabilidad de los reglamentos y la certificación del equipo, el personal y los procedimientos;

h) Sistemas de control de rendimiento que pueden detectar desviaciones de la práctica o desviaciones operacionales; e

i) Factores de la interfaz humano-máquina.-

6.4.3 Evaluación y mitigación de riesgos de la seguridad operacional

6.4.3.1 El proveedor de servicios deberá desarrollar y mantener un proceso que garantiza el análisis, la evaluación y el control de los riesgos de seguridad operacional asociados con los peligros identificados.-

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

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

b) La probabilidad que sucederá.

6.4.3.3 El proceso comienza con la identificación de los peligros y sus posibles consecuencias. Los riesgos de seguridad operacional se evalúan en términos de probabilidad y gravedad, para definir el nivel de riesgos de seguridad operacional (índice de riesgo de seguridad operacional). Si los riesgos de seguridad operacional evaluados se consideran tolerables, se debe tomar una medida adecuada y la operación puede continuar. La identificación de peligros completada y el proceso de evaluación y mitigación de riesgos de seguridad operacional se documentan y aprueba como corresponda y forma parte del sistema de gestión de información de seguridad operacional.-

6.4.3.4 Los tres enfoques genéricos de mitigación de riesgos de la seguridad operacional incluyen:

a) **Prevención.** La actividad se suspende a causa de que los riesgos de seguridad operacional asociados son intolerables o se consideran inaceptables en comparación con los beneficios asociados.-

b) **Reducción.** Se acepta cierta exposición de riesgos de seguridad operacional, aunque la gravedad o probabilidad asociada con los riesgos se aminora, posiblemente mediante medidas que mitigan las consecuencias relacionadas.-

c) **Segregación de la exposición.** Medida tomada para aislar la posible

consecuencia relacionada con el peligro o para establecer varias capas de defensas contra ella.-

6.4.3.5 Una estrategia de mitigación de riesgos puede implicar uno de los enfoques descritos anteriormente o puede incluir múltiples enfoques. Es importante considerar toda la gama de posibles medidas de control para encontrar una solución óptima. La eficacia de cada estrategia alternativa debe evaluarse antes de poder tomar una decisión. Cada alternativa de mitigación de riesgos de seguridad operacional propuesta debe examinarse a partir de las siguientes perspectivas:

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

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

c) **Practicidad.** El grado hasta donde la mitigación puede implementarse y cuán adecuado es en términos de tecnología disponible, recursos financieros y administrativos, legislación y reglamentos, voluntad política, etc.-

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

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

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

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

h) **Consecuencias accidentales.** La introducción de nuevos peligros y riesgos de seguridad operacional relacionados que estén asociados con la implementación de cualquier alternativa de mitigación.-

6.5 ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

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

6.5.1.1 El proceso de aseguramiento de la seguridad operacional complementa aquel del aseguramiento de la calidad; cada uno de estos procesos requiere de análisis, documentación, auditoría y revisiones para garantizar que se cumplan ciertos criterios de rendimiento. Si bien es común que el aseguramiento de la calidad se centre en el cumplimiento de requisitos reglamentarios, el aseguramiento de la seguridad operacional controla específicamente la eficacia de los controles de riesgos de la seguridad operacional.-

6.5.1.2 La relación complementaria entre el aseguramiento de la seguridad operacional y el aseguramiento de la calidad permite la integración de ciertos procesos de respaldo. Tal integración puede servir para lograr sinergias a fin de garantizar que se cumplan los objetivos de seguridad operacional, calidad y comerciales del proveedor de servicios.-

6.5.1.3 Finalmente, las actividades del aseguramiento de seguridad operacional deben incluir el desarrollo y la implementación de medidas correctivas en respuesta a los hallazgos de deficiencias sistémicas que podrían tener un impacto en la seguridad operacional. La responsabilidad institucional del desarrollo e implementación de medidas correctivas debe residir con los departamentos citados en los hallazgos.-

6.5.2 Control y medición del rendimiento en materia de seguridad operacional

6.5.2.1 El proveedor de servicios desarrollará y mantendrá los medios para verificar el rendimiento en materia de seguridad operacional de la organización y para validar la eficacia de los controles de riesgos de la seguridad operacional.-

6.5.2.2 El rendimiento en materia de seguridad operacional del proveedor de servicios se verificará en referencia a los indicadores de rendimiento en materia de seguridad operacional y los objetivos de rendimiento en materia de seguridad operacional del SMS.-

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

6.5.2.4 Existen dos tipos de sistemas de notificación:

a) Sistemas de notificación de incidentes obligatoria; y

b) Sistemas de notificación de incidentes voluntaria.

6.5.2.4.1 Los *sistemas de notificación de incidentes obligatoria* requieren ciertos tipos de eventos (por ejemplo, incidentes graves, incursiones en la pista). Esto necesita la implementación de reglamentos detallados que identifiquen los criterios de notificación y el alcance de sucesos que pueden notificarse. Los sistemas de notificación obligatoria tienden a recopilar más información relacionada con averías técnicas de alto impacto que otros aspectos de las actividades operacionales.-

6.5.2.4.2 Los *sistemas de notificación voluntaria* permiten el envío de información relacionada con los peligros observados o errores accidentales sin un requisito legal o administrativo asociado para hacerlo. En estos sistemas, las agencias reglamentarias o las organizaciones pueden ofrecer un incentivo para realizar un informe. Por ejemplo, se puede omitir una medida de cumplimiento para los informes de errores o infracciones accidentales. En estas circunstancias, la información notificada solo se usará para respaldar la mejora de la seguridad operacional. Tales sistemas se consideran “no punitivos” dado que ofrecen protección a los notificadores, con lo que se garantiza una disponibilidad continúa de dicha información para respaldar las mejoras constantes en el rendimiento en materia de seguridad operacional. Si bien la naturaleza y el grado de las políticas no punitivas de los proveedores de servicios pueden variar, la intención es promover una cultura de notificación eficaz e identificación proactiva de las deficiencias potenciales de la seguridad operacional.-

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

a) ***El estudio de seguridad operacional*** es un análisis usado para obtener una comprensión de los amplios temas de seguridad operacional o aquellos de una naturaleza global. Por ejemplo, la industria de las líneas aéreas puede producir recomendaciones de seguridad operacional e implementar medidas para reducir accidentes e incidentes durante las etapas de acercamiento y aterrizaje. Los proveedores de servicios individuales pueden encontrar que estas recomendaciones globales mejoran el rendimiento en materia de seguridad operacional en el contexto de sus actividades de aviación.-

b) ***Las revisiones de seguridad operacional*** son un componente fundamental de la gestión de cambio. Estas se llevan a cabo durante la introducción de

nuevas tecnologías, nuevos procedimientos o cambios sistémicos que afectan las operaciones de la aviación. Las revisiones de seguridad operacional tienen un objetivo claramente definido que se vincula con el cambio en consideración. Las revisiones de seguridad operacional garantizan que el rendimiento en materia de seguridad operacional se mantenga a niveles adecuados durante los períodos de cambio.-

c) ***Los estudios de seguridad operacional*** examinan los procedimientos o procesos relacionados con una operación específica. Implican el uso de listas de verificación, cuestionarios y entrevistas confidenciales e informales. Proporcionan generalmente información cualitativa que puede requerir de validación para determinar una medida correctiva correspondiente. Sin embargo, los estudios pueden proporcionar una fuente económica de información de seguridad operacional importante.-

d) ***Las auditorías*** se centran en la integridad del SMS de la organización y en sus sistemas de respaldo. Las auditorías proporcionan una evaluación de los controles de riesgos de seguridad operacional y los procesos de aseguramiento de la calidad relacionados. Las auditorías pueden realizarse con un proceso de auditoría interna que cuente con las políticas y los procedimientos necesarios para garantizar su independencia y objetividad. Las auditorías tienen como fin proporcionar el aseguramiento de las funciones de la gestión de la seguridad operacional, lo que incluye al personal, el cumplimiento de reglamentos aprobados, niveles de competencia y capacitación.-

e) ***Las investigaciones internas*** se llevan a cabo para ciertos eventos de seguridad operacional que pueden notificarse, de acuerdo con los requisitos internos o reglamentarios. Los accidentes e incidentes graves que investiga el Estado correspondiente o las autoridades regionales también pueden proporcionar el estímulo para llevar a cabo investigaciones internas mediante las organizaciones del proveedor de servicios.-

6.5.3 La gestión de cambio

6.5.3.1 El proveedor de servicios deberá desarrollar y mantener un proceso formal para identificar los cambios que podrían afectar el nivel de riesgos de seguridad operacional asociados con sus productos o servicios de aviación, y para identificar y gestionar los riesgos de seguridad operacional que puedan emerger de aquellos cambios.-

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

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

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

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

6.5.3.3 A medida que evolucionan los sistemas, los cambios incrementales pueden acumularse, lo que requiere enmiendas a la descripción inicial del sistema. Por lo tanto, la gestión de cambio necesita de revisiones periódicas de la descripción del sistema y el análisis de peligros de línea base para determinar su validez continua.-

6.5.4 Mejora continua del SMS

6.5.4.1 El proveedor de servicios deberá controlar y evaluar la eficacia de sus procesos de SMS para permitir la mejora continua del rendimiento general del SMS.-

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

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

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

6.5.4.2.3 Las autoridades pertinentes, responsables de la aceptación del SMS del proveedor de servicios, puede realizar las auditorías externas del SMS. Estas auditorías externas mejoran el sistema de auditoría interna, así como también, proporcionan vigilancia independiente.-

6.6 PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

6.6.1 La promoción de la seguridad operacional alienta una cultura de seguridad operacional positiva y crea un entorno que propicia el logro de los objetivos de seguridad operacional del proveedor de servicios. Una cultura de seguridad operacional positiva se caracteriza por tener valores, actitudes y conductas que se comprometen con los esfuerzos de seguridad operacional de la organización. Esto se logra mediante la combinación de competencias técnicas que mejoran continuamente con la capacitación y educación, las comunicaciones eficaces y la distribución de información. La administración superior proporciona el liderazgo para promover la cultura de seguridad operacional en toda la organización.-

6.6.1.1 Un esfuerzo de seguridad operacional institucional no puede tener éxito por sí solo siguiendo una orden o adherencia estricta de las políticas. La promoción de la seguridad operacional afecta la conducta tanto de personas como de organizaciones y complementa las políticas, los procedimientos y los procesos de la organización, lo que proporciona un sistema de valor que respalda los esfuerzos de la seguridad operacional.-

6.6.1.2 El proveedor de servicios debe establecer e implementar procesos y procedimientos que faciliten la comunicación eficaz en todos los niveles de la organización. Los proveedores de servicios deben comunicar sus objetivos de seguridad operacional, así como también, el estado actual de cualquier actividad o evento relacionado. Los proveedores de servicios también deben alentar la comunicación "jerárquica ascendente", lo que ofrece un entorno que permite a la administración superior recibir comentarios abiertos y constructivos del personal de operaciones.-

6.6.2 Capacitación y educación

6.6.2.1 El proveedor de servicios deberá desarrollar y mantener un programa de capacitación de seguridad operacional que garantice que el personal está capacitado y es competente para realizar sus tareas de SMS.-

6.6.2.2 El alcance del programa de capacitación de la seguridad operacional deberá ser adecuado para la participación de cada persona en el SMS.-

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

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

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

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

d) Sistemas de notificación de la seguridad operacional;

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

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

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

h) Adoctrinamiento inicial documentado y requisitos de capacitación recurrente.-

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

6.6.2.5 La capacitación de seguridad operacional dentro de una organización debe garantizar que el personal sea competente para realizar tareas relacionadas con la seguridad operacional. Los procedimientos de capacitación deben especificar normas de capacitación de seguridad operacional inicial y recurrente para el personal de operaciones, los gerentes y supervisores, los gerentes superiores y el ejecutivo responsable. La cantidad de capacitación de seguridad operacional debe ser adecuada para la responsabilidad y participación de la persona en el SMS. La documentación de capacitación del SMS también debe especificar las

responsabilidades para el desarrollo del contenido y programación de la capacitación, así como también, la gestión de los registros de la capacitación.-

6.6.3 Comunicación de la seguridad operacional

6.6.3.1 El proveedor de servicios deberá desarrollar y mantener medios formales para la comunicación de seguridad operacional que:

a) Garantice que el personal está consciente del SMS hasta un grado proporcional a sus cargos;

b) Transfiera información fundamental de seguridad operacional;

c) Explique por qué se toman medidas de seguridad operacional en particular; y

d) Explique por qué se introducen y cambian procedimientos de seguridad operacional.-

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

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

a) La diseminación del manual del SMS;

b) Los procesos y procedimientos de seguridad operacional;

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

d) Sitios web o correo electrónico.-

*****

CAPÍTULO 7

ENFOQUE DE IMPLEMENTACIÓN EN ETAPAS

7.1 GENERALIDADES

7.1.1 El objetivo de este capítulo es introducir un ejemplo de las cuatro etapas de implementación de un SMS. La implementación de un SMS es un proceso sistemático. Sin embargo, este proceso puede resultar ser una tarea bastante desafiante dependiendo de los factores, como la disponibilidad del material guía y recursos necesarios para la implementación, así como también, el conocimiento preexistente del proveedor de servicios de los procesos y procedimientos del SMS.-

7.1.2 Entre los motivos para un enfoque en etapas para la implementación del SMS se incluyen:

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

b) La necesidad de permitir la implementación de elementos del marco de trabajo del SMS en varias secuencias, según los resultados de cada análisis de brechas del proveedor de servicios;

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

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

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

7.1.4 Se proponen cuatro etapas de implementación para un SMS. Cada etapa se asocia con varios elementos (o subelementos) según el marco de trabajo del SMS de la OACI.-

7.2 ETAPA 1

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

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

7.2.1.2 Al finalizar la etapa 1, se deben finalizar las siguientes actividades de tal forma que cumplan las expectativas de la autoridad de vigilancia de la aviación civil, como se establece en los requisitos y el material guía pertinentes:

7.2.2 Compromiso y responsabilidad de la gestión – Elemento 1.1 (i)

a) Identificar al ejecutivo responsable y las responsabilidades de seguridad operacional de los gerentes.

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

1) desarrollar el plan de implementación de SMS;

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

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

c) Definir el alcance de las actividades de la organización según el cual el SMS será aplicable. El alcance de la aplicabilidad del SMS de la organización se deberá describir posteriormente en el documento del SMS, según corresponda.

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

7.2.3 Plan de implementación del SMS – Elemento 1.5 (i)

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

7.2.4 Nombramiento del personal de seguridad operacional clave – Elemento 1.3

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

b) Establecer la oficina de servicios de seguridad operacional.-

7.2.5 Capacitación y educación – Elemento 4.1 (i)

a) Realizar un análisis de las necesidades de capacitación.

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

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

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

2) la capacitación recurrente.

d) Identificar los costos asociados con la capacitación.

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

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

7.2.6 Comunicación de la seguridad operacional – Elemento 4.2 (i)

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

operacional.

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

1) folletos informativos, noticias y boletines de seguridad operacional;

2) sitios web;

3) correo electrónico.

7.3 ETAPA 2

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

7.3.2 Compromisos y responsabilidades de la gestión – Elemento 1.1 (ii)

a) Desarrollar una política de seguridad operacional.

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

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

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

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

1) indicadores de rendimiento en materia de seguridad operacional;

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

3) planes de acción.

f) Establecer los requisitos del proveedor para los subcontratistas o terceros:

1) establecer un procedimiento para escribir requisitos de SMS en el proceso contratante; y

2) establecer los requisitos de SMS en la documentación de licitación.

7.3.3 Responsabilidades de la seguridad operacional – Elemento 1.2

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

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

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

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

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

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

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

7.3.4 Coordinación de planificación de respuesta ante emergencias – Elemento 1.4

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

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

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

d) Evaluar los ERP respectivos de las entidades externas.

e) Establecer la coordinación entre los diferentes ERP.

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

7.3.5 Documentación del SMS – Elemento 1.5 (ii)

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

1) desarrollar un documento de SMS que sea un manual independiente o una sección distinta dentro de un manual institucional controlado existente;

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

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

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

7.4 ETAPA 3

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

7.4.2 Identificación de peligros – Elemento 2.1 (i)

a) Establecer un procedimiento de notificación voluntaria.-

b) Establecer un programa/plan para la revisión sistemática de todos los procesos/equipos relacionados con la seguridad operacional de aviación.-

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

7.4.3 Evaluación y mitigación de riesgos de seguridad operacional – Elemento 2.2

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

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

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

7.4.4 Control y medición del rendimiento en materia de seguridad operacional – Elemento 3.1 (i)

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

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

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

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

7.4.5 La gestión de cambio – Elemento 3.2

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

1) la vulnerabilidad de los sistemas y actividades;

2) la estabilidad de los sistemas y entornos operacionales;

3) rendimiento pasado;

4) cambios reglamentarios, industriales y tecnológicos.

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

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

7.4.6 Mejora continua del SMS – Elemento 3.3 (i)

a) Desarrollar formularios para las evaluaciones internas.

b) Definir un proceso de auditoría interna.

c) Definir un proceso de auditoría externa.

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

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

7.5 ETAPA 4

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

7.5.2 Compromiso y responsabilidad de la gestión – Elemento 1.1 (iii)

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

7.5.3 Identificación de peligros – Elemento 2.1 (ii)

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

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

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

7.5.4 Control y medición del rendimiento en materia de seguridad operacional – Elemento 3.1 (ii)

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

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

c) Lograr un acuerdo con la autoridad de vigilancia del Estado sobre indicadores de rendimiento en materia de seguridad operacional de bajo impacto y niveles de objetivos/alertas de rendimiento en materia de seguridad operacional.-

7.5.5 Mejora continua del SMS – Elemento 3.3 (ii)

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

b) Establecer otros programas de revisión/estudio de SMS operacional.-

7.5.6 Capacitación y educación – Elemento 4.1 (ii)

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

7.5.7 Comunicación de seguridad operacional – Elemento 4.2 (ii)

a) Establecer mecanismos para promover la distribución y el intercambio de información de seguridad operacional de forma interna y externa.-

7.6 ELEMENTOS DEL SMS IMPLEMENTADOS PROGRESIVAMENTE A TRAVÉS DE LAS ETAPAS 1 A 4

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

a) **Documentación del SMS – Elemento 1.5**

A medida que el SMS madura progresivamente, el manual del SMS pertinente y la

documentación de la seguridad operacional deben revisarse y actualizarse en conformidad. Esta actividad será inherente a todas las etapas de la implementación del SMS y también deberá mantenerse después de la implementación.

b) **Capacitación y educación – Elemento 4.1 y comunicación de la seguridad operacional – Elemento 4.2**

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

*****

CAPÍTULO 8

RECOPILACIÓN Y ANÁLISIS DE DATOS DE LA SEGURIDAD OPERACIONAL

8.1 RECOPILACIÓN Y CALIDAD DE LOS DATOS DE SEGURIDAD OPERACIONAL

8.1.1 La toma de decisiones basada en datos es una de las facetas más importantes de cualquier sistema de gestión. El tipo de datos de seguridad operacional que se recopila puede incluir accidentes e incidentes, eventos, no cumplimientos o desvíos e informes de peligros. Se debe considerar la calidad de los datos que se usan para permitir una toma de decisiones eficaz en todo el desarrollo e implementación del SMS. Desafortunadamente, muchas bases de datos carecen de la calidad de datos necesaria para ofrecer una base confiable a fin de evaluar las prioridades y la eficacia de las medidas de mitigación de riesgos. Si no se consideran las limitaciones de los datos usados para respaldar las funciones de la gestión de riesgos de seguridad operacional y el aseguramiento de la seguridad operacional, se generarán resultados erróneos del análisis, los que, a su vez, pueden producir decisiones incompletas y desacreditación del proceso de gestión de la seguridad.-

8.1.2 Dada la importancia de la calidad de los datos, las organizaciones deben evaluar los datos usados para respaldar la gestión de riesgos de seguridad operacional y los procesos de aseguramiento de la seguridad operacional mediante los siguientes criterios:

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

b) **Integridad.** No falta ningún dato relevante.

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

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

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

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

g) **Precisión.** Los datos no contienen errores.

8.2 BASE DE DATOS DE LA SEGURIDAD OPERACIONAL

8.2.1 En el contexto de la recopilación y análisis de datos de seguridad operacional, el término “base de datos de seguridad” puede incluir el siguiente tipo de datos o información que puede usarse para respaldar los análisis de datos de la seguridad operacional:

a) Datos de la investigación de accidentes;

b) Datos de la investigación de incidentes obligatoria;

c) Datos de la notificación voluntaria;

d) Datos de la notificación de la aeronavegabilidad continua;

e) Datos del control de rendimiento operacional;

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

g) Datos de los informes/hallazgos de la auditoría;

h) Datos de los estudios/revisiones de seguridad operacional.-

8.2.2 Una base de datos de seguridad operacional puede hacer referencia a las bases de datos relacionadas con SSP del Estado o con la base de datos relacionada con SMS de un proveedor de servicios, según el contexto. Los informes voluntarios pueden provenir del personal de operaciones (proveedores de servicio, pilotos, etc.) al igual que desde pasajeros o el público general.-

8.2.3 Las bases de datos de seguridad operacional están en el formato de informes relacionados con eventos complejos, como accidentes e incidentes. Los informes en estos tipos de bases de datos responden, normalmente, a una serie de preguntas. ¿Quién estuvo involucrado en el evento? ¿Qué pasó que produjo la redacción de un informe? ¿Cuándo sucedió el evento? ¿Dónde sucedió el evento? ¿Por qué sucedió? Otros tipos de bases de datos se relacionan con temas relativamente estrechos, como información de vuelo, clima y volúmenes de tránsito. Estos informes contienen hechos simples.-

8.2.4 Las bases de datos de seguridad operacional se alojan comúnmente en varias partes de una organización. Muchas organizaciones proporcionan acceso a las bases de datos mediante una interfaz que permite que los analistas de seguridad operacional especifiquen y extraigan eficientemente informes de interés. Los informes pueden verse de forma individual o colectiva. Las herramientas analíticas permiten que los analistas de seguridad operacional vean los datos extraídos en múltiples formatos. Entre los ejemplos se incluyen hojas de cálculo, mapas y diversos tipos de gráficos.-

8.2.5 Para garantizar que se comprenda y use correctamente una base de datos, la información relacionada con la base de datos (metadatos) debe documentarse debidamente y estar disponible para los usuarios. Entre los tipos de metadatos se incluyen las definiciones de campo, los cambios hechos a la base de datos con el tiempo, las reglas de uso, el formulario de recopilación de datos y las referencias a valores válidos.-

8.3 ANÁLISIS DE DATOS DE LA SEGURIDAD OPERACIONAL

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

a) Ayudar a decidir qué hechos son necesarios;

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

c) Ayudar a alcanzar conclusiones válidas; y

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

8.3.2 Se pueden usar los siguientes métodos de análisis de seguridad operacional:

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

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

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

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

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

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

8.4 GESTIÓN DE INFORMACIÓN DE LA SEGURIDAD OPERACIONAL

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

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

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

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

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

d) operar a un costo relativamente bajo.

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

a) Registrar eventos de seguridad operacional en varias categorías;

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

c) Controlar tendencias;

d) Compilar análisis, gráficos e informes;

e) Revisar registros históricos;

f) Compartir datos de seguridad operacional con otras organizaciones;

g) Controlar investigaciones de eventos; y

h) Controlar la implementación de medidas correctivas.

8.4.4 Si bien cualquier tipo de información agrupada de forma organizada puede considerarse como una base de datos, el análisis de registros en papel en un sistema de archivo simple será suficiente solo para operaciones pequeñas. El almacenamiento, el registro, el retiro y la recuperación mediante sistemas en papel son tareas difíciles de manejar. Es preferible que los datos se almacenen en una base de datos electrónica que facilite la consulta de los registros y la generación de resultados del análisis en varios formatos.-

8.5 PROTECCIÓN DE LOS DATOS DE SEGURIDAD OPERACIONAL

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

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

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

c) Eliminación de la identificación, al borrar todos los detalles que puedan causar que un tercero infiera la identidad de las personas (por ejemplo, números de vuelo, fechas/horas, ubicaciones y tipos de aeronave);

d) Seguridad de los sistemas de información, almacenamiento de datos y redes de comunicación;

e) Prohibiciones en el uso no autorizado de los datos.

*****