



DINAC

REPÚBLICA DEL PARAGUAY

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL

**DINAC R1105
MANUAL GUÍA DE IMPLEMENTACIÓN
DE LA GESTIÓN DE LA SEGURIDAD
OPERACIONAL**

Esta edición fue aprobada por Resolución Nº 260 / 2020.-

PRIMERA EDICIÓN – AÑO 2020

REGISTROS DE ENMIENDAS Y CORRIGENDOS

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

LISTA DE PÁGINAS EFECTIVAS

ÍTEM	TEMAS	EDICIÓN / REVISIÓN	PÁG.
TAPA	TAPA	PRIMERA EDICIÓN - R00	N/A
REGISTRO	ENMIENDAS Y CORRIGENDOS	PRIMERA EDICIÓN - R00	I
LISTA	PÁGINAS EFECTIVAS	PRIMERA EDICIÓN - R00	II
ÍNDICE	ÍNDICE	PRIMERA EDICIÓN - R00	III
CAPÍTULO 1	DEFINICIONES	PRIMERA EDICIÓN - R00	1-4
CAPÍTULO 2	GENERALIDADES		
2.1	Concepto de seguridad operacional.	PRIMERA EDICIÓN - R00	1-4
2.2	Cultura de seguridad operacional.	PRIMERA EDICIÓN - R00	1-4
2.3	Errores e infracciones.	PRIMERA EDICIÓN - R00	2-4
CAPÍTULO 3	GESTIÓN ESTATAL DE SEGURIDAD OPERACIONAL		
3.1	Programa estatal de seguridad operacional (SSP).	PRIMERA EDICIÓN - R00	1-18
3.2	Componente 1: Política, objetivos y recursos estatales de seguridad operacional.	PRIMERA EDICIÓN - R00	1-18
3.3	Componente 2: Gestión estatal de los riesgos de seguridad operacional.	PRIMERA EDICIÓN - R00	7-18
3.4	Componente 3: Aseguramiento estatal de la seguridad operacional.	PRIMERA EDICIÓN - R00	13-18
3.5	Componente 4: Promoción estatal de la seguridad operacional.	PRIMERA EDICIÓN - R00	16-18
CAPÍTULO 4	SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)		
4.1	Generalidades.	PRIMERA EDICIÓN - R00	1-18
4.2	Aviación general internacional – Aviones.	PRIMERA EDICIÓN - R00	1-18
4.3	Marco para un sistema de gestión de la seguridad operacional (SMS).	PRIMERA EDICIÓN - R00	1-18
CAPÍTULO 5	RECOPIACIÓN, ANÁLISIS, PROTECCIÓN, COMPARTICIÓN E INTERCAMBIO DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL		
5.1	Recopilación y procesamiento de datos sobre seguridad operacional.	PRIMERA EDICIÓN - R00	1-14
5.2	Análisis de datos e información sobre seguridad operacional.	PRIMERA EDICIÓN - R00	5-14
5.3	Protección de datos e información sobre seguridad operacional.	PRIMERA EDICIÓN - R00	7-14
5.4	Compartición e intercambio de información sobre seguridad operacional.	PRIMERA EDICIÓN - R00	9-14
5.5	Principios para la protección de datos e información sobre seguridad operacional y las fuentes conexas.	PRIMERA EDICIÓN - R00	10-14

CAPÍTULO 6	ENFOQUE DE IMPLEMENTACIÓN EN ETAPAS		
6.1	Generalidades.	<i>PRIMERA EDICIÓN - R00</i>	1-6
6.2	Etapa 1 / 12 Meses.	<i>PRIMERA EDICIÓN - R00</i>	1-6
6.3	Etapa 2 / 12 Meses.	<i>PRIMERA EDICIÓN - R00</i>	3-6
6.4	Etapa 3 / 18 Meses.	<i>PRIMERA EDICIÓN - R00</i>	4-6
6.5	Etapa 4 / 18 Meses.		6-6

ÍNDICE

ÍTEM	TEMAS	PÁG.
TAPA	TAPA	NA
REGISTRO	ENMIENDAS Y CORRIGENDOS	I
LISTA	PAGINAS EFECTIVAS	II
ÍNDICE	INDICE	III
CAPITULO 1	DEFINICIONES	
CAPITULO 2	GENERALIDADES	
2.1	Concepto de seguridad operacional.	1-4
2.2	Cultura de seguridad operacional.	1-4
2.3	Errores e infracciones.	2-4
CAPITULO 3	GESTIÓN ESTATAL DE SEGURIDAD OPERACIONAL	
3.1	Programa estatal de seguridad operacional (SSP).	1-18
3.2	Componente 1: Política, objetivos y recursos estatales de seguridad operacional.	1-18
3.3	Componente 2: Gestión estatal de los riesgos de seguridad operacional.	7-18
3.4	Componente 3: Aseguramiento estatal de la seguridad operacional.	13-18
3.5	Componente 4: Promoción estatal de la seguridad operacional.	16-18
CAPITULO 4	SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)	
4.1	Generalidades.	1-18
4.2	Aviación general internacional – Aviones.	1-18
4.3	Marco para un sistema de gestión de la seguridad operacional (SMS).	1-18
CAPITULO 5	RECOPIACIÓN, ANÁLISIS, PROTECCIÓN, COMPARTICIÓN E INTERCAMBIO DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL	
5.1	Recopilación y procesamiento de datos sobre seguridad operacional.	1-14
5.2	Análisis de datos e información sobre seguridad operacional.	5-14
5.3	Protección de datos e información sobre seguridad operacional.	7-14
5.4	Compartición e intercambio de información sobre seguridad operacional.	9-14
5.5	Principios para la protección de datos e información sobre seguridad operacional y las fuentes conexas.	10-14
CAPITULO 6	ENFOQUE DE IMPLEMENTACIÓN EN ETAPAS	
6.1	Generalidades.	1-6
6.2	Etapa 1 / 12 Meses.	1-6
6.3	Etapa 2 / 12 Meses.	3-6
6.4	Etapa 3 / 18 Meses.	4-6
6.5	Etapa 4 / 18 Meses.	6-6

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.*

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

EJECUTIVO RESPONSABLE. Persona única e identificable que es responsable del rendimiento eficaz y eficiente del SMS del proveedor de servicios.

ERRORES. Acción u omisión, por parte de un miembro del personal de operaciones, que da lugar a desviaciones de las intenciones o expectativas de organización o de un miembro del personal de operaciones.

GESTIÓN DEL CAMBIO. Proceso formal para gestionar los cambios dentro de una organización de forma sistemática, a fin de conocer los cambios que puede tener un impacto en las estrategias de mitigación de peligros y riesgos identificados antes de implementar tales cambios.

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.

MITIGACIÓN DE RIESGOS. Proceso de incorporación de defensas, controles preventivos o medidas de recuperación para reducir la gravedad o probabilidad de la consecuencia proyectada de un peligro.

NIVEL ACEPTABLE DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL (ALoSP). Nivel de rendimiento en materia de seguridad operacional de la aviación civil en un Estado, como se define en su programa estatal de seguridad operacional, expresado en términos de objetivos e indicadores de rendimiento en materia de seguridad operacional.

OBJETIVO DE SEGURIDAD OPERACIONAL. Una declaración breve y de alto nivel del logro de seguridad operacional o resultado deseado que ha de conseguirse mediante el programa estatal de seguridad operacional o el sistema de gestión de la seguridad operacional del proveedor de servicios.

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

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 CONCEPTO DE SEGURIDAD OPERACIONAL

2.1.1 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”.

2.1.2 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.

2.2 CULTURA DE SEGURIDAD OPERACIONAL

2.2.1 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.

2.2.2 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.

2.2.3 **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.

2.2.4 **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, 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. 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.

2.2.5 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 operativo, y el punto hasta donde se protege la información relacionada con la seguridad operacional.

2.2.6 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. 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.

2.2.7 El éxito de un sistema de notificación depende del flujo continuo de información. 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.

2.3 ERRORES E INFRACCIONES

2.3.1 La implementación eficaz del SMS por parte del proveedor de servicios, así como también, la vigilancia eficaz del SMS por parte la DINAC, 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.

2.3.2 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, la DINAC 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.

2.3.4 Errores

2.3.4.1 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.

2.3.4.2 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.

2.3.5 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.

2.3.6 Infracciones

2.3.6.1 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** 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.

CAPÍTULO 3.

GESTIÓN ESTATAL DE SEGURIDAD OPERACIONAL

3.1 PROGRAMA ESTATAL DE SEGURIDAD OPERACIONAL (SSP)

3.3.1 Elementos críticos del sistema estatal de supervisión de la seguridad operacional

Los CE del sistema estatal de supervisión de la seguridad operacional constituyen la base del SSP.

3.3.2 Panorama del programa estatal de seguridad operacional

3.3.2.1 El SSP es un conjunto integrado de reglamentos y actividades dirigidos a mejorar la seguridad operacional. Para el establecimiento y mantenimiento del SSP, están estructurados en los siguientes cuatro componentes:

- a) Política, objetivos y recursos estatales de seguridad operacional;
- b) Gestión estatal de los riesgos de seguridad operacional;
- c) Aseguramiento estatal de la seguridad operacional; y
- d) Promoción estatal de la seguridad operacional.

3.3.2.2 La implementación del SSP se dirige a mejorar estos procesos con elementos adicionales de rendimiento y basados en riesgos de seguridad operacional, así como facilitar la eficaz implementación del SMS por la industria de aviación de Paraguay.

3.3.2.3 El SSP se dirige a:

- a) Asegurar que Paraguay cuenta con un marco legislativo eficaz para apoyar reglamentos de operación específicos;
- b) Asegurar la coordinación del SRM y el aseguramiento de la seguridad operacional y la sinergia entre las autoridades aeronáuticas estatales pertinentes;
- c) Apoyar la implementación efectiva y la interacción apropiada con los SMS de los proveedores de servicios;
- d) Facilitar la observación y la medición del rendimiento en materia de seguridad operacional de la industria aeronáutica de Paraguay; y
- e) Mantener o mejorar continuamente el rendimiento general en materia de seguridad operacional.

3.2 COMPONENTE 1: POLÍTICA, OBJETIVOS Y RECURSOS ESTATALES DE SEGURIDAD OPERACIONAL

3.2.1 Legislación aeronáutica básica (CE-1)

3.2.1.1 Promulgación de una legislación aeronáutica completa y efectiva, que permita a la DINAC ejercer su vigilancia y gestión de la seguridad operacional. La “legislación aeronáutica básica” es el instrumento legislativo, conocido como “código de aviación civil” o “ley de aviación civil”, que se aplica a todas las personas y organizaciones sometidas a las leyes del Estado en cuestión. En la mayoría de sus artículos se refiere a las leyes y reglamentos nacionales relativos a la entrada y salida de su territorio de las aeronaves utilizadas en la aviación civil internacional. También hace referencia a los reglamentos respecto a la operación y navegación

de tales aeronaves mientras se hallan en su territorio, la matriculación de aeronaves y el vuelo y las maniobras de las aeronaves, incluida la certificación de la aeronavegabilidad y el otorgamiento de licencias al personal. Se refiere también al suministro de servicios de navegación aérea (ANS) y aeródromos para facilitar la navegación, así como que adopten legislación para permitir la investigación de accidentes.

3.2.1.2 DINAC establece una política de cumplimiento como parte de su SSP, que:

- a) Apoye y fomente una cultura de seguridad operacional positiva;
- b) Describa la forma en que asegura la protección de los datos y la información sobre seguridad operacional y fuentes conexas, especialmente si la información proporcionada es autoincriminatoria; y
- c) Especifique las condiciones y circunstancias en las cuales los proveedores de servicios que cuentan con un SMS están autorizados para abordar y resolver sucesos que involucren ciertos problemas internos de seguridad operacional, dentro del contexto de sus SMS y a satisfacción de la DINAC, siempre que el SMS se ajuste al marco SMS y demuestre ser eficaz y tener madurez.

Mediante la aplicación de principios de gestión de la seguridad operacional, la relación entre DINAC y sus proveedores de servicios debería evolucionar más allá del cumplimiento y la ejecución, para alcanzar una asociación dirigida a mantener o mejorar continuamente el rendimiento en materia de seguridad operacional.

3.2.1.3 La legislación aeronáutica básica otorga poder al personal que desempeña funciones de vigilancia de la seguridad operacional a supervisar activa y efectivamente las actividades de aviación civil y a, en particular respecto a:

- a) Las cualificaciones y competencia del personal aeronáutico, utilizando un sistema de otorgamiento de licencias al personal (p. ej., expedición/convalidación, renovación, suspensión o cancelación de licencias y certificados de competencia, según corresponda); y
- b) La operación de aeronaves y funciones de apoyo utilizando un sistema para la matrícula, expedición/convalidación, renovación, suspensión y cancelación de licencias, certificados, autorizaciones y aprobaciones, según corresponda. En estas funciones de apoyo se incluyen las siguientes:
 - inspección de aeronavegabilidad e ingeniería de la aeronavegabilidad, según corresponda; expedición de directrices de aeronavegabilidad y aprobaciones de diseño; y aprobación de organismos de fabricación y mantenimiento;
 - ATS y otros servicios ANS, incluidos servicios meteorológicos y búsqueda y salvamento; y
 - desarrollo, diseño y operación y certificación.

3.2.2 Reglamentos de explotación específicos (CE-2)

3.2.2.1 Los reglamentos de explotación específicos se elaboran para proporcionar los requisitos mínimos necesarios y deseables, que contengan detalles suficientes y sean coherentes con sus marcos jurídicos, incluidos los aspectos no relacionados con la aviación. Deben redactarse con fraseología jurídica de tal modo que puedan comprenderlos fácilmente la industria y el personal de la autoridad que otorga licencias, certificados y aprobaciones en la ejecución de sus actividades corrientes.

3.2.2.2 La DINAC elaborará e implantará un proceso para asegurar la enmienda oportuna de los reglamentos de explotación específicos, según corresponda, a fin de que sean pertinentes y apropiados. El sistema establecido debe asegurar que los reglamentos se publiquen a nivel apropiado. También debe asegurar que sea coherente y, en particular, que se eliminen los reglamentos cuando los reemplacen otros nuevos.

3.2.2.3 Reglamentos prescriptivos y basados en el rendimiento

3.2.2.3.1 Los reglamentos de seguridad operacional constituyen una herramienta importante que se puede utilizar para controlar los riesgos de seguridad operacional. Con la transición a la gestión de la seguridad operacional, también se ha registrado una tendencia hacia la introducción de reglamentos basados en el rendimiento. Para comprender el carácter de esos reglamentos basados en el rendimiento, se debe comprender en primer lugar los reglamentos de carácter prescriptivo. Los reglamentos de carácter prescriptivo son aquellos que establecen explícitamente lo que debe hacerse y cómo debe hacerse. La expectativa es que el cumplimiento de estos reglamentos alcanzará el nivel de seguridad operacional deseado. Desde la perspectiva del proveedor de servicios, la satisfacción de los requisitos prescriptivos significa implementar los reglamentos sin desviaciones.

3.2.2.3.2 Los SARPS de la OACI se habían concentrado en requisitos prescriptivos como medio de identificar normas mínimas y asegurar el interfuncionamiento. No obstante, es cada vez más necesario habilitar reglamentos basados en el rendimiento para apoyar enfoques de implementación innovadores que puedan mejorar la eficiencia y alcanzar o superar los objetivos de seguridad operacional.

3.2.2.3.3 Ejemplos de normas que permiten la introducción de reglamentos prescriptivos y basados en el rendimiento. El siguiente es un ejemplo de una Norma del Anexo 14 — Aeródromos, Volumen I — Diseño y operaciones de aeródromos, que permite introducir reglamentos prescriptivos:

3.3.1 Cuando el extremo de una pista no dispone de una calle de rodaje o de una curva de viraje en la calle de rodaje y la letra de clave es D, E o F, se proporcionará una plataforma de viraje en la pista para facilitar el viraje de 180 grados de los aviones.

El ejemplo permite introducir un reglamento prescriptivo dado que identifica solamente una forma de demostrar el cumplimiento si la pista es del tipo especificado: es decir, proporcionar una plataforma de viraje en la pista. La desviación con respecto a los reglamentos prescriptivos se permite normalmente como excepción de los mismos.

3.2.2.3.4 En contraste, las normas que permiten la introducción de reglamentos basados en el rendimiento se expresan en términos del resultado deseado. Los reglamentos basados en el rendimiento resultantes requieren que el proveedor de servicios demuestre que su enfoque propuesto alcanzará el resultado deseado.

3.2.2.3.5 El siguiente es un ejemplo de Norma basada en el rendimiento extraído del Anexo 6, Parte I.

7.2.11 El avión irá suficientemente provisto de equipo de navegación para asegurar que, en caso de falla de un elemento del equipo en cualquier fase del vuelo, el equipo restante permita que el avión navegue de conformidad con 7.2.1 y, cuando corresponda, con 7.2.2, 7.2.5 y 7.2.6.

Obsérvese que la Norma anterior no indica el equipo de navegación específico requerido. En vez de ello, describe el resultado deseado, es decir, que, en caso de falla de un elemento del equipo, el equipo restante debe permitir que el avión navegue en condiciones de seguridad. El equipo requerido dependería del diseño de la aeronave.

3.2.2.3.6 Los reglamentos redactados de esta forma requerirán que el explotador de servicios aéreos proporcione a la DINAC los datos necesarios para demostrar la forma en que cumple dicho requisito. Esto puede hacerse mediante su propio análisis, pero para tales tipos de reglamentos basados en el rendimiento, la información necesaria está a menudo disponible en otras fuentes. En este caso, tanto la DINAC como el explotador de servicios aéreos harían uso de los datos de fabricantes de aeronaves para orientar su decisión, y no es necesario que el explotador de servicios aéreos elabore su propia solución.

3.2.2.3.7 El siguiente es otro ejemplo de Norma basada en el rendimiento, extraído de 4.3.2.1.1 del DINAC R19.

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

3.2.2.3.8 En el ejemplo, aunque la norma exige que se implante un proceso para identificar peligros, no especifica el aspecto de dicho proceso. La DINAC puede permitir que los proveedores de servicios diseñen su propia metodología. La función será evaluar si la metodología, procesos y sistemas del proveedor de servicios resultarían en verdad en la identificación de peligros. También deberá evaluar el rendimiento del proceso de identificación de peligros del proveedor de servicios, por ejemplo, mediante la evaluación del volumen, tipos e importancia de los peligros identificados. Los reglamentos basados en el rendimiento redactados de esta forma requieren que los responsables de la elaboración de reglamentos posean la pericia y la experiencia técnica para evaluar el rendimiento del sistema, en vez de evaluar solamente el cumplimiento prescriptivo de la letra de los reglamentos.

3.2.2.3.9 Cabe señalar que los reglamentos basados en el rendimiento no siempre son apropiados. Los reglamentos prescriptivos continúan siendo apropiados cuando es necesario tener un medio de cumplimiento normalizado, por ejemplo, para facilitar el interfuncionamiento. Los requisitos relativos a las señales de pista, por ejemplo, son de carácter necesariamente prescriptivo.

3.2.3 Sistema y funciones estatales (CE-3)

3.2.3.1 Para que la DINAC pueda cumplir sus obligaciones como se indica en la legislación aeronáutica deberá prever un sistema de aviación civil debidamente organizado y financiado y con las facultades o responsabilidades necesarias, estructurado de modo que pueda llevar a cabo efectivamente las tareas previstas. Es necesario que DINAC establezca una organización apropiada y práctica y emplee el personal necesario, incluido personal técnico y de apoyo, para desempeñar sus funciones y obligaciones de vigilancia de la seguridad operacional.

3.2.3.2 Al seleccionar la estructura orgánica necesaria para el sistema de aviación civil, DINAC deberá evaluar sus requisitos basándose en los Anexos del Convenio y textos de orientación conexos. Deberá asegurarse de que en la estructura establecida se consideren todos los aspectos técnicos aplicables en relación con funciones relacionadas con la vigilancia de la seguridad operacional, la recopilación y procesamiento de datos sobre esta última y la investigación de accidentes e incidentes. Estas funciones deben definirse claramente y sin duplicación.

3.2.3.3 Las políticas estatales de seguridad operacional y los objetivos estatales de seguridad operacional son declaraciones de alto nivel apoyadas por la máxima autoridad de la DINAC. Combinados, orientan el comportamiento en materia de seguridad operacional y la asignación de recursos.

3.2.3.3.1 El compromiso de la administración superior deberá estar articulado en la política estatal de seguridad operacional. Esta política es un documento formal que describe las intenciones y la dirección estatal en materia de seguridad operacional. proyecta la actitud de la administración superior respecto de la seguridad y la promoción de una cultura de seguridad operacional positiva. Puede considerarse como una declaración de la misión y visión en materia de seguridad operacional.

Los principios reflejados en la política de seguridad operacional deberán ser claramente visibles en las prácticas cotidianas.

Una declaración de política típica es: “Alcanzaremos la seguridad operacional mediante:

- 1) nuestra aceptación de la obligación de rendir cuentas respecto de las condiciones y comportamientos de seguridad;

- 2) una cultura de liderazgo, colaboración, comunicación abierta en materia de seguridad operacional, etc.”.

3.2.3.3.2 La elaboración de objetivos de seguridad operacional comienza con una clara comprensión de los riesgos de seguridad operacional más elevados en el sistema aeronáutico. Son declaraciones breves y de alto nivel. Representan los resultados deseados en materia de seguridad operacional que procura alcanzar.

Los objetivos de seguridad operacional apoyan la identificación de los SPI y las SPT y el posterior establecimiento del nivel aceptable de performance en materia de seguridad operacional (ALoSP)I.

3.2.3.4 La política y los objetivos estatales de seguridad operacional deberán publicarse y revisarse periódicamente para asegurar sus progresos hacia el logro de sus objetivos de seguridad operacional y su continua pertinencia, teniendo en cuenta todas las reevaluaciones de los riesgos presentes.

3.2.3.5 Cuando DINAC comienza a implementar plenamente su SSP y adoptar prácticas de gestión de la seguridad operacional, el costo de contratación y mantenimiento de personal técnico cualificado, que cumpla satisfactoriamente los requisitos de la profesión, representa un compromiso financiero importante y puede exigir la revisión de los criterios y reglamentos tradicionales relativos a su remuneración. Para contratar y retener personal debidamente cualificado que reúna profesionalismo e integridad, es indispensable que la DINAC se convierta en un empleador competitivo. Más aún, deberán contar con políticas, condiciones de empleo y prácticas apropiadas.

3.2.3.6 Una instrucción apropiada y suficiente para los inspectores asegurará una supervisión o vigilancia coherente y que las capacidades requeridas sean eficaces en un entorno de la gestión de la seguridad operacional. La instrucción del personal técnico no se limita a disciplinas estrictamente profesionales, como el mantenimiento de la competencia y su vigencia. En particular, es esencial que los inspectores de aviación civil reciban instrucción relativa a cuestiones como los reglamentos aplicables, las habilidades, conocimientos, obligaciones y responsabilidades de los inspectores, así como los procedimientos para implantar requisitos y velar por su cumplimiento.

3.2.3.7 Es esencial que DINAC aplique una metodología para determinar sus necesidades de personal que desempeñe funciones de vigilancia de la seguridad operacional, teniendo en cuenta el tamaño y la complejidad de las actividades aeronáuticas. Deberá otorgarse particular atención para asegurar que las necesidades que se determinen permitan cubrir adecuadamente todas las disciplinas técnicas necesarias para una vigilancia efectiva de la seguridad operacional.

3.2.4 Personal técnico cualificado (CE-4)

3.2.4.1 La DINAC deberá identificar y tratar las competencias requeridas, teniendo en cuenta las funciones y responsabilidades desempeñadas por su personal en el marco del SSP. Estas competencias se añaden a las requeridas para la vigilancia del cumplimiento y pueden tratarse mediante la instrucción del personal existente o la contratación de personal adicional. Estas competencias comprenden, entre otras, las siguientes:

- a) Aptitud para el liderazgo mejorada;
- b) Comprensión de los procesos empresariales;
- c) Experiencia y buen juicio para evaluar rendimiento y eficacia;
- d) Vigilancia de la seguridad operacional basada en riesgos;
- e) Recopilación y análisis de datos de seguridad operacional;
- f) Medición y observación del rendimiento en materia de seguridad operacional; y

- g) Actividades de promoción de la seguridad operacional.
- 3.2.4.1.1** Para asegurar que el personal técnico reciba la instrucción requerida de manera efectiva y mantenga su competencia, la DINAC debe establecer e implantar un sistema de instrucción eficaz. Éste deberá basarse en una política de instrucción documentada, que sea establecida y firmada a nivel de la máxima autoridad.
- 3.2.4.1.2** La política de instrucción deberá garantizar que se proporcione toda la instrucción necesaria a todo el personal técnico en todos los campos, incluidas la instrucción inicial (p. ej., instrucción de ingreso y básica), instrucción en el puesto de trabajo (OJT), instrucción periódica e instrucción especializada o avanzada. Además, deberá exigirse, en la política de instrucción, el establecimiento de un programa de instrucción para cada puesto de personal técnico y planes de instrucción para cada miembro del personal técnico.
- 3.2.4.1.3** Debería darse prioridad al personal involucrado en la implementación del SSP-SMS y a los inspectores de aviación civil involucrados en la supervisión/vigilancia del SMS del proveedor de servicios.
- 3.2.4.2** La DINAC implantará un sistema para el mantenimiento de registros de instrucción para su personal técnico. Esto incluye registros de la OJT que se haya adquirido, reflejando las diversas fases de la OJT que se hayan finalizado (o sea, observación, realización de tareas bajo supervisión y evaluaciones finales), así como la evaluación de la competencia del personal.
- 3.2.5** **Orientación técnica, instrumentos y suministro de información crítica en materia de seguridad operacional (CE-5)**
- 3.2.5.1** El suministro de material de orientación suficiente tiene dos objetivos: primero, proporcionar orientación al personal técnico sobre la manera de desempeñar sus funciones y actividades específicas; y segundo, permitir a la administración asegurarse de que las funciones y actividades de vigilancia de la seguridad operacional se lleven a cabo de manera eficaz y normalizada.
- 3.2.5.1.1** De modo general, los procedimientos relacionados con una tarea o actividad específica deberán responder a la pregunta siguiente: *¿Quién hace qué cosa, ¿cómo, ¿cuándo y en coordinación con quién?* Esta lista tiene carácter ilustrativo y no es exhaustiva.
- QUIÉN:**
- Definir, lo más claramente posible, las entidades o puesto de trabajo pertinente encargadas de cada tarea;
 - Definir quién tiene la autoridad de decidir, particularmente sobre aspectos relativos al cumplimiento; y
 - Definir quién tiene la autoridad de aprobar los resultados, informes, etc., o firmar cartas, informes, licencias, certificados, etc.
- QUÉ:**
- Definir cada etapa del proceso y cada tarea que debe realizarse;
 - Indicar el resultado previsto (informe, licencia, certificado, etc.);
 - Cuando corresponda, indicar la plantilla que debe utilizarse (adjuntándola al procedimiento) o el formato del resultado; y
 - Según corresponda, establecer el vínculo con otros procedimientos.
- CÓMO:**
- Proporcionar los detalles prácticos y metodología necesarios, según corresponda, para cada tarea;
 - Indicar la secuencia de las acciones;

- c) Indicar el tipo de documentos que deben examinarse y la manera de hacerlo;
- d) Describir métodos y medios para asegurar el seguimiento de la actividad (incluidos los documentos, a menudo ejemplares de los mismos, que deben conservarse); y
- e) Mencionar las listas de verificación o formularios aplicables utilizados en determinados puntos del procedimiento para realizar la actividad.

CUÁNDO:

- a) Si el procedimiento forma parte de un proceso, la etapa de este último en que el procedimiento tiene lugar;
- b) Para acciones repetitivas (p. ej., vigilancia continua), frecuencia e intervalo máximo entre dos acciones; y
- c) Plazo máximo para concluir cada tarea o fecha límite para cada etapa.

EN COORDINACIÓN CON QUIÉN: Si unas entidades externas participan en la actividad, deben identificarse lo más claramente posible.

3.2.5.1.2 Los procedimientos pueden complementarse, según corresponda, mediante listas de verificación. Las listas deberán concentrarse en aspectos específicos relacionados con la verificación y cada resultado o documento que debe obtenerse. De modo general, los procedimientos se compilan en forma de manual del inspector, que deberá presentarse en forma lógica y de fácil consulta e incluir referencias a listas de verificación y plantillas apropiadas

3.2.5.1.3 Sería útil elaborar orientación para algunos elementos de las listas de verificación, según corresponda, describiendo:

- a) Lo que debe verificarse;
- b) Mediante qué método (p. ej., si determinado elemento exige que se consulte un documento o se aplique una inspección física);
- c) Tipo de resultados que deben obtenerse (p. ej., medición física, resultados de pruebas que deben registrarse, ejemplar de un documento de un proveedor de servicios, evaluación de una entrevista); y
- d) Método de conservación de las listas de verificación finalizadas y los correspondientes documentos.

3.2.5.1.4 Para fomentar la seguridad operacional en el entorno operacional aeronáutico son esenciales el suministro y la rápida divulgación de información crítica para la seguridad operacional, como los avisos a los aviadores (NOTAM) y las directrices de aeronavegabilidad. Constituyen también medidas importantes la enmienda y actualización periódica de publicaciones como las cartas aeronáuticas y otras relacionadas con la aviación para lograr un entorno operacional seguro.

3.2.5.2 La DINAC también elaborará orientación para la industria a fin de explicar la manera en que deberán aplicarse las disposiciones de reglamentación. Dicha orientación podría también abarcar plantillas y formato normalizado para los documentos que cada proveedor de servicios interesado debe establecer.

3.3 COMPONENTE 2: GESTIÓN ESTATAL DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

3.3.1 Obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones (CE-6)

3.3.1.1 Las obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones son componentes importantes de la estrategia estatal de control de riesgo de seguridad operacional. Estas brindan garantías de que los proveedores de servicios y otras organizaciones representativas de la industria pertinentes han

alcanzado las normas requeridas para operar dentro del sistema aeronáutico en condiciones de seguridad.

- 3.3.1.1.1** En el marco de un sistema eficaz de otorgamiento de licencias, certificación y aprobación, un personal cualificado lleva a cabo eficazmente todas las evaluaciones necesarias basándose en requisitos nacionales y siguiendo un proceso formal y completo. El personal puede proceder de la DINAC, o en caso de que no existan dentro de esta última todas las especialidades y competencias necesarias (como sucede a menudo), unos especialistas externos pueden llevar a cabo las evaluaciones mediante una delegación apropiada de funciones. En tales casos, la DINAC deberá designar oficialmente a los especialistas después de verificar su competencia y la ausencia de posibles conflictos de interés. Deberán documentarse y registrarse debidamente los resultados, conservándose en la DINAC todos los registros y pruebas pertinentes. Los registros son necesarios para determinar la eficacia y asegurar el seguimiento de las actividades de certificación, otorgamiento de licencias y aprobación realizadas.
- 3.3.1.1.2** Según corresponda y en cumplimiento de la legislación y procedimientos nacionales, las actividades de otorgamiento de licencias deberían abarcar, entre otras cosas, lo siguiente:
- a) Aprobación de cursos de instrucción;
 - b) Aprobación del uso de dispositivos de instrucción de simulación y autorización de utilizarlos, a fin de adquirir experiencia y demostrar la aptitud necesaria para la expedición de una licencia o habilitación;
 - c) Aprobación, designación y supervisión de personas u organizaciones (incluidos los examinadores médicos) delegados para llevar a cabo tareas específicas en nombre de la oficina de otorgamiento de licencias al personal, si corresponde;
 - d) Evaluación y aprobación de solicitudes de licencias y habilitaciones;
 - e) Evaluaciones de aptitud médica relacionadas con los requisitos de otorgamiento de licencias;
 - f) Expedición de licencias y habilitaciones; y
 - g) Validación y conversión de licencias y habilitaciones expedidas por otros Estados.
- 3.3.1.1.3** La documentación completa para cada expedición o renovación de licencia debe mantenerse confidencialmente e incluir toda correspondencia, solicitudes, evaluaciones, resultados de exámenes, informes médicos y otra documentación de otorgamiento de licencias. Todos estos últimos deben conservarse.
- 3.3.1.1.4** En los DINAC R´S 141, 121, 135, 145 y 14 se exige la certificación o aprobación, según corresponda, de organizaciones de instrucción aprobadas, explotadores de servicios aéreos, organizaciones de mantenimiento de aeronaves y aeródromos internacionales. Según corresponda y en cumplimiento de la legislación y procedimientos nacionales, las actividades de certificación y aprobación deberían seguir un proceso completo, oficial y documentado que abarque, entre otras cosas, lo siguiente:
- a) Consideración del interés expresado, incluida la coordinación con otras autoridades interesadas;
 - b) Examen inicial de la documentación presentada por el proveedor de servicios, incluidas las principales competencias del personal y los procedimientos operacionales;
 - c) Auditorías o inspectorías in situ para verificar aspectos técnicos y evaluar la organización, y competencia del proveedor de servicios, así como la aplicación de sus procedimientos operacionales;

- d) De ser necesario, evaluación de la exención solicitada y documentos que la apoyen (p. ej. estudios aeronáuticos) con las inspecciones in situ necesarias, dando lugar al otorgamiento (o rechazo) de exenciones con las correspondientes medidas de mitigación;
- e) Evaluación de los planes de medidas correctivas presentados por el proveedor de servicios para resolver los problemas observados y los casos de incumplimiento y aceptación (o rechazo) de las medidas correctivas o de mitigación y sus plazos;
- f) Expedición del certificado o aprobación, con indicación de condiciones operacionales (y limitaciones, si se aplica);
- g) Renovación o validez continua de los certificados a raíz de una supervisión apropiada; y
- h) Transferencia o entrega de certificados.

3.3.2 Obligaciones del sistema de gestión de la seguridad operacional

3.3.2.1 Requisitos normativos del SMS. El DINAC R19, exige que los proveedores de servicios y explotadores de la aviación general internacional implanten un SMS. Los requisitos se refieren al marco para un SMS que figura en el Capítulo 4 del DINAC R19, y en la orientación de apoyo presentada en el Capítulo 4 de este manual.

3.3.2.1.1 La DINAC deberá instituir un proceso que asegure que el SMS les resulta aceptable. Un enfoque es establecer cronogramas e hitos a nivel estatal que representen el progreso requerido de la implementación del SMS.

3.3.2.1.2 Los requisitos normativos del SMS y los textos de orientación sobre el SMS deberán revisarse periódicamente. Dicha revisión debería tener en cuenta: información recibida de la industria, examen periódico del perfil de riesgo de seguridad operacional, situación presente y aplicabilidad de SARPS y textos de orientación de la OACI sobre SMS.

3.3.2.1.3 El SMS del proveedor de servicios debe resultar aceptable para la DINAC. Se espera que los proveedores de servicios realicen un análisis de brecha y elaboren un plan de implementación ejecutable (incluyendo la aceptación por la DINAC como tarea planificada). La implementación del SMS se lleva a cabo generalmente en tres o cuatro etapas. La temprana colaboración entre el proveedor de servicios y la DINAC probablemente conduzca a un proceso de elaboración y aceptación más fluido.

3.3.2.2 Los indicadores de rendimiento propuestos por los proveedores de servicios son revisados y aceptados por la autoridad normativa de la DINAC como parte de la aceptación del SMS. La DINAC puede considerar la planificación de la aceptación de los indicadores de rendimiento de un proveedor de servicio más adelante en el proceso de implementación. Esto resulta especialmente práctico para los proveedores de servicios en la certificación inicial dado que a menudo no cuentan con suficientes datos para elaborar indicadores significativos. La autoridad normativa puede estar satisfecho de que los indicadores de rendimiento propuestos son apropiados y pertinentes a las actividades aeronáuticas de cada proveedor de servicio. Algunos de los indicadores y metas de rendimiento del proveedor de servicio pueden relacionarse con los indicadores y metas de rendimiento de la DINAC para la medición y observación del ALoSP.

3.3.2.2.1 La aceptación de las metas de rendimiento del proveedor de servicios puede abordarse después de que los indicadores de rendimiento han sido observados durante un período de tiempo. Esto establece el rendimiento básico. Puede basarse en metas establecidas a nivel estatal, regional o mundial. El logro de las SPT de Estado exigirá la coordinación de medidas de mitigación de riesgo de seguridad operacional con el proveedor de servicios.

- 3.3.2.3** Las disposiciones sobre SMS para la aviación general internacional se abordan con cierta flexibilidad en el DINAC R19 y, por consiguiente, no se incluyen en la lista correspondiente a los proveedores de servicios. La diferencia entre este sector y los demás sectores es que, en este caso, la DINAC puede ejercer un grado de flexibilidad en la forma en que establecen los requisitos.
- 3.3.2.3.1** El establecimiento de esos criterios deberá exigir la aplicación del marco SMS según se describe en el DINAC R19, pero ello puede lograrse de varias maneras:
- a) Estableciendo criterios dentro de los reglamentos de explotación específicos para Aviación general internacional existentes;
 - b) Publicando requisitos dentro del marco normativo en un instrumento jurídico distinto de los reglamentos de explotación específicos que definen los criterios; o
 - c) Haciendo referencia dentro del marco normativo a un código de práctica industrial del SMS que sea reconocido por la DINAC.
- 3.3.3 Investigación de accidentes e incidentes**
- 3.3.3.1** El proceso de investigación de accidentes e incidentes permite identificar factores contribuyentes y cualquier posible falla dentro del sistema aeronáutico, así como generar las recomendaciones necesarias para prevenir repeticiones. Esta actividad contribuye a la continua mejora de la seguridad operacional de la aviación mediante el descubrimiento de fallas activas y factores contribuyentes de accidentes o incidentes proporcionando, además, informes sobre cualesquiera enseñanzas obtenidas del análisis de sucesos. Esto puede apoyar la elaboración de decisiones sobre medidas correctivas y la correspondiente asignación de recursos identificando además mejoras necesarias del sistema de aviación.
- 3.3.4 Identificación de peligros y evaluación de riesgos de seguridad operacional**
- 3.3.4.1** Deberá elaborarse un proceso sistemático para asegurar la eficaz identificación de peligros. Este debería incluir los elementos siguientes:
- a) Acceso a las fuentes de datos necesario para apoyar la gestión de riesgos de seguridad operacional;
 - b) Equipo de análisis de seguridad operacional con pericia analítica y experiencia operacional apropiadas, así como instrucción y experiencia en varias técnicas de análisis de peligros; y
 - c) Mecanismos de análisis de peligros apropiados a los datos recopilados (o que se recopilarán) y al ámbito de las actividades aeronáuticas.
- 3.3.4.1.1** El análisis de los peligros identificados durante una investigación de incidente o accidente constituye un ejemplo de metodología reactiva.
- 3.3.4.1.2** Una metodología proactiva podría incluir los peligros identificados durante auditorías o inspectorías o de las notificaciones obligatorias. Esto a su vez podría incluir el estar alerta frente a los primeros signos de deterioro del rendimiento en materia de seguridad operacional que surjan de la observación cotidiana de la fiabilidad del sistema.
- 3.3.4.1.3** Un mecanismo importante para la identificación proactiva de peligros es un sistema de notificación voluntaria de seguridad operacional. En el Capítulo 5 figura orientación adicional sobre los sistemas de notificación voluntaria.
- 3.3.4.1.4** La identificación de peligros también puede considerar peligros generados fuera de la organización y peligros que escapan al control directo de la organización, como las condiciones meteorológicas extremas o las cenizas volcánicas.
- 3.3.4.1.5** Al identificar peligros debería tenerse en cuenta lo siguiente:
- a) Descripción del sistema

- b) Factores de diseño, incluyendo diseño de equipo y tareas;
- c) Limitaciones de la actuación humana (fisiológicas, psicológicas, físicas, etc.);
- d) Procedimientos y prácticas operacionales, incluyendo documentación y listas de verificación y su validación en condiciones de operación reales;
- e) Factores de comunicación, terminología e idioma;
- f) Factores institucionales, como los relacionados con la contratación, instrucción y retención de personal, compatibilidad de los objetivos de seguridad operacional, asignación de recursos y cultura de seguridad operacional corporativa;
- g) Factores relacionados con el entorno operacional (p. ej., condiciones meteorológicas, ruido y vibraciones ambientales, temperatura e iluminación);
- h) Factores de vigilancia normativa, incluyendo la aplicación del cumplimiento de reglamentos;
- i) Sistemas de observación del rendimiento que puedan detectar desviaciones de la práctica, desviaciones operacionales;
- j) Factores de la interfaz humano-máquina; y
- k) Factores relacionados con las interfaces SSP/SMS.

3.3.4.2

El proceso de evaluación de riesgos de seguridad operacional deberá utilizar cualesquiera datos e información sobre seguridad operacional que estén disponibles. Una vez evaluados los riesgos de seguridad operacional, emprenderá un proceso de toma de decisiones basada en datos para determinar los tipos de controles de riesgos de seguridad operacional que se necesitan.

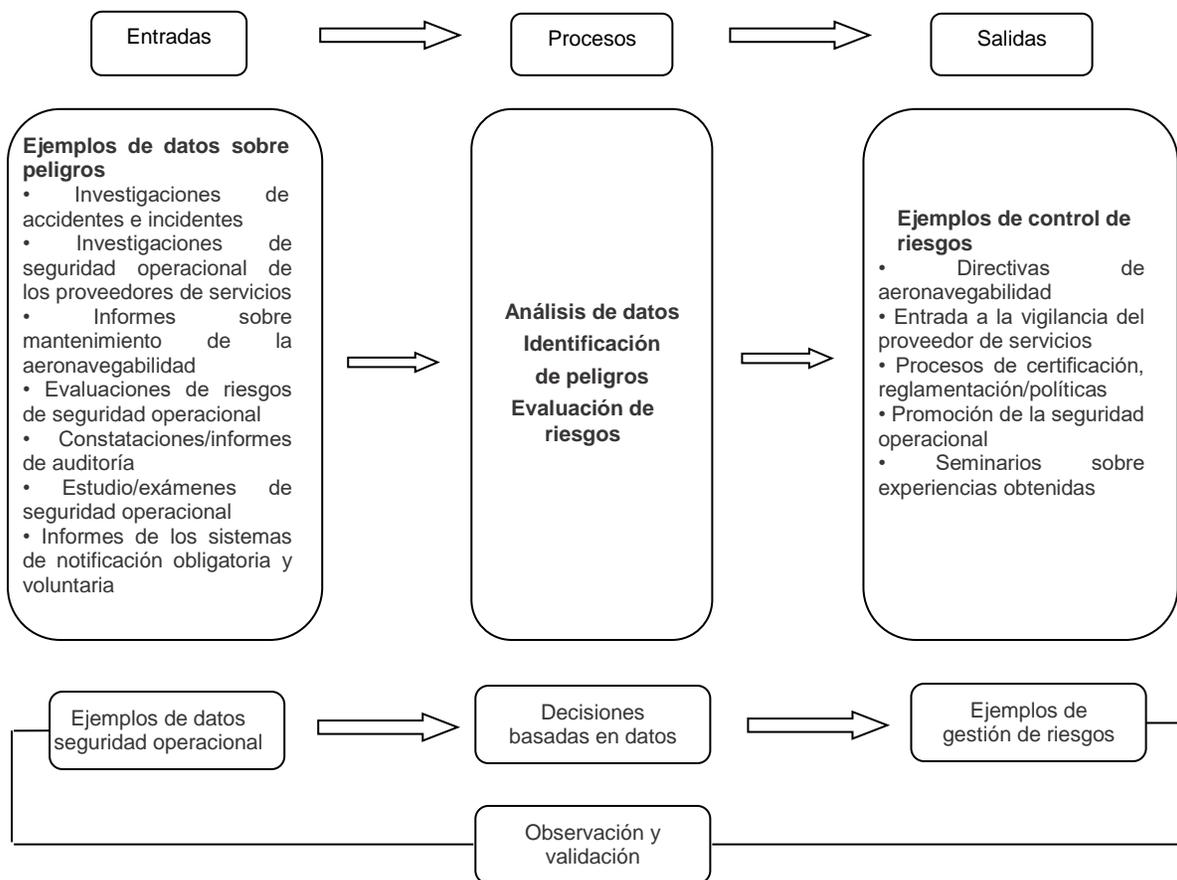


Figura. Programa de análisis basado en datos

- 3.3.5 Gestión de riesgos de seguridad operacional (CE-8)**
- 3.3.5.1** Los problemas de seguridad operacional detectados por la DINAC abarcan, entre otros, los siguientes:
- a) Incumplimiento de requisitos y otras deficiencias;
 - b) Sucesos de seguridad operacional notificados que se analizan;
 - c) Tendencias negativas en materia de seguridad operacional; y
 - d) Resultados de investigaciones de accidentes e incidentes de aviación (incluidas recomendaciones relativas a la seguridad operacional).
- 3.3.5.1.1** Si las actividades de vigilancia revelan que el titular de licencia, habilitación, certificado o aprobación no ha satisfecho o mantenido las normas requeridas o no está en condiciones de hacerlo, la DINAC deberá:
- 1) avisar rápidamente al titular de licencia, habilitación, certificado o aprobación acerca de la deficiencia observada;
 - 2) proporcionar plazos para la presentación del plan de medidas correctivas que el proveedor de servicios debe adoptar;
 - 3) verificar que las medidas correctivas y los plazos correspondientes son apropiados, antes de aceptar oficialmente el plan de medidas correctivas; y
 - 4) iniciar seguimiento apropiado para verificar la aplicación efectiva de medidas correctivas.
- 3.3.5.1.2** Si el titular de licencia, habilitación, certificado o aprobación no corrige la deficiencia en los plazos establecidos.
- 3.3.5.2** Para asegurar que las recomendaciones relativas a la seguridad operacional se tomen debidamente en cuenta, la DINAC debe establecer e implantar un proceso estructurado para su seguimiento. Dicho proceso debería incluir, entre otras cosas, lo siguiente:
- a) Coordinación entre las partes interesadas;
 - b) Proceso de comunicación con las partes afectadas por la recomendación;
 - c) Indicación de calendarios; y
 - d) Procedimientos para observar el progreso de las medidas adoptadas en respuesta a la recomendación relativa a la seguridad operacional hasta su plena aplicación, con seguimiento documentado.
- 3.3.5.2.1** Las medidas eficaces y oportunas adoptadas por la industria deberán permitir que se resuelvan efectivamente los problemas de seguridad operacional. De lo contrario, la DINAC deberá tomar medidas apropiadas en materia de cumplimiento, como la imposición de limitaciones, la suspensión o revocación de certificados, licencias o aprobaciones o la imposición de sanciones financieras.
- 3.3.5.3** La Ley N° 1860/02 Código Aeronáutico y el DINAC R1100 Reglamento de Infracciones y Sanciones Aeronáuticas y la Política de Cumplimiento Normativo otorga poderes a la DINAC para que tome tales medidas, que deberán corresponder a los riesgos en materia de seguridad operacional causados por el incumplimiento o las violaciones. Si, tras un examen cuidadoso de todas las circunstancias del caso, se determina la necesidad de suspender o revocar los privilegios del titular de licencia, habilitación, certificado o aprobación, la DINAC deberá informar al titular oficialmente y por escrito, resumiendo la medida propuesta y sus motivos.
- 3.3.5.3.1** Basándose en el marco legal, la DINAC deberá establecer e implantar políticas y procedimientos claros, completos y detallados en materia de cumplimiento para uso de su personal. Dichas políticas y procedimientos deberán permitir un enfoque efectivo, proporcional, gradual y coherente.

3.4 COMPONENTE 3: ASEGURAMIENTO ESTATAL DE LA SEGURIDAD OPERACIONAL

3.4.1 Obligaciones de vigilancia (CE-7)

3.4.1.1 La DINAC lleva a cabo actividades de supervisión para verificar, de manera preventiva, que los titulares de licencias, certificados, autorizaciones o aprobaciones en el ámbito de la aviación sigan satisfaciendo los requisitos establecidos y funcionen con el nivel de competencia y seguridad operacional exigido. Estas actividades abarcan la realización de inspecciones in situ (visitas anunciadas o no), el examen de documentos presentados por los proveedores de servicios, reuniones con partes interesadas y análisis de la información disponible sobre seguridad operacional.

3.4.1.2 La DINAC establece e implanta, en cada sector, un programa de supervisión que deberá incluir, como mínimo, los elementos indicados más abajo, que pueden ser adaptados si se utiliza un método basado en el riesgo:

- a) Tipos de actividades de supervisión (p. ej., auditorías, inspectorías, pruebas, análisis de sucesos relacionados con la seguridad operacional);
- b) Calendario o frecuencia de las actividades;
- c) Elementos que deben considerarse o alcance de las actividades; y
- d) Metodología o procedimientos relacionados, ayudas para el trabajo y orientación sobre la manera en que la actividad deberá llevarse a cabo, a partir de la notificación del proveedor de servicios, si corresponde, hasta la conclusión de las deficiencias observadas durante las actividades.

Nota.- Las actividades de supervisión abarcan actividades programadas y no programadas o no anunciadas, según corresponda, por ejemplo para verificar la corrección de deficiencias observadas o como seguimiento de sucesos notificados relacionados con la seguridad operacional, informes de denunciantes y cambios significativos.

3.4.1.2.1 La DINAC puede elaborar perfiles de riesgos de seguridad operacional institucionales que sean coherentes para cada sector aeronáutico a efectos de apoyar el proceso de modificar el alcance y la frecuencia de sus actividades de vigilancia. Pueden incluir factores como los siguientes:

- a) La solidez financiera de la organización;
- b) El número de años en funcionamiento;
- c) Índice de rotación del personal fundamental como el ejecutivo responsable y el gerente de seguridad operacional;
- d) Competencia y rendimiento del ejecutivo responsable;
- e) Competencia y rendimiento del gerente de seguridad operacional;
- f) Resultados de auditorías anteriores;
- g) Solución oportuna y efectiva de las constataciones anteriores;
- h) Medidas del nivel de actividad relativo (exposición a los riesgos de seguridad operacional);
- i) Indicadores del alcance y complejidad relativos de las actividades que se realizan;
- j) Grado de madurez del proceso de identificación de peligros y evaluación de riesgos de seguridad operacional; y
- k) Medición del rendimiento en materia de seguridad operacional a partir de análisis de datos de seguridad operacional y actividades de observación del rendimiento.

- 3.4.1.2.2** Para cada organización o proveedor de servicios aeronáuticos, deberá elaborarse un plan de supervisión periódica basado en el programa de supervisión aplicable. El plan de supervisión deberá incluir detalles relativos al tipo de actividades que deben realizarse y el calendario específico, así como el alcance de cada actividad, según corresponda. En el caso de un explotador certificado, debe asegurarse que se examinen todos los sectores cubiertos por la certificación dentro de un plazo definido. El calendario y la frecuencia de las actividades de supervisión pueden adaptarse para cada explotador, basándose en la información disponible.
- 3.4.1.2.3** Las metodologías para los diversos tipos de actividades de supervisión deberán abarcar las fases relativas a la preparación, realización, notificación y seguimiento. Deberán elaborarse y aplicarse para cada fase, según corresponda, procedimientos, plantillas y ayudas para el trabajo apropiados. Las metodologías deberán abarcar disposiciones para clasificar las conclusiones que resultan de la actividad de supervisión, basándose en su gravedad, dado que dicha clasificación determinará el tipo de seguimiento y la medida de cumplimiento, junto con los plazos correspondientes.
- 3.4.1.2.4** En todas las fases del programa de supervisión, las competencias de una organización deberán ser iguales o superiores a las que se exigen en el momento de la certificación, licencia o aprobación o autorización original. Por ello, el personal técnico de la DINAC deberá desempeñar actividades de supervisión completa y exigir que la organización demuestre de manera convincente que:
- a) Sus funciones y tareas se llevan a cabo de conformidad con los requisitos aplicables; y
 - b) Como consecuencia, los privilegios otorgados con la expedición inicial de la licencia, certificado, aprobación o autorización deberán mantenerse.
- 3.4.1.2.5** La DINAC establece e implanta, para cada área, un sistema de conservación de registros y archivo. Los registros deberán abarcar, entre otras cosas, lo siguiente:
- a) Listas de verificación finalizadas, informes de evaluación y documentación conexas, incluidas, según corresponda, evaluaciones de la seguridad operacional;
 - b) Actas de reuniones celebradas como parte de la supervisión; y
 - c) Informes de seguimiento sobre la aplicación de planes de medidas correctivas.
- 3.4.1.2.6** La conclusión efectiva y oportuna del programa de supervisión depende en gran medida de la disponibilidad de personal cualificado suficiente, que cubra todos los conocimientos especializados requeridos, y de la autoridad que la DINAC les confiere a sus inspectores.
- 3.4.1.3** Según lo establecido en 3.4.1.1 DINAC examinará periódicamente el rendimiento de seguridad operacional de cada proveedor de servicios. Para dicho examen deberá tener en cuenta el rendimiento y la eficacia de cada indicador y meta de rendimiento de seguridad operacional. El examen puede indicar la necesidad de introducir ajustes para apoyar la continua mejora de la seguridad operacional.
- 3.4.2 Rendimiento estatal en materia de seguridad operacional**
- 3.4.2.1** El nivel aceptable de rendimiento en materia de seguridad operacional (ALoSP) de la DINAC que ha de alcanzar puede lograrse por medio de:
- a) Implementación y mantenimiento del SSP y;
 - b) Implementación y mantenimiento de indicadores y metas de rendimiento que indiquen que la seguridad operacional se está gestionando eficazmente.
- 3.4.2.1.1** El ALoSP expresa los niveles de seguridad operacional que espera lograr en su sistema aeronáutico, incluyendo las metas que cada sector debe alcanzar y

mantener en relación con la seguridad operacional, así como las medidas para determinar la eficacia de sus propias actividades y funciones que afecten la seguridad operacional.

3.4.2.1.2 El ALoSP no deberá elaborarse aisladamente. En vez de ello, deberá definirse teniendo en cuenta una orientación estratégica de alto nivel (del GASP, planes regionales, etc.) y los objetivos de seguridad operacional establecidos en el SSP.

3.4.2.1.3 El ALoSP representa el acuerdo entre todas las autoridades aeronáuticas con respecto al nivel previsto de rendimiento en materia de seguridad operacional que su sistema aeronáutico deberá alcanzar y demuestra a los interesados, tanto internos como externos, la forma en que la DINAC está gestionando la seguridad operacional de la aviación. Comprende, entre otras cosas, las expectativas en cuanto a rendimiento en materia de seguridad operacional para cada sector y proveedor de servicios.

3.4.2.2 El proceso para evaluar la eficacia de las medidas emprendidas para manejar los riesgos de seguridad operacional será a través del establecimiento de indicadores y metas de rendimiento de seguridad operacional.

3.4.2.2.1 Los indicadores de rendimientos de seguridad operacional deberán reflejar el entorno operacional específico y enfatizar las condiciones que pueden utilizarse a efectos de identificar la forma en que se controlan los riesgos de seguridad operacional. La estrategia de observación y medición deberá incluir un conjunto de indicadores que abarque todos los sectores del sistema aeronáutico de los cuales la DINAC es responsable. Deberá reflejar también tanto los resultados (p. ej., accidentes, incidentes, infracciones a reglamentos) como las funciones y actividades (operaciones en las que las mitigaciones de riesgos de seguridad operacional implantadas tuvieron los resultados previstos). Esta combinación permite evaluar el rendimiento en materia de seguridad operacional no solamente por lo que no funciona (es decir resultados), sino también con respecto a lo que sí funciona (es decir actividades en las que las mitigaciones de riesgos de seguridad operacional produjeron los resultados previstos). En términos prácticos, este enfoque abarca la consideración de indicadores de rendimiento que reflejan dos tipos distintos de riesgos de seguridad operacional:

a) **Riesgos de seguridad operacional en la explotación.** Se concentran en las condiciones que podrían conducir a un resultado no deseado. Estas son las condiciones relacionadas con accidentes, incidentes, fallas y defectos. El riesgo de seguridad operacional en la explotación es esencialmente un subproducto de la prestación de servicios.

b) **Riesgos de seguridad operacional en la implementación del proceso.** Se concentran en los medios y recursos necesarios para gestionar el riesgo de seguridad operacional en la explotación. La gestión del riesgo de seguridad operacional desde la perspectiva de la implementación del proceso se inicia con la evaluación de la situación de aplicación de las leyes y reglamentos nacionales relacionados con la seguridad operacional, la implementación de procesos SMS dentro de la industria, y la implementación del SSP a nivel país (que incluye la vigilancia y observación eficaces de la industria). Si es necesario introducir mejoras en cualquiera de los anteriores, las actividades para lograrlo deberán planificarse, implementarse y observarse, y además asignarse recursos adecuados a las mismas. Los indicadores de rendimiento se elaboran posteriormente para permitir el seguimiento de la planificación, implementación o eficacia de los cambios.

3.4.2.2.2 Estos indicadores de rendimiento pueden establecerse con referencia a las mejoras necesarias, como lo indiquen los análisis USOAP y las actividades de mejora continua del SSP.

3.4.2.2.3 Los indicadores de rendimiento para los riesgos de seguridad operacional en la explotación y en la implementación del proceso constituyen una parte fundamental

del proceso de aseguramiento de la seguridad operacional. La consolidación de indicadores de rendimiento sobre riesgos de seguridad operacional en la explotación e indicadores de rendimiento de riesgos de seguridad operacional en la implementación del proceso amplía la fuente de información para establecer el ALoSP.

3.4.2.3 El equipo responsable del acuerdo ALoSP original deberá determinar la adecuación continua del mismo. El examen periódico del ALoSP deberá concentrarse en:

- a) Identificar problemas críticos para la seguridad operacional dentro de los sectores de la aviación, asegurando la inclusión de indicadores que permitan la gestión de rendimiento en materia de seguridad operacional en esas áreas;
- b) Identificación de las metas que definan el nivel de rendimiento en materia de seguridad operacional que debe mantenerse o la mejora deseada que ha de alcanzarse para el indicador de rendimiento pertinente de cada sector, con miras a mejorar la gestión del rendimiento en todo el sistema aeronáutico;
- c) Identificación de elementos activadores (si corresponde) cuando un indicador de rendimiento alcanza un punto que exija tomar medidas; y
- d) Examen de los indicadores de rendimiento para determinar si es necesario introducir modificaciones, metas de rendimiento y elementos activadores (si corresponde) existentes a efectos de alcanzar el ALoSP convenido.

3.4.2.3.1 Cada riesgo de seguridad operacional debe evaluarse para identificar las medidas de mitigación requeridas. Estas medidas se vigilan mediante los indicadores de rendimiento que miden su eficacia.

3.4.2.3.2 El rendimiento en materia de seguridad operacional indicado por sus indicadores y metas demuestra el ALoSP alcanzado. Si algunas de las metas no se alcanzan, es necesario realizar una evaluación para comprender mejor los motivos de ello y determinar las medidas que deberían adoptarse. Lo anterior puede deberse a:

- a) Las metas no eran alcanzables o realistas;
- b) Las medidas adoptadas para alcanzar la meta no eran apropiadas o se apartaban de la intención original (desviación de la práctica);
- c) Cambios en otras prioridades de riesgos de seguridad operacional desviaron recursos respecto del logro de una meta determinada; o
- d) Surgieron riesgos emergentes que no se habían considerado cuando se establecieron las metas.

3.5 COMPONENTE 4: PROMOCIÓN ESTATAL DE LA SEGURIDAD OPERACIONAL

3.5.1 Comunicación y divulgación internas de la información sobre seguridad operacional

3.5.1.1 El documento SSP y sus políticas estatales conexas sobre seguridad operacional y cumplimiento resultan fundamentales para lograr la integración de la instrucción, la comunicación y la difusión de la información conexas.

3.5.1.1.1 Las autoridades normativas responsables de los diferentes sectores de la aviación deberán adoptar un enfoque integrado de sus respectivas funciones en la promoción estatal de la seguridad operacional. La DINAC deberá establecer canales de comunicación formales entre los miembros del grupo de coordinación del SSP (Dependencias involucradas en la implementación y mantenimiento del SSP).

3.5.1.1.2 Desde el punto de vista operacional, es importante que las estrategias operacionales del SSP, incluyendo requisitos SMS armonizados y observación de

los respectivos proveedores de servicios se compartan, comuniquen y coordinen entre las autoridades aeronáuticas. Un canal de comunicación abierto puede evitar la creación de requisitos SMS contradictorios o criterios de aceptación conflictivos para diferentes sectores de la aviación.

3.5.1.1.3 Entre los ejemplos de la información que debe abordar en su comunicación y difusión internas figuran los siguientes:

- a) Documentación, políticas y procedimientos relativos al SSP;
- b) Indicadores de rendimiento de seguridad operacional;
- c) Información sobre rendimiento en materia de seguridad operacional del sector;
- d) Perfiles de riesgos de seguridad operacional institucionales del sector;
- e) Comunicación de responsabilidades de seguridad operacional del sistema;
- f) Enseñanzas obtenidas de accidentes e incidentes; y
- g) Conceptos y mejores prácticas de gestión de la seguridad operacional.

3.5.1.1.4 Algunos medios que pueden adoptar para transmitir comunicaciones de seguridad operacional son: circulares, boletines, folletos, publicaciones, seminarios, reuniones, instrucción, sitios web, listas de distribución, publicación en medios sociales, debates en grupos de colaboración, entre otros.

3.5.1.1.5 Al evaluar el tipo de medio que deberá utilizar para dar a conocer un mensaje particular, se deberá considerar el que sea más apropiado para cada mensaje y su público destinatario. Los documentos SSP pueden publicarse en un sitio web que ya esté disponible. Otra información como las enseñanzas obtenidas y mejores prácticas puede resultar más adecuada para boletines o circulares.

3.5.2 Comunicación y divulgación externas de la información sobre seguridad operacional

3.5.2.1 La DINAC establecerá plataformas o medios de comunicación apropiados para facilitar la implementación del SMS y mejorar la cultura de seguridad operacional de todo el sistema.

3.5.2.1.1 Al comunicar y difundir externamente información sobre seguridad operacional a la industria de aviación, además de los aspectos indicados en la sección anterior, también podrá considerar la inclusión de:

- a) Textos de orientación para la implementación del SMS;
- b) Importancia de las notificaciones;
- c) Identificación de instrucción de seguridad operacional disponible para la comunidad aeronáutica;
- d) Promoción del intercambio de información de seguridad operacional:
 - 1) con y entre los proveedores de servicios; y
 - 2) entre los Estados.

3.5.2.1.2 La documentación estatal sobre el SSP y sus políticas conexas de seguridad operacional y cumplimiento también deberá ponerse a disposición de los proveedores de servicio según corresponda.

3.5.2.1.3 Esencialmente los mismos medios de apoyo utilizados para las comunicaciones internas pueden emplearse externamente en la medida en que su contenido resulte útil para ambos públicos. No obstante, puede prestarse atención especial a las soluciones que alcanzan a públicos más amplios como los medios sociales, listas de correo, boletines, seminarios, creación de comunidades en la industria para el intercambio de información de seguridad operacional.

- 3.5.2.1.4** La DINAC debe promover el establecimiento de redes de compartición e intercambio de información sobre seguridad operacional entre la comunidad aeronáutica.

CAPITULO 4.

SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

4.1 GENERALIDADES

4.1.1 La finalidad de un SMS es proporcionar a los proveedores de servicios un enfoque sistemático para gestionar la seguridad operacional. Está diseñado para mejorar continuamente la seguridad operacional mediante la identificación de peligros, la recopilación y el análisis de datos y la evaluación continua de los riesgos de la seguridad operacional.

4.1.2 Los proveedores de servicios mencionados en el DINAC R19 Capítulo 4, 4.1 y 4.2 elaborarán un plan para la implementación y mantenimiento de sus SMS, independientemente de la envergadura y complejidad, deberá contar con los 4 componentes y 12 elementos del marco del SMS.

4.2 AVIACIÓN GENERAL INTERNACIONAL – AVIONES

4.2.1 El establecimiento de esos criterios debería exigir la aplicación del marco SMS según se describe en el DINAC R19, pero ello puede lograrse de varias maneras:

- a) Estableciendo criterios dentro de los reglamentos de explotación específicos para aviación general existentes;
- b) Publicando requisitos dentro del marco normativo en un instrumento jurídico distinto de los reglamentos de explotación específicos que definen los criterios; o
- c) Haciendo referencia dentro del marco normativo a un código de práctica industrial del SMS que sea reconocido por la DINAC.

4.3 MARCO PARA UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

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

A continuación, se proporciona un resumen de alto nivel de cada uno de los componentes, y para cada elemento.

4.3.1 Política y objetivos de la seguridad operacional

La política de seguridad operacional debe ser desarrollada y apoyada por la administración superior y llevar la firma de un ejecutivo responsable. Establece el compromiso de la administración superior con respecto a la seguridad operacional, sus objetivos y la estructura institucional de apoyo.

Teniendo debidamente en cuenta su política de seguridad operacional, el proveedor de servicios definirá sus objetivos en materia de seguridad operacional. Los objetivos de seguridad operacional:

- a) Constituirán la base para la verificación y la medición del rendimiento en materia de seguridad operacional;
- b) Reflejarán el compromiso del proveedor de servicios de mantener y mejorar continuamente la eficacia general del SMS;
- c) Se comunicarán a toda la organización; y
- d) Se examinarán periódicamente para asegurarse de que sigan siendo pertinentes y apropiados para el proveedor de servicios.

4.3.1.1 Compromiso de la dirección

4.3.1.1.1 La política de seguridad operacional:

- a) Reflejará el compromiso de la organización respecto de la seguridad operacional, incluida la promoción de una cultura positiva;
- b) Incluirá una declaración clara acerca de la provisión de los recursos necesarios para su puesta en práctica;
- c) Incluirá procedimientos de presentación de informes en materia de seguridad operacional;
- d) Indicará claramente qué tipos de comportamientos son inaceptables respecto a las actividades de aviación del proveedor de servicios e incluirá las circunstancias en las que no se podrían aplicar medidas disciplinarias;
- e) Estará firmada por el ejecutivo responsable de la organización;
- f) Se comunicará, apoyándola ostensiblemente, a toda la organización; y
- g) Se examinará periódicamente para asegurarse de que siga siendo pertinente y apropiada para el proveedor de servicios.

Modelo de una declaración de la política de seguridad operacional

DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD OPERACIONAL

La seguridad operacional es una de nuestras funciones centrales. Estamos comprometidos a desarrollar, implementar, mantener y mejorar constantemente las estrategias y los procesos para garantizar que todas nuestras actividades de aviación se lleven a cabo a partir de una correcta asignación de recursos institucionales, orientados a alcanzar el más alto nivel de rendimiento en materia de seguridad operacional y cumplir con requisitos reglamentarios.

Todos los niveles de administración y todos los empleados son responsables de proporcionar el más alto nivel de rendimiento en materia de seguridad operacional, comenzando por el ejecutivo responsable de la organización.

Nuestro compromiso es para:

- Respalda la gestión de la seguridad operacional mediante la disposición de los recursos correspondientes que generarán una cultura institucional que fomenta prácticas seguras, alienta una notificación y comunicación eficaces de la seguridad operacional y gestiona activamente la seguridad operacional;
- Garantizar que la gestión de la seguridad operacional sea una de las responsabilidades principales de todos los gerentes y empleados;
- Definir claramente, para todo el personal, gerentes y empleados por igual, sus responsabilidades para lograr el rendimiento en materia de seguridad operacional de la organización y el rendimiento de nuestro sistema de gestión de la seguridad operacional;
- Establecer y operar los procesos de identificación de peligros y gestión de riesgos, incluido un sistema de notificación de peligros, para eliminar o mitigar los riesgos de seguridad operacional de las consecuencias de peligros que se generen de nuestras operaciones o actividades, para alcanzar una mejora continua en nuestro rendimiento en materia de seguridad operacional;
- Garantizar que no se tome ninguna medida en contra de ningún empleado que divulgue una preocupación de seguridad operacional mediante el sistema de notificación de peligros, a menos que dicha divulgación indique, más allá de cualquier duda razonable, una negligencia grave o una despreocupación deliberada o consciente de los reglamentos y procedimientos;
- Cumplir con y, cuando sea posible, superar los requisitos y las normas reglamentarias y legislativas;
- Garantizar que estén disponibles suficientes recursos humanos cualificados y capacitados para implementar las estrategias y los procesos de seguridad operacional;
- Garantizar que todo el personal disponga de información y capacitación adecuadas y correspondientes de la seguridad operacional de la aviación, sea competente en asuntos de seguridad operacional y tengan asignadas solo tareas proporcionales a sus habilidades;
- Establecer y medir nuestro rendimiento en materia de seguridad operacional en contraste con indicadores de rendimiento en materia de seguridad operacional realistas y objetivos de rendimiento en materia de seguridad operacional;
- Mejorar continuamente el rendimiento en materia de seguridad operacional mediante un control y una medición continuos, revisión y ajuste regulares de los objetivos y las metas de seguridad operacional; y
- Garantizar que se implementen los sistemas y servicios suministrados de forma externa para respaldar nuestras operaciones y que cumplan nuestras normas de rendimiento en materia de seguridad operacional.

(Firmado)

Ejecutivo Responsable

- 4.3.1.2** Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional.
- 4.3.1.2.1** El proveedor de servicios:
- a) Identificará al ejecutivo responsable que, independientemente de sus otras funciones, tenga la obligación de rendir cuentas, en nombre de la organización, respecto de la implementación y el mantenimiento de un SMS eficaz;
 - b) Definirá claramente las líneas de obligación de rendición de cuentas sobre la seguridad operacional para toda la organización, incluida la obligación directa de rendición de cuentas sobre seguridad operacional al ejecutivo responsable de la organización;
 - c) Determinará las responsabilidades de rendición de cuentas de todos los miembros de la organización, independientemente de sus otras funciones, así como las de los funcionarios, en relación con el rendimiento en materia de seguridad operacional de la organización;
 - d) Documentará y comunicará la información relativa a la obligación de rendición de cuentas, las responsabilidades y las atribuciones de seguridad operacional de toda la organización; y
 - e) Definirá los niveles de gestión con atribuciones para tomar decisiones sobre la tolerabilidad de riesgos de seguridad operacional.
- 4.3.1.3** Designación del personal clave de seguridad operacional.
- 4.3.1.3.1** El gerente de seguridad operacional asesora al ejecutivo responsable y a los gerentes de línea respecto de asuntos de gestión de la seguridad operacional, y es responsable de coordinar y comunicar los problemas de seguridad operacional dentro de la organización, así como con los miembros externos de la comunidad aeronáutica.
- Nota.- Dependiendo de la dimensión del proveedor de servicios y la complejidad de sus productos o servicios de aviación, las responsabilidades de la implementación y el mantenimiento del SMS pueden asignarse a una o más personas que desempeñen la función de gerente de seguridad operacional, como su única función o en combinación con otras obligaciones, siempre que esto no ocasione conflictos de intereses.*
- 4.3.1.4** Coordinación de la planificación de respuestas ante emergencias.
- 4.3.1.4.1** El proveedor de servicios garantizará que el plan de respuesta ante emergencias se coordine en forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que deba interactuar al suministrar sus servicios.
- 4.3.1.4.2** El objetivo general es la continuación de las operaciones en condiciones de seguridad y el retorno a las operaciones normales tan pronto como sea posible. Esto deberá 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. Se incluye también el período de tiempo necesario para restablecer las operaciones “normales” después de una emergencia. La mayoría de estos casos exigirá acciones coordinadas entre diferentes organizaciones, posiblemente con otros proveedores de servicios y con otras organizaciones externas como las de servicios de emergencia no relacionados con la aviación.
- 4.3.1.5** Documentación SMS.
- 4.3.1.5.1** La documentación del SMS debería incluir un “manual SMS”, de alto nivel, en el que se describa las políticas, procesos y procedimientos SMS del proveedor de servicios a efectos de facilitar la administración, comunicación y mantenimientos internos del SMS por parte de la organización. Ello debería contribuir a que el

personal comprendiera la forma en que funciona el SMS de la organización y cómo se cumplirán las políticas y objetivos de seguridad operacional.

4.3.1.5.1.1 El manual SMS también sirve de mecanismo principal de comunicación de seguridad operacional entre el proveedor de servicios y los interesados principales en la seguridad operacional (p. ej., la DINAC para fines de aceptación, evaluación y subsiguiente observación del SMS). El manual SMS puede ser un documento independiente, o puede estar integrado en otros documentos institucionales mantenidos por el proveedor de servicios. Cuando los detalles de los procesos SMS de la organización ya están abarcados en los documentos existentes, alcanza con hacer referencia apropiada a tales documentos. Este documento SMS debe mantenerse actualizado. Antes de introducir enmiendas importantes en el manual SMS debe contar con la aprobación de la DINAC, dado que es un documento controlado.

4.3.1.5.1.2 El manual SMS abarca una descripción detallada de las políticas, procesos y procedimientos del proveedor de servicios incluyendo:

- a) Política y los objetivos de seguridad operacional;
- b) Referencias a cualesquiera requisitos SMS normativos aplicables;
- c) Una descripción del sistema;
- d) Obligaciones de rendición de cuentas en materia de seguridad operacional y personal clave de seguridad operacional;
- e) Procesos y procedimientos de sistemas de notificación voluntaria y obligatoria de seguridad operacional;
- f) Procesos y procedimientos de identificación de peligros y evaluación de riesgos de seguridad operacional;
- g) Procedimientos de investigación de seguridad operacional;
- h) Procedimientos para establecer y observar los indicadores de rendimiento en materia de seguridad operacional;
- i) Procesos y procedimientos de instrucción en SMS y comunicaciones;
- j) Procesos y procedimientos de comunicación de seguridad operacional;
- k) Procedimientos de auditoría interna;
- l) Gestión de procedimientos de cambio;
- m) Procedimientos de gestión de la documentación SMS; y
- n) Cuando corresponda, coordinación de la planificación de respuestas ante emergencias.

4.3.1.5.2 La documentación del SMS también comprende la recopilación y mantenimiento de registros operacionales que apoyen la existencia y el funcionamiento continuo del sistema. Los registros operacionales son las salidas de los procesos y procedimientos SMS tales como la gestión de riesgos y las actividades de aseguramiento de la seguridad operacional. Los registros operacionales del SMS deben almacenarse y mantenerse con arreglo a períodos de retención vigentes. Entre los registros operacionales SMS típicos deberían figurar los siguientes:

- a) Registros de informes de peligros e informes sobre peligros/seguridad operacional;
- b) SPI y gráficos relacionados;
- c) Registro de evaluaciones de seguridad operacional completadas;
- d) Registros de revisión o auditoría internas del SMS;

- e) Registros de auditoría interna;
- f) Registros de instrucción en SMS/seguridad operacional;
- g) Actas de reuniones del comité del SMS/ seguridad operacional;
- h) Plan de implementación del SMS (durante el período de implementación inicial); y
- i) Análisis de brechas para respaldar el plan de implementación.

4.3.2 **Gestión de riesgos de seguridad operacional**

Los proveedores de servicios deben asegurar que están gestionando sus riesgos de seguridad operacional. Este proceso se conoce como gestión de riesgos de seguridad operacional (SRM), y comprende la identificación de peligros, la evaluación de riesgos de seguridad operacional y la mitigación de dichos riesgos.

4.3.2.1 Identificación de peligros.

4.3.2.1.1 Existen varias fuentes para la identificación de peligros, tanto internas como externas a la organización.

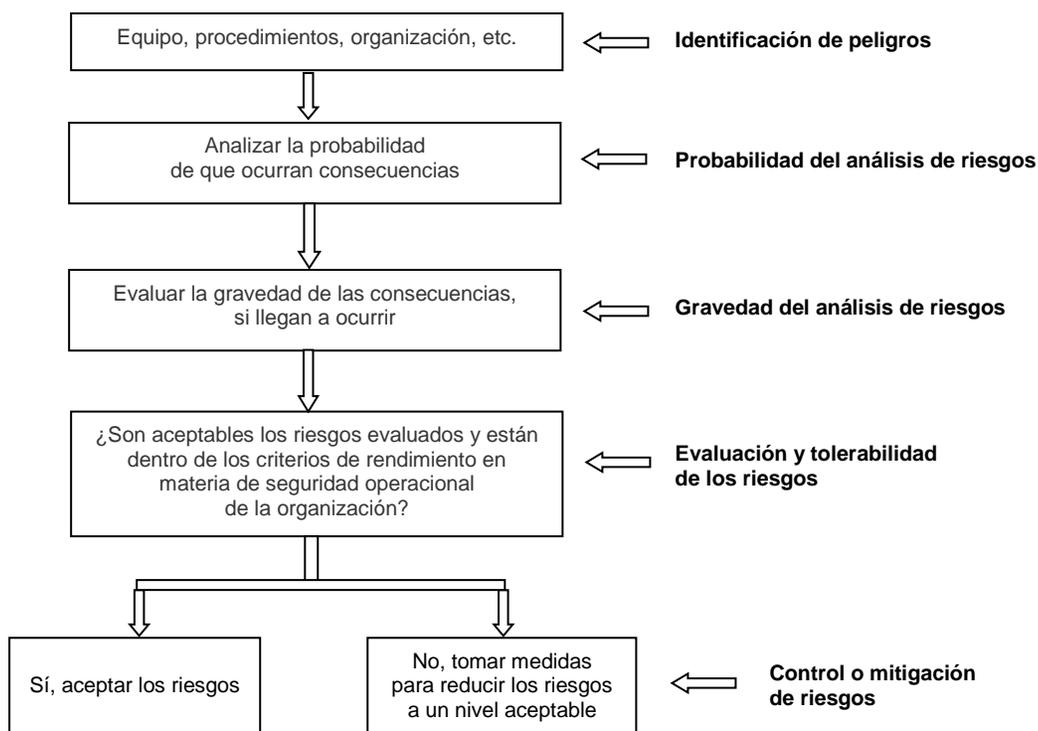
Entre algunas fuentes internas figuran:

- a) Observación normal de las operaciones; se aplican técnicas de observación para el seguimiento de las operaciones y actividades cotidianas como las auditorías de la seguridad de las operaciones en línea (LOSA).
- b) Sistemas automáticos de observación; se utilizan sistemas automáticos de registro para observar parámetros que puedan analizarse, como el análisis de datos de vuelo (FDM).
- c) Sistemas de notificación voluntaria y obligatoria de seguridad operacional; esto brinda a todos, incluyendo el personal de organizaciones externas, oportunidades para notificar a la organización peligros y otros problemas de seguridad operacional.
- d) Auditorías; pueden utilizarse para identificar peligros en la tarea o proceso que se está auditando.
- e) Comentarios procedentes de la instrucción; una instrucción interactiva (en ambos sentidos) puede facilitar la identificación de nuevos peligros por parte de los participantes.
- f) Investigaciones de la seguridad operacional del proveedor de servicios; peligros identificados en investigaciones internas de la seguridad operacional y notificaciones de seguimiento sobre accidentes/incidentes.

Entre las fuentes externas para la identificación de peligros figuran los siguientes:

- a) Informes de accidentes de aviación; informes de accidentes que pueden estar relacionados con accidentes en el mismo Estado o con un tipo similar de aeronave, región o entorno operacional.
- b) Sistemas estatales de notificación obligatoria y voluntaria de seguridad operacional; algunos Estados proporcionan resúmenes de las notificaciones de seguridad operacional recibidas de los proveedores de servicios.
- c) Auditorías estatales de vigilancia y auditorías de terceras partes; las auditorías externas pueden a veces estar en condiciones de identificar peligros que pueden haberse documentado como no identificados o captados en forma menos evidente dentro de una constatación de auditoría.

Modelo Proceso de identificación y gestión de riesgos



4.3.2.2 Evaluación y mitigación de riesgos de seguridad operacional.

4.3.2.2.1 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.

4.3.2.2.2 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). 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.

4.3.2.2.3 Probabilidad del riesgo de seguridad operacional

4.3.2.2.3.1 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) ¿Cuál es la exposición del peligro que se considera? Por ejemplo ¿durante qué porcentaje de la operación se utiliza el equipo o se realiza la actividad?

4.3.2.2.4 Gravedad del riesgo de seguridad operacional

- 4.3.2.2.4.1** Una vez completada la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional teniendo en cuenta las posibles consecuencias relacionadas con el peligro. La gravedad del riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La clasificación de la gravedad debería tener en cuenta:
- a) Muertes o lesiones graves que podrían ocurrir como resultado de:
 - 1) encontrarse en la aeronave;
 - 2) tener contacto directo con cualquier parte de la aeronave, incluyendo las que se hayan desprendido de la misma; o
 - 3) exposición directa al chorro de los reactores; y
 - b) Daños:
 - 1) daños o fallas estructurales sufridos por la aeronave que:
 - i) afecten adversamente la resistencia estructural, performance o características de vuelo de la aeronave;
 - ii) requerirían normalmente importantes reparaciones o sustituciones del componente afectado;
 - 2) daños sufridos por el equipo de ATS o aeródromo que:
 - i) afecten adversamente la gestión de la separación de aeronaves; o
 - ii) afecten adversamente la capacidad de aterrizaje.
- 4.3.2.2.5** Tolerabilidad del riesgo de seguridad operacional
- 4.3.2.2.5.1** El índice de riesgo de seguridad operacional se crea mediante la combinación de resultados de las evaluaciones de probabilidad y gravedad. Las respectivas combinaciones de gravedad/probabilidad se presentan en la matriz de evaluación de riesgos de seguridad operacional. Dicha matriz se aplica para determinar la tolerabilidad del riesgo de seguridad operacional.
- 4.3.2.2.5.2** El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a la matriz de tolerabilidad del riesgo de seguridad operacional que describe los criterios de tolerabilidad para la organización particular.
- 4.3.2.2.6** Los riesgos de seguridad operacional son evaluados en concepto como aceptables, tolerables o intolerables. Los riesgos evaluados que están 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 o la cancelación de la operación.
- 4.3.2.2.7** 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.
- 4.3.2.2.8** Los riesgos de seguridad operacional evaluados que están 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.
- 4.3.2.2.9** Estrategias de mitigación de riesgos de seguridad operacional
- 4.3.2.2.9.1** Los riesgos de seguridad operacional deben gestionarse a un nivel aceptable mitigándolos mediante la aplicación de adecuados controles de riesgos de

seguridad operacional. Esto debe equilibrarse con respecto al tiempo, costos y dificultades de adoptar medidas para reducir o eliminar el riesgo. El nivel de riesgo de seguridad operacional puede disminuirse mediante la reducción de la gravedad de las posibles consecuencias, la probabilidad de que el suceso ocurra o la reducción de la exposición a ese riesgo de seguridad operacional.

4.3.2.2.9.2

Las mitigaciones de riesgos de seguridad operacional son medidas que resultan a menudo en cambios de los procedimientos operacionales, equipo o infraestructura. Las estrategias de mitigación de riesgo de seguridad operacional corresponden a tres categorías:

- a) **Evitar:** Se cancela o evita la operación o actividad debido a que los riesgos de seguridad operacional superan los beneficios de continuarla, eliminando así el riesgo de seguridad operacional en su totalidad.
- b) **Reducir:** Se reduce la frecuencia de la operación o actividad o se adoptan medidas para reducir la magnitud de las consecuencias del riesgo.
- c) **Separar:** Se toman medidas para aislar los efectos de las consecuencias del riesgo o se introduce defensas redundantes de protección contra los riesgos.

Una estrategia de mitigación de riesgos puede implicar o incluir múltiples enfoques. La eficacia de cada estrategia debe evaluarse antes de 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.
- 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) **Ejecutabilidad.** El grado hasta donde el cumplimiento de nuevas reglas, reglamentos o procedimientos de operación pueden supervisarse.
- e) **Duración.** El grado hasta donde la mitigación será sostenible y eficaz.
- f) **Riesgos de seguridad operacional residual.** Riesgos de seguridad operacional secundario a la implementación de la mitigación inicial y que podría necesitar medidas de control de riesgos adicionales.
- g) **Tiempo.** El tiempo requerido para implementar la alternativa de mitigación de riesgo de seguridad operacional.

Modelo Tabla de probabilidad del riesgo de seguridad operacional

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

Nota.- El nivel de detalle y complejidad de las tablas y matrices debe adaptarse a las necesidades y complejidades particulares de cada organización. También se debe tener presente que las organizaciones pueden incluir criterios tanto cualitativos como cuantitativos.

Modelo Tabla de gravedad del riesgo de seguridad operacional

Gravedad	Descripción de la gravedad	Valor
Catastrófico	- Aeronave o equipo destruidos - Varias muertes	A
Peligroso	- Gran reducción de los márgenes de seguridad operacional, estrés físico o una carga de trabajo tal que ya no se pueda confiar en que personal de operaciones realicen sus tareas con precisión o por completo - Lesiones graves - Daño importante al equipo	B
Grave	- Reducción importante de los márgenes de seguridad operacional, reducción en la capacidad del personal de operaciones 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 a las personas	C
Leve	- Interferencias - Limitaciones operacionales - Uso de procedimientos de emergencia - Incidente leve	D
Insignificante	- Pocas consecuencias	E

Modelo 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

Modelo Matriz de tolerabilidad del riesgo de seguridad operacional

Descripción del riesgo	Índice de riesgo	Medida recomendada
Región intolerable	5A, 5B, 5C, 4A, 4B, 3A	Tomar medidas inmediatas para mitigar el riesgo o suspender la actividad. Realizar la mitigación de riesgos prioritaria para garantizar que haya controles preventivos o adicionales o mejorados para reducir el índice de riesgos al rango tolerable
Región tolerable	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Puede tolerarse sobre la base de la mitigación de riesgos de seguridad operacional. Puede necesitar una decisión de gestión para aceptar el riesgo
Región aceptable	3E, 2D, 2E, 1B, 1C, 1D, 1E,	Aceptable. No se necesita una mitigación de riesgos posterior.

Modelo Tabla de identificación, análisis y evaluación de riesgos

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

4.3.3 Aseguramiento de la seguridad operacional

4.3.3.1 Observación y medición del rendimiento en materia de seguridad operacional.

4.3.3.1.1 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. Esto involucra la observación continua de sus procesos internos, así como su entorno de operación para detectar cambios o desviaciones que puedan introducir riesgos de seguridad operacional emergentes o el deterioro de los controles de riesgos existentes. Tales cambios o desviaciones pueden abordarse mediante el proceso de gestión de riesgos de seguridad operacional.

4.3.3.1.2 Las actividades del aseguramiento de seguridad operacional incluyen el desarrollo y la implementación de medidas correctivas en respuesta a los hallazgos identificados con posibles consecuencias para la seguridad operacional.

4.3.3.1.3 Para verificar el rendimiento en materia de seguridad operacional y validar la eficacia de los controles de riesgos de seguridad operacional se requiere utilizar una combinación de auditorías internas, establecimiento y observación de indicadores del rendimiento en esa materia.

4.3.3.1.4 Auditorías internas

4.3.3.1.4.1 Las auditorías internas se llevan a cabo para evaluar la eficacia del SMS e identificar áreas de posible mejora. La mayoría de los reglamentos de seguridad operacional de la aviación son controles genéricos de riesgos de seguridad operacional. Garantizar el cumplimiento de los reglamentos mediante la realización de auditorías internas es un aspecto principal del aseguramiento de la seguridad operacional.

- 4.3.3.1.4.2** Las causas y los factores contribuyentes deben investigarse y analizarse cuando se han identificado casos de no cumplimiento y otros problemas. La auditoría interna se concentra principalmente en las políticas, procesos y procedimientos que proporcionen controles de los riesgos de seguridad operacional.
- 4.3.3.1.4.3** Dichas auditorías proporcionan al ejecutivo responsable y a la administración superior información y comentarios sobre la situación de:
- a) El cumplimiento de los reglamentos;
 - b) El cumplimiento de las políticas, procesos y procedimientos;
 - c) La eficacia de los controles de riesgos de seguridad operacional;
 - d) La eficacia de las medidas correctivas; y
 - e) La eficacia del SMS.
- 4.3.3.1.4.4** La evaluación del cumplimiento y la eficacia son esenciales para el logro de un buen rendimiento en materia de seguridad operacional. El proceso de auditoría interna puede aplicarse para determinar tanto el cumplimiento como la eficacia. Las preguntas siguientes pueden plantearse para evaluar el cumplimiento y la eficacia de cada proceso o procedimiento:
- a) Determinación del cumplimiento
 - 1) ¿Existe el proceso o procedimiento requerido?
 - 2) ¿Está documentado el proceso o procedimiento (se definen entradas, actividades, interfaces y salidas)?
 - 3) ¿Satisface el proceso o procedimiento los requisitos (criterios)?
 - 4) ¿Se está aplicando el proceso o procedimiento?
 - 5) ¿Aplica sistemáticamente el proceso o procedimiento todo el personal afectado?
 - 6) ¿Se obtienen los resultados definidos?
 - 7) ¿Se ha documentado e implementado algún cambio en el proceso o procedimiento?
 - b) Evaluación de la eficacia
 - 1) ¿Comprenden los usuarios el proceso o procedimiento?
 - 2) ¿Se logra sistemáticamente el propósito del proceso o procedimiento?
 - 3) ¿Son los resultados del proceso o procedimiento los que el “cliente” pidió?
 - 4) ¿Se examina regularmente el proceso o procedimiento?
 - 5) ¿Se realiza una evaluación de riesgos de seguridad operacional cuando se han introducido cambios en el proceso o procedimiento?
 - 6) ¿Han producido las mejoras del proceso o procedimiento los beneficios esperados?
- 4.3.3.1.4.5** Las auditorías internas deben observar los progresos hacia la solución de los casos de no cumplimiento identificados previamente. Estos deben haberse abordado mediante análisis de causas y elaboración e implementación de planes de medidas correctivas y preventivas.
- 4.3.3.1.4.6** Los resultados del proceso de auditoría interna constituyen una de las diversas entradas de las funciones de la gestión de riesgos y aseguramiento de la seguridad operacional.
- 4.3.3.1.5** Observación del rendimiento en materia de seguridad operacional

- 4.3.3.1.5.1** La observación del rendimiento en materia de seguridad operacional se lleva a cabo mediante la recopilación de datos e información sobre seguridad operacional de varias fuentes disponibles en una organización. La disponibilidad de datos para apoyar, sus decisiones bien fundamentadas es uno de los aspectos más importantes del SMS.
- 4.3.3.1.5.2** El rendimiento en materia de seguridad operacional alcanzado es una indicación del desempeño de la organización y también una medida de la eficacia de su SMS. Para ello la organización debe definir:
- a) Objetivos de seguridad operacional, que deben establecerse en primer lugar para reflejar los logros estratégicos o resultados deseados relativos a las preocupaciones de seguridad operacional;
 - b) Los indicadores de rendimiento, que son parámetros tácticos relativos a los objetivos de seguridad operacional y, por consiguiente, constituyen la referencia para la recopilación de datos; y
 - c) Las metas de rendimiento, que también son parámetros tácticos utilizados para vigilar el progreso hacia el logro de los objetivos de seguridad operacional.
- 4.3.3.1.5.3** Se alcanzará un panorama más completo y realista del rendimiento en materia de seguridad operacional del proveedor de servicios si los indicadores de rendimiento abarcan un amplio espectro de indicadores. Estos deberían comprender:
- a) Sucesos de baja probabilidad/alta gravedad (accidentes e incidentes graves);
 - b) Sucesos de alta probabilidad/baja gravedad (sucesos operacionales de poca consecuencia, informes de no cumplimiento, desviaciones, etc.): y
 - c) Rendimiento del proceso (instrucción, mejoras del sistema y procesamiento de informes).
- 4.3.3.1.5.4** Los indicadores de rendimiento se basan en la observación de datos e información procedente de diversas fuentes incluyendo el sistema de notificación de seguridad operacional. Dichos indicadores deben ser específicos de cada proveedor de servicios y estar relacionados con los objetivos de seguridad operacional.
- 4.3.3.1.5.5** Una vez establecidos los indicadores el proveedor de servicios debe considerar si resulta apropiado identificar metas de rendimiento y niveles de alerta. Las metas son útiles para contribuir a mejoras de la seguridad operacional, pero, si no se implementan bien, pueden conducir a comportamientos no deseados, es decir, individuos y departamentos demasiado concentrados en alcanzar la meta y que quizás pierdan de vista lo que ésta debía lograr, en vez de una mejora del rendimiento en materia de seguridad operacional. En tales casos, podría ser más apropiado vigilar los indicadores para determinar tendencias.
- 4.3.3.1.5.6** La organización debe observar el rendimiento de los indicadores y las metas establecidos para identificar cambios anormales en el rendimiento en materia de seguridad operacional. Las metas deben ser realistas, específicas del contexto y alcanzables.
- 4.3.3.1.6** Las actividades siguientes pueden ser fuentes para respaldar la observación y la medición del rendimiento en materia de seguridad operacional:
- a) Los estudios de seguridad operacional son análisis para obtener una comprensión más profunda de los temas de seguridad operacional o comprender mejor las tendencias en materia de rendimiento. Examinan los procedimientos o procesos relacionados con una operación específica. Dichos estudios pueden involucrar el uso de listas de verificación, cuestionarios y entrevistas confidenciales e informales. Proporcionan generalmente información cualitativa que puede requerir validación mediante la recopilación de datos para determinar si se necesitan medidas correctivas.

- b) Los análisis de datos de seguridad operacional utilizan los datos de las notificaciones de seguridad operacional para revelar problemas o tendencias comunes que puedan requerir investigación posterior.
- c) Las auditorías de seguridad operacional se centran en la integridad del SMS del proveedor de servicios y en sus sistemas de respaldo.
- d) Las constataciones y recomendaciones de investigaciones de seguridad operacional pueden proporcionar información útil en la materia que puede analizarse comparando con otros datos de seguridad operacional recopilados.
- e) Los sistemas de recopilación de datos operacionales como el FDA (Flight Data Analysis) o la información radar pueden proporcionar datos útiles de sucesos y rendimiento operacional.

4.3.3.1.6.1 La observación y medición del rendimiento en materia de seguridad operacional proporciona un medio para verificar la eficacia de los controles de riesgos de seguridad operacional. Además, proporcionan una medida de la integridad y eficacia de los procesos y actividades del SMS.

4.3.3.1.7 La DINAC ha establecido procesos específicos para la aceptación de indicadores y metas de rendimiento que deberán seguirse. Por consiguiente, durante la elaboración de indicadores y metas de rendimiento, el proveedor de servicios deberá consultar a la autoridad normativa de la organización, así como toda información conexas que la DINAC haya publicado.

4.3.3.2 La gestión del cambio

4.3.3.2.1 Los cambios pueden afectar la eficacia de los controles de riesgos de seguridad operacional existentes. Además, nuevos peligros y riesgos de seguridad operacional conexos pueden introducirse involuntariamente en una operación cuando ocurren cambios. Los peligros deben identificarse y los riesgos de seguridad operacional conexos evaluarse y controlarse, según se defina en los procedimientos de identificación de riesgos o de gestión de riesgos existentes en la organización.

4.3.3.2.2 La gestión de los procesos de cambios por parte de la organización tendrá en cuenta las consideraciones siguientes:

- a) Criticidad. Determinación de cuán crítico es el cambio. El proveedor de servicios debe considerar las consecuencias para las actividades de su organización, así como para otras organizaciones y el sistema aeronáutico.
- b) Disponibilidad de expertos temáticos. Es importante que miembros clave de la comunidad aeronáutica estén involucrados en las actividades de gestión de cambios, pudiéndose incluir individuos de organizaciones externas.
- c) Disponibilidad de datos e información sobre rendimiento en materia de seguridad operacional. Determinación de los datos e información que se disponen y que pueden utilizarse para proporcionar información sobre la situación y facilitar el análisis del cambio.

4.3.3.2.3 Los pequeños cambios incrementales pueden pasar desapercibidos, pero su efecto acumulativo puede ser considerable. Los cambios, tanto grandes como pequeños pueden afectar la descripción del sistema de la organización y conducir a la necesidad de su revisión. Por consiguiente, la descripción del sistema debe revisarse periódicamente para determinar su validez continua.

4.3.3.2.4 El proveedor de servicios definirá el elemento activador del proceso de cambios formal. Los cambios que probablemente activen una gestión de cambios oficial comprenden:

- a) Introducción de nueva tecnología o equipo;

- b) Cambios en el entorno operacional;
- c) Cambios en el personal clave;
- d) Cambios significativos en los niveles de plantilla;
- e) Cambios en los requisitos normativos de seguridad operacional;
- f) Reestructuración significativa de la organización; y
- g) Cambios físicos (nueva instalación o base, cambios en la disposición general del aeródromo, etc.).

4.3.3.2.5 El proveedor de servicios deberá considerar también las consecuencias del cambio sobre el personal. Esto podría afectar la forma en que las personas afectadas aceptan el cambio. La comunicación y participación temprana normalmente mejorarán la forma en que se perciben e implementan los cambios.

4.3.3.2.6 El proceso de gestión del cambio incluirá las actividades siguientes:

- a) Comprensión y definición del cambio; esto debe incluir una descripción del cambio y las razones de su implementación;
- b) Comprensión y definición de quiénes y qué aspectos se verán afectados; estos pueden ser individuos dentro de la organización, otros departamentos o personas u organizaciones externas. También puede haber consecuencias para los equipos, sistemas y procesos. Puede ser necesario realizar un examen de la descripción del sistema y de las interfaces de las organizaciones. Este aspecto constituye una oportunidad para determinar quienes deberían estar involucrados en el cambio;
- c) Identificación de peligros relacionados con el cambio y realización de evaluaciones de riesgos de seguridad operacional; deberán identificarse los peligros directamente relacionados con el cambio;
- d) Elaboración de un plan de acción; este definirá lo que ha de hacerse, por quiénes y para cuándo. También deberá haber un plan claro que describa la forma en que se implementará el cambio y quiénes serán responsables de las medidas que se apliquen, así como la secuencia y programación de las tareas;
- e) Aprobación del cambio; esto es necesario para confirmar que el cambio puede implementarse en condiciones de seguridad. El individuo con responsabilidad y autoridad para la implementación del cambio deberá firmar el plan correspondiente; y
- f) Plan de verificación; esto es para determinar las medidas de seguimiento que sean necesarias. Se habrá de considerar la forma en que se comunicará el cambio y si se requieren actividades adicionales (como auditorías) durante o después del mismo.

4.3.3.3 Mejora continua del SMS

4.3.3.3.1 El mantenimiento y la mejora continua de la eficacia del SMS del proveedor de servicios es apoyada por las actividades de aseguramiento de la seguridad operacional que comprende la verificación y seguimiento de las medidas y los procesos de auditoría interna. El mantenimiento y la mejora continua del SMS son actividades permanentes puesto que la propia organización y su entorno operacional estarán cambiando constantemente.

4.3.3.3.2 Las auditorías internas involucran la evaluación de las actividades aeronáuticas del proveedor de servicios que puede proporcionar información útil a los procesos de toma de decisiones. La función de auditoría interna comprende la evaluación de todas las funciones de gestión de la seguridad operacional en toda la organización.

4.3.3.3.3 La eficacia del SMS no debe basarse solamente en los indicadores de rendimiento;

los proveedores de servicios deberían proponerse la implementación de varios métodos para determinar su eficacia, medir los servicios, así como los resultados de los procesos y evaluar la información recopilada con estas actividades. Tales métodos pueden incluir lo siguiente:

- a) Auditorías; comprende las auditorías internas y las auditorías realizadas por otras organizaciones.
- b) Evaluaciones; comprende las evaluaciones de la cultura de seguridad operacional y la eficacia del SMS.
- c) Observación de sucesos: vigila la repetición de sucesos de seguridad operacional incluyendo accidentes e incidentes, así como errores y situaciones de infracción de reglamentos.
- d) Estudios de seguridad operacional; incluye estudios de carácter cultural para proporcionar información útil respecto de la participación del personal en el SMS. También puede servir de indicador de la cultura de seguridad operacional de la organización.
- e) Exámenes de la gestión; examinan si la organización está alcanzando sus objetivos de seguridad operacional y constituyen una oportunidad para realizar toda la información disponible sobre rendimiento en materia de seguridad operacional a efectos de identificar tendencias generales. Esto puede realizarse como una de las funciones del comité de seguridad operacional de más alto nivel.
- f) Evaluación de los indicadores y metas de rendimiento; posiblemente como parte del examen de la gestión. Considera tendencias y, cuando se dispone de datos apropiados, pueden compararse con los datos de otros proveedores de servicios o estatales o mundiales.
- g) Aprovechamiento de las enseñanzas obtenidas; a partir de sistemas de notificación de seguridad operacional e investigaciones de seguridad operacional del proveedor de servicios. Estas deberán conducir a la implementación de mejoras de la seguridad operacional.

4.3.3.3.4 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.

4.3.4 Promoción de la seguridad operacional

La promoción de la seguridad operacional alienta una cultura de seguridad operacional positiva y contribuye a alcanzar los objetivos de seguridad operacional del proveedor de servicios mediante la combinación de competencias técnicas que mejoran continuamente con la instrucción y la educación, la comunicación eficaz y la compartición de información. La promoción de la seguridad operacional afecta el comportamiento tanto individual como institucional y complementa las políticas, procedimientos y procesos de la organización, proporcionando un sistema de valores que respalda las actividades de seguridad operacional.

4.3.4.1 Instrucción y educación

4.3.4.1.1 El programa de instrucción debe incluir instrucción inicial, OJT y periódica para mantener las competencias. La instrucción inicial en seguridad operacional debe considerar, como mínimo, los siguientes aspectos:

- a) Políticas y objetivos de seguridad operacional de la organización;
- b) Funciones de seguridad operacional institucional y responsabilidades relacionadas con la seguridad operacional;
- c) Principios básicos de la SRM;

- d) Sistemas de notificación de seguridad operacional;
- e) Procesos y procedimientos SMS de la organización; y
- f) Factores humanos.

4.3.4.1.1.1 La instrucción periódica de seguridad operacional se concentran en los cambios que se introduzcan en las políticas, procesos y procedimientos SMS y deberían destacar problemas específicos de seguridad operacional pertinentes a la organización o enseñanzas obtenidas.

4.3.4.1.2 El programa de instrucción debe adaptarse a las necesidades de la función de cada individuo dentro del SMS. Por ejemplo, el nivel y profundidad de la instrucción para los gerentes superiores involucrados en los comités de seguridad operacional de la organización serán más extensos que para el personal involucrado directamente con la entrega de productos o servicios de la organización. El personal que no participa directamente en las operaciones puede requerir solamente un panorama general de alto nivel del SMS de la organización.

4.3.4.1.3 Análisis de las necesidades de instrucción

4.3.4.1.3.1 Para la mayoría de las organizaciones, es necesario realizar evaluaciones de las necesidades de instrucción formales para asegurar que existe una clara comprensión de la operación, las funciones de seguridad operacional del personal y la instrucción disponible. Un análisis típico por lo general comprende las etapas siguientes:

- a) Todos y cada uno de los miembros del personal del proveedor de servicios se verán afectados por la implementación del SMS, pero no de la misma manera o en el mismo grado. Se deberá identificar cada grupo de personal y las formas en que interactuarán con los procesos de gestión de la seguridad operacional, sus entradas y salidas, en particular con respecto a las funciones de seguridad operacional. Esta información debería estar disponible en las descripciones de puestos o funciones. Normalmente, comenzarán a surgir grupos de individuos con necesidades de aprendizaje similares.
- b) Identificar los conocimientos y las competencias necesarias para realizar cada función de seguridad operacional que requiere cada grupo de personal.
- c) Realizar un análisis para identificar las brechas entre las habilidades y conocimientos actuales en seguridad operacional de todo el personal y los necesarios para la realización eficaz de las funciones de seguridad operacional asignadas.
- d) Identificar el enfoque más apropiado para desarrollar habilidades y conocimientos respecto de cada grupo con miras a elaborar un programa de instrucción adecuado a la participación de cada individuo o grupo en la gestión de la seguridad operacional. El programa de instrucción también debería considerar las necesidades continuas del personal en materia de conocimientos y competencias de seguridad operacional; estas necesidades se abordarán normalmente mediante un programa de instrucción periódica.

4.3.4.1.4 También es importante notificar el método apropiado para impartir la instrucción. El objetivo principal es que, al terminar la instrucción, el personal tenga competencia para ejecutar sus funciones en el marco del SMS. La consideración más importante es normalmente contar con instructores competentes, cuyo compromiso, capacidad didáctica y experiencia en gestión de la seguridad operacional tendrán consecuencias importantes en la eficacia de la instrucción impartida. El programa de instrucción en seguridad operacional también debería especificar las responsabilidades para la elaboración de contenidos y programas de instrucción, así como la gestión de registros de instrucción y competencias.

4.3.4.1.5 Debería impartirse instrucción específica para el ejecutivo responsable y los gerentes superiores que comprenda los temas siguientes:

- a) Concientización específica para nuevos ejecutivos y titulares de puestos responsables con respecto a sus obligaciones de rendición de cuentas y responsabilidades;
- b) Importancia de cumplir los requisitos de seguridad operacional nacionales e institucionales;
- c) Compromiso de la administración;
- d) Asignación de recursos;
- e) Promoción de la política de seguridad operacional y del SMS;
- f) Promoción de la cultura de seguridad operacional positiva;
- g) Comunicación eficaz de seguridad operacional entre los departamentos;
- h) Objetivos de seguridad operacional, SPT y niveles de alerta; y
- i) Política disciplinaria.

4.3.4.2 Comunicación de la seguridad operacional

4.3.4.2.1 El proveedor de servicios debe comunicar los objetivos y procedimientos del SMS de la organización a todo el personal apropiado. Debería existir una estrategia de comunicación que permita que la comunicación de seguridad operacional sea transmitida por el método más apropiado sobre la base de la función de cada individuo y su necesidad de recibir dicha información. Esto puede realizarse mediante circulares informativas, avisos, boletines, sesiones informativas o cursos de instrucción. El gerente de seguridad operacional también debería garantizar que las enseñanzas extraídas de investigaciones y casos prácticos o experiencias, tanto internos como de otras organizaciones, se distribuyen ampliamente. Por consiguiente, la comunicación de seguridad operacional se dirige a:

- a) Garantizar que el personal es plenamente consciente del SMS; esta es una buena forma de promover la política y los objetivos de seguridad operacional de la organización.
- b) Transmitir información crítica para la seguridad operacional; la información crítica para la seguridad operacional es información específica relacionada con problemas y riesgos de seguridad operacional que podrían exponer a la organización a ese tipo de riesgo. Podría tratarse de información recopilada de fuentes internas o externas como enseñanzas obtenidas o relacionadas con controles de riesgos de seguridad operacional.
- c) Crear conciencia sobre nuevos controles de riesgos de seguridad operacional y medidas correctivas; los riesgos de seguridad operacional que enfrenta el proveedor de servicios cambiarán con el tiempo, y si se trata de un nuevo riesgo de seguridad operacional que ha sido identificado o de cambios en los controles de riesgos de seguridad operacional dichos cambios deberán comunicarse al personal apropiado.
- d) Proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados; cuando se actualizan los procedimientos de seguridad operacional es importante que las personas apropiadas tengan conocimientos de dichos cambios.
- e) Promover una cultura de seguridad operacional positiva y alentar al personal a identificar y notificar peligros; la comunicación de seguridad operacional es en ambos sentidos. Es importante que todo el personal comunique los problemas de seguridad operacional a la organización a través del sistema de notificaciones de seguridad operacional.

- f) Proporcionar comentarios e información; proporcionar comentarios al personal que presenta notificaciones de seguridad operacional respecto de las medidas que se han adoptado para abordar las preocupaciones identificadas.

4.3.4.2.2 Los proveedores de servicios deberían considerar si algunos de los tipos de información de seguridad operacional indicados anteriormente deben comunicarse a organizaciones externas.

4.3.4.2.3 Los proveedores de servicios deberían evaluar la eficacia de su comunicación de seguridad operacional mediante la verificación de que el personal ha recibido y comprendido la información crítica sobre seguridad operacional que se ha distribuido. Esto puede hacerse como parte de las actividades de auditoría interna o al evaluar la eficacia del SMS.

CAPITULO 5.

RECOPIACIÓN, ANÁLISIS, PROTECCIÓN, COMPARTICIÓN E INTERCAMBIO DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

5.1 RECOPIACIÓN Y PROCESAMIENTO DE DATOS SOBRE SEGURIDAD OPERACIONAL

5.1.1 La gestión eficaz de la seguridad operacional depende mucho de la eficacia de la recopilación, análisis y capacidades de gestión general de los datos de seguridad operacional. Los datos y la información sobre seguridad operacional fiables son necesarios para identificar tendencias, tomar decisiones y evaluar el rendimiento en materia de seguridad operacional en relación con las metas y objetivos de seguridad operacional, así como para evaluar los riesgos pertinentes.

5.1.1.1 El SDCPS es un término genérico utilizado para referirse a los sistemas de procesamiento y notificación, las bases de datos y esquemas para intercambio de información sobre seguridad operacional, así como la información registrada.

5.1.1.2 Los proveedores de servicios también deben elaborar y mantener los medios para verificar su rendimiento en materia de seguridad operacional con referencia a sus indicadores y metas de rendimiento en apoyo de sus objetivos de seguridad operacional mediante los SDCPS. Estos pueden basarse en métodos reactivos y proactivos de recopilación de datos e información sobre seguridad operacional.

5.1.1.3 La orientación que figura en este capítulo es igualmente válida para los proveedores de servicios a efectos de garantizar que los datos y la información sobre seguridad operacional recopilados permitirán tomar decisiones en forma eficaz y válida.

5.1.1.4 En algunos casos, el proceso de gestión de riesgos destacará la necesidad de contar con datos de seguridad operacional adicionales para evaluar en mejor forma las consecuencias (nivel de probabilidad y gravedad) y determinar los riesgos. Los esquemas para intercambio de información y la información registrada, comprende, entre otros:

5.1.1.4.1 Investigaciones de accidentes e incidentes

Las autoridades estatales encargadas de la aplicación del SSP deben tener acceso a la base de datos de accidentes e incidentes en apoyo de sus responsabilidades funcionales en materia de seguridad operacional. La información adicional para fundamentar medidas preventivas puede figurar en los informes finales sobre accidentes e incidentes que hayan sido objeto de investigación.

5.1.1.4.2 Investigaciones de seguridad operacional por autoridades estatales o proveedores de servicios de aviación

a) Se investigan los accidentes, así como los incidentes graves, de aeronaves con una masa máxima superior a 2.250 kg que hayan ocurrido en su territorio. Estas investigaciones son realizadas por la Centro de Investigación y Prevención de Accidentes Aeronáuticos (CIPAA) en cumplimiento del DINAC R13. La realización de tales investigaciones puede delegarse en otro Estado u organización regional de investigación de accidentes e incidentes (RAIO), por acuerdo y consentimiento mutuos.

b) Se fomenta la realización de investigaciones de seguridad operacional, aparte de las obligadas por el DINAC R13, dado que producen información

de seguridad operacional útil para apoyar la mejora del rendimiento en esa materia.

- c) Existe una clara distinción entre las investigaciones de accidentes e incidentes en el marco del DINAC R13 y las investigaciones de seguridad operacional del proveedor de servicios. Las investigaciones de seguridad operacional del proveedor de servicios son realizadas por este como parte de su SMS a efectos de apoyar los procesos de identificación de peligros y evaluación de riesgos. Existen varios sucesos de seguridad operacional que caen fuera del ámbito del DINAC R13 y que podrían proporcionar una fuente valiosa de identificación de peligros o de carencias en los controles de riesgos.
- d) El objetivo principal de la investigación de seguridad operacional del proveedor de servicios es comprender lo que sucedió y cómo prevenir que ocurran en el futuro situaciones similares mediante la eliminación o mitigación de las deficiencias de seguridad operacional que se hubieren encontrado.
- e) Las investigaciones de sucesos y peligros de seguridad operacional por parte del proveedor de servicios constituyen una actividad fundamental del proceso de gestión de riesgos. Entre las ventajas de realizar una investigación de seguridad operacional figuran:
 - 1) Obtener una mejor comprensión de los hechos que condujeron al suceso;
 - 2) Identificación de factores humanos, técnicos e institucionales contribuyentes;
 - 3) Identificación de peligros y realización de evaluaciones de riesgo;
 - 4) Formulación de recomendaciones para reducir o eliminar riesgos inaceptables; y
 - 5) Identificación de enseñanzas obtenidas que deberían compartirse con los miembros apropiados de la comunidad aeronáutica.

5.1.1.4.3 Sistemas de autonotificación incluidos sistemas automáticos

Los sistemas de los proveedores de servicios para la recopilación de datos de seguridad operacional, incluyendo la captación automática de datos como el programa de acción de seguridad operacional de la aviación y los programas FDA [programa de aseguramiento de la calidad de las operaciones de vuelo (FOQA), auditorías de la seguridad operacional de las operaciones de línea (LOSA) y el estudio de la seguridad de las operaciones normales (NOSS)], constituyen ejemplos de sistemas que captan datos de seguridad operacional mediante observaciones directas de las tripulaciones de vuelo o controladores de tránsito aéreo, respectivamente.

5.1.2 Los sistemas de notificación obligatoria de seguridad operacional sirven para la captación de toda la información valiosa sobre un suceso, incluyendo lo que sucedió, dónde y cuándo y cuál es el destinatario de la notificación. Además, deberían poder captar algunos peligros específicos que se sabe contribuyen a accidentes y cuya oportuna identificación y comunicación se considera valiosa (p. ej., condiciones meteorológicas rutinarias, actividad volcánica, etc.).

5.1.2.1 Independientemente del alcance de los sistemas de notificación obligatoria, se garantiza que todas las notificaciones recopiladas con carácter obligatorio estarán protegidas.

5.1.2.2 Los sistemas de notificación obligatoria de sucesos tienden a recopilar más información de carácter técnico (p. ej., fallas de equipo) que aspectos de actuación humana.

5.1.2.3

En la tabla se detalla las notificaciones obligatorias a realizar por parte de las áreas de la DINAC y proveedores de servicios de acuerdo a los Documentos OACI y Reglamentos DINAC R's que le afectan.

Sistema de notificación obligatoria	Referencia	Organismos afectados
Notificación de investigaciones de accidentes e incidentes de aviación	DINAC R13 – Investigación de accidentes e incidentes de aviación	DINAC
Notificación de incidentes de tránsito aéreo	DINAC R4444 – Gestión del tránsito aéreo	DINAC Proveedor de servicios
Notificación de accidentes e incidentes de mercancías peligrosas	DINAC R175 – Transporte sin riesgo de mercancías peligrosas por vía aérea Doc. 9284, Instrucciones Técnicas para el transporte sin riesgos de mercancías peligrosas por vía aérea	DINAC Proveedor de servicios
Notificación de dificultades en servicio	Doc. 9760, DINAC R43, DINAC R91, DINAC R145 – Aeronavegabilidad	DINAC
Notificación de incidentes de tránsito aéreo	Doc. 9426, Manual de planificación de servicios de tránsito aéreo, Parte 2	Proveedor de servicios
Notificación de choques con fauna silvestre/aves	Doc. 9332, Manual sobre el sistema de información de la OACI de los choques con aves (IBIS)	Proveedor de servicios
	Anexo 14 – Aeródromos, Volumen I – Diseño y operaciones de aeródromos	DINAC Proveedor de servicios
	Doc. 9137, Manual de servicios de aeropuertos, Parte 3 – Control y reducción del peligro que representa la fauna silvestre	DINAC Proveedor de servicios
Notificación de emisiones láser	Doc. 9815, Manual sobre emisores láser y seguridad de vuelo	DINAC
Notificación de casos de fatiga	DINAC R121 – Operación de aeronaves, Parte I – Transporte aéreo comercial internacional – Aviones	Proveedor de servicios
	Doc. 9966, Manual para la supervisión de los enfoques de gestión de la fatiga	Proveedor de servicios
Notificación de seguridad operacional en el aeródromo	Doc. 9981, Procedimientos para los servicios de navegación aérea (PANS) – Aeródromos	Proveedor de servicios
Sistemas de aeronaves pilotadas a distancia (RPAS)	Doc. 10019, Manual sobre sistemas de aeronaves pilotadas a distancia (RPAS)	Proveedor de servicios
Sucesos de incapacitación durante el vuelo y constataciones de evaluaciones médicas	DINAC R67 – Licencias al personal	DINAC

- 5.1.3** El sistema de notificación voluntaria va más allá de la notificación típica de incidentes. Los informes voluntarios tienden a destacar condiciones latentes, como procedimientos o reglamentos de seguridad inapropiados, errores humanos, etc. La notificación voluntaria constituye una forma de identificar peligros.
- 5.1.3.1** Se garantiza la protección a los datos de seguridad operacional captados por los sistemas de notificación voluntaria y fuentes conexas, así como a la información sobre seguridad operacional obtenida de los mismos. La aplicación apropiada de la protección asegurará la continua disponibilidad de datos e información sobre seguridad operacional.
- 5.1.3.2** Los sistemas de notificación voluntaria de seguridad operacional sirven para recopilar datos e información sobre seguridad operacional no captados por el sistema de notificación obligatoria de seguridad operacional.
- 5.1.4** Esto implica mucho más que el mero acceso a la visualización de los datos con fines de vigilar el rendimiento en materia de seguridad operacional de los proveedores de servicios. Además, la implementación de sistemas de notificación y bases de datos para la recopilación de datos e información sobre seguridad operacional no es suficiente para asegurar la disponibilidad de dichos datos a efectos de permitir su análisis. Es necesario elaborar leyes, reglamentos, procesos y procedimientos para garantizar que se obtienen, notifican y recopilan los datos e información sobre seguridad operacional a efectos de ingresarlos en el SDCPS.
- 5.1.4.1** Esto normalmente requiere individuos con sólidas habilidades en tecnología de la información, así como conocimiento de requisitos, normalización, recopilación y almacenamiento de datos además de la capacidad para entender posibles cuestiones que estén sujetas a análisis. Además, cada SDCPS debe tener un custodio designado para aplicar la protección de los datos e información.
- 5.1.5** Las taxonomías y definiciones comunes establecen un lenguaje estándar, mejorando la calidad de la información y la comunicación. Es conveniente categorizar los datos de seguridad operacional idealmente mediante taxonomías y definiciones de apoyo de modo que puedan captarse y almacenarse usando términos significativos. La capacidad de la comunidad de aviación para concentrarse en problemas de seguridad operacional mejora considerablemente si se comparte un lenguaje común. Estas clasificaciones permiten la realización de análisis y facilitan la compartición y el intercambio de información. Algunos ejemplos de taxonomías son los siguientes:
- a) Modelo de aeronave: la organización puede construir una base de datos con todos los modelos certificados para operar.
 - b) Aeropuerto: la organización puede utilizar los códigos de la OACI para identificar los aeropuertos.
 - c) Tipo de suceso: la organización puede utilizar taxonomías elaboradas por la OACI y otras organizaciones internacionales para clasificar los sucesos.
- 5.1.5.1** Existen varias taxonomías aeronáuticas comunes en la industria. Algunos ejemplos son:
- a) ADREP: taxonomía de categorías de sucesos que integra el sistema de notificación de accidentes de incidentes de la OACI. Constituye una recopilación de atributos y valores conexos que permiten realizar análisis de tendencias de seguridad operacional en esas categorías.
 - b) Equipo especial sobre indicadores del rendimiento en materia de seguridad operacional (SPI-TF): encargado de elaborar métricas armonizadas mundialmente para los SPI de los proveedores de servicios como parte de sus SMS, a efectos de asegurar la uniformidad en la recopilación de información y comparación de resultados de análisis.

5.1.5.2 Ejemplo de taxonomía típica

Tipo de operación	Actividad/ infraestructura/sistema	Valor
Aeródromo, proveedor de servicios de navegación aérea, explotador de servicios aéreos, organismo de mantenimiento, organización de diseño y fabricación	Reglamentador	Legislación o reglamentos ausentes, deficientes o ineficaces
		Capacidad de investigación de accidentes ausente o ineficaz
		Capacidad de vigilancia inadecuada
	Administración	Compromiso de la administración limitado o ausente – la administración no muestra apoyo a la actividad
		Descripción ausente o incompleta de funciones, obligaciones de rendir cuentas y responsabilidades
		Disponibilidad de recursos o planificación, incluso personal, limitada o ausente
		Ausencia o ineficacia de políticas
		Procedimientos, incluso instrucciones, incorrectos o incompletos
		Ausencia o deficiencia de relaciones entre administración y personal
		Estructura de organización ausente o ineficiente
		Deficiente cultura de seguridad operacional en la organización
		Ausencia o ineficiencia de procedimientos de auditoría
		Ausencia o limitación de la asignación de recursos

5.1.5.3 Las taxonomías sobre peligros son especialmente importantes. A menudo la identificación de un peligro es la primera etapa en el proceso de gestión de riesgos. Comenzar con un lenguaje reconocido en común hace que los datos de seguridad tengan más significado, sean más fáciles de clasificar y de procesamiento más sencillo. La estructura de una taxonomía de peligros puede comprender un componente genérico y uno específico.

5.1.5.4 El componente genérico permite a los usuarios captar el carácter de un peligro con miras a ayudar a su identificación, análisis y codificación. Algunos ejemplos de taxonomía de peligros se podrían clasificar los mismos en familias de tipos (ambientales, técnicos, institucionales y humanos).

5.1.5.5 El componente específico añade precisión a la definición y contexto del peligro. Esto permite realizar un procesamiento más detallado de la gestión de riesgos.

5.2 ANÁLISIS DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

5.2.1 El análisis de la seguridad operacional es el proceso de aplicar técnicas estadísticas o analíticas de otro tipo para verificar, examinar, describir, transformar, evaluar y visualizar los datos y la información sobre seguridad operacional a efectos de descubrir información útil, sugerir conclusiones y apoyar la toma de decisiones basada en datos. Los análisis ayudan a las organizaciones a generar información sobre seguridad operacional viable en forma de estadísticas, gráficos y presentaciones. El resultado de un análisis de seguridad operacional presenta la situación en esa materia en una forma que permita la toma de decisiones de seguridad operacional basadas en datos.

5.2.1.1 Uno de los objetivos del análisis de datos e información de seguridad operacional a nivel estatal es la identificación de peligros sistémicos e intersectoriales que de otra manera podrían no ser identificados por los procesos de análisis de datos de seguridad operacional de los proveedores de servicios.

5.2.1.2 Cabe señalar que las competencias requeridas para realizar análisis de la seguridad operacional efectivos pueden estar fuera del alcance de los inspectores

de seguridad operacional. Se deberían considerar cuáles son las cualificaciones necesarias para analizar la información de seguridad operacional y decidir si esta función, con instrucción apropiada, debería ser una extensión del puesto de trabajo actual o si sería más eficaz establecer un nuevo puesto, externalizar la función o aplicar una combinación de esos enfoques.

5.2.1.3 Para que sea eficaz, el análisis de la seguridad operacional debería integrarse con las herramientas, políticas y procesos básicos existentes en la organización. Una vez integrado, el desarrollo continuo el análisis en materia de seguridad operacional debería ser fluido y formar parte de las prácticas normales de la organización.

5.2.1.4 El uso de herramientas apropiadas para el análisis de los datos y la información sobre seguridad operacional proporciona una comprensión más precisa de la situación general mediante el examen de los datos en formas que revelan las relaciones, conexiones y tendencias existentes en la misma.

5.2.1.5 Es conveniente poseer una buena gama de fuentes de información apropiadas en sus análisis de seguridad operacional, y no solo de “datos de seguridad operacional”. Ejemplos de fuentes de información útiles al conjunto de datos son: condiciones meteorológicas, terreno, tránsito, geografía, etc. El acceso y la explotación de una gama más amplia de fuentes de datos permitirán asegurar que los analistas y responsables de tomar decisiones de seguridad operacional son conscientes del contexto más amplio.

5.2.2 Análisis predictivo

5.2.2.1 Comprende el análisis de probabilidad que extrae información a partir de datos históricos y actuales a efectos de predecir tendencias y patrones de comportamiento. Los patrones encontrados en los datos contribuyen a identificar riesgos emergentes y oportunidades. A menudo, el suceso de interés desconocido se encuentra en el futuro, pero el análisis predictivo puede aplicarse a cualquier tipo de elemento desconocido en el pasado, presente o futuro. El aspecto central del análisis predictivo se basa en captar relaciones entre variables de sucesos pasados y explotadas para predecir el resultado desconocido. Algunos sistemas permiten a los usuarios modelar escenarios diferentes de riesgos u oportunidades con diferentes resultados. Esto permite a los responsables de tomar decisiones evaluar las que puedan adoptar teniendo en cuenta las circunstancias desconocidas diferentes y evaluar la forma en que pueden asignar eficazmente los recursos limitados a sectores donde existen los mayores riesgos o las mejores oportunidades.

5.2.2.2 Los análisis de la seguridad operacional ayudan a:

- a)** Identificar las causas y los factores contribuyentes relacionados con peligros y elementos que afectan negativamente la mejora continua de la seguridad operacional de la aviación;
- b)** Examinar áreas que puedan mejorar y aumentar la eficacia de los controles de seguridad operacional; y
- c)** Apoyar la observación continua del rendimiento y tendencias en materia de seguridad operacional.

5.2.3 Notificación de los resultados de los análisis

5.2.3.1 Los resultados de los análisis de datos de seguridad operacional pueden destacar áreas de alto riesgo y ayudar a los encargados de tomar decisiones y a los administradores a:

- a)** Adoptar medidas correctivas inmediatas;
- b)** Implementar supervisión de la seguridad operacional basada en riesgos;
- c)** Definir o refinar políticas de seguridad operacional u objetivos en la materia;

- d) Definir o refinar los SPI;
- e) Definir o refinar las SPT;
- f) Establecer activadores de SPI;
- g) Promover la seguridad operacional; y
- h) Realizar ulteriores evaluaciones de riesgos de seguridad operacional.

5.2.3.2 Los resultados de los análisis de seguridad operacional deberían ponerse a disposición de todas las partes interesadas en la seguridad operacional de la aviación en la forma en que puedan comprenderse fácilmente. Los resultados deberían presentarse teniendo presente a quienes están dirigidos, como los responsables de tomar decisiones institucionales, proveedores de servicios internos y externos y otros Estados. Los resultados de los análisis de seguridad operacional pueden presentarse en varias formas, entre ellas las siguientes:

- a) Alertas de seguridad operacional inminentes: para transmitir los peligros de seguridad operacional con posibles resultados que podrían resultar catastróficos y que requieren medidas inmediatas.
- b) Informes de análisis de seguridad operacional: normalmente en ellos se presenta información cuantitativa y cualitativa con una clara descripción del grado y fuente de las incertidumbres involucradas en las constataciones de los análisis. Estos informes también pueden incluir recomendaciones de seguridad operacional pertinentes.
- c) Conferencias sobre seguridad operacional: para que puedan compartir información sobre seguridad operacional y resultados de análisis de seguridad operacional que puedan promover iniciativas de colaboración.

5.2.3.3 Resulta útil traducir las recomendaciones en planes de acción, decisiones y prioridades que los responsables de tomar decisiones en la organización deben considerar y, si es posible, señalar quiénes deben hacer qué con respecto a los resultados de los análisis y cuándo.

5.3 PROTECCIÓN DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

5.3.1 Los principios relativos a la protección de los datos y la información de seguridad operacional, así como de sus fuentes, proporcionan más claridad y transparencia, así como una igualdad de condiciones, con miras a facilitar el intercambio de datos e información sobre seguridad operacional entre los proveedores de servicios y otros Estados.

5.3.1.1 La protección se aplica a los datos de seguridad operacional captados por los sistemas de notificación voluntaria de seguridad operacional y fuentes conexas, así como a la información sobre seguridad operacional obtenida de los mismos. Las fuentes de los datos y la información sobre seguridad operacional pueden ser individuos u organizaciones.

5.3.2 Esto puede aplicarse también a los sistemas de notificación obligatoria de seguridad operacional cuando corresponda. Los sistemas de notificación de seguridad operacional eficaces contribuyen a asegurar que las personas están, y permanecen, dispuestas a notificar sus errores y experiencias, de modo que el Estado y los proveedores de servicios tengan acceso a los datos e información pertinentes necesarios para abordar deficiencias y peligros de seguridad operacional existentes y potenciales. Esta garantía se proporciona mediante la creación de un entorno en el que las personas pueden confiar en que los datos y la información sobre seguridad operacional se utilizarán exclusivamente para mantener y mejorar la misma, a menos que se aplique uno de los principios de excepción.

- 5.3.3** Es importante que tanto los individuos como las organizaciones estén protegidos, así como los datos e información sobre seguridad operacional que estos notifican. Los individuos y las organizaciones están protegidos por:
- a) Seguridades de que no serán objeto de sanciones sobre la base de sus notificaciones; y
 - b) Limitación del uso de los datos e información sobre seguridad operacional notificados a fines de mantener o mejorar la seguridad operacional.
- 5.3.3.1** Estas protecciones son válidas a menos que sea aplicable uno de los principios de excepción.
- 5.3.4** La DINAC y los proveedores de servicios pueden adoptar medidas preventivas, correctivas o de rectificación que sean necesarias, sobre la base de los datos e información sobre seguridad operacional notificados con el fin de mantener o mejorar la seguridad operacional, es decir, permitir que se adopten medidas apropiadas para:
- a) Protegerse contra la posibilidad de daño o lesiones inmediatas como resultado de un riesgo de seguridad operacional hasta que dicho riesgo pueda identificarse y mitigarse;
 - b) Asegurar que se adoptan medidas apropiadas para minimizar la probabilidad de que dicho riesgo pueda ocurrir nuevamente en el futuro;
 - c) Prevenir la exposición a un riesgo de seguridad operacional no mitigado; o
 - d) Asegurar la integridad del propio sistema de notificación y del sistema más amplio del que forma parte.
- 5.3.4.1** Las medidas de carácter preventivo, correctivo o de rectificación se dirigen a abordar circunstancias o condiciones que presenten riesgos inaceptables para la seguridad operacional de la aviación.
- 5.3.4.2** Las *medidas preventivas* son aquellas adoptadas para prevenir que ocurran o vuelvan a ocurrir sucesos o peligros que planteen riesgos para la seguridad operacional.
- 5.3.4.3** Las *medidas correctivas* son aquellas adoptadas para abordar carencias o deficiencias particulares relacionadas con la seguridad operacional, como el caso en que un titular de autorización no pueda demostrar el cumplimiento de las normas aplicables de seguridad operacional o competencia. Las medidas correctivas pueden ser necesarias para hacer que el titular de una autorización cumpla dichas normas.
- 5.3.4.4** Las *medidas de rectificación* son aquellas adoptadas para abordar las causas subyacentes de carencias o deficiencias particulares relacionadas con la seguridad operacional, como en la instrucción. Las medidas de rectificación también pueden involucrar la restricción, limitación, suspensión o revocación de los privilegios de un titular de autorización, certificado o licencia que no continúe satisfaciendo las cualificaciones necesarias para ejercer dichos privilegios.
- 5.3.4.5** Aunque pueden especificarse para uno u otro fin, dichas medidas pueden aplicarse a más de un propósito. Por ejemplo, el área reguladora o proveedor de servicios puede adoptar medidas que exijan que el titular de una licencia o certificado reciba instrucción adicional y que se abstenga de ejercer los privilegios de dicha licencia o certificado hasta haber completado satisfactoriamente dicha instrucción. El regulador también puede adoptar medidas para revocar, retirar o suspender determinados privilegios del certificado de una organización. Tales medidas, si bien son de rectificación porque abordan las causas subyacentes de un problema de seguridad operacional, pueden considerarse también como correctivas debido a que tratan una deficiencia particular.

- 5.3.5** Alentar a las personas a que notifiquen datos o información sobre seguridad operacional pertinentes requiere que las fuentes de dichas notificaciones estén protegidas respecto de medidas adoptadas con arreglo al DINAC R19, así como respecto a acciones tomadas en su entorno laboral.
- 5.3.5.1** La seguridad operacional de la aviación es una responsabilidad compartida a la cual todas las partes interesadas deberían contribuir, entre otras cosas, mediante el suministro de datos e información pertinentes a través de notificaciones de seguridad operacional.
- 5.3.6** Los principios de protección y excepción que se aplican a los datos de seguridad operacional, información sobre seguridad operacional y fuentes conexas deberían ser implementados por la DINAC y los proveedores de servicios por igual. Para asegurar el logro de este objetivo, se espera que se adopten leyes, reglamentos y políticas nacionales pertinentes para asegurar que se apliquen las disposiciones respectivas.
- 5.3.7** Las autoridades competentes podrían incluir a las autoridades judiciales, autoridades normativas u otras partes con responsabilidades en la aviación designadas con arreglo a las leyes nacionales y otros requisitos ejecutables. En cada caso particular, la tarea de la autoridad competente será decidir si se aplica un principio de excepción en particular.
- 5.3.7.1** La designación permanente de la oficina y jurisdicción de la autoridad competente (p. ej., autoridades judiciales para asuntos que involucren litigios, la CAA para medidas de reglamentación) puede considerarse para facilitar la rápida toma de decisiones. Una designación permanente también proporcionará la certeza de que la autoridad competente cuenta con atribuciones y experiencia para tratar estos asuntos. Además, resulta crítico que la autoridad competente cuente con reglas y procedimientos que rijan el proceso de toma de decisiones.
- 5.4** **COMPARTICIÓN E INTERCAMBIO DE INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL**
- 5.4.1** Teniendo en cuenta que uno de los principales objetivos de compartir e intercambiar información sobre seguridad operacional es garantizar una respuesta sistemática, basada en hechos y transparente a las preocupaciones de seguridad operacional a nivel estatal y mundial, en el proceso de compartir e intercambiar dicha información, la DINAC actuará con arreglo a los principios siguientes:
- a)** Cumplimiento del Convenio sobre Aviación Civil Internacional (Convenio de Chicago), sus Anexos y otras obligaciones multilaterales y bilaterales de los Estados;
 - b)** La compartición e intercambio de información sobre seguridad operacional no conducirá a una violación por parte de las autoridades estatales pertinentes de las leyes nacionales relativas a la protección de dicha información, entre ellas las leyes y reglamentos nacionales sobre acceso a la información pública, datos personales, así como sobre violación de los derechos de individuos y entidades jurídicas;
 - c)** La información sobre seguridad operacional compartida e intercambiada no debería utilizarse en una forma que afecte adversamente al propio Estado, sus líneas aéreas, sus funcionarios públicos y sus ciudadanos, así como para otros fines inapropiados, incluyendo los fines de lucro;
 - d)** El único propósito de proteger la información sobre seguridad operacional respecto del uso inapropiado es garantizar su continua disponibilidad de modo que puedan adoptarse medidas preventivas adecuadas y oportunas y mejorar la seguridad operacional de la aviación; y
 - e)** La compartición e intercambio de información sobre seguridad operacional debería ajustarse a los principios de protección que figura en el DINAC R19.

- 5.4.1.1** El marco jurídico para compartir e intercambiar información puede basarse en acuerdos bilaterales entre Estados, por ejemplo, en sus acuerdos sobre transporte aéreo (servicios aéreos). Para facilitar la compartición e intercambio de información, los Estados también pueden acordar que dichos arreglos bilaterales se apliquen con carácter provisional, si corresponde, pendientes de su ratificación y entrada en vigor.
- 5.4.2** Es pertinente promover y facilitar el establecimiento de redes para compartir e intercambiar información sobre seguridad operacional entre los usuarios del sistema aeronáutico. La compartición y el intercambio de información sobre seguridad operacional es fundamental para garantizar una respuesta sistemática, basada en hechos y consecuente a las preocupaciones de seguridad operacional a nivel estatal y mundial.
- 5.5** **PRINCIPIOS PARA LA PROTECCIÓN DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL Y LAS FUENTES CONEXAS**
- 5.5.1** **Principios generales**
- 5.5.1.1** El propósito básico de brindar protección es asegurar la continua disponibilidad de los datos y la información sobre seguridad operacional alentando a individuos y organizaciones a que identifiquen, notifiquen, analicen y corrijan las deficiencias que hubiere. Esto exige que todos los involucrados conozcan por adelantado las reglas y procesos que rigen dicha protección. Esas reglas y procesos deberían formalizarse y no estar sujetos a aplicaciones arbitrarias si se quiere que sirvan de fundamento de un sistema basado en la confianza.
- 5.5.1.1.1** El objetivo puede ser evidente a partir del tipo de datos e información que han de protegerse. En muchos casos, la protección tiene por objeto prevenir que se utilicen datos e información sobre seguridad operacional contra el individuo o la organización que notificó dichos datos o información. En otros casos, puede ser importante proteger los datos o la información sobre seguridad operacional respecto de su publicación general o su utilización en contextos no relacionados con la seguridad operacional, como controversias locales sobre utilización de terrenos que involucren operaciones aeroportuarias y aspectos de atenuación del ruido.
- 5.5.1.1.2** En este contexto, la importancia de implementar formas de protección resulta fundamental. Las formas de protección no tienen por objeto eximir a las fuentes de sus obligaciones relacionadas con la seguridad o interferir con la adecuada administración de justicia.
- 5.5.1.2** Este principio se aplica a partir del momento en que ocurre un accidente o incidente que corresponde al DINAC R13 y permanece aplicable aún después de la publicación del informe final. ***En el Manual sobre protección de la información de seguridad operacional Doc. 10053*** figura orientación sobre la protección de los registros de investigaciones de accidentes e incidentes.
- 5.5.2** **Principios de protección**
- 5.5.2.1** El término “procedimientos” puede tener un alcance más completo y más amplio que el término “actividades”. Puede también referirse en términos más estrechos a los procesos de un órgano particular para examinar o imponer “actividades” que han sido adoptadas por otras autoridades (o por un organismo dentro de la misma autoridad). En un sentido general, los términos “procedimientos” y “actividades” pueden considerarse como que abarcan todas las etapas o medidas adoptadas para iniciar, dar efecto o revisar una decisión de una autoridad que afecte los derechos, privilegios, intereses legítimos o expectativas razonables de una persona. Habida cuenta de los diferentes sistemas jurídicos, el carácter y alcance de las actividades o procedimientos pueden variar. Por ejemplo:
- a)** Las *actividades o procedimientos penales y civiles* normalmente involucran autoridades judiciales. Estos procedimientos pueden incluir el inicio de la

acción, la comparecencia del acusado, todas las etapas auxiliares o provisionales, los alegatos, los procesos de descubrimiento legal y otras consultas formales. Como consecuencia de tales actividades o procedimientos, una persona puede verse expuesta a daños monetarios, multas o en algunos casos encarcelamiento.

- b) Las *actividades o procedimientos administrativos* pueden involucrar una consulta, investigación o audiencia frente a una autoridad reguladora o a un tribunal que se relacione con medidas para variar, suspender, revocar o cancelar una autorización (con fines cuya relación con la seguridad operacional puede demostrarse en algunos casos, y con fines punitivos en otros).
- c) Las *actividades o procedimientos disciplinarios* pueden referirse al proceso por el cual un empleador responda a violaciones o infracciones reales o aparentes de reglas y procedimientos por parte de un empleado. El resultado de tales actividades o procedimientos puede ser la absolución del empleado respecto de las infracciones supuestas, o la sanción o despido del empleado si las acusaciones son corroboradas.

5.5.2.1.1 Es importante recordar que los principios de protección no se aplican cuando se adoptan una medida preventiva, correctiva o de rectificación necesaria para mantener o mejorar la seguridad operacional de la aviación. Esto también se aplica a todo procedimiento, actividad o medida relacionada con una decisión de carácter preventivo o de rectificación tomada con el fin de mantener o mejorar la seguridad operacional. Por ejemplo, el uso de datos o información sobre seguridad operacional para justificar la adopción de una medida preventiva, correctiva o de rectificación está permitido en los procedimientos iniciados por un individuo o una organización tendientes a impugnar la medida en cuestión.

5.5.2.1.2 Aunque puede haber casos en que los datos o información sobre seguridad operacional se utilicen en litigios iniciados por una tercera parte contra la fuente de la notificación, se alienta a que adopten todas las medidas necesarias para asegurar que los datos y la información sobre seguridad operacional no se utilicen para fines que no sean los de mantener y mejorar la seguridad operacional de la aviación (a menos que se aplique un principio de excepción).

5.5.2.2 La DINAC puede elaborar procedimientos, con arreglo a los cuales se considera la aplicación de los principios de excepción, la facultad de imponer requisitos para mantener el carácter confidencial de los datos o información sobre seguridad operacional después de haberse adoptado una decisión para permitir el acceso a los mismos.

5.5.2.2.1 La no identificación de la fuente de los datos e información sobre seguridad operacional es otra garantía que puede aplicarse antes de que la DINAC autorice la divulgación de los mismos para fines que no sean mantener o mejorar la seguridad operacional. No obstante, el anonimato puede resultar difícil cuando las fuentes que proporcionan los datos o información sobre seguridad operacional pueden ser fácilmente identificables a partir del contenido de los datos o información notificados. Por ejemplo, el informe de un suceso que involucró un tipo de aeronave utilizado solamente por un explotador único dentro de una jurisdicción particular puede poner inmediatamente en evidencia a dicho explotador (o incluso a un empleado en particular), sencillamente identificando el tipo de aeronave en cuestión. En tales casos, la forma y el lugar en que se propone divulgar o utilizar los datos o la información sobre seguridad operacional, así como el carácter de los mismos, tendrían especial importancia. Si el carácter de la información es principalmente técnico, podría no haber en la misma mucha información de identificación que deba suprimirse u ocultarse, lo que facilitaría la labor de protección.

5.5.2.2.2 La DINAC puede optar por implementar diversos tipos de garantías para permitir la divulgación limitada para un fin específico impidiendo al mismo tiempo el uso más

amplio o la divulgación al público de los datos o información sobre seguridad operacional. Ejemplos de dichas garantías son las órdenes de protección, audiencias a puerta cerrada y exámenes a puerta cerrada.

5.5.2.2.3 La DINAC y los proveedores de servicios también pueden adoptar mejores prácticas, como el asegurar que el entorno en que se recopila, almacena, procesa y transmite la información es suficientemente seguro y que los controles de acceso y las autorizaciones son suficientes para proteger los datos y la información sobre seguridad operacional.

5.5.2.2.4 Para evitar situaciones no deseadas, será prudente asegurar que los individuos y organizaciones comprendan claramente por adelantado cómo, cuándo, dónde y con qué fin podrían utilizarse los datos e información que proporcionan, con arreglo a la aplicación de los principios de excepción. Dicha comprensión es fundamental para establecer y mantener un entorno de notificación predecible basado en la confianza.

5.5.3 Principios de excepción

5.5.3.1 La autoridad competente tendrá que ser capaz de sopesar intereses conflictivos o contrapuestos, como las leyes relativas al derecho de saber, reglamentos no relacionados con la seguridad operacional de la aviación, reglas para divulgación en litigios y otros aspectos a efectos de que el público pueda tener confianza en sus capacidades de toma de decisiones.

5.5.3.2 El primer caso en que una autoridad competente puede hacer excepciones respecto de la protección es cuando *“determine que los hechos y circunstancias indican de manera razonable que el suceso pudo haber sido causado por un acto u omisión que, de acuerdo con las leyes nacionales, se considere que constituye una conducta de negligencia grave, un acto doloso o una actividad criminal”*. En la mayoría de los casos, la autoridad competente apropiada para tomar dicha determinación será una autoridad judicial, o de fiscalía.

5.5.3.2.1 Cuando la DINAC determine que, sobre la base de los hechos y circunstancias de un caso, el suceso pudo haber sido resultado de negligencia grave, acto doloso o actividad criminal, en el sentido que dichos términos tienen en las leyes nacionales — se aplica un principio de excepción y los datos o la información sobre seguridad operacional, así como sus fuentes conexas pueden divulgarse.

5.5.3.2.2 La negligencia se refiere a un acto u omisión cometido con grave desconsideración o indiferencia frente a un riesgo evidente, independientemente de si dicho riesgo ha sido plenamente tenido en cuenta por el actor. Esto se describe a veces como conducta imprudente. Un acto doloso es una acción u omisión ilícitas cuyo actor sabe conscientemente lo que es, indiferente frente a la cuestión de si lo es o no.

5.5.3.3 El segundo caso en que la DINAC puede aplicar una excepción a las reglas de protección es cuando habiendo efectuado un examen de los datos o la información sobre seguridad operacional en cuestión, se determine que su divulgación es *“necesaria para la administración apropiada de la justicia”* y que las *“ventajas de su divulgación pesan más que las repercusiones adversas que a escala nacional e internacional dicha divulgación tendrá en la futura recopilación y disponibilidad de los datos y la información sobre seguridad operacional”*.

5.5.3.3.1 Esto involucra un proceso de evaluación en dos etapas, en el cual la DINAC debe considerar en primer lugar si los datos o la información son *“necesarios para la administración apropiada de la justicia”*, que puede no ser el caso si se dispone de fuentes alternativas para la misma información, y en segundo lugar, si determina que la divulgación es necesaria para la administración apropiada de la justicia si, en comparación, la divulgación de dichos datos o información pesa más que las repercusiones adversas que su divulgación tendría en la futura recopilación y disponibilidad de los datos y la información sobre seguridad operacional para fines de mantener o mejorar dicha seguridad.

- 5.5.3.3.2** Si se prevé el uso de datos o información sobre seguridad operacional en una acción o procedimiento (civil, administrativo, penal o disciplinario), entonces el posible impacto negativo de dicho uso puede relacionarse con la fuente de tales datos o información. Aun así, pueden imponerse garantías para prevenir que los datos o información sobre seguridad operacional se divulguen fuera de los límites de la acción o procedimiento, toda consecuencia negativa del uso de tales datos o información durante un procedimiento podría desalentar futuras notificaciones o divulgaciones de datos e información sobre seguridad operacional para fines de mantener o mejorar dicha seguridad. Si el uso propuesto de los datos o la información involucra la difusión al público o publicación de tales datos o información más allá de los límites del procedimiento, la autoridad competente también debería considerar las posibles consecuencias perjudiciales sobre la comunidad más amplia (nacional e internacional).
- 5.5.3.4** La tercera excepción involucra casos en los cuales, *“después de efectuar un examen de los datos o información sobre seguridad operacional”*, la DINAC determina *“que su divulgación es necesaria para mantener o mejorar la seguridad operacional, y que las ventajas de su divulgación pesan más que las repercusiones adversas que a escala nacional e internacional dicha divulgación tendrá en la futura recopilación y disponibilidad de datos e información sobre seguridad operacional”*.
- 5.5.3.4.1** Las circunstancias contempladas involucran la consideración por parte de la DINAC de las ventajas de divulgar datos o información sobre seguridad operacional para fines más generales relativos al mantenimiento o mejora de la seguridad operacional, incluyendo, por ejemplo, fines de instrucción y educación o la publicación de información y asesoramiento sobre seguridad operacional para beneficio de la comunidad aeronáutica. El análisis de esta situación involucra el mismo tipo de proceso en dos etapas descrito en **5.5.3.3.1**.
- 5.5.3.4.2** Al considerar la segunda etapa de este análisis, se alienta a que tengan en cuenta *“el consentimiento de la fuente de los datos y la información sobre seguridad operacional”*.
- 5.5.4** **Divulgación al público**
- 5.5.4.1** Si se divulgan al público datos o información sobre seguridad operacional, no siempre es posible limitar la forma en que se utilizaría dicha información. Por cierto, la apertura y la transparencia deberían fomentarse, pero, al mismo tiempo, deben tenerse en cuenta los derechos y expectativas legítimas de las personas involucradas en notificar y analizar los datos y la información sobre seguridad operacional, así como la necesidad de protegerles de daños inapropiados a su persona o reputación.
- 5.5.4.2** El estado paraguayo cuenta con leyes que en efecto obliga a que se divulgue toda la información en poder de las instituciones estatales. Dichas leyes se conocen a veces como leyes relativas al derecho de saber. En el marco de estas leyes, a menos que exista una exención para un tipo particular de información, la misma debe divulgarse por la DINAC si se le solicita. Entre los ejemplos de exenciones figurarían la información confidencial, la información comercial delicada o la información de tipo registros médicos que están protegidas por leyes de privacidad. Con arreglo al DINAC R19, la DINAC puede optar por crear exenciones o reglas respecto a la divulgación al público.
- 5.5.4.3** La incorrecta evaluación de reclamaciones concurrentes para obtener acceso a datos o información sobre seguridad operacional puede tener consecuencias adversas para las actividades presentes y futuras en dos formas. La divulgación al público de ciertos datos o información puede percibirse como una violación de la privacidad de los individuos o de las expectativas de confidencialidad de organizaciones relacionadas con dichos datos e información. El uso de ciertos datos o información como parte de un argumento en apoyo de sanciones contra

individuos u organizaciones involucrados puede considerarse también como una violación de principios básicos de equidad. La futura disponibilidad de datos e información sobre seguridad operacional puede verse afectada por el comportamiento humano predecible de retener información debido a la percepción de una posible amenaza basada en su divulgación o uso incriminatorio. Esto puede tener un impacto evidente en las funciones de recopilación y análisis de datos de la gestión de la seguridad operacional.

5.5.4.4 Si la DINAC determina que los datos o la información sobre seguridad operacional pueden divulgarse al público, se espera que se asegure que dicha divulgación se efectúa con arreglo a las leyes de confidencialidad aplicables o que se hace sin revelar las identidades y en forma resumida o combinada.

5.5.5 Responsabilidad del custodio de los datos e información sobre seguridad operacional

5.5.5.1 El custodio del SDCPS debería tener conocimiento de las protecciones que se aplican a los datos y a la información sobre seguridad operacional y fuentes conexas y asegurar que los mismos se divulgan y utilizan con arreglo a las disposiciones del DINAC R19.

5.5.6 Protección de los datos registrados

5.5.6.1 Las grabaciones ambientes de las conversaciones en el lugar de trabajo deberían ser parte de toda política o reglamentación sobre protección. El uso de estos registros como parte de la gestión de la seguridad operacional cuando los reglamentos o políticas lo permitan debería respetar plenamente los principios de protección y excepción. La confianza de las personas que presenten informes es fundamental para la gestión eficaz de la seguridad operacional.

5.5.6.1.1 Las disposiciones del DINAC R19 se aplican a las funciones de gestión de la seguridad operacional relativas a la operación segura de las aeronaves o en apoyo directo de la misma. Las grabaciones ambientes de las conversaciones en el lugar de trabajo pueden estar regidas por leyes sobre confidencialidad que no están definidas en el DINAC R19.

5.5.6.2 Las grabaciones ambientes de las conversaciones en el lugar de trabajo pueden comprender registros de CVR, AIR u otros registradores de vuelo, así como registros de comunicaciones de fondo y del entorno acústico en los puestos de trabajo de los controladores del tránsito aéreo.

CAPÍTULO 6

ENFOQUE DE IMPLEMENTACIÓN EN ETAPAS

6.1 GENERALIDADES

6.1.1 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.

6.1.2 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.

6.1.3 El enfoque en etapas reconoce que la implementación de un SMS completamente maduro es un proceso que toma varios años. 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.

6.1.4 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.

6.2 ETAPA 1 / 12 MESES

6.2.1 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.

6.2.1.1 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.

6.2.1.2 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:

6.2.2 Compromiso de la dirección – Elemento 1.1

- 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.

6.2.3 Documentación SMS – Elemento 1.5

- a) Desarrollar la documentación 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.

6.2.4 Designación del personal clave de seguridad operacional – 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.

6.2.5 Instrucción y educación – Elemento 4.1

- a) Realizar un análisis de las necesidades de instrucción.
- b) Organizar y configurar programas para la instrucción correcta de todo el personal, de acuerdo con sus responsabilidades individuales y su participación en el SMS.
- c) Desarrollar la instrucción de la seguridad operacional, considerando:
 - 1) la instrucción inicial (seguridad operacional general) específica del trabajo; y
 - 2) la instrucción recurrente.
- d) Identificar los costos asociados con la instrucción.
- e) Desarrollar un proceso de validación que mide la eficacia de la instrucción.
- f) Establecer un sistema de registros de instrucción de la seguridad operacional.

6.2.6 Comunicación de la seguridad operacional – Elemento 4.2

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

- b) Establecer un medio para transferir información de seguridad operacional mediante cualquiera de las siguientes opciones:
 - 1) folletos informativos, noticias y boletines de seguridad operacional;
 - 2) sitios web;
 - 3) correo electrónico.

6.3 ETAPA 2 / 12 MESES

6.3.1 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.

6.3.2 Compromiso de la dirección – Elemento 1.1

- a) Desarrollar una política de seguridad operacional.
- b) Solicitar que el ejecutivo responsable firme la política de seguridad operacional.
- c) Comunicar la política de seguridad operacional en toda la organización.
- d) Establecer un programa de revisión de la política de seguridad operacional para garantizar que sigue siendo pertinente y adecuada para la organización.
- e) Establecer objetivos de seguridad operacional para el SMS mediante el desarrollo de normas de rendimiento en materia de seguridad operacional en términos de:
 - 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.

6.3.3 Obligación de rendición de cuentas y responsabilidades en materia de 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.

6.3.4 Coordinación de la planificación de respuesta ante emergencias – Elemento 1.4

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

6.3.5 Documentación SMS – Elemento 1.5

- 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 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 instrucción 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.

6.4 ETAPA 3 / 18 MESES

6.4.1 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.

6.4.2 Identificación de peligros – Elemento 2.1

- 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.

- 6.4.3 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 instrucción de la gestión de riesgos o SMS de la organización.
- 6.4.4 Observación y medición del rendimiento en materia de seguridad operacional – Elemento 3.1**
- a) Establecer un procedimiento interno de notificación e investigación de sucesos. Esto puede incluir informes obligatorios de defectos (MDR) o informes importantes, donde corresponda.
 - b) Establecer la recopilación, el procesamiento y el análisis de los datos de seguridad operacional de los resultados de alto impacto.
 - c) Establecer indicadores de seguridad operacional de alto impacto (ALoSP inicial) y su configuración de objetivos y alertas asociados. Entre los ejemplos de indicadores de seguridad operacional de alto impacto se incluyen tasas de accidentes, tasas de incidentes graves y el control de los resultados de no cumplimiento de alto riesgo.
 - d) Lograr un acuerdo con la autoridad de vigilancia de la DINAC sobre los indicadores de rendimiento en materia de seguridad operacional y objetivos de rendimiento en materia de seguridad operacional.
- 6.4.5 Gestión del cambio – Elemento 3.2**
- a) Establecer un proceso formal para la gestión de cambio que considere:
 - 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.
- 6.4.6 Mejora continua del SMS – Elemento 3.3**
- 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.

- 6.5 ETAPA 4 / 18 MESES**
- 6.5.1** 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.
- 6.5.2 Compromiso de la dirección – Elemento 1.1**
- a) Mejorar el procedimiento disciplinario, la política existente con una debida consideración de errores/equivocaciones accidentales de las infracciones deliberadas/graves.
- 6.5.3 Identificación de peligros – Elemento 2.1**
- a) Integrar los peligros identificados en los informes de investigación de sucesos con el sistema de notificación voluntaria.
- b) Integrar los procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o del cliente, donde corresponda.
- c) Si fuera necesario, desarrollar un proceso para priorizar peligros recopilados para la mitigación de riesgos según las áreas de mayor necesidad o preocupación.
- 6.5.4 Observación y medición del rendimiento en materia de seguridad operacional – Elemento 3.1**
- a) Mejorar el sistema de recopilación y procesamiento de datos de seguridad operacional para incluir eventos de bajo impacto.
- b) Establecer indicadores de seguridad operacional de bajo impacto con el control del nivel de objetivos/alertas, según corresponda (ALoSP maduro).
- c) Lograr un acuerdo con la autoridad de vigilancia de la DINAC sobre indicadores de rendimiento en materia de seguridad operacional de bajo impacto y niveles de objetivos/alertas de rendimiento en materia de seguridad operacional.
- 6.5.5 Mejora continua del SMS – Elemento 3.3**
- a) Establecer auditorías del SMS de auditoría interna.
- b) Establecer otros programas de revisión/estudio de SMS operacional.
- 6.5.6 Instrucción y educación – Elemento 4.1**
- a) Completar un programa de instrucción de SMS para todo el personal pertinente.
- 6.5.7 Comunicación de la seguridad operacional – Elemento 4.2**
- a) Establecer mecanismos para promover la distribución y el intercambio de información de seguridad operacional de forma interna y externa.
