Regulación Técnica Aeronáutica

RTA-19

GESTIÓN DE LA SEGURIDAD OPERACIONAL

SISTEMA DE EDICIÓN Y ENMIENDA

LAS ENMIENDAS A LA PRESENTE REGULACION SERAN INDICADAS MEDIANTE UNA BARRA VERTICAL EN EL MARGEN IZQUIERDO, ENFRENTE DEL RENGLÓN, SECCION O FIGURA QUE ESTE SIENDO AFECTADA POR EL MISMO. LA EDICIÓN SERÁ EL REEMPLAZO DEL DOCUMENTO COMPLETO POR OTRO.

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

REGISTRO DE EDICIONES Y ENMIENDAS

EDI / ENM.	Fecha de Emisión	Fecha de Inserción	Insertada por:
Edición Inicial	Diciembre / 13		
Edición 1	Marzo / 17		
Edición 2	Julio /19		

PREÁMBULO

La RTA-19 contiene las normas y métodos recomendados relativos a la Gestión de la Seguridad Operacional, basados en el cumplimiento del Anexo 19 de la Organización de Aviación Civil Internacional (OACI), primera edición adoptado unánimemente por el Consejo de la OACI el 25 de Febrero de 2013 y aplicable a partir del 14 de Diciembre 2013.

Teniendo como objetivo principal la importancia de la gestión de la seguridad operacional a nivel estatal y la mejora de la seguridad operacional al consolidar en una sola Regulación, todas las disposiciones sobre gestión de la seguridad operacional que se aplica a múltiples campos de la aviación. Además, se facilita la futura evolución de las disposiciones sobre gestión de la seguridad operacional y se promueve la implantación armonizada de las disposiciones relativas al Sistema de Gestión de la Seguridad Operacional (SMS) y el Programa Estatal de Seguridad Operacional (SSP).

EDICION INICIAL

De conformidad con las disposiciones del Artículo 37 del Convenio sobre Aviación Civil Internacional (Chicago 1944), el 25 de febrero de 2013, el Consejo adoptó por primera vez el Anexo 19 al Convenio, que contiene las Normas y Métodos Recomendados (SARPS) relacionados con las responsabilidades funcionales y los procesos que subyacen a la gestión de la seguridad operacional por parte de los Estados. Los SARPS se basaron en disposiciones sobre gestión de la seguridad operacional que inicialmente adoptó el Consejo en los Anexos 1; 6; Partes I, II y III; 8; 11; 13 y 14, Volumen I; y en las recomendaciones de la primera reunión especial del SMP (Montreal, 13 - 17 de febrero de 2012).

Debido a lo antes expuesto, el Instituto Nicaragüense de Aeronáutica Civil (INAC) determino la necesidad de contar con la Regulación Técnica Aeronáutica relativa a la Gestión de la Seguridad Operacional (RTA-19); la cual cumple con las normas y métodos recomendados por la OACI en el Anexo 19, primera edición y documentos asociados.

En virtud de la creciente complejidad del sistema mundial de transporte aéreo y de la interrelación de sus actividades de aviación necesarias para garantizar la operación segura de las aeronaves, esta RTA-19 sirve de apoyo a la evolución continua de una estrategia preventiva que permita mejorar el rendimiento en materia de seguridad operacional. Esta estrategia preventiva de seguridad operacional se basa en la implantación de un SSP que se ocupe sistemáticamente de los riesgos de seguridad operacional. La implantación eficaz de un SSP se lleva a cabo mediante un proceso gradual, ya que se requiere tiempo para su plena maduración. Entre los factores que afectan al tiempo que se necesita para establecer un SSP figuran la complejidad del sistema de transporte aéreo y la madurez de las capacidades del Estado en materia de supervisión de la seguridad operacional de la aviación.
La edición inicial de la RTA-19 fue revisada y aprobada por el Instituto Nicaragüense de Aeronáutica Civil (INAC) el 14 de Diciembre de 2013.

EDICIÓN 1

La Enmienda 1 al Anexo 19 fue adoptada por el Consejo de la OACI el 2 de marzo de 2016, con fecha para surtir efecto del 11 de julio de 2016 y con aplicación efectiva a partir del 7 de noviembre de 2019.

La Enmienda 1 del Anexo 19 contiene cambios sustantivos en las disposiciones sobre gestión de la seguridad operacional, entre los cuales se destacan el reconociendo de la necesidad de aclarar la relación entre los ocho elementos críticos (CE) de un sistema estatal de supervisión de la seguridad operacional (SSO) y los elementos del Programa estatal de seguridad operacional (SSP), importante mención tiene la integración de los ocho CE del sistema SSO con los elementos del marco SSP en un conjunto armonizado de SARPS, a fin de facilitar la implantación. También consolida las disposiciones relativas a la responsabilidad funcional estatal en materia de gestión de la seguridad operacional. Además, dicha Enmienda proporciona SARPS nuevos y enmendados sobre el sistema de gestión de la seguridad operacional (SMS) para facilitar la implantación, incluida la adición de

varias notas explicativas. Así mismo, amplía la aplicación de un SMS a las entidades responsables del tipo de diseño y fabricación de motores y hélices

Por último, la Enmienda 1 del Anexo 19 proporciona un mayor grado de protección a los datos e información sobre seguridad operacional, así como a sus fuentes, facilitando así su continua disponibilidad para apoyar, de manera preventiva, las estrategias para mejorar la seguridad operacional.

Considerando las nuevas disposiciones en materia de gestión de la seguridad operacional establecidas por la OACI mediante la Enmienda 1 del Anexo 19, el INAC ha incorporado dichas disposiciones a manera de normas dentro de la Edición 1 de la RTA-19, la cual fue revisada y aprobada por el Instituto Nicaragüense de Aeronáutica Civil (INAC) el 17 de Marzo de 2017.

EDICIÓN 2

La presente Edición 2 de la RTA 19, ha sido por necesidad del Estado de Nicaragua, tomando de guía la 4ta edición del Documento 9859 de OACI, el cual explica el funcionamiento de los componentes y elementos de un sistema de gestión de seguridad operacional (SMS) y las actividades y procesos de un proveedor de servicios, dejando de manera clara los requisitos específicos que debe cumplir todo SMS, de cara a mejorar los procesos de implementación y aceptación.

LISTA DE PÁGINAS EFECTIVAS

N0 DE PAGINA	NO DE EDICION	FECHA
Portada	Edición 2	Jul. /19
SEE – 1	Edición 2	Jul. /19
REE – 1	Edición 2	Jul. /19
P – 1	Edición 2	Jul. /19
P – 2	Edición 2	Jul. /19
LPE – 1	Edición 2	Jul. /19
LPE – 2	Edición 2	Jul. /19
LPE – 3	Edición 2	Jul. /19
TC – 1	Edición 2	Jul. /19
TC – 2	Edición 2	Jul. /19
Capítulo 1		
1 – 1	Edición 2	Jul. /19
1– 2	Edición 2	Jul. /19
1 – 3	Edición 2	Jul. /19
1 – 4	Edición 2	Jul. /19
1 – 5	Edición 2	Jul. /19
Capítulo 2		
2 – 1	Edición 2	Jul. /19
Capitulo 3		
3 – 1	Edición 2	Jul. /19
3 – 2	Edición 2	Jul. /19
3 – 3	Edición 2	Jul. /19
3 – 4	Edición 2	Jul. /19
Capítulo 4		
4 – 1	Edición 2	Jul. /19
Capitulo 5		
5 – 1	Edición 2	Jul. /19
5 – 2	Edición 2	Jul. /19
Apéndice 1		
APE 1 – 1	Edición 2	Jul. /19
APE 1 – 2	Edición 2	Jul. /19
Apéndice 2		
APE 2 – 1	Edición 2	Jul. /19
APE 2 – 2	Edición 2	Jul. /19
APE 2 – 3	Edición 2	Jul. /19
APE 2 – 4	Edición 2	Jul. /19
APE 2 – 5	Edición 2	Jul. /19
APE 2 – 6	Edición 2	Jul. /19
APE 2 – 7	Edición 2	Jul. /19
APE 2 – 8	Edición 2	Jul. /19
APE 2 – 9	Edición 2	Jul. /19
APE 2 – 10	Edición 2	Jul. /19
APE 2 – 11	Edición 2	Jul. /19
APE 2 – 12	Edición 2	Jul. /19
APE 2 – 13	Edición 2	Jul. /19
APE 2 – 14	Edición 2	Jul. /19
APE 2 – 15	Edición 2	Jul. /19
APE 2 – 16	Edición 2	Jul. /19

APE 2 – 17	Edición 2	Jul. /19
APE 2 – 18	Edición 2	Jul. /19
APE 2 – 19	Edición 2	Jul. /19
APE 2 – 20	Edición 2	Jul. /19
APE 2 – 21	Edición 2	Jul. /19
APE 2 – 22	Edición 2	Jul. /19
APE 2 – 23	Edición 2	Jul. /19
Apéndice 3		
APE 3 – 1	Edición 2	Jul. /19
APE 3 – 2	Edición 2	Jul. /19
APE 3 – 3	Edición 2	Jul. /19
ADJUNTO A		
ADJ A – 1	Edición 2	Jul. /19
ADJUNTO B		
ADJ B – 1	Edición 2	Jul. /19
ADJ B – 2	Edición 2	Jul. /19
ADJ B – 3	Edición 2	Jul. /19
ADJ B – 4	Edición 2	Jul. /19
ADJ B – 5	Edición 2	Jul. /19
ADJ B – 6	Edición 2	Jul. /19
ADJ B – 7	Edición 2	Jul. /19
ADJ B – 8	Edición 2	Jul. /19
ADJUNTO C		
ADJ C – 1	Edición 2	Jul. /19
ADJ C – 2	Edición 2	Jul. /19
ADJ C – 3	Edición 2	Jul. /19
ADJ C – 4	Edición 2	Jul. /19
ADJ C – 5	Edición 2	Jul. /19
ADJ C – 6	Edición 2	Jul. /19
ADJ C – 7	Edición 2	Jul. /19
ADJUNTO D		
ADJ D – 1	Edición 2	Jul. /19
ADJ D – 2	Edición 2	Jul. /19
ADJ D – 3	Edición 2	Jul. /19
ADJUNTO E		
ADJ E – 1	Edición 2	Jul. /19
ADJ E – 2	Edición 2	Jul. /19
ADJ E – 3	Edición 2	Jul. /19
ADJ E – 4	Edición 2	Jul. /19
ADJ E – 5	Edición 2	Jul. /19
ADJ E – 6	Edición 2	Jul. /19
ADJ E – 7	Edición 2	Jul. /19
ADJ E – 8	Edición 2	Jul. /19
ADJ E – 9	Edición 2	Jul. /19
ADJ E– 10	Edición 2	Jul. /19
ADJUNTO F		
ADJ F – 1	Edición 2	Jul. /19
ADJ F – 2	Edición 2	Jul. /19
ADJ F – 3	Edición 2	Jul. /19
ADJUNTO G		
ADJ G – 1	Edición 2	Jul. /19

ADJ G – 2	Edición 2	Jul. /19
ADJ G – 3	Edición 2	Jul. /19
ADJ G – 4	Edición 2	Jul. /19
ADJ G – 5	Edición 2	Jul. /19
ADJ G – 6	Edición 2	Jul. /19
ADJUNTO H		
ADJ H – 1	Edición 2	Jul. /19

TABLA DE CONTENIDOS

CAPÍTULO I DEFINICIONES

Definiciones

Los términos y expresiones indicados a continuación, empleados en la presente Regulación Técnica Aeronáutica (RTA) sobre 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 (para uniformidad estadística, 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) 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 (en el Adjunto G de la RTA 13 figura orientación para determinar los daños de aeronave) 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 a álabes del rotor principal, álabes 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 (una aeronave se considera desaparecida cuando se da por terminada la búsqueda oficial y no se han localizado los restos) o es totalmente inaccesible.

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.

Autoridades u organismos competentes: Se emplea en un sentido genérico que incluye a todas las autoridades responsables de la supervisión de la seguridad operacional de la aviación que pueden ser establecidas por el Estado como entidades independientes; para el caso de Nicaragua se entiende como la autoridad de aviación civil al INAC, como la autoridad aeroportuaria a la EAAI, como las autoridades ATS a la EAAI y a COCESNA como organismo competente al ser el proveedor de servicios ATS del espacio aéreo superior de los Estados Centroamericanos y para la autoridad meteorológica al INETER.

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.

Base de datos sobre seguridad operacional: se refiriere a una base de datos o a varias y puede incluir la base de datos de accidentes e incidentes. En la RTA-13 – Investigación de accidentes e incidentes de aviación figuran disposiciones relativas a una base de datos de accidentes e incidentes.

Custodio: Puede referirse a un individuo o a una organización.

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

a) investigaciones de accidentes o incidentes;

b) notificaciones de seguridad operacional;

c) notificaciones sobre el mantenimiento de la aeronavegabilidad;

d) supervisión de la eficiencia operacional;

e) inspecciones, auditorías, constataciones; o

f) estudios y exámenes de seguridad operacional.

Estado de diseño: El Estado que tiene jurisdicción sobre la entidad responsable del diseño de tipo.

Estado de fabricación: El Estado que tiene jurisdicción sobre la entidad responsable del montaje final de la aeronave.

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

Giroavión: Para efectos de interpretación algunos Estados emplean este término como alternativa de “helicóptero”.

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.

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. Entre los tipos de incidentes que son de interés para los estudios relacionados con la seguridad operacional figuran los incidentes enumerados en la RTA-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.

Inspectores: Son un subconjunto del personal que desempeña funciones de supervisión 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 Organización de Aviación Civil Internacional, otros requisitos de seguridad operacional de la aviación y las mejores prácticas que se consideren apropiadas. El INAC, acepta las mejores prácticas de la industria que se mencionan en las Regulaciones Técnicas Aeronáuticas y otros documentos jurídicos vigentes, con el objetivo de cumplir los requisitos establecidos en la presente RTA-19 y otros requerimientos sobre seguridad operacional.

Meta de rendimiento en materia de seguridad operacional: La meta proyectada o prevista del Estado o proveedor de servicios que se desea conseguir, en cuanto a un indicador de rendimiento en materia de seguridad operacional, en un período de tiempo determinado que coincide con los objetivos de seguridad operacional.

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

Personal de operaciones: Personal que participa en las actividades de aviación y está en posición de notificar información sobre seguridad operacional. 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 gestión de la seguridad operacional.

Proveedor de servicios: Se refiere a las organizaciones enumeradas en el Capítulo 3, RTA - 19. 3.3.2.1 y no incluye a los explotadores de la aviación general internacional.

Reglamentos: Se emplea en un sentido genérico y abarca, entre otras cosas, instrucciones, reglas, edictos, directivas, conjuntos de leyes, requisitos, políticas y órdenes.

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.

Abreviaturas

ADREP: Sistema de notificación de datos sobre accidentes/incidentes.

AIS: Servicios de Información Aeronáutica.

ATS: Servicios de Tránsito Aéreo.

EAAI: Empresa Administradora de Aeropuertos Internacionales.

ERP: Plan de respuesta ante emergencias.

FH: Horas de Vuelo.

FIR: Región de información de vuelo

CNS: Comunicaciones, Navegación y Vigilancia.

COCESNA: Corporación Centroamericana de Servicios de Navegación Aérea.

CVR: Registrador de la voz en el puesto de pilotaje.

DGR: Reglamentos sobre mercancías peligrosas.

DOA: Aprobación como organización de diseño

HIRA: Identificación de peligros y evaluación de riesgos.

HIRM: Identificación de peligros y mitigación de riesgos.

IFSD: Parada de motor en vuelo.

INAC: Instituto Nicaragüense de Aeronáutica Civil

INETER: Instituto Nicaragüense de Estudios Territoriales.

LEI: Falta de aplicación eficaz

MET: Servicios Meteorológicos.

MRO: Organización de reparación de mantenimiento.

POA: Aprobación como organización de producción

SAG: Grupo de acción de seguridad operacional

SAR: Servicios de Búsqueda y Salvamento.

SARPS: Normas y Métodos Recomendados.

SD: Desviación estándar

SDCPS: Sistemas de Recopilación y Procesamiento de Datos sobre Seguridad Operacional.

SMM: Manual de Gestión de la Seguridad Operacional.

SMS: Sistema de Gestión de la Seguridad Operacional.

SOP: Procedimientos operacionales normalizados

SPI: Indicador de rendimiento en materia de seguridad operacional

SSP: Programa Estatal de Seguridad Operacional.

INTENCIONALMENTE EN BLANCO

CAPÍTULO II APLICACIÓN

Las disposiciones de la presente Regulación Técnica Aeronáutica (RTA) se aplican a las funciones de gestión de la seguridad operacional que atañen y sirven de apoyo directo a la operación más segura de las aeronaves.

En el Capítulo 4 figuran disposiciones sobre gestión de la seguridad operacional para los proveedores y explotadores de servicios aeronáuticos que se especifican, las cuales se relacionan con los Sistemas de Gestión de Seguridad Operacional (SMS

Ninguna disposición de esta RTA tiene por objeto transferir al Estado las responsabilidades del proveedor o explotador de servicios de aviación. Esto incluye las funciones que atañen, o sirven de apoyo directo, a la operación segura de las aeronaves.

En el contexto de esta RTA, por “responsabilidad” (en singular) se entiende la “responsabilidad estatal” con respecto a las obligaciones internacionales contraídas en el marco del Convenio sobre Aviación Civil Internacional, en tanto que al término “responsabilidades” (en plural) se le da su significado ordinario (es decir, se usa al referirse a las funciones y actividades que pueden delegarse).

Independientemente de la fecha de aplicación de la presente Regulación, Edición 2, del 07 de Noviembre de 2019, y de las enmiendas consiguientes en las otras Regulaciones Técnicas Aeronáuticas pertinentes, los requerimientos y requisitos sobre gestión de la seguridad operacional que se adoptaron previamente conservaran su fecha de aplicación original.

INTENCIONALMENTE EN BLANCO

CAPÍTULO III RESPONSABILIDADES FUNCIONALES ESTATALES EN MATERIA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

Los elementos críticos (CE) del sistema estatal de supervisión de la seguridad operacional (SSO) del Apéndice 1 constituyen el fundamento de un SSP.

Las disposiciones sobre gestión de la seguridad operacional relativas a tipos específicos de actividades de aviación se tratan en las RTA pertinentes.

La RTA-LPTA.1.2.4.2 contiene principios básicos de gestión de la seguridad operacional que se aplican al proceso de evaluación médica de los titulares de licencias.

RTA-19.3.1 Programa estatal de seguridad operacional (SSP)

El INAC debe establecer y mantener un SSP que se ajuste a la dimensión y complejidad del sistema de aviación civil del Estado, pero se podrán delegar las funciones y actividades relacionadas con la gestión de la seguridad operacional a otro Estado, organización regional de vigilancia de la seguridad operacional (RSOO) u organización regional de investigación de accidentes e incidentes (RAIO); sin embargo el INAC debe conservar la responsabilidad de dichas funciones y actividades.

RTA-19.3.2: Política, objetivos y recursos estatales de la seguridad operacional

RTA-19.3.2.1: Legislación aeronáutica básica

RTA-19.3.2.1.1: El Estado de Nicaragua debe establecer una legislación aeronáutica básica de conformidad con la Sección 1 del Apéndice 1 de la presente RTA.

RTA-19.3.2.1.2: El INAC debe establecer una política de cumplimiento que especifique las condiciones y circunstancias en las cuales los proveedores de servicios con un SMS pueden encargarse de sucesos que suponen algunos problemas respecto de la seguridad operacional, y resolverlos, internamente, en el contexto de su SMS, a satisfacción de la autoridad estatal competente.

RTA-19.3.2.2: Reglamentos de explotación específicos

RTA-19.3.2.2.1: El INAC debe establecer reglamentos de explotación específicos de conformidad con la Sección 2 del Apéndice 1 de la presente RTA.

RTA-19.3.2.2.2: El INAC debe examinar periódicamente los reglamentos específicos de funcionamiento, los textos de orientación y las políticas de implantación para asegurarse de que sigan siendo pertinentes y apropiados.

RTA-19.3.2.3: Sistema y funciones estatales

RTA-19.3.2.3.1: El Estado de Nicaragua debe establecer un sistema y funciones estatales de conformidad con la Sección 3 del Apéndice 1 de la presente RTA.

RTA-19.3.2.3.2 El INAC debe identificar, definir y documentar los requisitos, las obligaciones, funciones, y actividades relativas a la creación y el mantenimiento del SSP, comprendidas las directrices para planificar, organizar, desarrollar, mantener, controlar y mejorar permanentemente el SSP de manera tal que cumpla los objetivos de seguridad operacional del Estado.

RTA-19.3.2.3.3: El INAC debe establecer una política y objetivos de seguridad operacional que reflejen su compromiso con respecto a la seguridad operacional y faciliten la promoción de una cultura positiva en la comunidad de la aviación con respecto a la seguridad operacional.

RTA-19.3.2.3.4: La política y los objetivos de seguridad operacional deben ser publicados y examinados periódicamente para garantizar que sigan siendo pertinentes y apropiados para el Estado.

RTA-19.3.2.4: Personal técnico cualificado

El INAC debe establecer requisitos en relación con las cualificaciones del personal técnico de conformidad con la Sección 4 del Apéndice 1 de la presente RTA. El término "personal técnico" se refiere a las personas que desempeñan funciones relacionadas con la seguridad operacional para el Estado de Nicaragua o en nombre del mismo.

RTA-19.3.2.5: Orientación técnica, instrumentos y suministro de información crítica en materia de seguridad operacional

El INAC debe establecer orientación técnica e instrumentos y suministrarán información crítica para la seguridad operacional de conformidad con la Sección 5 del Apéndice 1 de la presente RTA.

RTA-19.3.3 Gestión estatal de los riesgos de seguridad operacional

RTA-19.3.3.1: Obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones

El INAC debe cumplir con las obligaciones de otorgamiento de licencias, certificación, autorización y aprobación de conformidad con la Sección 6 del Apéndice 1 de la presente RTA.

RTA-19.3.3.2: Obligaciones del sistema de gestión de la seguridad operacional

RTA-19.3.3.2.1: El INAC exige que los siguientes proveedores de servicios bajo su autoridad implanten un SMS:

a) organizaciones de instrucción reconocidas, de conformidad con la RTA-LPTA, que están expuestas a riesgos de seguridad operacional relacionados con las operaciones de aeronave al prestar sus servicios;

b) explotadores de aviones o helicópteros autorizados para llevar a cabo actividades de transporte aéreo comercial internacional, de conformidad con la RTA-OPS-1 y RTA-OPS-3, respectivamente;

c) organismos de mantenimiento reconocidos que ofrecen servicios a los explotadores de aviones o helicópteros dedicados al transporte aéreo comercial internacional, de conformidad con la RTA-145.

d) Reservado;

e) proveedores de servicios de tránsito aéreo (ATS), de conformidad con la RTA-11; y

f) explotadores de aeródromos certificados, de conformidad con la RTA-14 Volumen I.

RTA-19.3.3.2.2: El INAC se debe asegurar de que los indicadores y metas de rendimiento en materia de seguridad operacional establecidos por los proveedores de servicios y los explotadores sean aceptables para el Estado de Nicaragua.

RTA-19.3.3.2.3: El INAC debe establecer criterios para que los aviones grandes o de turborreactor de matrícula nicaragüense de explotadores de la aviación general internacional, de conformidad con la RTA-OPS-2.400, implanten un sistema SMS.

RTA-19.3.3.2.4: En los criterios establecidos por el INAC de conformidad con la RTA-19.3.3.2.3 se deben tener en cuenta los elementos y el marco SMS que figuran en el Apéndice 2 de la presente RTA.

RTA-19.3.3.3: Investigación de accidentes e incidentes

El Estado de Nicaragua debe establecer un proceso para investigar accidentes e incidentes de conformidad con la RTA-13, en apoyo de la gestión de la seguridad operacional en el Estado.

RTA-19.3.3.4: Identificación de peligros y evaluación de riesgos de seguridad operacional

RTA-19.3.3.4.1: El INAC debe establecer y mantener un proceso para identificar peligros a partir de los datos recopilados sobre seguridad operacional.

RTA-19.3.3.4.2: El INAC debe crear y mantener un proceso para garantizar la evaluación de los riesgos de seguridad operacional asociados a peligros identificados.

RTA-19.3.3.5: Gestión de riesgos de seguridad operacional

RTA-19.3.3.5.1: El INAC debe establecer mecanismos para la solución de problemas de seguridad operacional de conformidad con la Sección 8 del Apéndice 1 de la presente RTA.

RTA-19.3.3.5.2: El INAC debe elaborar y mantener un proceso para manejar los riesgos de seguridad operacional.

RTA-19.3.4: Aseguramiento estatal de la seguridad operacional

RTA-19.3.4.1: Obligaciones de vigilancia

RTA-19.3.4.1.1: El INAC debe cumplir las obligaciones de vigilancia de conformidad con la Sección 7 del Apéndice 1 de la presente RTA.

En la vigilancia del SMS del proveedor de servicios se debe tener en cuenta el rendimiento en materia de seguridad operacional, así como la dimensión y complejidad de sus productos o servicios de aviación.

RTA-19.3.4.1.2: El INAC debe establecer procedimientos para priorizar las inspecciones, auditorías y encuestas relacionadas con los elementos que plantean más preocupación o que requieren mayor atención. Los perfiles organizativos de riesgos, los resultados de la identificación de peligros y de la evaluación de riesgos, al igual que los resultados en materia de vigilancia, pueden proporcionar información para priorizar las inspecciones, auditorías y encuestas.

RTA-19.3.4.1.3: El INAC debe examinar periódicamente el rendimiento en materia de seguridad de cada proveedor de servicios.

RTA-19.3.4.2: Rendimiento estatal en materia de seguridad operacional

RTA-19.3.4.2.1: El Estado de Nicaragua debe determinar el nivel aceptable de rendimiento en materia de seguridad operacional por medio de su SSP.

RTA-19.3.4.2.2: El INAC debe elaborar y mantener un proceso para evaluar la eficacia de las medidas emprendidas para manejar los riesgos de seguridad operacional y resolver los problemas de seguridad operacional. Los resultados de la evaluación de la seguridad operacional pueden utilizarse para establecer las prioridades de las medidas para manejar los riesgos de seguridad operacional.

RTA-19.3.4.2.3: El INAC debe evaluar la eficacia de su SSP para mantener o mejorar continuamente su nivel global de rendimiento en materia de seguridad operacional.

RTA-19.3.5: Promoción estatal de la seguridad operacional

RTA-19.3.5.1: Comunicación y divulgación interna de la información sobre seguridad operacional

El INAC debe promover el conocimiento con respecto a la seguridad operacional y la compartición e intercambio de información sobre seguridad operacional para respaldar, en las organizaciones de aviación del Estado de Nicaragua, el desarrollo de una cultura organizativa positiva de seguridad operacional que promueva un SSP eficaz.

RTA-19.3.5.2: Comunicación y divulgación externa de la información sobre seguridad operacional

El INAC debe promover el conocimiento con respecto a la seguridad operacional y la compartición e intercambio de información sobre seguridad operacional con la comunidad de la aviación para fomentar el mantenimiento y mejoramiento de la seguridad operacional y respaldar el desarrollo de una cultura positiva de seguridad operacional. El Capítulo 5 de la presente RTA contiene más detalles acerca de la compartición e intercambio de información sobre seguridad operacional.

INTENCIONALMENTE EN BLANCO

CAPÍTULO IV SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

RTA-19.4.1 Generalidades

RTA-19.4.1.1: El SMS de un proveedor de servicios:

a) se debe establecer de conformidad con los elementos del marco que figuran en el Apéndice 2 de la presente RTA; y

b) se debe ajustar a la dimensión del proveedor de servicios y a la complejidad de sus productos o servicios de aviación.

RTA-19.4.1.2: El Estado se asegurará de que el proveedor de servicios elabore un plan para facilitar la implantación del SMS.

RTA-19.4.1.3: El SMS de una organización de instrucción reconocida, de conformidad con la RTA-LPTA, que esté expuesta a riesgos de seguridad operacional relacionados con las operaciones de aeronave al prestar sus servicios debe ser aceptable para el INAC.

RTA-19.4.1.4: El SMS de un explotador de aviones o helicópteros certificado que esté autorizado a realizar actividades de transporte aéreo comercial internacional, de conformidad con la RTA-OPS 1 o RTA-OPS 3, respectivamente, debe ser aceptable para el INAC.

RTA-19.4.1.5: El SMS de un organismo de mantenimiento reconocido que preste servicios a explotadores de aviones o helicópteros dedicados al transporte aéreo comercial internacional, de conformidad con la RTA-145, debe ser aceptable para el INAC.

RTA-19.4.1.6: Reservado

RTA-19.4.1.7: Reservado

RTA-19.4.1.8: El SMS de un proveedor ATS, de acuerdo con la RTA-11, debe ser aceptable para el INAC. Si el proveedor de servicios ATS tiene bajo su autoridad, total o parcial, otros servicios de navegación aérea (AIS, CNS, MET y/o SAR), éstos deben incluirse en el ámbito de aplicación de su SMS.

RTA-19.4.1.9: El SMS de un explotador de un aeródromo certificado, de acuerdo con la RTA-14 Volumen I, debe ser aceptable para el INAC.

RTA-19.4.2 Aviación general internacional - aviones

El SMS de un explotador de la aviación general internacional que realice operaciones con aviones grandes o de turborreactor de conformidad con RTA-OPS 2.400, se debe ajustar a la dimensión y complejidad de la operación y debe cumplir los criterios establecidos por el Estado de matrícula de la aeronave.

INTENCIONALMENTE EN BLANCO

CAPÍTULO V RECOPILACIÓN, ANÁLISIS, PROTECCIÓN, COMPARTICIÓN E INTERCAMBIO DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL

Este capítulo tiene por finalidad garantizar la continua disponibilidad de datos e información sobre seguridad operacional para servir de base a las actividades de gestión de la seguridad operacional.

RTA-19.5.1: Sistemas de recopilación y procesamiento de datos sobre seguridad operacional

RTA-19.5.1.1: El INAC debe establecer un sistema de recopilación y procesamiento de datos sobre seguridad operacional (SDCPS) para captar, almacenar, agregar y permitir el análisis de datos e información sobre seguridad operacional. El SDCPS se refiere a los sistemas de procesamiento y notificación, las bases de datos sobre seguridad operacional, los esquemas para intercambio de información y la información registrada, y comprende, entre otros:

a) datos e información relativos a las investigaciones de accidentes e incidentes;

b) datos e información relativos a las investigaciones de seguridad operacional efectuadas por las autoridades estatales o los proveedores de servicios de aviación;

c) sistemas de notificación obligatoria de seguridad operacional, como se indica en RTA-19.5.1.2;

d) sistemas de notificación voluntaria de seguridad operacional, como se indica en RTA-19.5.1.3; y

e) sistemas de autonotificación, incluidos los sistemas automáticos de captura de datos, según se describe en el RTA-OPS1.037 (a), así como sistemas manuales de captura de datos.

RTA-19.5.1.2: El INAC debe establecer un sistema de notificación obligatoria de seguridad operacional que incluya la notificación de incidentes.

RTA-19.5.1.3: El INAC debe establecer un sistema de notificación voluntaria de seguridad operacional para recopilar datos e información sobre seguridad operacional no recopilados por los sistemas de notificación obligatoria de seguridad operacional.

RTA-19.5.1.4: El INAC como la autoridad responsable de implementar el SSP del Estado de Nicaragua debe tener acceso a los SDCPS a los que se hace referencia en RTA-19.5.1.1 para cumplir con sus responsabilidades de seguridad operacional de conformidad con los principios contemplados en el Apéndice 3 de la presente RTA.

RTA-19.5.1.5: Las bases de datos sobre seguridad operacional deben utilizar una taxonomía normalizada para facilitar la compartición y el intercambio de información sobre seguridad operacional. Para el caso del INAC se debe utilizar un sistema compatible con el ADREP.

RTA-19.5.2: Análisis de datos e información sobre seguridad operacional

RTA-19.5.2.1: El INAC debe establecer y mantener un proceso para analizar los datos e información sobre seguridad operacional obtenida de los SDCPS y bases de datos sobre seguridad operacional conexas.

Los análisis de datos e información sobre seguridad operacional llevados a cabo por el INAC tienen por objeto identificar peligros sistémicos e intersectoriales que quizá no sería posible identificar de otro modo mediante los procesos de análisis de datos sobre seguridad operacional de los proveedores de servicios o explotadores individuales.

RTA-19.5.3: Protección de datos e información sobre seguridad operacional

RTA-19-5.3.1: El INAC debe brindar protección a los datos sobre seguridad operacional recopilados por medio de los sistemas de notificación voluntaria de seguridad operacional y a la información sobre seguridad operacional derivada de dichos sistemas, así como a sus fuentes conexas (individuos u organizaciones), de conformidad con el Apéndice 3 de la presente RTA.

RTA-19.5.3.2: El INAC debe hacer extensiva la protección aludida en RTA-19.5.3.1 a los datos sobre seguridad operacional recopilados por medio de los sistemas de notificación obligatoria de seguridad operacional y a la información sobre seguridad operacional derivada de dichos sistemas, así como a sus fuentes conexas.

RTA-19.5.3.3: Con sujeción a lo dispuesto en RTA-19.5.3.1 y RTA-19.5.3.2 el INAC no debe proporcionar o utilizará los datos o información sobre seguridad operacional recopilados, almacenados o analizados de conformidad con RTA-19.5.1 y RTA-19.5.2 para fines que no sean los de mantener o mejorar la seguridad operacional, a menos que la autoridad competente determine que, de conformidad con el Apéndice 3 de la presente RTA se aplica un principio de excepción.

RTA-19.5.3.4: No obstante lo dispuesto en RTA-19.5.3.3 no se impedirá que el INAC utilice los datos e información sobre seguridad operacional para tomar medidas de carácter preventivo, correctivo o de rectificación que sean necesarias para mantener o mejorar la seguridad operacional de la aviación.

RTA-19.5.3.5: El INAC debe tomar las medidas necesarias, incluida la promoción de una cultura positiva de seguridad operacional para alentar las notificaciones de seguridad operacional mediante los sistemas aludidos en RTA-19.5.1.2 y RTA-19.5.1.3.

RTA-19.5.3.6: Las autoridades competentes del Estado de Nicaragua deben facilitar y promover las notificaciones de seguridad operacional armonizando sus leyes, reglamentos y políticas aplicables, según sea necesario.

RTA-19.5.3.7: Para apoyar la determinación a la que se hace referencia en RTA-19.5.3.3, las autoridades competentes del Estado de Nicaragua deben establecer y hacer uso de arreglos apropiados concertados con antelación entre sus autoridades encargadas de la seguridad operacional de la aviación y aquellas encargados de la administración de la justicia. Dichos arreglos deben tener en cuenta los principios establecidos en el Apéndice 3 de la presente RTA, los cuales pueden formalizarse mediante legislación, protocolos, acuerdos o memorandos de acuerdo.

RTA-19.5.4: Compartición e intercambio de información sobre seguridad operacional

RTA-19.5.4.1: Si al analizar la información contenida en su SDCPS, el INAC identifica asuntos relacionados con la seguridad operacional considerados de interés para otros Estados, el INAC debe facilitar dicha información sobre seguridad operacional lo antes posible. Antes de compartir dicha información, el INAC acordará con el otro u otros Estados el nivel de protección y las condiciones bajo las cuales se compartirá la información sobre seguridad operacional. El nivel de protección y las condiciones debe ser consecuente con el Apéndice 3 de la presente RTA.

RTA-19.5.4.2: El INAC debe promover el establecimiento de redes para compartir o intercambiar información sobre seguridad operacional entre los usuarios del sistema aeronáutico y debe facilitar la compartición y el libre intercambio de información sobre seguridad operacional, a menos que en la legislación nacional se disponga otra cosa.

CAPÍTULO VI: ACEPTACIÓN SMS Y OTRAS DISPOSICIONES

RTA-19.6.1: Aceptación del SMS

RTA-19.6.1.1 El SMS del proveedor de servicios debe adecuarse a la complejidad y realidad de la organización.

RTA-19.6.1.2 El INAC dará una Carta de Aceptación Inicial del SMS cuando se trate de un proveedor de servicios nuevo en proceso de certificación cuando el proveedor de servicios cumpla con la documentación de la Designación del Ejecutivo Responsable de Acuerdo al Apéndice 2, Análisis de Brechas y Plan de Implementación del SMS. Posteriormente, deberá cumplir con todo lo requerido por el Apéndice 2 de esta RTA 19 en relación a la Etapa 1,2,3 y 4.

RTA-19.6.1.3 El INAC realizará una evaluación a cada una de las 4 Etapas del SMS del Proveedor de Servicios y dará una Carta de Aceptación cuando cada etapa se considere satisfactoria de acuerdo a los requisitos establecidos en la presente RTA 19.

RTA-19.6.1.4 El INAC otorgará al proveedor de servicios una carta de Aceptación Completa del Sistema (SMS) y un Certificado de Aceptación del Sistema (SMS) cuando se hayan completado satisfactoriamente todas las etapas de implementación.

RTA-19.6.2: Aplicación de Sanciones

RTA-19.6.2.1: El proveedor de servicios con un SMS implementado se someterá a las regulaciones y normativas emitidas por el INAC para la aplicación de sanciones según corresponda.

APÉNDICE 1 ELEMENTOS CRITICOS (CE) DEL SISTEMA ESTATAL DE SUPERVISIÓN DE LA SEGURIDAD OPERACIONAL (SOO)

1. Legislación aeronáutica básica (CE-1)

1.1 El Estado de Nicaragua debe promulgar una legislación sobre aviación completa y efectiva, que sea acorde con la dimensión y complejidad de la actividad aeronáutica y que concuerde con los requisitos que figuran en el Convenio sobre Aviación Civil Internacional, para permitir la supervisión y gestión de la seguridad operacional de la aviación civil y el cumplimiento de los reglamentos por conducto de las autoridades u organismos competentes establecidos para dicho fin.

1.2 La legislación sobre aviación civil debe contener disposiciones que proporcionen al personal que lleva a cabo funciones de supervisión de la seguridad operacional acceso a las aeronaves, operaciones, instalaciones, personal y registros conexos, según convenga, de las personas y organizaciones que llevan a cabo una actividad aeronáutica.

2. Reglamentos de explotación específico (CE-2)

El INAC debe promulgar reglamentos que como mínimo cubran los requisitos nacionales dimanantes de su legislación aeronáutica básica, en lo que respecta a procedimientos operacionales, productos, servicios, equipo e infraestructura normalizados, de conformidad con los Anexos al Convenio sobre Aviación Civil Internacional.

3. Sistema y funciones estatales (CE-3)

3.1 El Estado de Nicaragua debe establecer autoridades u organismos competentes, según convenga, que cuenten con el apoyo de personal suficiente y cualificado y con recursos financieros adecuados para la gestión de la seguridad operacional.

3.2 Se deben establecer las funciones y los objetivos de seguridad operacional para las autoridades u organismos estatales, a fin de que cumplan sus responsabilidades de gestión de la seguridad operacional.

3.3 El INAC debe tomar las medidas necesarias en relación con, entre otras cosas, la remuneración y las condiciones de empleo, a fin de garantizar la contratación y retención de personal cualificado para que desempeñe funciones de supervisión de la seguridad operacional.

3.4 El INAC debe asegurarse de que el personal que desempeña funciones de supervisión de la seguridad operacional reciba la orientación sobre ética y conducta personal que le permita evitar conflictos de intereses reales o que se perciban en el desempeño de sus obligaciones oficiales.

3.5 El INAC debe aplicar una metodología para determinar sus requisitos de dotación de personal encargado de desempeñar funciones de supervisión de la seguridad operacional, teniendo en cuenta la dimensión y complejidad de las actividades de la aviación en Nicaragua.

4. Personal técnico cualificado (CE-4)

4.1 El INAC debe establecer los requisitos mínimos en relación con las cualificaciones del personal técnico que desempeña las funciones relacionadas con la seguridad operacional y debe tomar las medidas necesarias para ofrecer instrucción inicial y continua que resulte apropiada para mantener y mejorar la competencia de dicho personal al nivel deseado.

4.2 El INAC debe implantar un sistema para mantener registros de instrucción para el personal técnico.

5. Orientación técnica, instrumentos y suministro de información crítica en materia de seguridad operacional (CE-5)

5.1 El INAC debe proporcionar instalaciones apropiadas, textos de orientación y procedimientos de carácter técnico actualizado y completo, información crítica sobre seguridad operacional, instrumentos y equipo y medios de transporte, según convenga, al personal técnico para que éste desempeñe sus funciones de supervisión de la seguridad operacional con eficacia, de acuerdo con los procedimientos establecidos y de manera normalizada.

5.2 El INAC debe proporcionar a la industria de la aviación orientación técnica sobre la aplicación de los reglamentos pertinentes.

6. Obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y/o aprobaciones (CE-6)

El INAC debe implantar procesos y procedimientos documentados para garantizar que las personas y organizaciones que realizan una actividad aeronáutica cumplan los requisitos establecidos antes de que se les permita ejercer los privilegios que les otorga una licencia, un certificado, una autorización o una aprobación para llevar a cabo la actividad aeronáutica pertinente.

7. Obligaciones de vigilancia (CE-7)

El INAC debe implantar procesos de vigilancia documentados, definiendo y planificando inspecciones, auditorías y actividades de observación continua, a fin de asegurarse, en forma preventiva, de que los titulares de una licencia, certificado, autorización y aprobación en el ámbito de la aviación sigan cumpliendo los requisitos establecidos. Esto abarca la vigilancia del personal designado por la autoridad para que, en su nombre, desempeñe las funciones de supervisión de la seguridad operacional.

8. Solución de problemas de seguridad operacional (CE-8)

8.1 El INAC debe hacer uso de un procedimiento documentado para adoptar las medidas apropiadas, incluyendo medidas para el cumplimiento, que permitan resolver los problemas de seguridad operacional detectados.

8.2 El INAC debe asegurarse de que los problemas de seguridad operacional detectados se resuelvan de manera oportuna por medio de un sistema que permita observar y registrar el progreso, así como las medidas adoptadas por las personas y organizaciones que realizan una actividad aeronáutica, para solucionar los mismos.

INTENCIONALMENTE EN BLANCO

APÉNDICE 2 MARCO PARA UN SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL (SMS)

En el contexto de este Apéndice, en relación con los proveedores de servicios, el concepto de "obligación de rendición de cuentas" se refiere a una "obligación" que no puede delegarse, y "responsabilidades" se refiere a las funciones y actividades que pueden delegarse.

En este Apéndice se especifica el marco para la implantación y el mantenimiento de un SMS. El marco consta de cuatro componentes y doce elementos que constituyen los requisitos mínimos para la implantación de un SMS:

1. Política y objetivos de seguridad operacional

1.1 Compromiso de la dirección

1.1.1 El proveedor de servicios debe definir su política de seguridad operacional de conformidad con los requisitos nacionales e internacionales pertinentes. La política de seguridad operacional debe:

a) reflejar el compromiso de la organización respecto de la seguridad operacional, incluida la promoción de una cultura positiva de seguridad operacional;

b) incluir una declaración clara acerca de la provisión de los recursos necesarios para su puesta en práctica;

c) incluir procedimientos de presentación de informes en materia de seguridad operacional;

d) indicar claramente qué tipos de comportamientos son inaceptables en lo que respecta a las actividades de aviación del proveedor de servicios e incluir las circunstancias en las que no se pueden aplicar medidas disciplinarias;

e) estar firmada por el directivo responsable de la organización;

f) ser comunicada, apoyándola ostensiblemente, a toda la organización; y

g) ser examinada periódicamente para asegurarse de que siga siendo pertinente y apropiada para el proveedor de servicios.

1.1.2 Teniendo debidamente en cuenta su política de seguridad operacional, el proveedor de servicios debe definir 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, como se dispone en 3.1.2;

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.

En el Adjunto A de esta RTA se encuentra un ejemplo sobre cómo preparar una Declaración de Política de Seguridad Operacional para un proveedor de servicios.

1.2 Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional

El proveedor de servicios debe:

a) identificar al directivo que, independientemente de sus otras funciones, tenga la obligación de rendir cuentas, en nombre de la organización, respecto de la implantación y el mantenimiento de un SMS eficaz;

b) definir 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 de la administración superior;

c) determinar las responsabilidades de rendición de cuentas de todos los miembros de la administración, independientemente de sus otras funciones, así como las de los empleados, en relación con el rendimiento en materia de seguridad operacional de la organización;

d) documentar y comunicar la información relativa a la obligación de rendición de cuentas, las responsabilidades y las atribuciones de seguridad operacional de toda la organización; y

e) definir los niveles de gestión con atribuciones para tomar decisiones sobre la tolerabilidad de riesgos de seguridad operacional.

1.3 Designación del personal clave de seguridad operacional

El proveedor de servicios debe designar un gerente de seguridad operacional para ser responsable de la implantación y el mantenimiento del SMS. En el Adjunto C de esta RTA se encuentra una muestra de descripción del trabajo de un gerente de seguridad operacional para un proveedor de servicios.

Dependiendo de la dimensión del proveedor de servicios y la complejidad de sus productos o servicios de aviación, las responsabilidades de la implantación 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.

1.4 Coordinación de la planificación de respuestas ante emergencias

El proveedor de servicios a quien se le exige que establezca y mantenga un plan de respuesta ante emergencias para accidentes e incidentes en operaciones de aeronaves y otras emergencias de aviación debe garantizar 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 o productos.

1.5 Documentación SMS

1.5.1: El proveedor de servicios debe preparar y mantener un manual de SMS en el que se describa:

a) su política y objetivos de seguridad operacional;

b) sus requisitos del SMS;

c) sus procesos y procedimientos del SMS;

d) su obligación de rendición de cuentas, sus responsabilidades y las atribuciones relativas a los procesos y procedimientos del SMS; y

1.5.2 El proveedor de servicios debe preparar y mantener registros operaciones de SMS como parte de su documentación SMS. Orientación sobre el desarrollo de un Manual SMS figura como Adjunto D.

2. Gestión de riesgos de seguridad operacional

2.1 Identificación de peligros

2.1.1 El proveedor de servicios debe definir y mantener un proceso para identificar los peligros asociados a sus productos o servicios de aviación.

2.1.2 La identificación de los peligros se debe basar en una combinación de métodos reactivos y preventivos.

2.2. Evaluación y mitigación de riesgos de seguridad operacional

El proveedor de servicios debe definir y mantener un proceso que garantice el análisis, la evaluación y el control de riesgos de seguridad operacional asociados a los peligros identificados.

3. Aseguramiento de la seguridad operacional

3.1 Observación y medición del rendimiento en materia de seguridad

3.1.1 El proveedor de servicios debe desarrollar y mantener los medios para verificar el rendimiento en materia de seguridad operacional de la organización y para confirmar la eficacia de los controles de riesgo de seguridad operacional.
Un proceso de auditoría interna es un medio para verificar el cumplimiento de la reglamentación sobre seguridad operacional, que es el fundamento del SMS, y evaluar la eficacia de estos controles de riesgos de seguridad operacional y del SMS.

3.1.2 El rendimiento en materia de seguridad operacional del proveedor de servicios se debe verificar en referencia a los indicadores y las metas de rendimiento en materia de seguridad operacional del SMS para contribuir a los objetivos de la organización en materia de seguridad operacional.

3.2 Gestión del cambio

El proveedor de servicios debe definir y mantener un proceso para identificar los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus productos o servicios de aviación, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios.

3.3 Mejora continua del SMS

El proveedor de servicios debe observar y evaluar sus procesos SMS para mantener y mejorar continuamente la eficacia general del SMS.

4. Promoción de la seguridad operacional

4.1 Instrucción y educación

4.1.1 El proveedor de servicios debe crear y mantener un programa de instrucción en seguridad operacional que garantice que el personal cuente con la instrucción y las competencias necesarias para cumplir sus funciones en el marco del SMS.

4.1.2 El alcance del programa de instrucción en seguridad operacional debe ser apropiado para el tipo de participación que cada persona tenga en el SMS.

4.2 Comunicación de la seguridad operacional

El proveedor de servicios debe crear y mantener un medio oficial de comunicación en relación con la seguridad operacional que:

a) garantice que el personal conozca el SMS, con arreglo al puesto que ocupe;

b) difunda información crítica para la seguridad operacional;

c) explique por qué se toman determinadas medidas para mejorar la seguridad operacional; y

explique por qué se introducen o modifican procedimientos de seguridad operacional.

REQUISITOS ESPECÍFICOS DEL SMS RTA 19:

Etapa 1: Compromiso y Responsabilidades

1. Elemento 1.1 Compromiso de la Dirección (9.3)

1.1. Ejecutivo Responsable

1.1.1. Se debe Identificar al Ejecutivo Responsable a través de reunión de junta directiva u órgano máximo de la institución. El ejecutivo responsable puede ser un socio con autoridad dentro de la organización, el gerente o una autoridad que se considere que tenga la autoridad en temas de recursos humanos, financieros y legales dentro de la organización, así como para tomar acción en los riesgos de seguridad operacional y respuesta ante incidentes-accidentes o el gerente general cuando este sea principalmente el dueño o se encuentre definido en los estatutos que es el representante legal o tiene el poder sobre los asuntos de la organización.

1.1.2. Dentro de las responsabilidades del Ejecutivo Responsable, se debe encontrar la disposición de recursos para el rendimiento eficaz del SMS; la responsabilidad directa de la conducta de los asuntos de la organización; la autoridad final sobre las operaciones con certificación/aprobación de la organización, incluyendo la autoridad para detener o suspender la operación o actividad; el establecimiento y la promoción de la política de seguridad operacional; el establecimiento de los objetivos de seguridad operacional de la organización, actuación como promotor de la seguridad operacional en la organización; responsabilidad final para la resolución de todos los problemas de seguridad operacional; el establecimiento y mantenimiento de la competencia de la organización para aprender del análisis de los datos recopilados mediante sus sistemas de notificación de seguridad operacional

1.1.3. Las responsabilidades del ejecutivo responsable deben estar definidas dentro del perfil de puesto.

1.1.4. El ejecutivo responsable debe recibir Instrucción de SMS o se tiene un plan para brindarle instrucción SMS inicial y continua.

1.1.5. La documentación relacionada al cumplimiento de los requisitos anteriores, debe ser enviada al INAC para su aceptación.

2. Elemento 1.3: Designación del personal clave de seguridad operacional

2.1. Persona de SMS clave dentro de la organización que será responsable de administrar el SMS en nombre del ejecutivo responsable. (Gerente SMS)

2.1.1. El proveedor de servicios debe designar un Gerente SMS y que cumpla con los siguientes requisitos :

2.1.1.1. Personal con experiencia en el campo aeronáutico,

2.1.1.2. Experiencia operacional o Antecedentes técnicos para comprender los sistemas que respaldan las operaciones.
2.1.1.3.
2.1.1.4. Habilidades para relacionarse con las personas
2.1.1.5. Habilidades analíticas y de solución de problemas
2.1.1.6. Habilidades de gestión de proyectos
2.1.1.7. Habilidades de comunicaciones oral y escrita.
2.1.1.8. Nombramiento realizado por parte del Ejecutivo Responsable.
2.1.1.9. Responsabilidades y funciones definidas en el perfil de puesto.
2.1.1.10. Cuenta con relación directa y comunicación al Ejecutivo Responsable.
2.1.1.11. No tiene otra función que pueda entrar en conflicto con sus responsabilidades de gerente SMS, tales como la entrega de productos o servicios de la organización.
2.1.1.12. Cuenta con relación directa con todo el personal de la organización.
2.1.1.13. Nombramiento divulgado en la organización.

2.1.2. Entre las funciones que debe tener un Gerente de Seguridad Operacional definidas en su perfil de puesto se encuentran:

2.1.2.1. Gestionar el plan de implementación del SMS en nombre del ejecutivo responsable;
2.1.2.2. realizar/facilitar la identificación de peligros y el análisis de riesgos de seguridad operacional;
2.1.2.3. controlar las medidas correctivas y evaluar sus resultados;
2.1.2.4. proporcionar informes periódicos sobre el rendimiento en materia de la seguridad operacional de la organización;
2.1.2.5. mantener registros y documentación de la seguridad operacional;
2.1.2.6. planificar y facilitar capacitación constante de seguridad operacional para el personal;
2.1.2.7. proporcionar sugerencias independientes al Ejecutivo Responsable sobre asuntos de seguridad operacional;
2.1.2.8. controlar las preocupaciones de seguridad operacional en la industria de la aviación y su impacto percibido en las operaciones de la organización orientadas a la entrega de servicios;
2.1.2.9. coordinarse y comunicarse (en nombre del ejecutivo responsable) con la autoridad de vigilancia del Estado y otras entidades estatales, según sea necesario, sobre temas relacionados con la seguridad operacional; y
2.1.2.10. coordinarse y comunicarse (en nombre del ejecutivo responsable) con organizaciones internacionales sobre temas relacionados con la seguridad operacional.

2.2. Oficina de servicios de seguridad operacional

2.2.1. La organización debe designar un espacio físico para la oficina o gerencia de seguridad operacional.
2.2.2. debe integrarse formalmente en el organigrama de la organización, con relación directa al ejecutivo responsable.
2.2.3. La documentación anterior relacionada a la creación de la oficina, nombramiento del gerente SMS y la divulgación, debe ser enviada al INAC para su aceptación.

3. Elemento 1.1 Compromiso de la Dirección (9.3)

3.1. Equipo de implementación del SMS

3.1.1. El Equipo debe ser definido por el ejecutivo responsable.
3.1.2. Se debe garantizar un equipo por cada área que maneje la organización: AGA, ATS, Línea Aérea, OMA, Escuela de Instrucción que requiera un SMS.
3.1.3. Las funciones del equipo deben ser documentadas.
3.1.4. El equipo debe ser capacitado en SMS.

3.1.5. El equipo debe ser multidisciplinario con especialistas en las áreas correspondientes de alcance del SMS.
3.1.6. El equipo debe tener conocimientos de herramientas informáticas.
3.1.7. Se deben formular las funciones de los equipos de implementación, entre las que se encuentran la formulación e implementación de los procesos del SMS.
3.1.8. Los nombramientos, funciones, evidencia de divulgación y cualquier otra documentación asociada, deben ser enviados al INAC para su aceptación.

3.2. Alcance de las actividades de la organización (9.7.7)

3.2.1. La organización debe realizar una descripción del sistema de la organización con el que presta o genera los productos y servicios de aviación.
3.2.2. Se deben detectar los procesos y procedimientos actuales de la organización.
3.2.3. Se debe llevar a cabo un análisis de cultura organizacional.
3.2.4. Se deben definir las interfaces del SMS.
3.2.5. La organización debe definir a qué departamentos/áreas o divisiones será aplicable el SMS: (Áreas de AGA, Áreas de ATS, OMA, Áreas Administrativas, Proyectos, etc).

4. Elemento 1.5: Documentación SMS

4.1. Plan de implementación del SMS acerca de cómo se implementará el SMS sobre la base del sistema identificado y las brechas del proceso que se generan del análisis de Brechas.

4.1.1. Se debe completar un Análisis de Brechas del SMS.
4.1.2. Definir Actividades por etapas de acuerdo a RTA 19: Gestión de la Seguridad Operacional, en base al Análisis de Brechas, Alcance del SMS, descripción del Sistema y análisis de cultura organizacional.
4.1.3. Definir Responsables por actividad.
4.1.4. Definir Fechas de ejecución de cada actividad .
4.1.5. Revisión del Plan por el Gerente SMS y Aprobado por el Ejecutivo Responsable.
4.1.6. Toda la documentación asociada al cumplimiento de los requisitos anteriores, relacionada con el Plan de Implementación y el Análisis de Brechas aprobado por el Ejecutivo Responsable debe ser enviada al INAC para su aceptación.

5. Elemento 4.1: Instrucción y Educación

5.1. Necesidades de capacitación - Programa de Capacitación de Seguridad Operacional

5.1.1. Se debe conformar un Programa de Capacitación que, considerando los diferentes niveles de personal e involucramiento en el SMS y las actividades de aviación de la organización, contenga:
5.1.1.1. Instrucción SMS,
5.1.1.2. Estadísticas,
5.1.1.3. Gestión de Proyectos,
5.1.1.4. Investigación de Accidentes
5.1.1.5. Metodología de la Investigación
5.1.1.6. Sistemas de Gestión y Auditoría.
5.1.1.7. Peligro Aviario
5.1.1.8. Procesos del SMS, en dependencia de las responsabilidades del personal al SMS.
5.1.2. El Programa debe ser aprobado por el ejecutivo responsable.
5.1.3. El programa debe incluir Registros de la capacitación del personal.
5.1.4. La documentación anterior relacionada al programa de capacitación, ejecución y divulgación, debe ser enviada al INAC para su aceptación.

6. Elemento 4.2: Comunicación de la Seguridad Operacional

6.1. Canales de Comunicación de Seguridad Operacional.

6.1.1. Se deben crear Boletines de seguridad operacional establecidos

6.1.2. Sitio Web o Correo Electrónico establecido
6.1.3. Información divulgada a través de los medios.

6.2. Mecanismo de Comunicación.

6.2.1. Se debe establecer un mecanismo de comunicación que permita:
6.2.1.1. Definir las partes interesadas a quien se debe comunicar.
6.2.1.2. Definir la información que debe comunicarse.
6.2.1.3. Definir por qué medio se va a comunicar la información.
6.2.1.4. Definir cuándo se va a comunicar la información.
6.2.1.5. Definir quién va a comunicar la información
6.2.1.6. Definir una retroalimentación de la comunicación, de tal manera que se mejore el mecanismo y la efectividad de la comunicación.
6.2.1.7. Garantizar que el personal conozca el SMS, con arreglo al puesto que ocupe;
6.2.1.8. Difundir información crítica para la seguridad operacional;
6.2.1.9. Explicar por qué se toman determinadas medidas para mejorar la seguridad operacional; y
6.2.1.10. Explicar por qué se introducen o modifican procedimientos de seguridad operacional.

6.2.2. Formatos y Registros

6.2.2.1. Registro de retroalimentación de la comunicación.

Etapa 2: Responsabilidades y Respuesta ante Emergencias

7. Elemento 1.1 Compromiso de la Dirección.

7.1. Política de seguridad operacional

7.1.1. Se debe desarrollar una política de seguridad operacional.
7.1.2. La política debe reflejar el compromiso de la organización respecto de la seguridad operacional, incluida la promoción de una cultura positiva de seguridad operacional.
7.1.3. Debe Incluir una declaración clara acerca de la provisión de los recursos necesarios para su puesta en práctica.
7.1.4. Debe Incluir procedimientos de presentación de informes en materia de seguridad operacional.
7.1.5. Debe Indicar claramente qué tipo de comportamientos son inaceptables en lo que respecta a las actividades de aviación del proveedor de servicios e incluirá las circunstancias en las que no se podrían aplicar medidas disciplinarias de acuerdo a algún parámetro establecido (ej: Reason).
7.1.6. Debe estár firmada por el ejecutivo responsable de la organización.
7.1.7. Debe comunicarse, apoyándola visiblemente a toda la organización.
7.1.8. Debe contener disposiciones para revisarse periódicamente para garantizar que sigue siendo pertinente y adecuada para el proveedor de servicios.

7.2. Objetivos generales de seguridad operacional para el SMS: (9.3.4.7. - 4.2)

7.2.1. Los objetivos deben estar relacionados a Indicadores de rendimiento en materia de seguridad operacional, orientados usualmente a reducir los accidentes e incidentes.
7.2.2. Garantizar el compromiso de buscar un nivel aceptable de seguridad operacional.
7.2.3. Los objetivos deben estar orientados a procesos. (establecidos en términos de comportamientos esperados del personal operacional o el rendimiento de las acciones implementadas por la organización para manejar los riesgos: ej: incrementar los niveles de reporte de seguridad operacional)
7.2.4. Los objetivos deben estar orientados a salidas o resultados. (abarca acciones y tendencias con respecto a la contención de accidentes de pérdidas operacionales, Ej: reducir el número anual de eventos adversos en plataforma del año anterior).

7.3. *Obligación del proveedor de servicios de rendir cuentas y responsabilidades respecto de organizaciones externas*

7.3.1. Todo proveedor de servicios autorizado por el INAC, debe asegurar que cuando subcontrate los servicios de terceros, cumpla con:

7.3.1.1. Identificar a los subcontratistas u organizaciones externas que proporcionan productos o servicios para las actividades de aviación de la organización.

7.3.1.2. Identificar los servicios y productos que brindan los subcontratistas al proveedor de servicios.

7.3.1.3. Establecer que el subcontratista realizará una correcta identificación de peligros en los productos/servicios que le brindarán a la organización.

7.3.1.4. Definir una política que establezca claramente un flujo de responsabilidad y autoridad de seguridad operacional entre el proveedor de servicios y el subcontratista;

7.3.1.5.

7.3.1.6. Establecer indicadores de seguridad operacional/calidad para controlar el rendimiento del subcontratista, donde corresponda;

7.3.1.7. Incluir al subcontratista u organización externa en los mecanismos de promoción de la seguridad operacional del proveedor de servicios, para que se garantice que los empleados del subcontratista cuenten con las comunicaciones y políticas de seguridad operacional correspondientes de la organización.

7.3.1.8. Identificar cualquier papel, responsabilidad y función del subcontratista pertinente para el plan de respuesta ante emergencias del proveedor de servicios.

8. Elemento 1.2. Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional. (9.3.5)

8.1. Responsabilidades de la seguridad operacional y comunicación en toda la organización.

8.1.1. Se deben definir los participantes dentro del SMS.

8.1.2. Se debe definir la responsabilidad de cada participante dentro del SMS, incluyendo la administración superior y líderes de departamento.

8.1.3. Se debe documentar las responsabilidades de todos los participantes.

8.1.4. Las responsabilidades y funciones de SMS deben estar contenidas en los perfiles de puesto correspondientes.

8.1.5. Se deben definir los niveles de toma de decisiones referente a la tolerabilidad de riesgos de seguridad operacional.

8.1.6. Se debe comunicar a toda la organización, las responsabilidades dentro del SMS.

8.1.7. La documentación asociada al establecimiento y divulgación de las responsabilidades de seguridad operacional deben ser enviadas al INAC para su aceptación.

8.2. Grupos de acción de seguridad operacional (SAG). (9.3.6.9)

8.2.1. Se debe definir un SAG por cada área de especialidad dentro de la organización.

Nota 1: La propuesta de conformación de SAG durante la implementación, debería ser formulada por el/los equipos de implementación y deberían considerar la complejidad y tamaño de la organización.

Nota 2: La cantidad de SAG se puede establecer en dependencia del interés de la organización en medir el rendimiento de seguridad operacional en áreas específicas.

8.2.2. Los SAG deben estár conformados por personal técnico de las áreas en contacto directo e indirecto con las operaciones, incluyendo el Runway Safety Team (RST).

8.2.3. Deben existir Líneas de comunicación establecidas.

8.2.4. Los SAG deben tener comunicación directa con el Comité de Seguridad Operacional y Gerente del SMS.

8.2.5. Se deben establecer SAG locales en otras localizaciones o lugares de la organización para la identificación de peligros y gestión de riesgos. (9.4.6.6).

8.2.6. Se debe documentar la conformación y responsabilidades de los SAG.

8.2.7. Se debe comunicar en la organización, la conformación y responsabilidades de los SAG.

8.2.8. Se deben definir las funciones de los SAG, entre las que se encuentran:

8.2.8.1. Supervisan el rendimiento en materia de seguridad operacional dentro de las áreas funcionales de la organización y garantizan que se lleven a cabo las actividades de gestión de riesgos de seguridad operacional correspondientes, con participación del personal, según sea necesario, para generar conciencia de la seguridad operacional;

8.2.8.2. Coordinan la resolución de las estrategias de mitigación para las consecuencias de peligros identificadas y garantizan que existan disposiciones satisfactorias para la captura de los datos de seguridad operacional y los comentarios del empleado;

8.2.8.3. evalúan el impacto de la seguridad operacional relacionado con la introducción de cambios operacionales o nuevas tecnologías;

8.2.8.4. Coordinan la implementación de planes de medidas correctivas y garantizan que se tome la medida correctiva de forma oportuna;

8.2.8.5. revisan la eficacia de las recomendaciones de seguridad operacional anteriores; y

8.2.8.6. supervisan las actividades de promoción de la seguridad operacional, según sea necesario, para aumentar la conciencia de los empleados sobre temas de seguridad operacional y para garantizar que se les proporcione oportunidades adecuadas para participar en las actividades de la gestión de seguridad operacional.

8.2.9. La conformación, funciones y responsabilidades están aprobadas por el ejecutivo responsable.

8.2.10. La conformación y documentación asociada del SAG, incluyendo la divulgación, debe ser enviada al INAC para su aceptación.

8.3. Comité de coordinación de la seguridad operacional/SMS. (9.3.6.8)

8.3.1. El Comité debe ser conformado por personal directivo/ gerentes de área de la organización y Gerente SMS como parte activa del Comité.

8.3.2. Tratará temas estratégicos y toma de decisiones sobre el rendimiento en materia de SO y la asignación de recursos para garantizar las medidas de mitigación de riesgos.

8.3.3. Será Liderado por el Ejecutivo Responsable como Coordinador del Comité.

8.3.4. Se deben establecer Funciones y responsabilidades, nombrar a los miembros , mecanismo de modificación del reglamento del Comité y secuencia de reuniones.

8.3.5. Se debe realizar Promoción del Comité en la organización.

8.3.6. Se debe definir las funciones del Comité de Seguridad Operacional, entre las que se encuentran:

8.3.6.1. Controlar la eficacia del SMS;

8.3.6.2. controlar que se tome cualquier medida correctiva necesaria de forma oportuna;

8.3.6.3. controlar el rendimiento en materia de seguridad operacional en comparación con la política y los objetivos de seguridad operacional de la organización;

8.3.6.4. controlar la eficacia de los procesos de gestión de seguridad operacional de la organización, la que respalda la prioridad empresarial declarada de la gestión de seguridad operacional como otro proceso comercial principal;

8.3.6.5. controlar la eficacia de la supervisión de seguridad operacional de las operaciones subcontratadas; y

8.3.6.6. garantizar que los recursos correspondientes estén asignados para lograr el rendimiento en materia de seguridad operacional.

8.3.7. Su conformación y documentación relacionada, debe ser enviada al INAC para aceptación.

9. Elemento 1.4: Coordinación de la planificación de respuestas ante emergencias. ERP (Ap.7 Cap 5 9859 3ra ed. – 9.3.7 4ta ed.)

Considerando aquellos proveedores de servicios a quienes se les exige que establezcan y mantengan un plan de respuesta ante emergencias para accidentes e incidentes en operaciones de aeronaves y otras emergencias de aviación, la presente RTA 19 requiere que esos planes de emergencia cumplan con los siguientes requisitos.

9.1. El ERP o procedimientos de contingencia debe estar documentado.

9.2. El ERP debe ser adecuado para la envergadura, naturaleza y complejidad de la organización.

9.3. El ERP debe abordar escenarios de emergencia/crisis posibles o probables relacionados con las entregas de productos o servicios de la aviación de la organización.
9.4. El ERP debe incluir procedimientos para la producción, la entrega y el respaldo seguros y continuos de los productos o servicios de la aviación durante tales emergencias o contingencias.
9.5. El ERP debe contar con un plan de ensayos o ejercicios.
9.6. Los ensayos o ejercicios del ERP deben llevarse a cabo de acuerdo al plan y el resultado de los ensayos efectuados se documentan.
9.7. El ERP debe abordar la integración relevante con organizaciones del cliente o el subcontratista, donde corresponda.
9.8. El ERP debe contar con coordinaciones con otras organizaciones para hacer frente a un accidente de gran magnitud.
9.9. El ERP debe contar con un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continua, considerando en el equipo de revisión a la oficina de SMS.
9.10. El documento ERP debe estar presente en la biblioteca de la oficina SMS.
9.11. El ERP debe ser aprobado por el Ejecutivo Responsable.

10. Elemento 1.5: Documentación SMS (9.3.8)

10.1. Sistema de documentación de SMS para describir, guardar, recuperar y archivar toda la información y los registros relacionados con SMS:

10.1.1. Se debe desarrollar un Manual SMS con las siguientes características:
10.1.1.1. Es un manual independiente o una sección distinta dentro de un manual institucional controlado existente, ejemplo: Sección X Manual de Aeródromo;
10.1.1.2. Contiene el Control de documento del Manual indicando su lista de distribución, cuál es la relación con otros manuales de la organización, disposiciones de revisión tales como: cuándo se revisa, quién lo revisa, quién lo aprueba, cómo se envía a la autoridad para aceptación.
10.1.1.3. Establece los requisitos reglamentarios del SMS o el marco del SMS contenido en la presente RTA 19.;
10.1.1.4. Incluye una descripción de todo el sistema SMS.
10.1.1.5. Identifica el alcance e integración del sistema de gestión de la seguridad operacional;
10.1.1.6. Incluye la Política de seguridad operacional;
10.1.1.7. Establece los Objetivos de seguridad operacional;
10.1.1.8. Establece las Responsabilidades de la seguridad operacional y personal clave;
10.1.1.9. Contiene cómo se realizará la Notificación de seguridad operacional y medidas correctivas;
10.1.1.10. Establece como se realizará la Identificación de peligros y evaluación de riesgos;
10.1.1.11. Establece como se realizará la observación y medición del rendimiento en materia de seguridad operacional;
10.1.1.12. Establece como se realizarán las Investigaciones relacionadas con la seguridad operacional y medidas correctivas;
10.1.1.13. Establece como se realizará la Capacitación y comunicación de seguridad operacional;
10.1.1.14. Indica cómo funcionará la Mejora continua y auditoría de SMS;
10.1.1.15. Establece como se realizará la Gestión de los registros de SMS;
10.1.1.16. Indica cómo funcionará la Gestión de cambio; y
10.1.1.17. Contiene un resumen del Plan de respuesta ante emergencias/contingencia.
10.1.2. Se debe establecer un sistema de archivo de SMS para recopilar y mantener los registros actuales en relación con los procesos de SMS constantes de la organización;
10.1.3. Se debe mantener registros para proporcionar una referencia histórica, así como también, el estado actual de todos los procesos de SMS, como, por ejemplo: un registro de peligros; un índice de evaluaciones de seguridad operacional completadas; registros de capacitación de SMS/ seguridad operacional; los SPI actuales y los objetivos de seguridad operacional asociados; informes de auditoría interna de SMS y externa; actas de la reunión del comité de SMS/seguridad operacional y el plan de implementación de SMS;

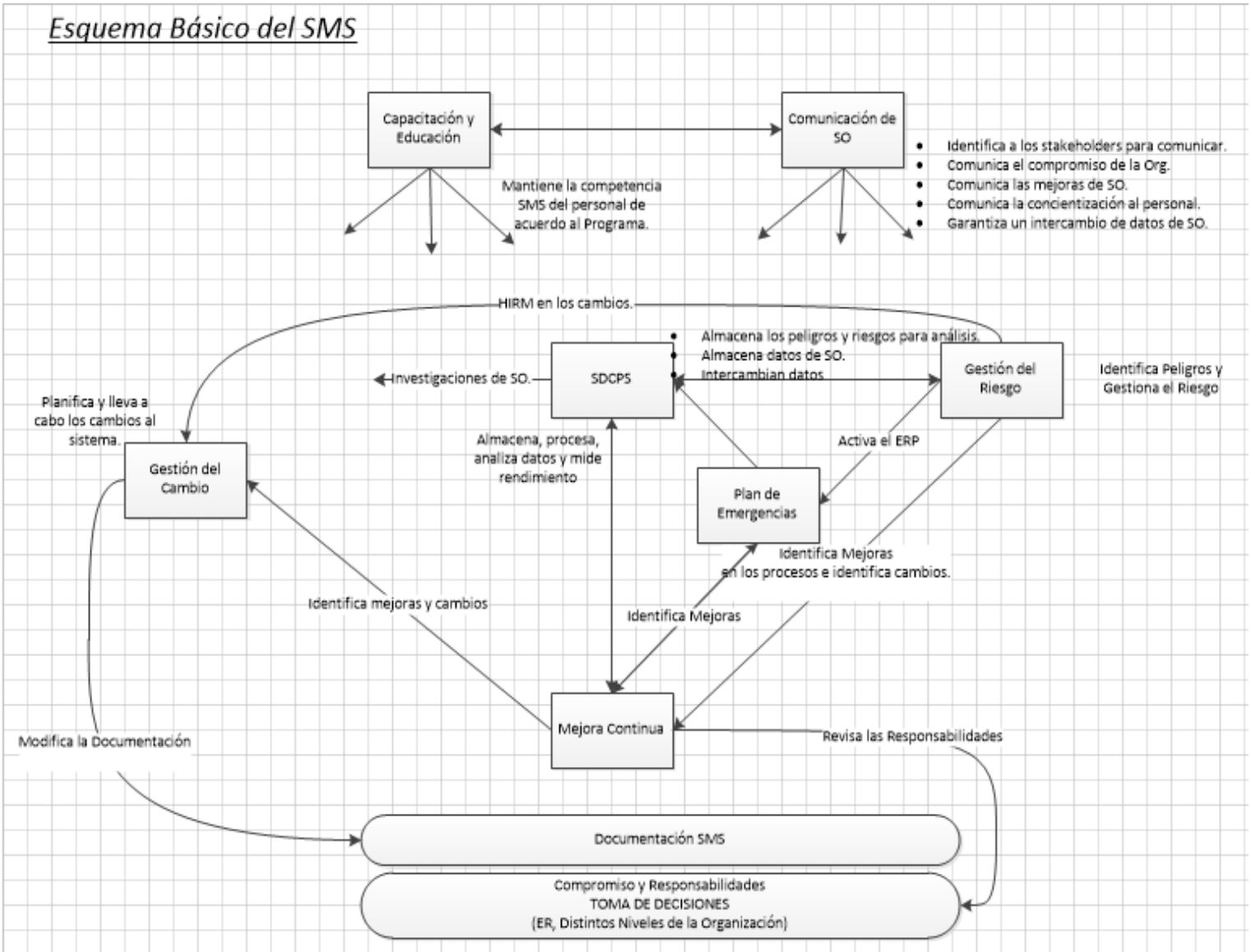
10.1.4. El Manual SMS de la organización y la evidencia del sistema de archivos, incluyendo la divulgación del Manual, debe ser enviada al INAC para su aceptación.

Etapa 3 del SMS: Procesos Específicos del SMS

Durante la primera y segunda etapa de implementación del SMS, se establecen las bases del SMS, siendo Responsabilidades, Compromiso, Documentación y Planes de Emergencia/Contingencia. En esta sección, la RTA 19 establece los requisitos para el montaje de los procesos específicos del SMS.

Esta sección de procesos específicos se estructura de la siguiente manera: primeramente, se identifica el proceso, posteriormente se establecen los requisitos de los procesos, incluyendo la definición de entradas y salidas, de tal manera que se pueda establecer una correcta integración o conexión de procesos del SMS de acuerdo a la realidad o complejidad de la organización, posteriormente se detalla con lo que debe de contar el proceso para realizar sus actividades, por último, se enumeran los formatos y registros que se requieren llevar dentro del proceso.

Un esquema sencillo de la interacción de los procesos del SMS se indica a continuación, el proveedor de servicios puede incluir más interacciones entre sus procesos en dependencia de su configuración y características de la organización.



11. Elemento 2.1: Proceso de Gestión de Riesgos de Seguridad Operacional (HIRM o SRM) (9.4 – 2.5)

El proceso de gestión de riesgos incluye la Identificación de Peligros, Evaluación del Riesgo (Determinar la Probabilidad del riesgo, Determinar la Gravedad del Riesgo, Determinar la tolerabilidad), Tomar las medidas correspondientes para tratar el riesgo, Evaluar las Medidas, Mejorar las Medidas y el proceso, entre otras actividades descritas a continuación.

Fuente: Doc. 9859: Manual de Gestión de Seguridad Operacional.

5-16 *Manual de gestión de la seguridad operacional (SMM)*

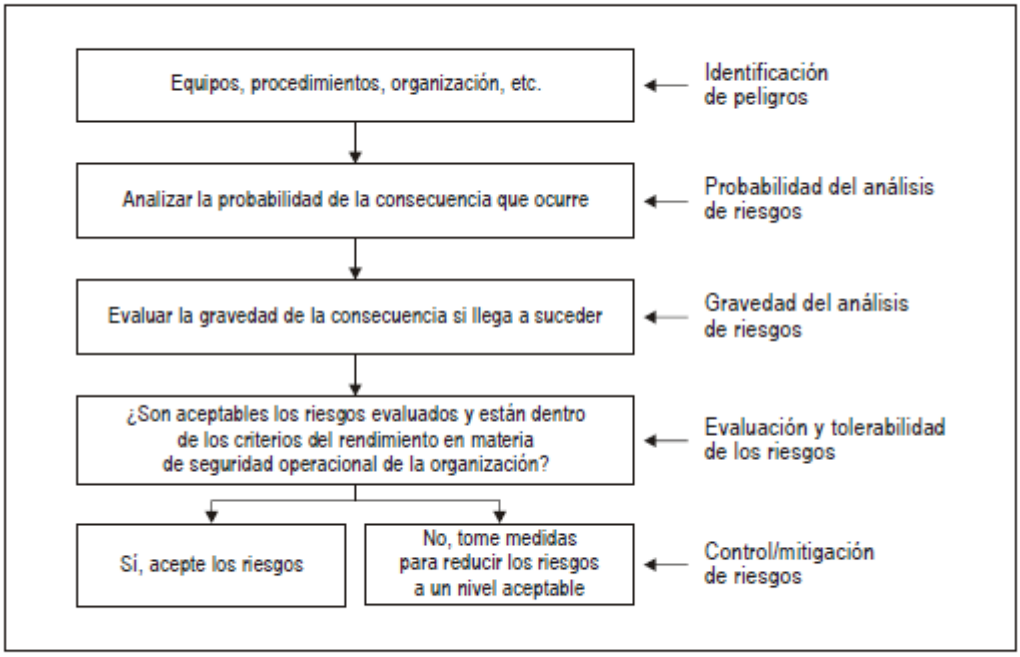


Figura 5-2. El proceso de gestión de riesgos de la seguridad operacional

11.1. Generalidades

11.1.1. El proceso debe establecer las responsabilidades de todos los involucrados de la organización en relación a Identificación de Peligros y Gestión de Riesgo.

11.1.2. El proceso debe ser aprobado por el Ejecutivo Responsable.

11.1.3. El proceso debe ser comunicado a toda la organización.

11.2. Entradas y salidas

Las entradas corresponden a los insumos para que el proceso pueda ejecutar sus actividades y tener así los resultados esperados. Durante el montaje del SMS, el proveedor de servicios debe identificar las entradas y salidas de sus procesos.

11.2.1. El proceso debe tener definidas las entradas necesarias para realizar la identificación de peligros y gestión de riesgos.

11.2.2. Se debe definir las salidas o resultados del proceso de gestión de riesgos.

11.3. Las actividades del proceso de gestión de riesgos deben incluir:

11.3.1. Elemento 2.1: Identificación de peligros.

11.3.1.1. El procedimiento debe incluir la identificación de peligros a partir de los procesos de la organización, equipos e instalaciones que intervienen en la entrega de productos o servicios de aviación.

11.3.1.2. El procedimiento debe incluir la identificación de peligros a partir de los Reportes de la notificación voluntaria.

11.3.1.3. El procedimiento debe incluir la identificación de peligros a partir de la revisión de reportes de accidentes/incidentes externos para la mitigación de riesgos donde corresponda.

11.3.1.4. El procedimiento debe incluir la identificación de peligros a partir del monitoreo normal de las operaciones, sistemas de monitoreo automatizado (si se cuenta), auditorías, retroalimentación de la capacitación, investigaciones del proveedor de servicios.

11.3.1.5. El procedimiento debe incluir la identificación de peligros a partir de la revisión de reportes de fuentes externas oextraoficiales. , sistemas de reporte obligatorio y voluntario del Estado, auditorías de terceras partes para el Estado.

11.3.1.6. El procedimiento debe incluir que durante la identificación de peligros se tome en consideración los siguientes factores:

11.3.1.6.1. Descripción del sistema.

11.3.1.6.2. Factores de diseño, como el diseño del equipo y las tareas

11.3.1.6.3. limitaciones del desempeño humano (por ejemplo, fisiológico, sicológico y cognitivo)

11.3.1.6.4. procedimientos y prácticas de operación, como su documentación y las listas de verificación bajo condiciones de operación reales

11.3.1.6.5. factores de comunicación, como medios, terminología e idioma

11.3.1.6.6. factores institucionales, como aquellos relacionados con el reclutamiento, capacitación y retención de personal, la compatibilidad de metas de producción y seguridad operacional, la asignación de los recursos, las presiones de operación y la cultura de seguridad operacional empresarial

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

11.3.1.6.8. factores de vigilancia reglamentaria, como la aplicabilidad y ejecutabilidad de los reglamentos y la certificación del equipo, el personal y los procedimientos.

11.3.1.6.9. sistemas de control de rendimiento que pueden detectar desviaciones de la práctica o desviaciones operacionales

11.3.1.6.10. factores de la interfaz humano-máquina

11.3.1.6.11. factores relacionados a las interfaces del SMS con otras organizaciones.

11.3.1.7. El proceso debe contar con procedimientos para la investigación de seguridad operacional de peligros y ocurrencias por parte del proveedor de servicios. Los procedimientos deben incluir:

11.3.1.7.1. Establecimiento de línea de tiempo de eventos claves y las acciones de las personas involucradas.

11.3.1.7.2. Revisión de cualquier política y procedimiento relacionado a las actividades.

11.3.1.7.3. Revisión de cualquier decisión realizada relacionada al evento.

11.3.1.7.4. Identificación de cualquier control de riesgo establecido que debió haber prevenido la ocurrencia del evento.

11.3.1.7.5. Revisión de cualquier data de seguridad operacional en busca de eventos similares previos.

Nota: Se pueden utilizar distintas taxonomías sugeridas por el Manual de Gestión de la Seguridad Operacional: Doc. 9859.

11.3.1.8. El procedimiento debe incluir los activadores de cuándo realizar o no una investigación de seguridad operacional, incluyendo

11.3.1.8.1. La severidad o potencial seguridad de la consecuencia.

11.3.1.8.2. Requerimientos regulatorios u organizacionales para llevar a cabo una investigación.
11.3.1.8.3. Valor de seguridad operacional a ser obtenido.
11.3.1.8.4. Oportunidades para que acciones de seguridad operacional sean tomadas.
11.3.1.8.5. Riesgos asociados con no investigar.
11.3.1.8.6. Tendencias identificadas
11.3.1.8.7. Oportunidades y beneficios que sirvan para capacitación.
11.3.1.8.8. Disponibilidad de recursos.

11.3.2. Elemento 2.2: Evaluación y mitigación de riesgos de seguridad operacional- Evaluación

11.3.2.1. Procedimiento de evaluación de riesgos de la seguridad operacional.

11.3.2.1.1. Se debe establecer un procedimiento en el que se establece que se defina los riesgos asociados al peligro identificado.
11.3.2.1.2. El procedimiento debe establecer quienes realizan la definición de los riesgos y su evaluación, incluyendo expertos cuando no se tenga suficiente información disponible sobre el peligro (9.4.6.5)
11.3.2.1.3. El procedimiento debe establecer los niveles de probabilidad que puede tener un riesgo.
11.3.2.1.4. El procedimiento debe establecer los niveles de gravedad que puede tener un riesgo.
11.3.2.1.5. El procedimiento debe establecer una matriz de riesgo o mapa de calor en la que se identifique los niveles de tolerabilidad del índice de los riesgos operacionales y de producción de la organización.
11.3.2.1.6. El procedimiento debe establecer como calcular el índice de riesgo y la tolerabilidad.
11.3.2.1.7. El procedimiento debe incluir la priorización de los riesgos que le permita (9.4.6.7.):
11.3.2.1.7.1. Evaluar y controlar los riesgos de seguridad operacional más altos.
11.3.2.1.7.2. Colocar recursos a los riesgos de seguridad operacional más altos.
11.3.2.1.7.3. Mantener o mejorar efectivamente la seguridad operacional.
11.3.2.1.7.4. Alcanzar los objetivos de seguridad operacional establecidos y acordados y metas de seguridad operacional.
11.3.2.1.7.5. Satisfacer los requerimientos de las regulaciones del Estado de Nicaragua en relación al control de riesgos de seguridad operacional.

11.3.3. Elemento 2.2: Evaluación y mitigación de riesgos de seguridad operacional- Mitigación o Tratamiento del riesgo.

11.3.3.1. El procedimiento debe definir cuáles son las estrategias para el tratamiento del riesgo identificado, entre las que se encuentran:
11.3.3.1.1. *Prevención:* La actividad se suspende a causa de que los riesgos de seguridad operacional asociados son intolerables o se consideran inaceptables en comparación con los beneficios asociados.
11.3.3.1.2. *Reducción*: Se acepta cierta exposición de riesgos de seguridad operacional, aunque la gravedad o probabilidad asociada con los riesgos se aminora, posiblemente mediante medidas que mitigan las consecuencias relacionadas.
11.3.3.1.3. *Segregación de la exposición*: Medida tomada para aislar la posible consecuencia relacionada con el peligro o para establecer varias capas de defensas contra ella.
11.3.3.2. El proceso debe definir que se tome en consideración el factor humano o especialistas como una parte integral en identificar mitigaciones efectivas. (2.5.7.3)

11.3.3.3. El procedimiento debe incluir que se examinen al menos las siguientes perspectivas cuando se identifican y evalúan las medidas de mitigación: (2.5.7.4)

11.3.3.3.1. Efectividad
11.3.3.3.2. Costo/Beneficio
11.3.3.3.3. Practicidad
11.3.3.3.4. Aceptabilidad
11.3.3.3.5. Exigibilidad
11.3.3.3.6. Durabilidad
11.3.3.3.7. Riesgos residuales
11.3.3.3.8. Consecuencias Involuntarias
11.3.3.3.9. Tiempo

11.3.3.4. El procedimiento establecerá que se definirán los responsables para las medidas que se tomen y fechas de implementación, considerando los niveles de decisión para tales medidas.

11.3.4. Elemento 2.2: Evaluación y mitigación de riesgos de seguridad operacional – Evaluación de las medidas (2.5.7.5).

11.3.4.1. El procedimiento debe establecer la evaluación o monitoreo de las medidas a implementar en el tratamiento del riesgo, para verificar la eficacia de las medidas o resultado esperado.

11.3.5. Mejora del Proceso

11.3.5.1. Se debe establecer disposiciones para que el proceso sea revisado constantemente.

11.4. Formatos y Registros

- Formato de Identificación de peligros
- Formato de Matriz de Riesgos
- Registro de Peligros
- Registro de Evaluaciones de Riesgos
- Registro de las medidas tomadas.
- Registro de verificación o monitoreo de las medidas de mitigación implementadas.
- Registro de mejoras del proceso.

12. Elemento 3.1: Proceso de Recopilación, Procesamiento y Análisis de Datos de Seguridad Operacional (SDCPS). Observación y medición del rendimiento en materia de seguridad operacional (9.5.4 – 4 – 5 – 6 – 7)

Este proceso es parte del Componente 3 del SMS: Aseguramiento de la Seguridad Operacional. En esta parte, se requiere que el proveedor de servicios desarrolle y mantenga los medios para verificar el rendimiento de seguridad operacional de la organización y valide la efectividad de los controles de riesgo de seguridad operacional. El aseguramiento de seguridad operacional consiste en procesos y actividades emprendidas a determinar si el SMS está operando de acuerdo a las expectativas y requerimientos. Esto envuelve continuamente el monitoreo de sus procesos, así como su entorno operacional para detectar cambios o desviaciones que pueden producir riesgos emergentes de seguridad operacional o la degradación de los controles existentes de seguridad operacional. Tales controles o desviaciones pueden ser dirigidos a través del proceso de Gestión de Riesgos.

A continuación se detallan los requisitos para el Proceso de Recopilación, Procesamiento y Análisis de Datos, este proceso, tiene principalmente como entrada los datos de los distintos mecanismos de notificación, tanto obligatoria como voluntaria, resultados de auditorías o estudios de seguridad operacional, resultado de la vigilancia por parte del INAC, informes de accidentes e incidentes, detalles relacionados a la capacitación, datos de procesos organizacionales y demás que pueda almacenarse para una posterior salida que sirva para la identificación de peligros y toma de decisiones basada en datos. **El proceso SDCPS debe cumplir con los siguientes requisitos específicos:**

12.1. Generalidades

12.1.1. El proceso debe establecer las responsabilidades y la interacción de los involucrados de la organización en relación a la recopilación, procesamiento y análisis de datos de seguridad operacional.

12.1.2. El proceso debe ser aprobado por el Ejecutivo Responsable.

12.1.3. El proceso debe ser comunicado a toda la organización.

12.2. Entradas y salidas

12.2.1. Se debe definir cuáles son las entradas o los datos que se van a colectar a raíz de los diferentes mecanismos de colección de datos del SDCPS.

12.2.2. Se debe definir cuáles son las salidas o resultados del SDCPS, incluyendo los informes de análisis de seguridad operacional.

12.3. Las actividades para la observación y medición del rendimiento en materia de seguridad operacional deben cumplir los siguientes requisitos:

12.3.1. Recopilación, Captura o Colección de Datos.

12.3.1.1. Los procedimientos para la colección de datos deben definir que se recopilen datos a partir de los diferentes mecanismos, considerando:

12.3.1.1.1. Mecanismos de Contribución Voluntaria

12.3.1.1.2. Mecanismos de Notificación Obligatoria

12.3.1.1.2.1. Este mecanismo contempla la Notificación de Accidentes/incidentes graves a la Agencia Nacional de Investigación de Accidentes (ANIA) del Estado de Nicaragua y al INAC.

12.3.1.1.2.2. Este mecanismo contempla la notificación de ocurrencias al INAC que no sean accidentes/incidentes graves.

12.3.1.1.3. Estudios de seguridad operacional

12.3.1.1.4. Investigaciones de seguridad operacional

12.3.1.1.5. Encuestas de seguridad operacional

12.3.1.1.6. Auditorias de seguridad operacional

12.3.1.1.7. Hallazgos y recomendaciones de seguridad operacional de la vigilancia de seguridad operacional del Estado de Nicaragua.

12.3.1.1.8. Procesos Organizacionales y su comportamiento.

12.3.1.1.9. Sistemas de colección de datos operacional (FDA) si aplica de acuerdo a lo establecido por RTA OPS 1.

12.3.1.1.10. Otras fuentes

12.3.1.2. Se deben definir los procedimientos para los mecanismos de recopilación anteriores.

12.3.1.3. Los procedimientos deben definir que se designe a un custodio de los sistemas de reportes o notificación.

12.3.2. Procesamiento

12.3.2.1. Los procedimientos para el procesamiento de los datos, deben definir que se revise la **Calidad de los datos** que se están colectando, considerando:

12.3.2.1.1. **Limpieza:** Consiste en detectar o corregir registros incorrectos e inexactos de un conjunto de registros, tabla o base de datos y se refiere a identificar partes incompletas, incorrectas, imprecisa o irrelevante de la data y luego reemplazarla, modificarla o eliminar la suciedad de la data.

12.3.2.1.2. Relevancia: Consiste en la data que reúne las necesidades de la organización y representa sus más importantes problemas. Una organización debería evaluar la relevancia de la data basada en sus necesidades y actividades.

12.3.2.1.3. Puntualidad: La puntualidad de la data e información de seguridad operacional es una función de su actualidad. La data usada para toma de decisiones debería reflejar qué está pasando en tiempo real tanto como sea

posible. El juicio es a menudo requerido basado en la volatilidad de la situación. Por ejemplo, la data colectada dos años atrás en un tipo de aeronave que sigue volando la misma ruta, sin cambios significativos, puede proveer una reflexión oportuna de la situación. Mientras, la data recopilada una semana atrás en un tipo de aeronave que ya no está en servicio puede no proveer una significativa y oportuna reflexión de la realidad actual.

12.3.2.1.4. Precisión y exactitud: la precisión de la data se refiere a los valores correctos y reflejan el escenario como fue descrito. La imprecisión de la data comúnmente ocurre cuando los usuarios ingresan un valor equivocado o hacen un error de tipografía o digitación. Este problema puede sobreponerse teniendo personal con habilidades y entrenamiento sobre digitación de la data o teniendo componentes en la aplicación tal como el chequeo deletreado. Los valores de los datos pueden volverse imprecisos a lo largo del tiempo, también conocido como decaimiento de la data. El movimiento es otra causa de data imprecisa. Como la data sea extraída, transformada o movida de una base de datos hacia otra, puede ser alterada en algún grado, especialmente si el software no es robusto.

12.3.2.2. Los procedimientos deben establecer la **Agregación de data e información de seguridad operacional.**

La agregación de data está referida a que la data e información es recogida y almacenada en el SDCPS de la organización y expresada en forma de resumen para el análisis. El agregar data e información significa colectarla y juntarla, resultando en data más grande.

12.3.2.3. Los procedimientos deben establecer la **Fusión de la Data.**

La fusión de la data es el proceso de combinar múltiples conjuntos de datos. La integración del conjunto de data de seguridad operacional seguida por su reducción o reemplazo mejora la confiabilidad y usabilidad de dicha data. Además, por ejemplo, data proveniente de los sistemas FDA de los operadores aéreos podría combinarse o fusionarse con data meteorológica y radar para obtener un conjunto más útil de datos para posterior procesamiento.

12.3.2.4. Los procedimientos deben establecer el **Filtro de la data de seguridad operacional y seguridad de información.**

Los filtros de data de seguridad operacional se refieren a un rango de estrategias o soluciones para refinar los conjuntos de datos. Esto significa que los conjuntos de datos son refinados en simplemente lo que el tomador de decisiones necesita, sin incluir otra data que puede ser repetitiva, irrelevante o incluso sensible. Diferentes tipos de filtros de datos pueden ser utilizados para generar reportes, resultados de consultas u otras vías para comunicar resultados.

12.3.3. Análisis

12.3.3.1. Los procedimientos deben definir los tipos de análisis de datos de seguridad operacional que realizará el proveedor de servicios. Entre los que se encuentran:

12.3.3.1.1. Análisis Descriptivo: habilita a los usuarios a presentar y ver la data en una manera más significativa, permitiendo interpretación más simple de la data. Herramientas tales como tablas y matrices, así como gráficos y mapas son ejemplos de herramientas usadas para resumir data. La estadística descriptiva incluye la medición de tendencia central tal como la media, la mediana y la moda, así como también mide la variabilidad tal como el rango, cuartiles, mínimo y máximo, distribución de frecuencia, varianza y desviación estándar (SD).

12.3.3.1.2. Análisis Inferencial: estadística inferencial o inductiva apunta al uso de data para aprender acerca de una población más grande en la muestra que se presenta. No siempre es conveniente o posible examinar cada ítem de una población entera y tener acceso a toda la población. La estadística inferencial

son técnicas que permiten a los usuarios tener acceso a data disponible para hacer generalizaciones, inferencias y conclusiones sobre una población de la cual fueron tomadas muestras para describir tendencias. Estas incluyen métodos para la estimación de parámetros, pruebas de hipótesis estadísticas, comparaciones del desempeño del rango de dos grupos en la misma medición para identificar diferencias o similitudes e identificar posibles correlaciones y relaciones entre las variables.

12.3.3.1.3. Análisis Predictivo: otro tipo de análisis incluye la probabilidad de análisis predictivo que extrae información de data histórica y actual y la usa para predecir tendencias y patrones de comportamiento. Los patrones encontrados en la data ayudan a identificar riesgos emergentes y oportunidades. A menudo el evento desconocido de interés está ubicado en el futuro, pero el análisis predictivo puede ser aplicado a cualquier tipo de evento en el pasado, presente o futuro. El núcleo del análisis predictivo se basa en la captura de relaciones entre variables de las ocurrencias del pasado y explotarlas para predecir lo desconocido por venir. Algunos sistemas permiten a los usuarios modelar diferentes escenarios de riesgos u oportunidades con diferentes resultados. Esto habilita a los tomadores de decisiones a evaluar las decisiones que pueden tomar para enfrentar diferentes circunstancias desconocidas y evaluar cómo pueden efectivamente colocar recursos limitados hacia las áreas donde existen los mayores riesgos o mejores oportunidades.

12.3.3.1.4. Análisis Combinados: varios tipos de análisis estadísticos están interconectados y son a menudos conducidos juntos. Por ejemplo, una técnica inferencial puede ser la herramienta principal usada para sacar conclusiones en relación a un conjunto de datos, pero la estadística descriptiva también es usualmente usada y presentada. También, las salidas o resultados de las estadísticas inferenciales son a menudo usadas como la base del análisis predictivo.

12.3.3.2. El procedimiento debe establecer quiénes interactúan en la realización los análisis de seguridad operacional.

Nota Importante 1: El numeral 2.3.3. establecido en esta RTA, establece que esos análisis son al menos los que debería incluir su proceso de SDCPS. La forma en cómo realizar estos análisis se puede encontrar en una bibliografía específica sobre Metodología de la Investigación: Ejemplo: Libro Metodología de la Investigación – Editorial McGrawHill.

Nota Importante 2: El manejo de estos métodos debe ser parte del programa de capacitación SMS de los proveedores de servicios, tal como se especifica en el punto de Instrucción y Educación de la Seguridad Operacional de esta RTA 19.

12.3.4. Entrega de los Análisis.

12.3.4.1. Los procedimientos de reporte de los resultados de análisis de seguridad operacional, deben definir que se identifique y realce para los tomadores de decisiones y gerentes como parte de los resultados de análisis lo siguiente:

12.3.4.1.1. La toma inmediata de acciones correctivas.

12.3.4.1.2. Implementación de vigilancia basada en riesgo

12.3.4.1.3. Definir o afinar la política de seguridad operacional y objetivos de seguridad operacional.

12.3.4.1.4. Definir o afinar indicadores de rendimiento de seguridad operacional

12.3.4.1.5. Definir o afinar metas de rendimiento de seguridad operacional.

12.3.4.1.6. Establecer activadores de los indicadores de seguridad operacional

12.3.4.1.7. Promover la seguridad operacional

12.3.4.1.8. Conducir posteriores evaluaciones de riesgos de seguridad operacional.

12.3.4.2. Los procedimientos de reporte de los resultados de análisis de seguridad operacional identifican las formas en que los mismos se pueden entregar, incluyendo:

12.3.4.2.1. Alertas inminentes de seguridad operacional.
12.3.4.2.2. Reportes de análisis de seguridad operacional
12.3.4.2.3. Conferencias de seguridad operacional.

12.3.5. Intercambio de Datos

12.3.5.1. Los procedimientos deben establecer el intercambio de datos de seguridad operacional con otros sectores de la aviación.

12.3.6. Indicadores

12.3.6.1. El proveedor de servicios debe definir una línea base de rendimiento de seguridad operacional, la cual es el punto de partida para establecer los posteriores indicadores, metas y alertas de seguridad operacional. (4.4.3.)
12.3.6.2. El proveedor de servicios debe definir una descripción de qué va a medir el indicador.
12.3.6.3. debe definir el propósito del indicador
12.3.6.4. Las unidades de medida y cualquier requerimiento para su cálculo.
12.3.6.5. Quién es responsable de colectar, validar y monitorear el indicador.
12.3.6.6. Dónde y cómo debe ser recopilada la data.
12.3.6.7. La frecuencia de reporte, recopilación, monitoreo y análisis de los datos de los indicadores.
12.3.6.8. Swe debe definir los indicadores de rendimiento de alto impacto de seguridad operacional.
12.3.6.8.1. Los indicadores de alto impacto están orientados a eventos reactivos de baja probabilidad/alta severidad (accidentes e incidentes serios – Excursiones de pista/1000 aterrizajes.), alta probabilidad/baja severidad (ej: avistamiento de aves o detecciones de aves en radar, número de aproximaciones desestabilizadas/1000 aterrizajes.).
12.3.6.9. Se debe definir los indicadores de rendimiento de bajo impacto de seguridad operacional.
12.3.6.9.1. Los indicadores de bajo impacto están orientados a procesos y sus insumos y los cambios en el entorno operacional (% del personal que ha completado satisfactoriamente y a tiempo el entrenamiento de seguridad operacional o la frecuencia de las actividades de ahuyentar aves, % de pilotos que han recibido entrenamiento en procedimientos de aproximaciones estabilizadas, % de sitios que han implementado X procedimiento producto de un cambio).
12.3.6.10. Se han definido las metas de seguridad operacional.
12.3.6.10.1. Las metas están asociadas a los objetivos de seguridad operacional.
12.3.6.10.2. Las metas se han definido con base en el criterio SMART:
12.3.6.11. Se debe definir las alertas para los indicadores de seguridad operacional
12.3.6.12. Los indicadores están soportados por los datos estadísticos correspondientes.
12.3.6.13. La data estadística de soporte está autorizada y avalada por el Ejecutivo Responsable.
12.3.6.14. El proveedor de servicios debe definir procedimientos para la revisión, mejora e introducción de nuevos indicadores, metas y alertas de rendimiento seguridad operacional. Considerando:
12.3.6.14.1. De manera rutinaria, en concordancia con el ciclo periódico establecido y acordado por el Comité de Seguridad Operacional.
12.3.6.14.2. Basado en insumos de los análisis de seguridad operacional.
12.3.6.14.3. En respuesta a cambios en la operación, los riesgos más altos o el entorno.
12.3.6.15. Se ha logrado un acuerdo con el INAC sobre el rendimiento de seguridad operacional.

12.3.7. Protección de la Información de seguridad operacional.

12.3.7.1. El proveedor de servicios debe tener procedimientos para la protección de los datos y fuentes de datos de seguridad operacional, proveniente de los distintos métodos de recopilación de datos de seguridad operacional.

12.3.7.2. Los procedimientos se encuentran alineados a la Normativa para la Protección de las Fuentes de Información del INAC.

12.4. Registros y Formatos.

12.4.1. Formatos de notificación
12.4.2. Registro de tipos de sucesos notificados.
12.4.3. Registro estadístico de sucesos de alto impacto.
12.4.4. Registro estadístico de sucesos de bajo impacto.
12.4.5. Registro de cantidad de operaciones del operador.
12.4.6. Indicadores de rendimiento.

13. Elemento 3.2: Proceso de La Gestión del Cambio (9.5.5.)

La gestión del cambio, es un proceso formal para identificar, administrar o llevar a cabo los cambios dentro de una organización asociados con sus productos o servicios de aviación y que podrían afectar el nivel de riesgos de seguridad operacional, así como para identificar y gestionar los riesgos de seguridad operacional que puedan emerger de aquellos cambios una vez implementados.

13.1. Generalidades

13.1.1. El proceso debe establecer las responsabilidades de todos los involucrados de la organización en relación a la gestión del cambio.
13.1.2. El proceso debe ser aprobado por el Ejecutivo Responsable.
13.1.3. El proceso debe ser comunicado a toda la organización y partes interesadas.

13.2. Entradas y Salidas del Proceso

13.2.1. El proceso debe definir las entradas o insumos necesarios para que se ejecuten las actividades necesarias para llevar a cabo una gestión de los cambios en la organización. Las entradas deben considerarse en base a los siguientes factores (la siguiente lista puede ampliarse de acuerdo a la realidad de cada organización). (9.5.5.1.)

13.2.1.1. Expansión o contracción organizacional.
13.2.1.2. Mejoras en el negocio que impacten la seguridad, esto puede resultar en cambios a los sistemas internos, procesos o procedimientos que soporten la entrega segura de productos y servicios.
13.2.1.3. Cambios en el ambiente operacional de la organización.
13.2.1.4. Cambios a las interfaces del SMS con organizaciones externas.
13.2.1.5. Cambios externos relacionados a la reglamentación, cambios económicos y riesgos emergentes.
13.2.1.6. Introducción de nueva tecnología o equipamiento
13.2.1.7. Cambios en el personal clave de la organización.
13.2.1.8. Cambios significativos en los niveles de staff.
13.2.1.9. Reestructuración de la organización.
13.2.1.10. Cambios físicos tales como nuevas instalaciones o bases, cambios de diseño del aeródromo, otros.

13.2.2. El proceso tiene definidas las salidas o resultados necesarios producto de las actividades que se llevaron a cabo para gestionar los cambios en la organización. Una de las salidas que debe considerar el proceso es:

13.2.2.1. La revisión en la descripción del sistema de la organización cada vez que se implemente un cambio. (9.5.5.4.)

Nota: Puede ser que existan organizaciones en las que sus actividades y procedimientos de gestión de cambio sean más complejos e incluyan la Gestión de Proyectos como actividades principales para planificar y ejecutar dichos cambios.

13.3. Las actividades del proceso deben incluir:

13.3.1. Identificación del cambio

13.3.1.1. Los procedimientos establecen que se identifiquen y comprendan los cambios a realizar dentro de la organización, incluyendo una descripción del cambio y por qué está siendo implementado. (9.5.5.7.)

13.3.1.2. Los procedimientos establecen que se defina y comprenda quién y qué va a afectar el cambio, pudiendo ser individuos dentro de la organización, otros departamentos o personal externo u organizaciones. Equipos, sistemas y procesos también pueden ser impactados. Una revisión de la descripción del sistema y las interfaces de las organizaciones podría necesitarse. Esta es una oportunidad para determinar quién debería estar involucrado en el cambio. Los cambios podrían afectar controles de riesgos establecidos para mitigar otros riesgos y además, el cambio podría incrementar riesgos en áreas que no serían visibles inmediatamente.

13.3.2. Evaluación del impacto del cambio.

13.3.2.1. Los procedimientos establecen que se identifiquen los peligros relacionados al cambio y llevar a cabo una evaluación de riesgos de seguridad operacional, esto debería identificar cualquier riesgo directamente relacionado al cambio. El impacto en los peligros existentes y controles de riesgo de seguridad operacional que podrían ser afectados por el cambio deberían también ser revisados. Este paso debería utilizar el proceso existente de identificación de peligros y gestión de riesgos de la organización

13.3.2.2. Los procedimientos establecen que durante la evaluación se considere:

13.3.2.2.1. Criticidad: Qué tan crítico es el cambio? Considerar el impacto en sus actividades de la organización y su impacto en otras organizaciones y el sistema de aviación.

13.3.2.2.2. Disponibilidad de expertos en la materia. Es importante que miembros claves de la comunidad de aviación estén envueltos en las actividades de gestión de cambio. Esto puede incluir individuos de organizaciones externas.

13.3.2.2.3. Disponibilidad de datos e información de seguridad operacional. Qué información está disponible que pueda ser utilizada para dar información en la situación y establecer el análisis en el cambio a realizar.

13.3.3. Planificación y realización de la introducción del cambio.

13.3.3.1. Se ha definido el desarrollo de un plan de acción, este debe definir que será realizado, por quién y para cuándo. Debe haber un plan claro describiendo cómo el cambio será implementado y quién será responsable para cuáles acciones, así como la secuencia y la programación de cada tarea.

13.3.3.2. Se ha definido la aprobación del cambio, esto para confirmar que el cambio es seguro para implementar. La persona con la responsabilidad general y la autoridad para implementar el cambio debería firmar el plan del cambio.

13.3.4. Evaluación del cambio

13.3.4.1. Se ha definido un plan de aseguramiento, esto es para determinar qué acciones de seguimiento son necesarias. Considere cómo el cambio será comunicado y si las actividades adicionales (tales como auditorías) son necesarias durante o después del cambio.

13.4. Formatos y Registros

13.4.1. Registro de identificación de cambios
13.4.2. Evaluaciones de riesgos asociadas a los cambios.
13.4.3. Registros de cambios realizados.
13.4.4. Registros de evaluaciones posteriores
13.4.5. Registro de acciones de seguimiento a tomar.

14. Elemento 3.3: Mejora continua del SMS (9.5.6)

14.1. Generalidades

14.1.1. Los mecanismos de mejora continua deben establecer las responsabilidades de todos los involucrados de la organización en relación a la mejora continua.

14.1.2. Los métodos de mejora continua deben ser aprobados por el Ejecutivo Responsable.

14.1.3. Los métodos deben ser comunicados a toda la organización.

14.2. Métodos para la mejora continua.

14.2.1. El proveedor de servicios debe establecer diferentes mecanismos para garantizar la mejora continua, entre los que se encuentran:

14.2.1.1. Auditorías: esto incluye auditorías internas y auditorías llevadas a cabo por otras organizaciones (auditorías externas).

14.2.1.2. Evaluaciones: incluye evaluaciones de cultura de seguridad operacional y efectividad del SMS.

14.2.1.3. Monitoreo de ocurrencias: monitoreo de la recurrencia de eventos de seguridad operacional incluyendo accidentes e incidentes, así como errores y situaciones de violación de las normas.

14.2.1.4. Encuestas de seguridad operacional: incluyen encuestas culturales que proveen retroalimentación útil en el compromiso del personal con el SMS. También puede proveer un indicador de la cultura de seguridad operacional de la organización.

14.2.1.5. Revisiones por la Dirección: examinar si los objetivos de seguridad operacional están siendo alcanzados por la organización y sea una oportunidad para mirar toda la información disponible de rendimiento de seguridad operacional para identificar tendencias en general. Es importante que la Dirección revise la efectividad del SMS. Esto puede ser llevado a cabo como una de las funciones del Comité de Seguridad Operacional.

14.2.1.6. Evaluación de Indicadores y metas de rendimiento de seguridad operacional: como parte de la revisión por la dirección, considera tendencias y cuando la data apropiada está disponible, puede ser comparada con otro proveedor de servicios o la data global del Estado.

14.2.1.7. Direccionamiento de lecciones aprendidas: proveniente de los sistemas de reporte de seguridad operacional y de las investigaciones de seguridad operacional del proveedor de servicios. Esto debe liderar a que las mejoras de seguridad operacional sean implementadas.

14.3. Resultados de los métodos

14.3.1. Los resultados de los métodos de mejora continua se utilizarán para mejorar los diferentes procesos de la organización y el rendimiento de seguridad operacional.

14.4. Formatos y Registros

14.4.1. Estructura del Programa/Plan de Auditoría
14.4.2. Listas de chequeo de auditorías
14.4.3. Registro de No Conformidades
14.4.4. Registro de acciones correctivas.
14.4.5. Encuestas de seguridad operacional.
14.4.6. Registro de la revisión por la Dirección
14.4.7. Registro de lecciones aprendidas.
14.4.8. Otros necesarios para los diferentes métodos de mejora.

Etapa 4 del SMS

15. Elemento 1.1: Compromiso y responsabilidad de la gestión.

15.1. Mejora del Procedimiento disciplinario, la política existente con una debida consideración de errores/ equivocaciones accidentales de las infracciones deliberadas/graves.

15.1.1. Se debe considerar para este tratamiento alguna metodología (ej: algoritmo de condiciones inseguras de James Reason).
15.1.2. Se debe definir en el procedimiento las acciones para actuar en caso de violaciones o errores.
15.1.3. El comité de seguridad operacional se debe revisar las acciones a tomarse en caso de errores o violaciones.
15.1.4. El Ejecutivo Responsable deb aprobar el procedimiento disciplinario.
15.1.5. Se debe comunicar y capacitar a todo el personal respecto del tratamiento de los errores y violaciones.

INTENCIONALMENTE EN BLANCO

APÉNDICE 3. PRINCIPIOS PARA LA PROTECCIÓN DE DATOS E INFORMACIÓN SOBRE SEGURIDAD OPERACIONAL Y LAS FUENTES CONEXAS

La protección de los datos y la información sobre seguridad operacional y las fuentes conexas es esencial para garantizar su continua disponibilidad, ya que el uso de datos e información sobre seguridad operacional para fines que no sean los de mantener y mejorar la seguridad operacional puede impedir la disponibilidad futura de esos datos e información y tener un importante efecto adverso en dicha seguridad.

1 Principios generales

1.1 El INAC, por medio de sus leyes, reglamentos y políticas nacionales que protejan los datos y la información sobre seguridad operacional, y las fuentes conexas, debe garantizar que:

a) exista un equilibrio entre la necesidad de proteger los datos y la información sobre seguridad operacional y las fuentes conexas, y la de administrar debidamente la justicia, a fin de mantener o mejorar la seguridad operacional de la aviación;

b) se protejan los datos y la información sobre seguridad operacional y las fuentes conexas, de conformidad con este Apéndice; y

c) se especifiquen las condiciones bajo las cuales los datos, la información sobre seguridad operacional y las fuentes conexas califican para ser protegidos; y

d) se mantengan disponibles los datos y la información sobre seguridad operacional para los fines de mantener o mejorar la seguridad operacional de la aviación.

La protección de los datos y la información sobre seguridad operacional, así como de las fuentes conexas, no debe tener como intención interferir con la debida administración de la justicia ni con el mantenimiento o el mejoramiento de la seguridad operacional.

1.2 Cuando se ha instituido una investigación de conformidad con la RTA 13, los registros relativos a las investigaciones de accidentes e incidentes que se enumeran en la RTA-13.099 de dicha RTA deben estar sujetos a la protección acordada en dicha disposición en lugar de la protección acordada en virtud de este Apéndice.

2 Principios de protección

2.1 El INAC debe asegurarse de que los datos y la información sobre seguridad operacional no se utilicen para:

a) procedimientos disciplinarios, civiles, administrativos y penales contra empleados, personal de operaciones u organizaciones;

b) la divulgación al público; o

c) para fines que no sean mantener o mejorar la seguridad operacional;

a menos que se aplique un principio de excepción.

2.2 El INAC debe conceder protección a los datos y la información sobre seguridad operacional, así como a las fuentes conexas garantizando que:

a) se especifique la protección con base en la naturaleza de los datos y la información sobre seguridad operacional;

b) se establezca un procedimiento formal para proteger los datos y la información sobre seguridad operacional y las fuentes conexas, dicho procedimiento puede incluir el requisito de que toda persona que solicite la divulgación de datos o información sobre seguridad operacional presente justificaciones para su divulgación;

c) los datos y la información sobre seguridad operacional no se utilizarán para fines distintos de aquellos para los que fueron recopilados, a menos que se aplique un principio de excepción; y

d) en la medida en que se aplique un principio de excepción, se debe garantizar de que el uso de datos e información sobre seguridad operacional en procedimientos disciplinarios, civiles, administrativos y penales, se llevará a cabo sólo bajo garantías autorizadas, dichas garantías incluyen limitaciones o restricciones legales tales como órdenes de protección, audiencias a puerta cerrada, exámenes a puerta cerrada y no revelación de las identidades de los datos para la utilización o divulgación de información sobre seguridad operacional en procedimientos judiciales o administrativos.

3. Principios de excepción

El INAC debe hacer excepciones respecto de la protección de los datos y la información sobre seguridad operacional y las fuentes conexas, sólo cuando:

a) 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, o a un acto doloso o una actividad criminal;

b) después de efectuar un examen de los datos o la información sobre seguridad operacional, 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; o

c) después de efectuar un examen de los datos o información sobre seguridad operacional, determine 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.

4 Divulgación al público

4.1 Considerando que el Estado de Nicaragua dispone de la Ley de Acceso a la Información Pública (Ley 621), el INAC debe crear, en el contexto de las solicitudes de divulgación al público, excepciones respecto a la divulgación al público para garantizar la continua confidencialidad de los datos y la información sobre seguridad operacional que se han suministrado voluntariamente.

4.2 Cuando se hace la divulgación de conformidad con la RTA-19.150, el INAC debe asegurarse de que:

a) la divulgación al público de información personal pertinente incluida en los datos o la información sobre seguridad operacional cumple las leyes de confidencialidad que resulten aplicables; o

b) la divulgación al público de los datos o la información sobre seguridad operacional se hace sin revelar las identidades y en forma resumida o combinada.

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

El INAC se debe asegurar de que cada SDCPS cuente con un custodio designado para que aplique la protección a los datos e información sobre seguridad operacional, de conformidad con las disposiciones aplicables de este Apéndice.

6 Protección de los datos registrados

6.1 El INAC debe proporcionar, por medio de las leyes y reglamentos nacionales, medidas específicas de protección en relación con el carácter confidencial y el acceso del público a las grabaciones ambiente de las conversaciones en el lugar de trabajo.

6.2 El INAC, por medio de las leyes y reglamentos nacionales, debe considerar las grabaciones ambiente de las conversaciones en el lugar de trabajo exigidas por las leyes y reglamentos nacionales como datos privilegiados y protegidos sujetos a los principios de protección y excepción que figuran en este apéndice.

INTENCIONALMENTE EN BLANCO

ADJUNTO A EJEMPLO DE UNA DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD OPERACIONAL

La seguridad operacional es una de nuestras funciones comerciales 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, mientras prestamos nuestros servicios.

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 con [Funcionario ejecutivo principal director ejecutivo/o lo que corresponda para la organización].

Nuestro compromiso es para:

respaldar 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 con la misma atención a los resultados como la atención a los resultados de otros sistemas de gestión de la organización;

- 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 la entrega del 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 nuestro 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 el logro diligente de estos; 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) _____
Director ejecutivo/o quien corresponda

ADJUNTO B LISTA DE VERIFICACIÓN DEL ANÁLISIS DE BRECHAS Y PLAN DE IMPLANTACIÓN DEL SMS

1. Lista de verificación del análisis de brechas inicial

La lista de verificación del análisis de brechas inicial puede usarse como una plantilla para realizar el primer paso de un análisis de brechas del SMS. Este formato con sus respuestas generales "Sí/No/Parcial" proporciona una indicación inicial del amplio alcance de las brechas y, por lo tanto, la carga de trabajo general que puede esperarse. El cuestionario puede ajustarse para adaptarse a las necesidades de la organización y a la naturaleza del producto o servicio suministrado. Esta información inicial debe ser útil para que la administración superior anticipe la escala del esfuerzo de implementación del SMS y, por lo tanto, los recursos que se deben proporcionar. Esta lista de verificación inicial necesita de seguimiento con un plan de implementación adecuado.

Una respuesta "Sí" indica que la organización satisface o supera las expectativas de la pregunta en cuestión. Una respuesta "No" indica una brecha importante en el sistema existente, en relación con la expectativa de la pregunta. Una respuesta "Parcial" indica que se requiere una posterior mejora o trabajo de desarrollo para un proceso existente a fin de satisfacer las expectativas de la pregunta.

Núm.	*Aspecto que debe analizarse o pregunta que debe responderse*	*Pregunta*	*Estado de implementación*
Componente 1 — POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL			
Elemento 1.1 — Compromiso y responsabilidad de la gestión			
1.1-1	¿Está implementada una política de seguridad operacional?	☐ Si ☐ No ☐ Parcial	
1.1-2	¿Refleja la política de seguridad operacional el compromiso de la administración superior acerca de la gestión de la seguridad operacional?	☐ Si ☐ No ☐ Parcial	
1.1-3	¿Es adecuada la política de seguridad operacional según la envergadura, naturaleza y complejidad de la organización?	☐ Si ☐ No ☐ Parcial	
1.1-4	¿Es pertinente la política de seguridad operacional para la seguridad operacional de la aviación?	☐ Si ☐ No ☐ Parcial	
1.1-5	¿Ha firmado el ejecutivo responsable la política de seguridad operacional?	☐ Si ☐ No ☐ Parcial	
1.1-6	¿Se comunica la política de seguridad operacional, con un respaldo visible, en toda la [Organización]?	☐ Si ☐ No ☐ Parcial	
1.1-7	¿Se revisa periódicamente la política de seguridad operacional para garantizar que siga siendo pertinente y adecuada para la [Organización]?	☐ Si ☐ No ☐ Parcial	
Elemento 1.2 — Responsabilidades de la seguridad operacional			

1.2-1	¿Ha identificado [Organización] a un ejecutivo responsable que, sin importar otras funciones, tenga la máxima responsabilidad, en nombre de [Organización], de la implementación y mantenimiento del SMS?	☐ Si ☐ No ☐ Parcial	
1.2-2	¿Tiene el ejecutivo responsable total control de los recursos financieros y humanos necesarios para las operaciones autorizadas que se realizarán según el certificado de operaciones?	☐ Si ☐ No ☐ Parcial	
1.2-3	¿Tiene el ejecutivo responsable la autoridad final sobre todas las actividades de aviación de su organización?	☐ Si ☐ No ☐ Parcial	
1.2-4	¿Ha identificado y documentado [Organización] las responsabilidades de seguridad operacional de la gestión, así como también, del personal de operaciones, en relación con el SMS?	☐ Si ☐ No ☐ Parcial	
1.2-5	¿Existe un comité de seguridad operacional o consejo de revisión para el propósito de revisión del SMS y el rendimiento en materia de seguridad operacional?	☐ Si ☐ No ☐ Parcial	
1.2-6	¿Lidera al comité de seguridad operacional un ejecutivo responsable o un delegado asignado correctamente, confirmado debidamente en el manual del SMS?	☐ Si ☐ No ☐ Parcial	
1.2-7	¿Incluye el comité de seguridad operacional a líderes de departamento u operacionales pertinentes, según corresponda?	☐ Si ☐ No ☐ Parcial	
1.2-8	¿Existen grupos de acción de seguridad operacional que trabajan junto con el comité de seguridad operacional (en particular para las organizaciones grandes/complejas)?	☐ Si ☐ No ☐ Parcial	
Elemento 1.3 — Nombramiento del personal de seguridad operacional clave			
1.3-1	¿Ha asignado [Organización] a una persona calificada para gestionar y vigilar la operación diaria del SMS?	☐ Si ☐ No ☐ Parcial	
1.3-2	¿Tiene la persona calificada acceso o notificación directa al ejecutivo responsable, acerca de la implementación y operación del SMS?	☐ Si ☐ No ☐ Parcial	
1.3-3	¿Tiene el gerente responsable de administrar el SMS otra responsabilidad más que pueda entrar en conflicto o perjudicar su papel como gerente de SMS?	☐ Si ☐ No ☐ Parcial	
1.3-4	¿Es el puesto de gerente de SMS un puesto administrativo superior que no es inferior jerárquicamente o subordinado a otros puestos operacionales o de producción?	☐ Si ☐ No ☐ Parcial	

Elemento 1.4 — Coordinación de la planificación de respuesta ante emergencias			
1.4-1	¿Tiene [Organización] un plan de respuesta ante emergencias/contingencia adecuado para la envergadura, naturaleza y complejidad de la organización?	☐ Si ☐ No ☐ Parcial	
1.4-2	¿Aborda el plan de emergencia/contingencia todos los escenarios de emergencia/crisis posibles o probables, en relación con los suministros de productos o servicios de aviación de la organización?	☐ Si ☐ No ☐ Parcial	
1.4-3	¿Incluye el ERP procedimientos para la producción, la entrega y el respaldo seguros y continuos de los productos o servicios de la aviación durante tales emergencias o contingencias?	☐ Si ☐ No ☐ Parcial	
1.4-4	¿Existe un plan y registro para los ensayos o ejercicios en relación con el ERP?	☐ Si ☐ No ☐ Parcial	
1.4-5	¿Aborda el ERP la coordinación necesaria de sus procedimientos de respuesta ante emergencias/contingencia con los procedimientos de contingencia de emergencia/respuesta de otras organizaciones, donde corresponda?	☐ Si ☐ No ☐ Parcial	
1.4-6	¿Tiene [Organización] un proceso para distribuir y comunicar el ERP a todo el personal pertinente, incluidas las organizaciones externas pertinentes?	☐ Si ☐ No ☐ Parcial	
1.4-7	¿Existe un procedimiento para la revisión periódica del ERP para garantizar su relevancia y eficacia continuas?	☐ Si ☐ No ☐ Parcial	
Elemento 1.5 — Documentación de SMS			
1.5-1	¿Existe un resumen de SMS de nivel superior o documento de exposición que esté aprobado por el gerente responsable y aceptado por la CAA?	☐ Si ☐ No ☐ Parcial	
1.5-2	¿Aborda la documentación del SMS el SMS de la organización y sus componentes y elementos asociados?	☐ Si ☐ No ☐ Parcial	
1.5-3	¿Está el marco de trabajo de SMS de [Organización] en alineación con el marco de trabajo del SMS reglamentario?	☐ Si ☐ No ☐ Parcial	
1.5-4	¿Mantiene [Organización] un registro de documentación de respaldo pertinente para la implementación y operación del SMS?	☐ Si ☐ No ☐ Parcial	
1.5-5	¿Tiene [Organización] un plan de implementación de SMS para establecer su proceso de implementación de SMS, incluidas las tareas específicas y sus hitos de implementación pertinentes?	☐ Si ☐ No ☐	

		Parcial	
1.5-6	¿Aborda el plan de implementación de SMS la coordinación entre el SMS del proveedor de servicios y el SMS de las organizaciones externas, donde corresponde?	☐ Si ☐ No ☐ Parcial	
1.5-7	¿Respalda el ejecutivo responsable el plan de implementación de SMS?	☐ Si ☐ No ☐ Parcial	
Componente 2 — GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL			
Elemento 2.1 — Identificación de peligros			
2.1-1	¿Existe un proceso para la notificación de peligros/amenazas voluntaria de todos los empleados?	☐ Si ☐ No ☐ Parcial	
2.1-2	¿Es simple la notificación de peligros/amenazas voluntaria, está disponible a todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios?	☐ Si ☐ No ☐ Parcial	
2.1-3	¿Incluye el SDCPS de [Organización] procedimientos para la notificación de incidentes/accidentes mediante personal operacional o producción?	☐ Si ☐ No ☐ Parcial	
2.1-4	¿Es simple la notificación de incidentes/accidentes, es accesible para todo el personal involucrado en tareas relacionadas con la seguridad operacional y es proporcional a la envergadura del proveedor de servicios?	☐ Si ☐ No ☐ Parcial	
2.1-5	¿Tiene [Organización] procedimientos para la investigación de todos los incidentes/accidentes notificados?	☐ Si ☐ No ☐ Parcial	
2.1-6	¿Existen procedimientos para garantizar que los peligros/amenazas identificados o descubiertos durante los procesos de investigación de incidentes/accidentes se explican correctamente y se integran en la recopilación de peligros y el procedimiento de mitigación de riesgos de la organización?	☐ Si ☐ No ☐ Parcial	
2.1-7	¿Existen procedimientos para revisar peligros/amenazas de informes industriales pertinentes para medidas de seguimiento o la evaluación de riesgos, donde corresponda?	☐ Si ☐ No ☐ Parcial	
Elemento 2.2 — Evaluación y mitigación de riesgos de seguridad operacional			
2.2-1	¿Existe un procedimiento de identificación de peligros y mitigación de riesgos (HIRM) documentado que implique el uso de herramientas de análisis de riesgos objetivas?	☐ Si ☐ No ☐ Parcial	
2.2-2	¿Aprobaron los gerentes de departamento o un nivel superior los informes de evaluación de riesgos, donde corresponda?	☐ Si ☐ No ☐ Parcial	
2.2-3	¿Existe un procedimiento para la revisión periódica de los registros de mitigación de riesgos existentes?	☐ Si ☐	

		☐ No ☐ Parcial	
2.2-4	¿Existe un procedimiento para explicar las medidas de mitigación cada vez que se identifican niveles de riesgos inaceptables?	☐ Si ☐ No ☐ Parcial	
2.2-5	¿Existe un procedimiento para priorizar los peligros identificados para las medidas de mitigación de riesgos?	☐ Si ☐ No ☐ Parcial	
2.2-6	¿Existe un programa para la revisión sistemática y progresiva de todas las operaciones, los procesos, las instalaciones y los equipos relacionados con la seguridad operacional de la aviación sujetos al proceso de HIRM, como lo identificó la organización?	☐ Si ☐ No ☐ Parcial	
Componente 3 — ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL			
Elemento 3.1 — Control y medición del rendimiento en materia de seguridad operacional			
3.1-1	¿Existen indicadores de rendimiento en materia de seguridad operacional identificados para medir y controlar el rendimiento en materia de seguridad operacional de las actividades de aviación de la organización?	☐ Si ☐ No ☐ Parcial	
3.1-2	¿Son pertinentes los indicadores de rendimiento en materia de seguridad operacional para la política de seguridad operacional de la organización, así como también, los objetivos/metas de seguridad operacional de alto nivel?	☐ Si ☐ No ☐ Parcial	
3.1-3	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional una configuración de alerta/objetivo para definir regiones de rendimiento inaceptables y metas de mejora planificadas?	☐ Si ☐ No ☐ Parcial	
3.1-4	¿Se basa la configuración de niveles de alerta o los criterios fuera de control en principios de métricas de seguridad operacional objetivos?	☐ Si ☐ No ☐ Parcial	
3.1-5	¿Incluyen los indicadores de rendimiento en materia de seguridad operacional un control cuantitativo de resultados de seguridad operacional de alto impacto (por ejemplos, tasas de incidentes de accidentes e incidentes graves), así como también, eventos de bajo impacto (por ejemplo, tasa de no cumplimiento, desviaciones)?	☐ Si ☐ No ☐ Parcial	
3.1-6	¿Están los indicadores de rendimiento en materia de seguridad operacional y su configuración de rendimiento asociada desarrollados en función del acuerdo de la autoridad de aviación civil y sujetos a este?	☐ Si ☐ No ☐ Parcial	
3.1-7	¿Existe un procedimiento para una medida correctiva o de seguimiento que puede tomarse cuando no se logran los objetivos o se violan los niveles de alerta?	☐ Si ☐ No ☐ Parcial	
3.1-8	¿Se revisan periódicamente los indicadores de rendimiento en materia de seguridad operacional?	☐ Si ☐ No ☐ Parcial	
Elemento 3.2 — La gestión de cambio			

3.2-1	¿Existe un procedimiento para la revisión de instalaciones y equipos existentes relacionados con la seguridad operacional de la aviación (incluidos los registros de HIRM) cada vez que haya cambios pertinentes a aquellas instalaciones y equipos?	☐ Si ☐ No ☐ Parcial	
3.2-2	¿Existe un procedimiento para revisar las operaciones y los procesos existentes relacionados con la seguridad operacional de la aviación pertinente (como cualquier registro de HIRM) cada vez que haya cambios a aquellas operaciones o procesos?	☐ Si ☐ No ☐ Parcial	
3.2-3	¿Existe un procedimiento para revisar las nuevas operaciones y los procesos relacionados con la seguridad operacional de la aviación en busca de peligros/riesgos antes de implementarlos?	☐ Si ☐ No ☐ Parcial	
3.2-4	¿Existe un procedimiento para revisar las instalaciones, los equipos, las operaciones o los procesos existentes pertinentes (incluidos los registros de HIRM) cada vez que existan cambios pertinentes que sean externos a la organización, como normas reglamentarias/industriales, mejores prácticas o tecnología?	☐ Si ☐ No ☐ Parcial	
Elemento 3.3 — Mejora continua del SMS			
3.3-1	¿Existe un procedimiento para la evaluación/auditoría interna periódica del SMS?	☐ Si ☐ No ☐ Parcial	
3.3-2	¿Existe un plan actual de la auditoría/evaluación de SMS interna?	☐ Si ☐ No ☐ Parcial	
3.3-3	¿Incluye la auditoría de SMS la toma de muestras de las evaluaciones existentes completadas/de riesgos de seguridad operacional?	☐ Si ☐ No ☐ Parcial	
3.3-4	¿Incluye el plan de auditoría del SMS la toma de muestras de los indicadores de rendimiento en materia de seguridad operacional para conocer la actualidad de los datos y el rendimiento de su configuración de objetivos/alertas?	☐ Si ☐ No ☐ Parcial	
3.3-5	¿Aborda el plan de auditoría de SMS la interfaz de SMS con los subcontratistas o clientes, donde corresponda?	☐ Si ☐ No ☐ Parcial	
3.3-6	¿Existe un proceso para que los informes de auditoría/evaluación de SMS puedan enviarse o destacarse para la atención del gerente responsable, cuando sea necesario?	☐ Si ☐ No ☐ Parcial	
Componente 4 — PROMOCIÓN DE LA SEGURIDAD OPERACIONAL			
Elemento 4.1 — Capacitación y educación			
4.1-1	¿Existe un programa para proporcionar la capacitación/familiarización de SMS al personal que participa en la implementación u operación del SMS?	☐ Si ☐ No ☐ Parcial	
4.1-2	¿Ha tomado el ejecutivo responsable un curso de familiarización, sesión informativa o capacitación de SMS adecuado?	☐ Si ☐ No	

		☐ Parcial	
4.1-3	¿Se brinda al personal que participa en la evaluación de riesgos capacitación o familiarización adecuadas de la gestión de riesgos?	☐ Si ☐ No ☐ Parcial	
4.1-4	¿Existe evidencia de esfuerzos de educación o toma de conciencia del SMS a nivel de la organización?	☐ Si ☐ No ☐ Parcial	
Elemento 4.2 — Comunicación de la seguridad operacional			
4.2-1	¿Participa [Organización] en la distribución de información de seguridad operacional a proveedores de productos y servicios u organizaciones industriales externos pertinentes, incluidas las organizaciones reglamentarias de aviación pertinentes?	☐ Si ☐ No ☐ Parcial	
4.2-2	¿Existe evidencia de una publicación, un circular o un canal de seguridad operacional (SMS) para comunicar la seguridad operacional y asuntos de SMS a los empleados?	☐ Si ☐ No ☐ Parcial	
4.2-3	¿Hay un manual de SMS de [Organización] y material guía relacionado accesible o distribuido a todo el personal pertinente?	☐ Si ☐ No ☐ Parcial	

2. Las cuatro etapas del plan de implementación del SMS

Etapa 1 (12 meses)	*Etapa 2 (12 meses)*	*Etapa 3 (18 meses)*	*Etapa 4 (18 meses)*
1. Elemento 1.1 del SMS: *a) identificar al ejecutivo responsable del SMS;* *b) establecer un equipo de implementación del SMS;* *c) definir el alcance del SMS;* *d) realizar un análisis de brechas de SMS.* 2. Elemento 1.5 del SMS: *a) desarrollar un plan de implementación del SMS.* 3. Elemento 1.3 del SMS: *a) establecer una persona/oficina clave responsable de la administración y el mantenimiento del SMS.* 4. Elemento 4.1 del SMS: *a) establecer un programa de capacitación de SMS para el personal, con prioridad para el equipo de implementación*	1. Elemento 1.1 del SMS: *a) establecer la política y los objetivos de seguridad operacional.* 2. Elemento 1.2 del SMS: *a) definir las responsabilidades de la gestión de la seguridad operacional en los departamentos pertinentes de la organización;* *b) establecer un mecanismo/comité de coordinación de SMS/ seguridad operacional;* *c) establecer SAG por departamento/divisional, donde corresponda.* 3. Elemento 1.4 del SMS: *a) establecer un plan de respuesta ante emergencias.* 4. Elemento 1.5 del SMS:	1. Elemento 2.1 del SMS: *a) establecer un procedimiento de notificación de peligros voluntaria.* 2. Elemento 2.2 del SMS: *a) establecer procedimientos de gestión de riesgos de la seguridad operacional.* 3. Elemento 3.1 del SMS: *a) establecer procedimientos de notificación e investigación de sucesos;* *b) establecer un sistema de recopilación y procesamiento de datos de seguridad operacional para los resultados de alto impacto;* *c) desarrollar SPI de alto impacto y una configuración de objetivos y alertas asociada.* 4. Elemento 3.2 del SMS:	1. Elemento 1.1 del SMS: *a) mejorar el procedimiento disciplinario/la política existentes con una debida consideración de los errores o las equivocaciones accidentales de las infracciones deliberadas o graves.* 2. Elemento 2.1 del SMS: *a) integrar los peligros identificados a partir de los informes de investigación de sucesos con el sistema de notificación de peligros voluntaria;* *b) integrar procedimientos de identificación de peligros y gestión de riesgos con el SMS del subcontratista o el cliente, donde corresponda.* 3. Elemento 3.1 del SMS: *a) mejorar el sistema de recopilación y procesamiento*

del SMS. 1. Elemento 4.2 del SMS: *a) iniciar canales de comunicación del SMS/seguridad operacional.*	*a) iniciar el desarrollo progresivo de un documento/manual de SMS y otra documentación de respaldo.*	*a) establecer un procedimiento de gestión de cambio que incluye la evaluación de riesgos de seguridad operacional.* 5. Elemento 3.3 del SMS: *a) establecer un programa interno de auditoría de la calidad;* *b) establecer un programa externo de auditoría de la calidad.*	*de datos de seguridad operacional para incluir eventos de bajo impacto;* *b) desarrollar SPI de bajo impacto y una configuración de objetivos/alertas asociada.* 4. Elemento 3.3 del SMS: *a) establecer programas de auditoría de SMS o integrarlos en programas de auditoría internos y externos existentes;* *b) establecer otros programas de revisión/estudio de SMS operacional, donde corresponda.* 5. Elemento 4.1 del SMS: *a) garantizar que se haya completado el programa de capacitación de SMS para todo el personal pertinentes.* 6. Elemento 4.2 del SMS: *a) promover la distribución e intercambio de información de la seguridad operacional de forma interna y externa.*
Elemento 1.5 del SMS: documentación del SMS (Etapas 1 a 4)			
Elementos 4.1 y 4.2 del SMS: capacitación, educación y comunicación de SMS (Etapas 1 y posteriores)			

INTENCIONALMENTE EN BLANCO

ADJUNTO C MUESTRA DE DESCRIPCIÓN DEL TRABAJO DE UN GERENTE DE SEGURIDAD OPERACIONAL

1. Propósito general

1.1. El gerente de seguridad operacional es responsable ante el ejecutivo responsable de proporcionar una guía e instrucciones para la planificación, implementación y operación del sistema de gestión de la seguridad operacional (SMS) de la organización. El gerente de seguridad operacional proporciona servicios relacionados con el SMS a áreas de las organizaciones certificadas, no certificadas y de terceros que se incluyen en el SMS y podría haber delegado responsabilidades en nombre de las personas que están en los cargos que requieren los reglamentos.

2. Funciones clave

2.1. Defensor de la seguridad operacional: Demuestra una excelente conducta y actitud de seguridad operacional, sigue las prácticas y reglas reglamentarias, reconoce e informa los peligros y promueve la notificación eficaz de la seguridad operacional.

2.2. Líder: Modela y promueve una cultura institucional que impulsa las prácticas de seguridad operacional mediante un liderazgo eficaz.

2.3. Comunicador:

2.3.1. Actúa como un conducto de información para llevar temas de seguridad operacional a la atención de la administración y para entregar información de seguridad operacional al personal, los contratistas o los accionistas de la organización.

2.3.2. Proporciona y articula la información acerca de temas de seguridad operacional dentro de la organización.

2.4. Desarrollador: Ayuda en la mejora continua de los diagramas de la evaluación de identificación de peligros y gestión de riesgos de seguridad operacional y el SMS de la organización.

2.5. Creador de relaciones: Construye y mantiene una excelente relación de trabajo con el grupo de acción de seguridad operacional (SAG) de la organización y dentro de la oficina de servicios de seguridad operacional (SSO).

2.6. Embajador: Representa a la organización ante comités industriales, gubernamentales y de organizaciones internacionales (por ejemplo, OACI, IATA, CAA, AIB, etc.).

2.7. Analista: Analiza datos técnicos en busca de tendencias relacionadas con peligros, eventos y sucesos.

2.8. Gestión del proceso:

2.8.1. Usa eficazmente los procesos y procedimientos correspondientes para satisfacer las funciones y responsabilidades.

2.8.2. Investiga las oportunidades de aumentar la eficiencia de los procesos.

2.8.3. Mide la eficacia y busca mejorar continuamente la calidad de los procesos.

3. Responsabilidades

3.1. Entre otras tareas, el gerente de seguridad operacional es responsable de:

3.1.1. Gestionar la operación del sistema de gestión de seguridad operacional;

3.1.2. Recopilar y analizar la información de la seguridad operacional de forma oportuna;

3.1.3. Administrar cualquier estudio relacionado con la seguridad operacional;

3.1.4. Controlar y evaluar los resultados de las medidas correctivas;

3.1.5. Garantizar que las evaluaciones de riesgos se lleven a cabo cuando corresponda;

3.1.6. Controlar la industria en busca de preocupaciones de seguridad operacional que pudiesen afectar a la organización;

3.1.7. Participar en las respuestas ante emergencias reales o prácticas;

3.1.8. Participar en el desarrollo y actualización del plan y procedimientos de respuesta ante emergencias; y

3.1.9. Garantizar que la información relacionada con la seguridad operacional, como las metas y los objetivos institucionales, esté disponible para todo el personal mediante los procesos de comunicación establecidos.

4. Naturaleza y alcance

4.1. El gerente de seguridad operacional debe interactuar con el personal de operaciones, los gerentes superiores y los líderes de departamento en toda la organización. El gerente de seguridad operacional también debe fomentar relaciones positivas con las autoridades, las agencias y los proveedores de servicios y productos reglamentarios fuera de la organización. Otros contactos se establecerán en niveles de trabajo, según sea necesario.

5. Calificaciones

5.1. Para calificar como gerente de seguridad operacional, una persona debe tener:

5.1.1. Experiencia de tiempo completo en la seguridad operacional de la aviación, en capacidad de un investigador de seguridad operacional de la aviación, gerente de seguridad operacional/calidad o gerente de riesgos de la seguridad operacional;

5.1.2. Conocimientos sólidos de las operaciones, procedimientos y actividades de la organización;

5.1.3. Un amplio conocimiento técnico de aviación;

5.1.4. Un extenso conocimiento de los sistemas de gestión de la seguridad operacional (SMS) y haber completado la capacitación de SMS correspondiente;

5.1.5. Una comprensión de los principios y las técnicas de la gestión de riesgos para respaldar al SMS;

5.1.6. Experiencia en la implementación o gestión de un SMS;

5.1.7. Experiencia y calificaciones en la investigación de accidentes/incidentes de la aviación y factores humanos;

5.1.8. Experiencia y calificaciones en la realización de auditorías e inspecciones de seguridad operacional/ calidad;

5.1.9. Un conocimiento sólido de los marcos de trabajo reglamentarios de la aviación, incluidas las normas y métodos recomendados (SARPS) de la OACI y los reglamentos de aviación civil pertinentes;

5.1.10. La capacidad de comunicarse en todos los niveles tanto dentro como fuera de la empresa;

5.1.11. La capacidad de tener una postura firme, promover una "cultura justa e imparcial" y aun así fomentar una atmósfera abierta y no punitiva para la notificación;

5.1.12. La capacidad y confianza de comunicarse directamente con el ejecutivo responsable como su asesor o confidente;

5.1.13. Habilidades de comunicación bien desarrolladas y habilidades interpersonales demostradas de alto orden, con la capacidad de vincularse con una variedad de personas y representantes institucionales, como aquellos de diferentes entornos culturales;

5.1.14. Alfabetización computacional y habilidades analíticas superiores.

6. Autoridad

6.1. Acerca de los temas de seguridad operacional, el gerente de seguridad operacional debe tener acceso directo con el ejecutivo responsable y la administración superior y de cargo medio correspondiente.

6.2. El gerente de seguridad operacional debe tener autorización, según las instrucciones del ejecutivo responsable, de realizar auditorías de seguridad operacional, estudios e inspecciones de cualquier aspecto de la operación, de acuerdo con los procedimientos especificados en la documentación del sistema de gestión de seguridad operacional.

6.3. El gerente de seguridad operacional debe tener autorización, según las instrucciones del ejecutivo responsable, de realizar investigaciones de los eventos de seguridad operacional internos, de acuerdo con los procedimientos especificados en la documentación del SMS de la organización.

6.4. El gerente de seguridad operacional no debe tener otros cargos ni responsabilidades que puedan entrar en conflicto o perjudicar su función como un gerente de seguridad operacional de SMS. Este debe ser un cargo administrativo superior que no sea inferior jerárquicamente o subordinado a las funciones de producción u operacionales de la organización.

ADJUNTO D GUÍA SOBRE EL DESARROLLO DE UN MANUAL DE SMS

1. Generalidades

1.1. Este Adjunto sirve para guiar a las organizaciones en su compilación de un manual (o documento) de SMS de alto nivel para definir su marco de trabajo de SMS y sus elementos asociados. Puede ser un manual de SMS independiente o puede integrarse como una sección/capítulo de SMS consolidada dentro de un manual aprobado correspondiente de la organización (por ejemplo, el manual de exposición o el manual de la empresa de la organización). La configuración real puede depender de la expectativa reglamentaria.

1.2. Al usar el formato sugerido y los elementos del contenido en este Adjunto y adaptarlos como corresponda, es una forma en que la organización puede desarrollar su propio manual de SMS de nivel superior. Los elementos del contenido real dependerán del marco de trabajo de SMS específico y los elementos de la organización. La descripción debajo de cada elemento será proporcional al alcance y la complejidad de los procesos del SMS de la organización.

1.3. El manual servirá para comunicar el marco de trabajo de SMS de la organización de forma interna, así como también, con las organizaciones externas pertinentes. El manual debe someterse a aprobación del INAC como evidencia de la aceptación del SMS.

1.4. Se debe hacer una distinción entre un manual de SMS y sus registros y documentos de respaldo operacional. El último hace referencia a registros y documentos históricos y actuales generados durante la implementación y operación de los diversos procesos del SMS. Estos constituyen evidencia documental de las actividades constantes de SMS de la organización.

2. Formato del manual de SMS

2.1. El manual de SMS puede asumir un formato de la siguiente manera:

2.1.1. Encabezado de sección;

2.1.2. objetivo;

2.1.3. criterios;

2.1.4. documentos de referencia cruzada.

2.2. Debajo de cada “encabezado de sección” numerado se incluye una descripción del “objetivo” de esa sección, seguido de sus “criterios” y “documentos de referencia cruzada”. El “objetivo” es lo que intenta lograr la organización al hacer lo que se describe en esa sección. Los "criterios" definen el alcance de lo que se debe considerar al escribir esa sección. Los “documentos de referencia cruzada” vinculan la información con otros manuales pertinentes o SOP de la organización, los que contienen detalles del elemento o proceso, según corresponda.

3. Contenido del manual

3.1. Entre los contenidos del manual se pueden incluir las siguientes secciones:

3.1.1. Control de documentos;

3.1.2. Requisitos reglamentarios del SMS;

3.1.3. Alcance e integración del sistema de gestión de la seguridad operacional;

3.1.4. Política de seguridad operacional;

3.1.5. Objetivos de seguridad operacional;

3.1.6. Responsabilidades de la seguridad operacional y personal clave;

3.1.7. Notificación de seguridad operacional y medidas correctivas;

3.1.8. Identificación de peligros y evaluación de riesgos;

3.1.9. Control y medición del rendimiento en materia de seguridad operacional;

3.1.10. Investigaciones relacionadas con la seguridad operacional y medidas correctivas;

3.1.11. Capacitación y comunicación de seguridad operacional;

3.1.12. Mejora continua y auditoría de SMS;

3.1.13. Gestión de los registros de SMS;

3.1.14. Gestión de cambio; y

3.1.15. Plan de respuesta ante emergencias/contingencia.

3.2. A continuación se indica un ejemplo del tipo de información que puede incluirse en cada sección mediante el formato descrito en párrafo 2.2 del presente Adjunto:

3.2.1. Control de documentos

3.2.1.1. *Objetivo:* Describir cómo los manuales se mantendrán actualizados y cómo garantizará la organización que el personal que participa en las tareas relacionadas con la seguridad operacional tenga la versión más actual.

3.2.1.2. *Criterios:*

3.2.1.2.1. Copia impresa o medio electrónico controlado y lista de distribución.

3.2.1.2.2. La correlación entre el manual de SMS y otros manuales existentes, como el manual de control de mantenimiento (MCM) o el manual de operaciones.

3.2.1.2.3. El proceso de revisión periódica del manual y sus formularios/documentos relacionados para garantizar su sustentabilidad, suficiencia y eficacia constantes.

3.2.1.2.4. El proceso de administración, aprobación y aceptación reglamentaria del manual.

3.2.1.3. *Documentos de referencia cruzada:* Manual de la calidad, manual de ingeniería, etc.

3.2.2. Requisitos reglamentarios de SMS

3.2.2.1. *Objetivo:* Abordar los reglamentos de SMS y el material guía actuales para obtener una referencia necesaria y toma de conciencia de todos los interesados.

3.2.2.2. *Criterios:*

3.2.2.2.1. Explicar en detalle los reglamentos/normas actuales de SMS. Incluir el marco de tiempo del cumplimiento y las referencias del material de asesoramiento, según corresponda.

3.2.2.2.2. Donde corresponda, elaborar o explicar la importancia y las implicaciones de los reglamentos para la organización.

3.2.2.2.3. Establecer una correlación con otros requisitos o normas relacionados con la seguridad operacional, donde corresponda.

3.2.2.3. *Documentos de referencia cruzada:* Referencias de reglamentos/requisitos de SMS, referencias de documentos de guía de SMS, etc.

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

3.2.3.1. *Objetivo:* Describir el alcance y extensión de las operaciones e instalaciones relacionadas con la aviación de la organización, dentro de las cuales se aplicará el SMS. También se debe abordar el alcance de los procesos, los equipos y las operaciones consideradas idóneas para el programa de identificación de peligros y mitigación de riesgos (HIRM) de la organización.

3.2.3.2. *Criterios:*

3.2.3.2.1. Explicar la naturaleza del negocio de aviación de la organización y su posición o función dentro de la industria como un todo.

3.2.3.2.2. Identificar las áreas, los departamentos, los talleres y las instalaciones principales de la organización, dentro de las cuales se aplicará el SMS.

3.2.3.2.3. Identificar los procesos, las operaciones y los equipos principales que se consideran idóneos para el programa HIRM de la organización, especialmente aquellos que son pertinentes para la seguridad operacional de la aviación. Si el alcance de los procesos, las operaciones y los equipos idóneos de HIRM es demasiado detallado o extenso, se puede controlar de acuerdo con un documento complementario, según corresponda.

3.2.3.2.4. Donde se espera que el SMS se opere o administre en un grupo de organizaciones o contratistas interconectados, defina y documente dicha integración y las responsabilidades asociadas, según corresponda.

3.2.3.2.5. Donde hayan otros sistemas de control/gestión relacionados dentro de la organización, como QMS, OSHE y SeMS, identifique su integración pertinente (donde corresponda) dentro del SMS de la aviación.

3.2.3.3. *Documentos de referencia cruzada:* Manual de la calidad, manual de ingeniería, etc.

3.2.4. Política de seguridad operacional

3.2.4.1. *Objetivo:* Describir las intenciones de la organización, sus principios de gestión y su compromiso con la mejora de la seguridad operacional de la aviación, en términos del proveedor de productos o servicios. Una política de seguridad operacional debe ser una descripción corta, parecida a una declaración de la misión.

3.2.4.2. *Criterios:*

3.2.4.2.1. La política de seguridad operacional debe ser adecuada para la envergadura y complejidad de la organización.

3.2.4.2.2. La política de seguridad operacional señala las intenciones de la organización, sus principios de gestión y el compromiso con la mejora continua en la seguridad operacional de la aviación.

3.2.4.2.3. El ejecutivo responsable aprueba y firma la política de seguridad operacional.

3.2.4.2.4. El ejecutivo responsable y el resto de los gerentes promueven la política de seguridad operacional.

3.2.4.2.5. La política de seguridad operacional se revisa periódicamente.

3.2.4.2.6. El personal en todos los niveles participa en el establecimiento y mantenimiento del sistema de gestión de la seguridad operacional.

3.2.4.2.7. La política de seguridad operacional se comunica a todos los empleados con la intención de crear conciencia de sus obligaciones de seguridad operacional individuales.

3.2.4.3. *Documentos de referencia cruzada:* Política de seguridad operacional de OSHE, etc.

3.2.5.Objetivos de seguridad operacional

3.2.5.1. *Objetivo:* Describir los objetivos de seguridad operacional de la organización. Los objetivos de seguridad operacional deben ser una declaración corta que describa a grandes rasgos lo que espera lograr la organización.

3.2.5.2. *Criterios:*

3.2.5.2.1. Se hayan establecido los objetivos de seguridad operacional.

3.2.5.2.2. Los objetivos de seguridad operacional se expresan como una declaración de nivel superior que describe el compromiso de la organización para lograr la seguridad operacional.

3.2.5.2.3. Existe un proceso formal para desarrollar un conjunto coherente de objetivos de seguridad operacional.

3.2.5.2.4. Los objetivos de seguridad operacional se difunden y distribuyen.

3.2.5.2.5. Se han asignado recursos para lograr los objetivos.

3.2.5.2.6. Los objetivos de seguridad operacional se vinculan con los indicadores de seguridad operacional para facilitar el control y la medición, como corresponda.

3.2.5.3. *Documentos de referencia cruzada:* Documento de indicadores de rendimiento en materia de seguridad operacional, etc.

3.2.6.Funciones y responsabilidades

3.2.6.1. *Objetivo:* Describir las autoridades y responsabilidades de la seguridad operacional para el personal que participa en el SMS.

3.2.6.2. *Criterios:*

3.2.6.2.1. El ejecutivo responsable se encarga de garantizar que el sistema de gestión de la seguridad operacional se implemente correctamente y se desempeñe según los requisitos en todas las áreas de la organización.

3.2.6.2.2. Se asignó un gerente (oficina) de seguridad operacional correspondiente, un comité de seguridad operacional o grupos de acción de seguridad operacional, según corresponda.

3.2.6.2.3. Las autoridades y responsabilidades de seguridad operacional del personal en todos los niveles de la organización están definidos y documentados.

3.2.6.2.4. Todo el personal comprende sus autoridades y responsabilidades en relación con los procesos, las decisiones y las medidas de la gestión de seguridad operacional.

3.2.6.2.5. Se dispone de un diagrama de responsabilidades institucionales del SMS.

3.2.6.3. *Documentos de referencia cruzada:* Manual de exposición de la empresa, manual de SOP, manual de administración, etc.

3.2.7.Notificación de seguridad operacional

3.2.7.1. *Objetivo:* Un sistema de notificación debe incluir medidas reactivas (informes de accidentes/incidentes, etc.) y proactivas/predictivas (informes de peligros). Describir los sistemas de notificación respectivos. Entre los factores que se deben considerar se incluyen: el formato del informe, la confidencialidad, los destinatarios, los procedimientos de investigación/evaluación, las medidas correctivas/preventivas y la divulgación del informe.

3.2.7.2. *Criterios:*

3.2.7.2.1. La organización tiene un procedimiento que proporciona la captura de sucesos internos, como accidentes, incidentes y otros sucesos pertinentes para el SMS.

3.2.7.2.2. Se debe hacer una distinción entre los informes obligatorios (accidentes, incidentes graves, defectos importantes, etc.) que se deben notificar a la CAA y otros informes de sucesos de rutina, que permanecen dentro de la organización.

3.2.7.2.3. También existe un sistema de notificación de peligros/sucesos voluntaria y confidencial, que incorpora la protección de identidad/datos adecuada, según corresponda.

3.2.7.2.4. Los procesos de notificación respectivos son simples, accesibles y proporcionales a la envergadura de la organización.

3.2.7.2.5. Los informes de alto impacto y las recomendaciones asociadas se abordan y revisan según el nivel de gestión correspondiente.

3.2.7.2.6. Los informes se recopilan en una base de datos adecuada para facilitar el análisis necesario.

3.2.7.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.8.Identificación de peligros y evaluación de riesgos

3.2.8.1. *Objetivo:* Describir el sistema de identificación de peligros y cómo se recopilan tales datos. Describir el proceso para la categorización de peligros/riesgos y su posterior priorización para una evaluación de seguridad operacional documentada. Describir cómo se lleva a cabo el proceso de evaluación de seguridad operacional y cómo se implementan planes de acción preventiva.

3.2.8.2. *Criterios:*

3.2.8.2.1. Los peligros identificados se evalúan, priorizan y procesan para la evaluación de riesgos, según corresponda.

3.2.8.2.2. Existe un proceso estructurado para la evaluación de riesgos que implica la evaluación de gravedad, probabilidad, tolerabilidad y controles preventivos.

3.2.8.2.3. Los procedimientos de identificación de peligros y evaluación de riesgos se centran en la seguridad operacional de la aviación, así como también, en su contexto fundamental.

3.2.8.2.4. El proceso de evaluación de riesgos usa hojas de cálculo, formularios o software correspondientes a la complejidad de la organización y las operaciones involucradas.

3.2.8.2.5. El nivel de gestión correspondiente aprueba las evaluaciones de seguridad operacional completadas.

3.2.8.2.6. Existe un proceso para evaluar la eficacia de las medidas correctivas, preventivas y de recuperación que se han desarrollado.

3.2.8.2.7. Existe un proceso para la revisión periódica de las evaluaciones de seguridad operacional completadas y la documentación de sus resultados.

3.2.8.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.9.Control y medición del rendimiento en materia de seguridad operacional

3.2.9.1. *Objetivo:* Describir el componente de control y medición del rendimiento en materia de seguridad operacional del SMS. Esto incluye los indicadores de rendimiento en materia de seguridad operacional (SPI) del SMS de la organización.

3.2.9.2. *Criterios:*

3.2.9.2.1. El proceso formal para desarrollar y mantener un conjunto de indicadores de rendimiento en materia de seguridad operacional y sus objetivos eficaces asociados.

3.2.9.2.2. Correlación establecida entre los SPI y los objetivos de seguridad operacional de la organización, donde corresponda, y el proceso de aceptación reglamentaria de los SPI, donde sea necesario.

3.2.9.2.3. El proceso de control del rendimiento de estos SPI, incluido el procedimiento de medidas correctivas, cada vez que se activen tendencias inaceptables o anormales.

3.2.9.2.4. Cualquier otro criterio o proceso de control y medición del rendimiento en materia de seguridad operacional o de SMS complementario.

3.2.9.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.10. Investigaciones relacionadas con la seguridad operacional y las medidas correctivas

3.2.10.1. *Objetivo:* Describir cómo se investigan y procesan los accidentes/incidentes/sucesos dentro de la organización, incluida la correlación con el sistema de identificación de peligros y gestión de riesgos del SMS de la organización.

3.2.10.2. *Criterios:*

3.2.10.2.1. Procedimientos para garantizar que se investiguen de forma interna los accidentes e incidentes notificados.

3.2.10.2.2. Divulgación interna de los informes de investigación completados al igual que al INAC, según corresponda.

3.2.10.2.3. Un proceso para garantizar que se lleven a cabo las medidas correctivas tomadas o recomendadas y para evaluar sus resultados/eficacia.

3.2.10.2.4. Procedimiento sobre la consulta y las medidas disciplinarias asociadas con los resultados del informe de investigación.

3.2.10.2.5. Condiciones definidas claramente según las cuales se podrían considerar medidas disciplinarias punitivas (por ejemplo, actividad ilegal, imprudencia, negligencia grave o conducta impropia deliberada).

3.2.10.2.6. Un proceso para garantizar que las investigaciones incluyan la identificación de averías activas, así como también, factores y peligros que contribuyen.

3.2.10.2.7. El procedimiento y el formato de la investigación proporcionan hallazgos sobre factores o peligros contribuyentes que se procesarán para la medida de seguimiento con el sistema de identificación de peligros y gestión de riesgos de la organización, donde corresponda.

3.2.10.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.11. Capacitación y comunicación de seguridad operacional

3.2.11.1. *Objetivo:* Describir el tipo de SMS y otra capacitación relacionada con la seguridad operacional que reciba el personal y el proceso para garantizar la eficacia de la capacitación. Describir cómo se documentan tales procedimientos de

capacitación. Describir los procesos/canales de comunicación de seguridad operacional dentro de la organización.

3.2.11.2. *Criterios:*

3.2.11.2.1. Se documenta el programa de capacitación, la idoneidad y los requisitos.

3.2.11.2.2. Existe un proceso de validación que mide la eficacia de la capacitación.

3.2.11.2.3. La capacitación incluye capacitación inicial, recurrente y de actualización, donde corresponda.

3.2.11.2.4. La capacitación de SMS de la organización es parte del programa de capacitación general de la organización.

3.2.11.2.5. Se incorpora la toma de conciencia de SMS en el programa de empleo o adoctrinamiento.

3.2.11.2.6. Los procesos/canales de comunicación de la seguridad operacional dentro de la organización.

3.2.11.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.12. Mejora continua y auditoría de SMS

3.2.12.1. *Objetivo:* Describir el proceso para la revisión y mejora continuas del SMS.

3.2.12.2. *Criterios:*

3.2.12.2.1. El proceso para una auditoría/revisión internas regulares del SMS de la organización para garantizar su continua sustentabilidad, suficiencia y eficacia.

3.2.12.2.2. Describir cualquier otro programa que contribuya con la mejora continua del SMS de la organización y el rendimiento en materia de seguridad operacional, por ejemplo, MEDA, estudios de seguridad operacional, sistemas ISO.

3.2.12.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.13. Gestión de los registros de SMS

3.2.13.1. *Objetivo:* Describir el método de almacenamiento de todos los registros y documentos relacionados con SMS.

3.2.13.2. *Criterios:*

3.2.13.2.1. La organización tiene registros de SMS o un sistema de archivo que garantiza la conservación de todos los registros generados en conjunto con la implementación y operación del SMS.

3.2.13.2.2. Los registros que deben guardarse incluyen informes de peligros, informes de evaluación de riesgos, notas de grupos de acción de seguridad operacional/reuniones de seguridad operacional, diagramas de indicadores de rendimiento en materia de seguridad operacional, informes de auditoría del SMS y registros de la capacitación de SMS.

3.2.13.2.3. Los registros deben permitir que se rastreen todos los elementos del SMS y que estén accesibles para la administración de rutina del SMS, así como también, para propósitos de auditorías internas y externas.

3.2.13.3. *Documentos de referencia cruzada:* - - - - - - - - - - - - - -

3.2.14. Gestión de cambio

3.2.14.1. *Objetivo:* Describir el proceso de la organización para gestionar los cambios que pueden tener un impacto en los riesgos de la seguridad operacional y cómo tales procesos se integran con el SMS.

3.2.14.2. *Criterios:*

3.2.14.2.1. Procedimientos para garantizar que los cambios institucionales y operacionales sustanciales consideran cualquier impacto que puedan tener en los riesgos existentes de la seguridad operacional.

3.2.14.2.2. Procedimientos para garantizar que se lleva a cabo una evaluación de seguridad operacional correspondiente antes de la introducción de nuevos equipos o procesos que tengan implicaciones de riesgos de seguridad operacional.

3.2.14.2.3. Procedimientos para la revisión de evaluaciones de seguridad operacional existentes cada vez que se apliquen cambios al proceso o equipo asociado.

3.2.14.3. *Documentos de referencia cruzada:* SOP de la empresa relacionado con la gestión de cambio, etc.

3.2.15. Plan de respuesta ante emergencias/contingencia

3.2.15.1. *Objetivo:* Describir las intenciones de la organización acerca de situaciones de emergencia y sus controles de recuperación correspondientes, además de su compromiso para abordar dichas situaciones. Describir las funciones y responsabilidades del personal clave. El plan de respuesta ante emergencias puede ser un documento separado o puede ser parte del manual de SMS.

3.2.15.2. *Criterios (como corresponda para la organización):*

3.2.15.2.1. La organización tiene un plan de emergencia que describe las funciones y responsabilidades en caso de un incidente, una crisis o un accidente importante.

3.2.15.2.2. Existe un proceso de notificación que incluye una lista de llamadas de emergencia y un proceso de movilización interno.

3.2.15.2.3. La organización tiene disposiciones con otras agencias para recibir ayuda y la disposición de servicios de emergencia, según corresponda.

3.2.15.2.4. La organización tiene procedimientos para las operaciones del modo de emergencia, donde corresponda.

3.2.15.2.5. Existe un procedimiento para vigilar el bienestar de todas las personas afectadas y para notificar al familiar más cercano.

3.2.15.2.6. La organización ha establecido procedimientos para tratar con los medios de comunicación y temas relacionados con el seguro.

3.2.15.2.7. Existen responsabilidades de investigación de accidentes definidas dentro de la organización.

3.2.15.2.8. El requisito para preservar la evidencia, asegurar el área afectada y la notificación obligatoria/gubernamental está claramente declarada.

3.2.15.2.9. Existe una capacitación de preparación y respuesta ante emergencias para el personal afectado.

3.2.15.2.10. La organización desarrolló un plan de evacuación en caso de una aeronave o un equipo averiado con el asesoramiento de propietarios de aeronaves/equipos, explotadores de aeródromo u otras agencias, según corresponda.

3.2.15.2.11. Existe un procedimiento para registrar las actividades durante una respuesta ante emergencias.

3.2.15.3. *Documentos de referencia cruzada:* Manual de ERP, etc.

INTENCIONALMENTE EN BLANCO

ADJUNTO E SISTEMAS DE NOTIFICACIÓN VOLUNTARIA Y CONFIDENCIAL

La siguiente guía se basa en el ejemplo de un explotador aéreo integrado y la organización de mantenimiento. Para otros tipos de organizaciones de proveedores de servicios, este material guía podría personalizarse, si fuera necesario.

El sistema de notificación voluntaria y confidencial de una organización debe, como mínimo, definir:

1. El objetivo del sistema de notificación

Ejemplo:

El objetivo clave del sistema de notificación voluntaria y confidencial de [Nombre de la organización] es mejorar la seguridad operacional de nuestras actividades de aviación de la empresa mediante la recopilación de informes sobre deficiencias reales y posibles de la seguridad operacional que, de lo contrario, no se informarían mediante otros canales. Tales informes pueden implicar sucesos, peligros o amenazas pertinentes para la seguridad operacional de nuestras actividades de aviación. Este sistema no elimina la necesidad de la notificación formal de accidentes e incidentes, de acuerdo con los SOP de nuestra empresa, ni tampoco, el envío de los informes obligatorios de sucesos a las autoridades reglamentarias pertinentes.

El [Nombre del sistema] es un sistema de notificación de sucesos y peligros voluntario, no punitivo y confidencial que administra [Nombre del departamento/oficina]. Proporciona un canal para la notificación voluntaria de sucesos y peligros de aviación pertinentes para las actividades de seguridad operacional de nuestra organización, mientras protege la identidad del notificado.

Al establecer dicho sistema, la organización tendrá que decidir si integra o segrega su sistema de notificación de seguridad, salud y ambiente en el trabajo (OSHE) del sistema de notificación de seguridad operacional de la aviación. Esto puede depender de las expectativas o los requisitos de las autoridades de OSHE y aviación respectivas. Donde exista un sistema de notificación de OSHE separado en la empresa, se debe destacar en conformidad en este párrafo para guiar al notificador, según sea necesario.

2. El alcance de los sectores/áreas de aviación que aborda el sistema

Ejemplo:

El [Nombre del sistema] aborda áreas como:

a. operaciones de vuelo;
b. mantenimiento de la aeronave en el hangar;
c. mantenimiento de componentes en el taller;
d. gestión de la flota técnica;
e. gestión técnica del inventario;
f. planificación de ingeniería;
g. servicios técnicos;
h. registros técnicos;
i. mantenimiento de línea;
j. etc.

3. Quien pueda hacer un informe voluntario

Ejemplo:

Si pertenece a cualquiera de estas áreas o departamentos operacionales, puede contribuir con la mejora de la seguridad operacional de la aviación mediante [Nombre del sistema] al notificar los sucesos, los peligros o las amenazas pertinentes para las actividades de aviación de nuestra organización:

k. miembros de la tripulación de vuelo y de la cabina;
l. controladores de tránsito aéreo;
m. ingenieros, técnicos o mecánicos de aeronaves con licencia;
n. empleados de organizaciones de mantenimiento, diseño y fabricación;
o. explotadores de servicios de escala del aeropuerto;
p. empleados del aeródromo;
q. personal de aviación general;
r. etc.

4. Cuando se debe hacer dicho informe

Ejemplo:

Debe hacer un informe cuando:

s. desee que otros aprendan y se beneficien del incidente o peligro, pero está preocupado de proteger su identidad;
t. no existe otro procedimiento o canal de notificación adecuado; y
u. ha probado con otro procedimiento o canal de notificación sin que el problema se haya abordado.

5. Cómo se procesan los informes

Ejemplo:

El [Nombre del sistema] presta particular atención a la necesidad de proteger la identidad del notificador cuando se procesan todos los informes. El gerente leerá y validará cada informe. El gerente puede comunicarse con el notificador para asegurarse de que comprenda la naturaleza y las circunstancias del suceso/peligro informado o para obtener información y clarificación adicional necesarias.

Cuando el gerente esté satisfecho con que la información obtenida es completa y coherente, omitirá la identidad de quien entrega la información e ingresará los datos en la base de datos del [Nombre del sistema]. En caso que se deba buscar aportes de cualquier tercero, solo se usarán datos no identificados.

El formulario del [Nombre del sistema], con la fecha de retorno anotada, será devuelto finalmente al notificador. El gerente intentará completar el procesamiento dentro de diez (10) días hábiles si no se necesita información adicional. En los casos donde el gerente debe conversar con el notificador o consultar a un tercero, se necesitará más tiempo.

Si el gerente no está en su oficina por un tiempo prolongado, el gerente suplente procesará el informe. Los notificadores pueden estar tranquilos de que el gerente o el gerente suplente leerá y seguirá cada informe de [Nombre del sistema].

6. Distribución de información de seguridad operacional dentro de la empresa y la comunidad de la aviación

Ejemplo:

Si el contenido de un informe de [Nombre del sistema] sugiere una situación o condición que represente una amenaza inmediata o urgente para la seguridad operacional de la aviación, el informe se tratará con prioridad y se derivará, luego de eliminar la identidad del notificador, a las organizaciones o autoridades pertinentes lo antes posible, para permitirles tomar las medidas de seguridad operacional necesarias.

Se pueden compartir informes y extractos no identificados pertinentes dentro de la empresa, así como también, con accionistas de aviación externa, según se considere adecuado. Esto permitirá que todo el personal y los departamentos interesados dentro de la empresa, además de los accionistas de aviación externos, revisen sus propias operaciones y respalden la mejora de la seguridad operacional de la aviación como un todo.

7. Comunicación con el gerente de [Nombre del sistema]

Ejemplo:

Si lo desea, puede llamar al gerente de [Nombre del sistema] para consultar sobre [Nombre del sistema] o para solicitar un análisis preliminar con el gerente de [Nombre del sistema] antes de hacer un informe.

Puede comunicarse con el gerente y el gerente suplente durante horas de oficina de lunes a viernes en los siguientes números de teléfono:

Administrador del [Nombre del sistema]
El Sr. ABC
Tel.:

Administrador suplente
El Sr. XYZ
Tel.:

INTENCIONALMENTE EN BLANCO

ADJUNTO F INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DEL SMS

Las Tablas que se presentan a continuación (ejemplos de indicadores de seguridad operacional) proporcionan ejemplos ilustrativos de los indicadores de rendimiento en materia de seguridad operacional (SPI) colectivos del Estado de Nicaragua.

Los SPI del SMS se reflejan en el lado derecho de las tablas. Los criterios del nivel de alerta y objetivos correspondientes para cada indicador se deben explicar como se muestra.

Los indicadores de rendimiento en materia de seguridad operacional del SSP a la izquierda de las tablas aparecen para indicar la correlación necesaria entre los indicadores de seguridad operacional de SMS y SSP. Los proveedores de productos y servicios deben desarrollar los SPI del SMS con el asesoramiento de sus organizaciones reglamentarias estatales respectivas. Sus SPI propuestos deberán ser coherentes con los indicadores de seguridad operacional de SSP del INAC; por lo tanto, se debe obtener un acuerdo/aceptación necesario.

INTENCIONALMENTE EN BLANCO

Tabla 1. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores aéreos

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores aéreos (solo explotadores aéreos del Estado)											
Tasa de accidentes/ incidentes graves mensual/ trimestral del explotador aéreo colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador aéreo colectivo de CAA (hallazgos por auditoría	Consideración	Consideración	Tasa de incidentes graves mensual de la flota individual del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes mensual de la flota combinada del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
Tasa de incidentes de IFSD trimestral del motor del explotador aéreo colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anua	Tasa de % o hallazgos de LEI anual de la inspección de la estación de línea del explotador aéreo colectivo de CAA (hallazgos por inspección)	Consideración	Consideración	Tasa de incidentes graves mensual de la flota combinada del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador (hallazgos por auditoría)	Consideración	Consideración
			% de LEI promedio anual de la inspección de vigilancia de la plataforma del explotador aéreo extranjero de CAA (para cada explotador extranjero)	Consideración	Consideración	Tasa de incidentes de IFSD del explotador aéreo (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros voluntario del explotador (por ejemplo, cada 1 000 FH)	Consideración	Consideración
			Tasa del informe de incidentes de DGR del explotador colectivo de CAA (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anua				Tasa del informe de incidentes de DGR del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
Etc.											

Tabla 2. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores del aeródromo

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores de aeródromos											
Tasa de incidentes graves/ accidentes en tierra mensual/ trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 movimientos en tierra	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anua	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador del aeródromo colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa de incidentes graves/accidentes en tierra trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador del aeródromo (hallazgos por auditoría	Consideración	Consideración
Tasa de incidentes en la excursión en pista mensual/trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa de incidentes en la excursión en pista trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros de objetos extraños/suciedad trimestral del explotador del aeródromo (por ejemplo, cada 10 000 movimientos en tierra))	Consideración	Consideración
Tasa de incidentes en la incursión en pista mensual/trimestral del aeródromo colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual				Tasa de incidentes en la incursión en pista trimestral del explotador del aeródromo — Implica cualquier aeronave (por ejemplo, cada 10 000 salidas)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa del informe de peligros voluntario del explotador (por personal de operaciones por trimestre	Consideración	Consideración

									Tasa trimestral del informe de incidentes de daños por objetos extraños en la aeronave del explotador del aeródromo — Implica daños a la aeronave (por ejemplo, cada 10 000 movimientos en tierra)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anual
Etc.											

Tabla 3. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para los explotadores de ATS

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
Explotadores de ATS											
Tasa de incidentes graves (espacio aéreo) de FIR trimestral de ATS colectivos de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes trimestral del RA de los TCAS de la FIR de ATS colectivos de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes graves de FIR trimestral del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimien- tos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes trimestral del RA de los TCAS de la FIR del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anual
			Tasa de incidentes trimestral (LOS) de salidas de nivel de suelo de FIR de ATS colectivo de CAA — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de incidentes de cuasicolisión trimestral/anual del explotador de ATS (por ejemplo, cada 100 000 movi-mientos en vuelo	Suponiendo que el promedio anual histórico es 3, la tasa de alerta posible podría ser 5.	Suponiendo que el promedio anual histórico es 3, la tasa de objetivo posible podría ser 2	Tasa de incidentes trimestral (LOS) de salidas de nivel de suelo de FIR del explotador de ATS — Implica cualquier aeronave (por ejemplo, cada 100 000 movimientos en vuelo)	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual
			Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia del explotador de ATS colectivo de CAA (hallazgos por auditoría)	Consideración	Consideración				Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna del explotador de ATS (hallazgos por auditoría)	Consideración	Consideración
Etc.											

Tabla 4. Ejemplos de indicadores de rendimiento en materia de seguridad operacional para organizaciones de mantenimiento, producción y diseño (DOA/POA/MRO)

Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*			*Indicadores de alto impacto (basados en sucesos/resultados)*			*Indicadores de bajo impacto (basados en eventos/actividad)*		
Indicador de seguridad operacional	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*	*Indicador de rendimiento en materia de seguridad operacional*	*Criterios del nivel de alerta*	*Criterios del nivel de objetivos*
DOA/POA/MRO											
Informes obligatorios de defectos (MDR) trimestrales de la MRO colectiva de CAA recibidos	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años)	__% (por ejemplo 5%) de mejora entre cada tasa media anual	Tasa de % o hallazgos de LEI anual de la auditoría de vigilancia de MRO/POA/DOA colectivas de CAA (hallazgos por auditoría)	Consideración	Consideración	Tasa trimestral de MRO/POA de reclamos de la garantía técnica de los componentes	Promedio + 1/2/3 SD (restableci-miento anual o cada 2 años	__% (por ejemplo 5%) de mejora entre cada tasa media anua	Tasa de % o hallazgos de LEI anual de la auditoría de QMS/SMS interna de MRO/POA/DOA (hallazgos por auditoría)	Consideración	Consideración
Tasa trimestral de POA/DOA colectiva de CAA de los productos operacionales que están sujetos a AD/ASB (por línea de producto	Consideración	Consideración				Tasa trimestral de POA/DOA de los productos operacionales que están sujetos a AD/ASB (por línea de producto)	Consideración	Consideración	Tasa de averías/rechazos trimestral de la inspección final/ pruebas de MRO/POA/DOA (debido a problemas de calidad interna)	Consideración	Consideración
						Tasa trimestral de MRO/POA de los informes obliga-torios/importantes de defectos de componentes emitidos (debido a problemas de calidad interna)	Consideración	Consideración	Tasa de informes de peligros voluntarios de MRO/POA/DOA (por personal de operaciones por trimestre)	Consideración	Consideración
Etc.											

ADJUNTO G ILUSTRACIÓN DE UN PROCEDIMIENTO DE PRIORIZACIÓN DE PELIGROS

<table>
<tr><th></th><th>Opción 1 (básico)</th><th>Opción 2 (avanzado)</th></tr>
<tr><td>Criterios</td><td>Priorización en relación con la categoría de peor consecuencia posible del peligro (gravedad del incidente).</td><td>Priorización en relación con la categoría del índice de riesgo (gravedad y probabilidad) de la peor consecuencia posible del peligro.</td></tr>
<tr><td>Metodología</td><td>a) proyectar la peor consecuencia posible del peligro;
b) proyectar la clasificación de suceso probable de esta consecuencia (es decir, ¿se considerará un accidente, incidente grave o incidente?);
c) concluir que la priorización del peligro es:
<table><tr><th>Consecuencia proyectada</th><th>Nivel de peligro</th></tr><tr><td>Accidente</td><td>Nivel 1</td></tr><tr><td>Incidente grave</td><td>Nivel 2</td></tr><tr><td>Incidente</td><td>Nivel 3</td></tr></table></td><td>a) proyectar el número de índice de riesgo (según la matriz de gravedad y probabilidad pertinente) de la peor consecuencia posible del peligro;
b) en relación con la matriz de tolerabilidad relacionada, determine la categoría de tolerabilidad del índice de riesgo (es decir, intolerable, tolerable o aceptable) o terminología/categorización equivalente;
c) concluir que la priorización del peligro es:
<table><tr><th>Índice de riesgo proyectado</th><th>Nivel de peligro</th></tr><tr><td>Intolerable/alto riesgo</td><td>Nivel 1</td></tr><tr><td>Tolerable/riesgo moderado</td><td>Nivel 2</td></tr><tr><td>Aceptable/bajo riesgo</td><td>Nivel 3</td></tr></table></td></tr>
<tr><td>Observaciones</td><td>La Opción 1 considera solo la gravedad de la consecuencia proyectada del peligro.</td><td>La Opción 2 considera la gravedad y probabilidad de la consecuencia proyectada del peligro; este es un criterio más completo que la Opción 1.</td></tr>
</table>

Luego de que cada peligro se haya priorizado, será aparente que se organicen como peligros de Nivel 1, 2 y 3. Entonces, se puede asignar la prioridad o atención de la mitigación de riesgos según su nivel (1, 2 o 3), según corresponda.

ADJUNTO H RIESGOS DE LA SEGURIDAD OPERACIONAL

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

1. Definición de un riesgo de seguridad operacional;

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

2. Probabilidad del riesgo de seguridad operacional;

2.1. El proceso de controlar los riesgos de seguridad operacional comienza al evaluar la probabilidad de que las consecuencias de los peligros se materialicen durante las actividades de aviación realizadas por la organización.

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

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

2.2.2. ¿Qué otros equipos o componentes del mismo tipo tienen defectos similares?

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

2.2.4. ¿Qué porcentaje del tiempo se usa el equipo sospechoso o el procedimiento cuestionable?

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

2.3. Cualquier factor subyacente a estas preguntas ayudará a evaluar la probabilidad de que exista un peligro, considerando todos los casos potencialmente válidos. La determinación de la probabilidad puede usarse para ayudar a determinar la probabilidad del riesgo de seguridad operacional.

2.4. La siguiente es una tabla de probabilidad de riesgo de seguridad operacional típica, en este caso, una tabla de cinco puntos. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un evento o una condición inseguros, la descripción de cada categoría y una asignación de valor a cada categoría.

Probabilidad	*Significado*	*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
Sumamente improbable	Es casi inconcebible que ocurra el evento	1

2.5. Se debe enfatizar que este es solo un ejemplo y que el nivel de detalle y complejidad de las tablas y matrices debe adaptarse para ser proporcional con las necesidades y complejidades particulares de las diferentes organizaciones. Además, se debe tener presente que las organizaciones pueden incluir criterios tanto cualitativos como cuantitativos, que pueden incluir hasta 15 valores.

3. Gravedad del riesgo de seguridad operacional;

3.1. Luego de completar la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional, considerando las posibles consecuencias relacionadas con el peligro. La gravedad del riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La evaluación de la gravedad puede basarse en:

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

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

3.2. La evaluación de gravedad debe considerar todas las posibles consecuencias relacionadas con una condición o un objeto inseguros, considerando la peor situación predecible. La siguiente es una tabla de gravedad de riesgo de seguridad operacional típico. Incluye cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada categoría. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla solo es un ejemplo.

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

4. Tolerabilidad del riesgo de seguridad operacional;

4.1. El proceso de evaluación de la probabilidad y gravedad del riesgo de seguridad operacional puede usarse para derivar un índice de riesgo de seguridad operacional. El índice que se crea mediante la metodología descrita anteriormente consta de un identificador alfanumérico, que indica los resultados combinados de las evaluaciones de probabilidad y gravedad. Las combinaciones de gravedad/probabilidad respectivas se presentan en la matriz de evaluación del riesgo de seguridad operacional en siguiente Tabla.

Probabilidad del riesgo		*Gravedad del riesgo*				
		Catastrófico	Peligroso	Importante	Leve	Insignificante
		A	B	C	D	E
Frecuente	5	5A	5B	5C	5D	5E
Ocasional	4	4A	4B	4C	4D	4E
Remoto	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Sumamente improbable	1	1A	1B	1C	1D	1E

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

4.3. El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a una matriz de tolerabilidad del riesgo de seguridad operacional (véanse las tablas a continuación como ejemplos) que describen los criterios de tolerabilidad para una organización en particular. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B cae en la categoría “inaceptable bajo las circunstancias existentes”. En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por tanto, la organización debe:

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

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

4.3.3. Cancelar la operación si la mitigación no es posible.

Descripción de la tolerabilidad	*Índice de riesgo evaluado*	*Criterios sugeridos*
Región Intolerable	5A, 5B, 5, 4A, 4B, 3A	Inaceptable según las circunstancias existentes
Región Tolerable	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D,2A, 2B, 2C, 1A	Aceptable según la mitigación de riesgos. Puede necesitar una decisión de gestión.
Región Aceptable	3E, 2D, 2E, 1B, 1C, 1D, 1E	Aceptable

Rango del índice del riesgo	*Descripción*	*Medida recomendada*
5A, 5B, 5, 4A, 4B, 3A	Riesgo alto	Cese o disminuya la operación oportunamente si fuera necesario. Realice la mitigación de riesgos de prioridad para garantizar que haya controles preventivos adicionales o mejorados implementados para reducir el índice de riesgos al rango moderado o bajo
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D,2A, 2B, 2C, 1A	Riesgo moderado	Programe el performance de una evaluación de seguridad operacional para reducir el índice de riesgos hasta el rango bajo, si fuera factible.
3E, 2D, 2E, 1B, 1C, 1D, 1E	Riesgo bajo	Aceptable tal cual. No se necesita una mitigación de riesgos posterior.

5. Gestión del riesgo de seguridad operacional.

La gestión de riesgo de seguridad operacional abarca la evaluación y mitigación de los riesgos de seguridad operacional. El objetivo de la gestión de riesgo de seguridad operacional es evaluar los riesgos asociados con los peligros identificados y desarrollar e implementar mitigaciones eficaces y adecuadas. Por lo tanto, la gestión de riesgos de seguridad operacional es un componente clave del proceso de gestión de la seguridad operacional a nivel de Estado y del proveedor de productos/servicios.

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

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.

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