REGULACION DE AERONAUTICA CIVIL

RAC - 19

Agencia Hondureña de Aeronáutica Civil
Gobierno de la República

GESTIÓN DE LA SEGURIDAD OPERACIONAL

Julio 2025

SISTEMA DE EDICION Y ENMIENDAS

Las enmiendas a la presente regla serán indicadas mediante una barra vertical en el margen izquierdo, enfrente al renglón, sección o figura que esté siendo afectada por el mismo. la edición será el reemplazo del documento completo por otro.

Estas enmiendas se deben anotar en el registro de ediciones y enmiendas, indicando el número correspondiente, la fecha de efectividad y la fecha de inserción.

Control de Firmas

No. Edición/ No. Enmienda	Fecha	Elaborado por:	Revisado por:	Aprobado por:
Primera Edición	Julio 2025	Lic. Ernesto España **Jefe Departamento SSP**	Lic. Jorge Corrales **Subdirector Técnico**	Lic. Gerardo G. Rivera **Director Ejecutivo**

Registro de Edición y Enmiendas

EDI./ ENM.	Fecha de Emisión	Fecha de inserción	Insertada por
Primera Edición	Julio 2025		

Preámbulo

Conscientes de la responsabilidad de preservar la vida humana, proteger los bienes y garantizar la eficiencia del sistema aeronáutico nacional, la Agencia Hondureña de Aeronáutica Civil establece la edición inicial de la Regulación de Aviación Civil 19, como manifestación de su compromiso con una cultura de seguridad operacional sólida, proactiva y sostenible en la cual se establecen los requerimientos obligatorios para la Gestión de Seguridad Operacional, consignados en la segunda edición del anexo 19 de la OACI.

En fiel cumplimiento con los compromisos adquiridos por el Estado de Honduras, como Estado contratante del Convenio Internacional de Aviación Civil, conocido como Convenio de Chicago, aprobado por Honduras mediante decreto legislativo N0. 89 del 18 de febrero de 1953, se emite la presente RAC 19 Gestión de la Seguridad Operacional, la cual se fundamenta en los principios y lineamientos de la Organización de Aviación Civil Internacional (OACI) cumpliendo con las normas y métodos recomendados relativos a la gestión de seguridad operacional.

Se busca fortalecer la gestión del riesgo, la vigilancia continua y la mejora constante de los sistemas de aviación civil del Estado de Honduras.

Lista de Páginas Efectivas

Página #	Edición/ Enmienda	Fecha
Portada	Primera Edición	15 Julio de 2025
CF-1	Primera Edición	15 Julio de 2025
SEE-1	Primera Edición	15 Julio de 2025
REE-1	Primera Edición	15 Julio de 2025
PRE-1	Primera Edición	15 Julio de 2025
LPE-1	Primera Edición	15 Julio de 2025
LPE-2	Primera Edición	15 Julio de 2025
LPE-3	Primera Edición	15 Julio de 2025
LPE-4	Primera Edición	15 Julio de 2025
TC-1	Primera Edición	15 Julio de 2025
TC-2	Primera Edición	15 Julio de 2025
TC-3	Primera Edición	15 Julio de 2025
TC-4	Primera Edición	15 Julio de 2025
TC-5	Primera Edición	15 Julio de 2025
TC-6	Primera Edición	15 Julio de 2025
SECCION 1		
1-1-1	Primera Edición	15 Julio de 2025
1-1-2	Primera Edición	15 Julio de 2025
LISTA DE ABREVIATURAS		
LA-1	Primera Edición	15 Julio de 2025
LA-2	Primera Edición	15 Julio de 2025
LA-3	Primera Edición	15 Julio de 2025
LA-4	Primera Edición	15 Julio de 2025
SUBPARTE A		
1-A-1	Primera Edición	15 Julio de 2025
1-A-2	Primera Edición	15 Julio de 2025
1-A-3	Primera Edición	15 Julio de 2025
1-A-4	Primera Edición	15 Julio de 2025
1-A-5	Primera Edición	15 Julio de 2025
1-A-6	Primera Edición	15 Julio de 2025
SUBPARTE B		
1-B-1	Primera Edición	15 Julio de 2025
1-B-2	Primera Edición	15 Julio de 2025
SUBPARTE C		
1-C-1	Primera Edición	15 Julio de 2025
1-C-2	Primera Edición	15 Julio de 2025
1-C-3	Primera Edición	15 Julio de 2025
1-C-4	Primera Edición	15 Julio de 2025
SUBPARTE D		
1-D-1	Primera Edición	15 Julio de 2025
1-D-2	Primera Edición	15 Julio de 2025

Página #	Edición/ Enmienda	Fecha
SUBPARTE E		
1-E-1	Primera Edición	15 Julio de 2025
1-E-2	Primera Edición	15 Julio de 2025
1-E-3	Primera Edición	15 Julio de 2025
1-E-4	Primera Edición	15 Julio de 2025
1-E-5	Primera Edición	15 Julio de 2025
1-E-6	Primera Edición	15 Julio de 2025
1-E-7	Primera Edición	15 Julio de 2025
1-E-8	Primera Edición	15 Julio de 2025
1-E-9	Primera Edición	15 Julio de 2025
1-E-10	Primera Edición	15 Julio de 2025
SUBPARTE F		
1-F-1	Primera Edición	15 Julio de 2025
1-F-2	Primera Edición	15 Julio de 2025
1-F-3	Primera Edición	15 Julio de 2025
1-F-4	Primera Edición	15 Julio de 2025
SUBPARTE G		
1-G-1	Primera Edición	15 Julio de 2025
1-G-2	Primera Edición	15 Julio de 2025
1-G-3	Primera Edición	15 Julio de 2025
1-G-4	Primera Edición	15 Julio de 2025
1-G-5	Primera Edición	15 Julio de 2025
1-G-6	Primera Edición	15 Julio de 2025
SUBPARTE H		
1-H-1	Primera Edición	15 Julio de 2025
1-H-2	Primera Edición	15 Julio de 2025
1-H-3	Primera Edición	15 Julio de 2025
1-H-4	Primera Edición	15 Julio de 2025
1-H-5	Primera Edición	15 Julio de 2025
1-H-6	Primera Edición	15 Julio de 2025
SUBPARTE I		
1-I-1	Primera Edición	15 Julio de 2025
1-I-2	Primera Edición	15 Julio de 2025
1-I-3	Primera Edición	15 Julio de 2025
1-I-4	Primera Edición	15 Julio de 2025
1-I-5	Primera Edición	15 Julio de 2025
1-I-6	Primera Edición	15 Julio de 2025
1-I-7	Primera Edición	15 Julio de 2025
1-I-8	Primera Edición	15 Julio de 2025
1-I-9	Primera Edición	15 Julio de 2025
1-I-10	Primera Edición	15 Julio de 2025
SUBPARTE J		
1-J-1	Primera Edición	15 Julio de 2025
1-J-2	Primera Edición	15 Julio de 2025
SUBPARTE K		
1-K-1	Primera Edición	15 Julio de 2025
1-K-2	Primera Edición	15 Julio de 2025
SUBPARTE L		
1-L-1	Primera Edición	15 Julio de 2025
1-L-2	Primera Edición	15 Julio de 2025

Página #	Edición/ Enmienda	Fecha
SUBPARTE M		
1-M-1	Primera Edición	15 Julio de 2025
1-M-2	Primera Edición	15 Julio de 2025
SUBPARTE N		
1-N-1	Primera Edición	15 Julio de 2025
1-N-2	Primera Edición	15 Julio de 2025
1-N-3	Primera Edición	15 Julio de 2025
1-N-4	Primera Edición	15 Julio de 2025
1-N-5	Primera Edición	15 Julio de 2025
1-N-6	Primera Edición	15 Julio de 2025
1-N-7	Primera Edición	15 Julio de 2025
1-N-8	Primera Edición	15 Julio de 2025
APENDICE 1		
1-AP1-1	Primera Edición	15 Julio de 2025
1-AP1-2	Primera Edición	15 Julio de 2025
APENDICE 2		
1-AP2-1	Primera Edición	15 Julio de 2025
1-AP2-2	Primera Edición	15 Julio de 2025
1-AP2-3	Primera Edición	15 Julio de 2025
1-AP2-4	Primera Edición	15 Julio de 2025
APENDICE 3		
1-AP3-1	Primera Edición	15 Julio de 2025
1-AP3-2	Primera Edición	15 Julio de 2025
1-AP3-3	Primera Edición	15 Julio de 2025
1-AP3-4	Primera Edición	15 Julio de 2025
1-AP3-5	Primera Edición	15 Julio de 2025
1-AP3-6	Primera Edición	15 Julio de 2025
APENDICE 4		
1-AP4-1	Primera Edición	15 Julio de 2025
1-AP4-2	Primera Edición	15 Julio de 2025
1-AP4-3	Primera Edición	15 Julio de 2025
1-AP4-4	Primera Edición	15 Julio de 2025
1-AP4-5	Primera Edición	15 Julio de 2025
1-AP4-6	Primera Edición	15 Julio de 2025
1-AP4-7	Primera Edición	15 Julio de 2025
1-AP4-8	Primera Edición	15 Julio de 2025
1-AP4-9	Primera Edición	15 Julio de 2025
1-AP4-10	Primera Edición	15 Julio de 2025
1-AP4-11	Primera Edición	15 Julio de 2025
1-AP4-12	Primera Edición	15 Julio de 2025
1-AP4-13	Primera Edición	15 Julio de 2025
1-AP4-14	Primera Edición	15 Julio de 2025
1-AP4-15	Primera Edición	15 Julio de 2025
1-AP4-16	Primera Edición	15 Julio de 2025
1-AP4-17	Primera Edición	15 Julio de 2025
1-AP4-18	Primera Edición	15 Julio de 2025
APENDICE 5		
1-AP5-1	Primera Edición	15 Julio de 2025
1-AP5-2	Primera Edición	15 Julio de 2025

Página #	Edición/ Enmienda	Fecha
APENDICE 6		
1-AP6-1	Primera Edición	15 Julio de 2025
1-AP6-2	Primera Edición	15 Julio de 2025
1-AP6-3	Primera Edición	15 Julio de 2025
1-AP6-4	Primera Edición	15 Julio de 2025
1-AP6-5	Primera Edición	15 Julio de 2025
1-AP6-6	Primera Edición	15 Julio de 2025
1-AP6-7	Primera Edición	15 Julio de 2025
1-AP6-8	Primera Edición	15 Julio de 2025
1-AP6-9	Primera Edición	15 Julio de 2025
1-AP6-10	Primera Edición	15 Julio de 2025
APENDICE 7		
1-AP7-1	Primera Edición	15 Julio de 2025
1-AP7-2	Primera Edición	15 Julio de 2025
1-AP7-3	Primera Edición	15 Julio de 2025
1-AP7-4	Primera Edición	15 Julio de 2025
1-AP7-5	Primera Edición	15 Julio de 2025
1-AP7-6	Primera Edición	15 Julio de 2025
1-AP7-7	Primera Edición	15 Julio de 2025
1-AP7-8	Primera Edición	15 Julio de 2025
1-AP7-9	Primera Edición	15 Julio de 2025
1-AP7-10	Primera Edición	15 Julio de 2025
APENDICE 8		
1-AP8-1	Primera Edición	15 Julio de 2025
1-AP8-2	Primera Edición	15 Julio de 2025
1-AP8-3	Primera Edición	15 Julio de 2025
1-AP8-4	Primera Edición	15 Julio de 2025
1-AP8-5	Primera Edición	15 Julio de 2025
1-AP8-6	Primera Edición	15 Julio de 2025
1-AP8-7	Primera Edición	15 Julio de 2025
1-AP8-8	Primera Edición	15 Julio de 2025
1-AP8-9	Primera Edición	15 Julio de 2025
1-AP8-10	Primera Edición	15 Julio de 2025
1-AP8-11	Primera Edición	15 Julio de 2025
1-AP8-12	Primera Edición	15 Julio de 2025
1-AP8-13	Primera Edición	15 Julio de 2025
1-AP8-14	Primera Edición	15 Julio de 2025
APENDICE 9		
1-AP9-1	Primera Edición	15 Julio de 2025
1-AP9-2	Primera Edición	15 Julio de 2025
1-AP9-3	Primera Edición	15 Julio de 2025
1-AP9-4	Primera Edición	15 Julio de 2025

Tabla de Contenido

Portada.....**Port-1**
Control de Firmas CF-1
SISTEMA DE EDICION Y ENMIENDAS.....SSE-1
Registro de Edición y Enmiendas REE-1
Preámbulo PRE-1
Lista de Páginas Efectivas LPE-1
Tabla de Contenido.....,.TC-1
SECCIÓN 1. REQUISITOS.....1-1-1
Lista de Abreviaturas..... .....LA-1
SUBPARTE A. DEFINICIONES 1-A-1
SUBPARTE B. GENERALIDADES 1-B-1
RAC 19.005 Presentación 1-B-1
RAC 19.010 Introducción General 1-B-1
SUBPARTE C. APLICABILIDAD.....1-C-1
RAC 19.015 Aplicabilidad.....1-C-1
RAC 19.020 Enunciado de los Componentes y Elementos del SMS 1-C-2
RAC 19.025 Reconocimiento del SMS de Organizaciones de Instrucción de otros estados 1-C-2
RAC 19.030 Reconocimiento del SMS de Organismos de Mantenimiento de otros Estados. 1-C-3
RAC 19.035 Reconocimiento del SMS de Proveedores de Servicios de Navegación Aérea de otros Estados.....1-C-3
RAC 19.040 Aplicabilidad de las Sanciones..... 1-C-3
SUBPARTE D. EFECTIVIDAD..... 1-D-1
RAC 19.045 Efectividad 1-D-1
RAC 19.050 Directivas Operacionales 1-D-1
SUBPARTE E. COMPONENTE I: POLITICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL.....
..... 1-E-1
RAC 19.055 Responsabilidad Funcional y Compromiso de la Dirección 1-E-1
RAC 19.060 Obligación de Rendición de Cuentas sobre la Seguridad Operacional..... 1-E-2
RAC 19.065 Responsabilidad Respecto a las Actividades Contratadas 1-E-2
RAC 19.070 Designación del Personal Clave de Seguridad Operacional..... .1-E-3
RAC 19.075 Designación y Responsabilidad del Ejecutivo Responsable 1-E-3
RAC 19.080 Designación y Responsabilidades del Gerente de Seguridad Operacional..... 1-E-4
RAC 19.085 Grupos para la Gestión de la Seguridad Operacional..... 1-E-5
RAC 19.090 Coordinación de la Planificación de Respuestas ante Emergencias (ERP)..... .1-E-6

RAC 19.095 Documentación SMS 1-E-8

SUBPARTE F. COMPONENTE II: GESTION DE RIESGOS DE SEGURIDAD OPERACIONAL1-F-1

RAC 19.100 Generalidades 1-F-1

RAC 19.105 Identificación de peligros (Ver Apéndice 3) 1-F-1

RAC 19.110 Evaluación y mitigación de riesgos de seguridad operacional ……1-F-2

RAC 19.115 Documentación para la identificación de los peligros y para la evaluación y mitigación de riesgos de seguridad operacional 1-F-3

SUBPARTE G. COMPONENTE III: ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL..1-G-1

RAC 19.120 Observación y medición del rendimiento en materia de seguridad operacional 1-G-1

RAC 19.125 Gestión del cambio 1-G-3

RAC 19.130 Mejora continua del SMS.....1-G-5

RAC 19.135 Documentación para la observación y medición del rendimiento en materia de seguridad operacional, para la gestión del cambio y para la mejora continua del SMS 1-G-6

SUBPARTE H. COMPONENTE IV: PROMOCION DE LA SEGURIDAD OPERACIONAL.....1-H-1

RAC 19.140 Generalidades 1-H-1

RAC 19.145 Instrucción y educación 1-H-1

RAC 19.150 Comunicación de la seguridad operacional.....1-H-4

RAC 19.155 DOCUMENTACIÓN PARA LA INSTRUCCIÓN Y EDUCACIÓN Y PARA LA COMUNICACIÓN DE LA SEGURIDAD OPERACIONAL 1-H-5

SUBPARTE I. COMPONENTES PARA LA IMPLEMENTACION Y ACEPTACION DEL SMS 1-I-1

RAC 19.160 ENFOQUE POR COMPONENTES PARA LA IMPLEMENTACIÓN Y LA ACEPTACIÓN DEL SMS 1-I-1

RAC 19.165 Componente I. Requisitos para la implementación y aceptación Componente I…….....1-I-1

RAC 19.170 Componente II. Requisitos para la implementación y aceptación del componente II…….....1-I-2

RAC 19.175 Componente III. Requisitos para la implementación y la aceptación del componente III. …….....1-I-4

RAC 19.180 Componente IV. Requisitos para la implementación y la aceptación del componente IV. 1-I-5

RAC 19.185 TIEMPO DE ACEPTACIÓN DE LOS COMPONENTES DEL SMS PARA TODOS LOS PROVEEDORES DE SERVICIOS AERONÁUTICOS:.....1-I-8

RAC 19.190 Plan de implementación del SMS.....1-I-8

RAC 19.195 Procedimiento de aceptación del plan de implementación de un SMS.....1-I-8

RAC 19.200 Aceptación o Negación de un plan de implementación de un SMS.....1-I-8

RAC 19.205 Procedimiento de aceptación de los componentes de un SMS

.....1-I-9
RAC 19.210 Procedimiento de aceptación final de un SMS 1-I-9
RAC 19.215 Auditorías de seguimiento 1-I-9
SUBPARTE J. NOTIFICACION 1-J-1
RAC 19.220 Sistema de notificación obligatorio 1-J-1
RAC 19.225 Categorías de los sucesos..... 1-J-1
SUBPARTE K. NOTIFICACION VOLUNTARIA........1-K-1
RAC 19.230 Sistema de notificación voluntaria. 1-K-1
RAC 19.235 Alcance 1-K-1
SUBPARTE L. TRATAMIENTO DE LA INFORMACION 1-L-1
RAC 19.240 Recolección y conservación de la información.....1-L-1
RAC 19.245 Calidad y contenido de las notificaciones de sucesos 1-L-1
SUBPARTE M. ANALISIS DE LOS SUCESOS 1-M-1
RAC 19.250 Análisis de sucesos y seguimiento a nivel nacional 1-M-1
SUBPARTE N. CONFIDENCIALIDAD Y PROTECCION DE LA FUENTES DE INFORMACION....
.....1-N-1
RAC 19.255 Naturaleza y Objetivo 1-N-1
RAC 19.260 Alcance 1-N-1
RAC 19.265 Uso apropiado de la información sobre seguridad operacional 1-N-1
RAC 19.270 Principios de protección de las fuentes de información 1-N-1
RAC 19.275 Excepciones al principio de confidencialidad 1-N-1
RAC 19.280 Medidas de salvaguarda.....1-N-2
RAC 19.285 Medidas de salvaguarda concerniente a la información sobre terceros 1-N-2
RAC 19.290 Excepciones a la protección de la recopilación y el procesamiento de datos 1-N-2
RAC 19.295 Registrador de datos de vuelo.....1-N-3
RAC 19.300 Acuerdos tomados con el proveedor de servicios 1-N-3
RAC 19.305 Protección de la información contenida en los acuerdos 1-N-3
RAC 19.310 Excepciones a la confidencialidad de los acuerdos 1-N-4
RAC 19.315 Confidencialidad de los informes voluntarios 1-N-4
RAC 19.320 Excepciones a la confidencialidad de los informes voluntarios.....1-N-4
RAC 19.325 Uso de la información de seguridad operacional 1-N-5
RAC 19.330 Difusión de información de seguridad operacional entre los Estados contratantes de la OACI 1-N-6
Apéndice 1 Ejemplo de una declaración de la Política de Seguridad Operacional 1-AP1-1
Apéndice 2 Ejemplo de Designación de Clave de Seguridad Operacional 1-AP2-1
Propósito General.....1-AP2-1

Funciones Claves 1-AP2-1

Apéndice 3 Coordinación de la Planificación de Respuesta ante Emergencias.....1-AP3-1
Documentación del SMS.....1-AP3-2
Componente 2: Gestión de Riesgos de Seguridad Operacional.....1-AP3-2
Identificación de peligros.....1-AP3-4
Fuentes para la identificación de peligros.....1-AP3-4

Ejemplo de Proceso de Identificación y Gestión del Riesgo..... 1-AP3-5

Apéndice 4 Indicadores y metas de rendimiento en materia de seguridad operacional 1-AP4-1

Indicadores cualitativos y cuantitativos 1-AP4-1

Indicadores de resultados (lagging en inglés) y avanzados (leading en inglés) 1-AP4-2

Selección y definición de los SPI..... 1-AP4-4

Definición de los SPI 1-AP4-6

Los SPI y las notificaciones de seguridad operacional..... 1-AP4-6

Establecimiento de metas de rendimiento en materia de seguridad operacional..... 1-AP4-7

Establecimiento de metas con objetivos de seguridad operacional de alto nivel 1-AP4-8

Establecimiento de metas con objetivos de seguridad SMART 1-AP4-8

Consideraciones adicionales para la selección de SPI y SPT 1-AP4-10

Advertencias para el establecimiento de SPT 1-AP4-11

Medición del rendimiento en materia de seguridad operacional..... 1-AP4-11

Uso de SPI y SPT 1-AP4-12

Observación del rendimiento en materia de seguridad operacional..... 1-AP4-12

Rendimiento básico en materia de seguridad operacional..... 1-AP4-12

Perfeccionamiento de los SPI y los SPT 1-AP4-12

Actividades de seguridad operacional 1-AP4-14

Advertencia sobre los indicadores 1-AP4-16

Apéndice 5 Gestión Estatal de los Riesgos de Seguridad Operacional.....1-AP5-1

Obligaciones de Otorgamiento de Licencias, Certificaciones, Autorizaciones y Aprobaciones.....
.....1-AP5-1
Obligaciones del Sistema de Gestión de la Seguridad Operacional.....1-AP5-2

Apéndice 6 Guía sobre el desarrollo de un manual de SMS 1-AP6-1
1.Control de documentos.....1-AP6-2

2. Requisitos Reglamentarios.....1-AP6-3

3. Alcance e integración del sistema de gestión de la seguridad operacional.....1-AP6-3

4.Política de seguridad operacional.....1-AP6-4

5. Objetivos de seguridad operacional.....1-AP6-4

6.Funciones y responsabilidades.....1-AP6-5

7.Notificación de seguridad operacional.....1-AP6-5

8.Identificación de peligros y evaluación de riesgos……1-AP6-6
9.Control y medición del rendimiento en materia de seguridad operacional……..1-AP6-6
10. Investigaciones relacionadas con la seguridad operacional y las medidas correctivas……1-AP6-7
11.Capacitación y comunicación de seguridad operacional 1-AP6-7
12. Mejora continua y auditoría de SMS……1-AP6-8
13.Gestión de los registros de SMS……..1-AP6-8
14.Gestión de cambio……..1-AP6-8
15.Plan de respuesta ante emergencias/contingencia……..1-AP6-9
Apéndice 7 Matrices de Gestión de Riesgo de Seguridad Operacional 1-AP7-1
Tabla 1 – Tabla de probabilidad de riesgo de seguridad operacional 1-AP7-2
Gravedad del Riesgo de Seguridad Operacional……..1-AP7-2
Tabla 2 – Ejemplo de gravedad del riesgo de seguridad operacional 1-AP7-3
Tolerabilidad del Riesgo de Seguridad Operacional……..1-AP7-4
Tabla 3 – Ejemplo de matriz de riesgos de seguridad operacional 1-AP7-4
Tabla 4. Ejemplo de tabla de tolerabilidad del riesgo de seguridad operacional……1-AP7-5
Evaluación de Riesgos relacionados con Factores Humanos……..1-AP7-5
Estrategias de Mitigación riesgos de seguridad operacional……..1-AP7-6
Documentación de la gestión de riesgos de seguridad operacional……1-AP7-8
Analisis de Costo Beneficios……1-AP7-9
Apéndice 8 Lista de Clasificación de Sucesos Operacionales.....1-AP8-1
A. Sucesos Operacionales 1-AP8-1
1.1 Preparación del vuelo:..... 1-AP8-1
1.2 Preparación de la aeronave: 1-AP8-1
1.3 Despegue y aterrizaje: 1-AP8-1
1.4 Cualquier fase del vuelo 1-AP8-2
1.5 Otros tipos de sucesos 1-AP8-2
1.6 Sucesos Técnicos... ..... 1-AP8-2
1.7 Sistemas de propulsión (incluidos motores, hélices y rotores) y unidades de potencia auxiliar (APU) 1-AP8-3
2. Interacción con los servicios de navegación aérea (ANS) y la gestión del tránsito aéreo(ATM)…… 1-AP8-4
3. Emergencias y otras situaciones críticas.....1-AP8-4

4.Entorno exterior y meteorología 1-AP8-5

B. Sucesos relacionados con las condiciones técnicas, el mantenimiento y la reparación de las aeronaves…….. .....1-AP8-5

1. Fabricación 1-AP8-5

2. Diseño.....1-AP8-5

3. Mantenimiento y gestión de la aeronavegabilidad continuada.....1-AP8-6

C. Sucesos relacionados con los servicios e instalaciones de navegación aérea. 1-AP8-7

1. Sucesos relacionados con aeronaves..... 1-AP8-7

2. Degradación o pérdida total de servicios o funciones 1-AP8-8

3. Otros sucesos 1-AP8-8

D. Sucesos relacionados con los aeródromos y los servicios en tierra. 1-AP8-9

1. Gestión de la Seguridad Operacional de un Aeródromo..... 1-AP8-9

1.1 Sucesos relacionados con aeronaves y obstáculos 1-AP8-9

1.2 Degradación o pérdida total de servicios o funciones 1-AP8-9

1.3 Otros sucesos.....1-AP8-10

2. Asistencia en tierra de una aeronave.....1-AP8-10

E. Sucesos relacionados con aeronaves distintas de los moto propulsadas complejas, incluidos los planeadores y los vehículos más ligeros que el aire.....1-AP8-11

1.1 Operaciones aéreas….....1-AP8-11

1.2 Sucesos técnicos…….....1-AP8-11

1.3 Interacción con los servicios de navegación aérea y la gestión del tránsito aéreo 1-AP8-11

1.4 Emergencias y otras situaciones críticas.....1-AP8-11

1.5 Entorno exterior y meteorología.....1-AP8-12

2. Vehículos más ligeros que el aire (globos y dirigibles).....1-AP8-12

2.1 Operaciones Aéreas.....1-AP8-12

2.2 Sucesos técnicos 1-AP8-12

2.3 Interacción con los servicios de navegación aérea y la gestión del tránsito aéreo 1-AP8-12

2.4 Emergencias y otras situaciones críticas 1-AP8-12

2.5 Entorno exterior y meteorología..... 1-AP8-13

Apéndice 9 Lista de Requisitos aplicables a los sistemas obligatorios y voluntarios de los sucesos 1-AP9-1

A. Campos de datos obligatorios comunes 1-AP9-1

B. Campos de datos relacionados con las aeronaves 1-AP9-1

C. Campos de datos relacionados con los servicios de navegación aérea 1-AP9-2

D. Campos de datos relacionados con una infracción de las mínimas de separación/pérdida de separación y violación del espacio aéreo 1-AP9-3

E. Campos de datos relacionados con los aeródromos 1-AP9-3

F. Campos de datos relacionado con daños a la aeronave o lesiones producidas a la personal 1-AP 9-3

SECCIÓN 1. REQUISITOS

(a) PRESENTACION

(1) La sección uno del RAC 19 se presenta en páginas sueltas formadas por una sola columna. Cada página se identifica mediante la fecha de la edición o enmienda mediante la cual se incorporó.

(2) La letra de esta sección es arial 10.

(b) INTRODUCCIÓN

(1) En virtud de la creciente complejidad del sistema mundial de transporte aéreo y la interrelación de sus actividades, la RAC 19 surge como una herramienta esencial para fortalecer la seguridad operacional en la aviación civil. Esta regulación establece los lineamientos necesarios para implementar un Programa Estatal de Seguridad Operacional (SSP), promoviendo una estrategia preventiva que permita mejorar el rendimiento en materia de seguridad.

(2) La RAC 19 integra en un solo cuerpo normativo las disposiciones que orientan a los proveedores de servicios aeronáuticos y a las autoridades estatales en la identificación, evaluación y mitigación de riesgos, fomentando una cultura de seguridad proactiva y sostenible.

INTENCIONALMENTE EN BLANCO

Lista de Abreviaturas:

AHAC	Agencia Hondureña de Aeronáutica Civil
ADREP	Sistema de notificación de datos sobre accidentes/incidentes
ADRS	Sistema registrador de datos de aeronave
AIG	Unidad de Investigación de Accidentes e Incidentes
AIR	Unidad de Aeronavegabilidad
AIRS	Sistema registrador de imágenes de a bordo
AIS	Servicios de información aeronáutica
ALoSP	Nivel aceptable de rendimiento en materia de seguridad operacional
AMO	Organismo de mantenimiento reconocido
AMS	Programa de mantenimiento de aeronaves
ANS	Servicios de Navegación Aérea
AOC	Certificado de explotador de servicios aéreos
AOG	Aeronave en tierra
APU	Unidad de poder auxiliar
ATC	Control de Tránsito Aéreo
ATM	Gestión del Tránsito Aéreo
ATS	Servicios de Tránsito Aéreo
CA	Circular de Asesoramiento
CARS	Sistema registrador de audio en el puesto de pilotaje
CBA	Análisis de costo beneficio
CFIT	Impacto contra el suelo sin pérdida de control
CMA	Enfoque de observación continua
CIAIA	Comisión de Investigación de Accidentes e Incidentes de Aviación
CMC	Centro de gestión de crisis
CNS	Comunicaciones, navegación y vigilancia
IATA	Asociación del Transporte Aéreo Internacional
ILS	Sistema de aterrizaje por instrumentos
IMC	Condiciones meteorológicas de vuelo por instrumentos

ISO	Organización Internacional de Normalización
LOC-I	Pérdida de control en vuelo.
LOSA	Auditoría de la seguridad de las operaciones de línea
MDR	Informe obligatorio de defectos
MEL	Lista de equipo mínimo
OACI	Organización de Aviación Civil Internacional
OHSMS	Sistema de gestión sobre cuestiones de salud y seguridad del trabajo
OPS	Operaciones
PMI	Inspector principal de mantenimiento
POI	Inspector principal de operaciones
QA	Aseguramiento de la calidad
RAC	Regulación Aeronáutica Civil
RAIO	Organización regional de investigación de accidentes e incidentes
SAR	Servicio de búsqueda y salvamento
SARPs	Normas y métodos recomendados de la OACI
SD	Desviación estándar
SDCPS	Sistema de recopilación y procesamiento de datos sobre seguridad operacional
SMM	Manual de Gestión de la Seguridad Operacional

SMP	Grupo de expertos sobre gestión de la seguridad operacional
SMS	Sistema de Gestión de la Seguridad Operacional
SPI	Indicador de rendimiento en materia de seguridad operacional
SPT	Objetivos de rendimiento en materia de seguridad operacional
SRB	Comité de revisión de seguridad operacional
SSP	Departamento del Programa Estatal de Seguridad Operacional

INTENCIONALMENTE EN BLANCO

SUBPARTE A DEFINICIONES Y ABREVIATURAS

DEFINICIONES:

Las siguientes definiciones ofrecen el marco de referencia común para los proveedores de servicios del Programa Estatal de Seguridad Operacional (SSP).

Cuando los términos y expresiones indicados a continuación se emplean en la presente Regulación, tendrán los significados siguientes:

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

(a) cualquier persona sufre lesiones mortales o graves a consecuencia de:

- hallarse en la aeronave, o
- por contacto directo con cualquier parte de la aeronave, incluso las partes que se hayan desprendido de la aeronave, o
- por exposición directa al chorro de un reactor,

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

(b) la aeronave sufre daños o roturas estructurales que:

- afectan adversamente su resistencia estructural, su performance o sus características de vuelo; y
- que normalmente exigen una reparación importante o el recambio del componente afectado,

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

(c) la aeronave desaparece o es totalmente inaccesible.

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

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

Nota 3. — El tipo de sistema de aeronave no tripulada que se investigará se trata en 5.1 del Anexo 13 al Convenio de Aviación Civil Internacional.

Nota 4. — En el Adjunto E del Anexo 13 al Convenio de Aviación Civil Internacional figura orientación para determinar los daños de aeronave.

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

Aeronave propulsada compleja:

(d) un avión:

- con una masa máxima certificada de despegue superior a 5700 kg; o
- certificado para una configuración máxima de más de 19 asientos de pasajeros, o
- certificado para operar con una tripulación mínima de dos pilotos, o
- equipado con un turborreactor o con más de un motor turbohélice, o

(e) un helicóptero certificado:

- para una masa máxima certificada de despegue superior a 3 175 kg, o
- para una configuración máxima de más de nueve asientos de pasajeros, o
- para operar con una tripulación mínima de dos pilotos, o

(f) una aeronave de rotor basculante.

Anonimización: La eliminación, en las notificaciones de sucesos, de todos los datos personales referentes al notificante y a las personas mencionadas en relación con el suceso, y de todos aquellos datos, como el nombre de la organización o las

organizaciones implicadas en el suceso, que permitan identificar al notificante o a terceros o que den lugar a que esa identidad se deduzca de dicha información.

Coordinador SMS: Profesional designado para coordinar actividades específicas del Sistema de Gestión de Seguridad Operacional, facilitando la implementación de procesos, el seguimiento de indicadores y la integración de la seguridad operacional.

Cultura justa: Aquella en la que no se castigue a los operadores y demás personal de primera línea por sus acciones, omisiones o decisiones cuando sean acordes con su experiencia y capacitación, pero en la cual no se toleren la negligencia grave, las infracciones intencionadas ni los actos destructivos

Datos sobre seguridad operacional. Conjunto de hechos definidos o conjunto de valores de seguridad operacional recopilados de diversas fuentes de aviación, que se utiliza para mantener o mejorar la seguridad operacional.

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

(a) investigaciones de accidentes o incidentes;

(b) notificaciones de seguridad operacional;

(c) notificaciones sobre el mantenimiento de la aeronavegabilidad;

(d) supervisión de la eficiencia operacional;

(e) inspecciones, auditorías, constataciones; o

(f) estudios y exámenes de seguridad operacional.

Ejecutivo responsable: Es la autoridad máxima dentro de la organización en cuanto a seguridad operacional. Encargado de garantizar que el Sistema de Gestión de la Seguridad Operacional esté implementado, mantenido y reciba los recursos necesarios para su funcionamiento. Su liderazgo es estratégico, institucional y transversal, articulando la seguridad operacional con la visión organizacional y los objetivos empresariales.

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.

Gerente de seguridad operacional*:* Profesional designado para operar y coordinar técnicamente el SMS en la práctica diaria. Lidera su implementación, seguimiento y mejora continua, siendo el puente entre los procesos operativos y la estructura de gestión.

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

Nota. — Algunos Estados emplean el término "giro avión" como alternativa de "helicóptero".

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

Nota. — Entre los tipos de incidentes que son de interés para los estudios relacionados con la seguridad operacional figuran los incidentes enumerados en el Anexo 13, Adjunto C al Convenio de Aviación Civil Internacional.

Indicador de rendimiento en materia de seguridad operacional. Parámetro basado en datos que se utiliza para observar y evaluar el rendimiento en materia de seguridad operacional.

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

Lesión grave. Cualquier lesión sufrida por una persona en un accidente y que:

(a) requiera hospitalización durante más de 48 horas dentro de los siete días contados a partir de la fecha en que se sufrió la lesión; o/y
(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/y
(c) ocasione laceraciones que den lugar a hemorragias graves, lesiones a nervios, músculos o tendones; o/y
(d) ocasione daños a cualquier órgano interno; o/y
(e) ocasione quemaduras de segundo o tercer grado u otras quemaduras que afecten más del 5% de la superficie del cuerpo; o/y
(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.

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

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

No conformidades: Aspectos de la organización que requieren medidas de subsanación. Se categorizan en tres niveles:

Nivel 1: Tiene una influencia mayor en la seguridad operacional donde representan un peligro. Deben de ser rectificados de manera inmediata a menos que el inspector disponga lo contrario, siendo que se podría dar un plazo no

mayor a 72 horas para su solución. Si se refiere a un sistema o procedimiento que necesita ser documentado e implementado, el proveedor de servicios contará con un periodo no mayor a 30 días hábiles, después de recibido el informe, para iniciar con el desarrollo de la acción correctiva.
Nivel 2: Tiene una influencia moderada en la seguridad de las operaciones por tanto requiere una medida de mitigación. Estos hallazgos deben de ser rectificados dentro de un periodo no mayor de 90 días después de recibido el informe.
Nivel 3: Tiene una influencia menor en la seguridad operacional. Estos hallazgos deben ser rectificados dentro de un período no mayor a 120 días después de recibido el informe.
Observaciones: Son hallazgos que tienen la característica de una recomendación para la mejora del SMS. El proveedor de servicios determinará si las implementa. Al momento de presentar el plan de acción correctivo se debe indicar si se implementan o no. En caso de no hacerlo se debe de justificar por parte del proveedor de servicios la decisión.

Notificante: una persona física que notifica un suceso en virtud de la presente regulación.

Organización: Cualquier organización que ofrezca productos en el sector de la aviación o que emplee, contrate o utilice los servicios de personas que deban notificar los sucesos de conformidad con lo establecido en esta regulación.

Parte interesada: Cualquier persona física, cualquier persona jurídica o cualquier organismo oficial, con o sin personalidad jurídica propia, que pueda contribuir a mejorar la seguridad de la aviación civil accediendo a la información sobre sucesos que se intercambien los estados y organizaciones.

***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 están en posición de notificar información sobre seguridad operacional.

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

Planeador: una aeronave más pesada que el aire sustentado en vuelo por la reacción dinámica del aire contra sus superficies de sustentación fijas y cuyo vuelo libre no depende de un motor, incluidos alas delta, parapentes y otras embarcaciones comparables.

Programa Estatal de Seguridad Operacional (SSP). Conjunto integrado de reglamentos y actividades destinado a mejorar la seguridad operacional.

Proveedores de servicios: para efectos de la presente regulación entiéndase como

cualquier proveedor/explotador de servicios aeronáuticos, centro de instrucción, organización de mantenimiento, servicio de tránsito aéreo, operador de aeródromo, operador aéreo, a los que se les deba de exigir un SMS de acuerdo RAC-19.015.

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.

Suceso: Cualquier acontecimiento relacionado con la seguridad que ponga en peligro que, en caso de no ser corregido o abordado, pueda poner en peligro una aeronave, sus ocupantes o cualquier otra persona, incluidos, en particular, los accidentes e incidentes graves.

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.

SUBPARTE B. GENERALIDADES

RAC 19.005 Presentación

(a) El contenido de la sección 1 es de acatamiento obligatorio, todos y cada uno de los requisitos que se encuentren dentro de esta sección, como de los apéndices a las mismas, las tablas, figuras a las que se haga referencia específica y que estén igualmente dentro de la sección. De igual forma, a todas las normas se les ha dotado de un título que implique un resumen del contenido de la misma, de manera que facilite su manejo y compresión.

(b) El contenido de la sección 2 ilustra los medios o los alternativos, pero no necesariamente los únicos medios posibles, para suplir con un párrafo específico cada una de las normas que lo necesite, teniendo en el formato electrónico su respectivo hipervínculo que permite un manejo más ágil y eficiente del documento.

RAC 19.010 Introducción General

En virtud de la creciente complejidad del sistema mundial de transporte aéreo y la interrelación de sus actividades, la **RAC 19** surge como una herramienta esencial para fortalecer la seguridad operacional en la aviación civil de Honduras. Esta regulación establece los lineamientos necesarios para implementar un **Programa Estatal de Seguridad Operacional (SSP)**, promoviendo una estrategia preventiva que permita mejorar el rendimiento en materia de seguridad operacional a través de los **Sistemas de Gestión de Seguridad Operacional (SMS).**

La RAC 19 integra en un solo cuerpo normativo las disposiciones que orientan a los proveedores de servicios y a las autoridades estatales en la identificación, evaluación y mitigación de riesgos, fomentando una cultura de seguridad proactiva y sostenible.

.

INTENCIONALMENTE EN BLANCO

SUBPARTE C. APLICABILIDAD

RAC 19.015 Aplicabilidad

(a) Este RAC 19 prescribe las normas que regulan un Sistema de Gestión de la Seguridad Operacional aplicable a:

(1) Organizaciones de instrucción reconocidas, de conformidad con el RAC-LPTA, RAC-141, regulación de las Escuelas de Aviación vigente, que están expuestas a riesgos de seguridad operacional relacionados con las operaciones de aeronaves al prestar sus servicios;
(2) Explotadores de aviones o helicópteros autorizados para llevar a cabo actividades de transporte aéreo comercial internacional, de conformidad con el RAC OPS 1, el RAC 02, y la RAC OPS 3 Transporte Aéreo Comercial Nacional e Internacional (Helicópteros).
(3) Organismos de mantenimiento reconocidos que ofrecen servicios a los explotadores de aviones o helicópteros dedicados al transporte comercial internacional, de conformidad con el RAC-OPS 1, RAC-43, RAC-145, RAC-39 y RAC-21.
(4) Proveedores de servicios de tránsito aéreo (ATS), de conformidad con el RAC-ATS.
(5) Aeródromos de conformidad con el RAC-139 y el RAC-14.

(b) Todo proveedor de servicios establecerá y mantendrá actualizado un SMS, según las dimensiones y complejidad de su organización o servicios de aviación, de la forma y manera aceptable por la Agencia Hondureña de Aeronáutica Civil, a través del Departamento del Programa Estatal de Seguridad Operacional (SSP).
(c) Sin perjuicio a que el proveedor de servicios pudiera establecer un alcance mayor o requisitos más estrictos para su SMS, esta regulación establece los requerimientos mínimos aceptables para un SMS de un proveedor de servicios aeronáuticos, que deberá comprender procesos, procedimientos y actividades relacionados con la seguridad operacional de la aviación y no la seguridad laboral, la protección del medio ambiente, los servicios a los clientes o la calidad de los productos.
(d) Esta regulación establece la responsabilidad del proveedor de servicios, respecto a la seguridad de los servicios o productos contratados o subcontratados o adquiridos de otras organizaciones.
(e) La aceptación del SMS en un proveedor de servicios, no lo exime del cumplimiento con cualquier otro programa o sistema requerido por la Ley de Aeronáutica o los Reglamentos Aeronáuticos Hondureños que le apliquen.
(f) Toda prestación de servicios de información aeronáutica (AIS), comunicaciones, navegación y vigilancia (CNS), meteorología para la navegación aérea (MET) y/o de búsqueda y salvamento (SAR), que esté bajo la autoridad de un proveedor ATS, deberá incluirse en el ámbito de aplicación del SMS del proveedor ATS. Cuando la prestación de servicios AIS, CNS, MET y /o SAR está parcial o totalmente a cargo de una entidad que no sea un proveedor ATS, los servicios conexos que se prestan bajo la autoridad del proveedor ATS, o aquellos aspectos de los servicios que tienen implicaciones directas de carácter operacional, deberán incluirse en el ámbito de aplicación del SMS del proveedor ATS.

RAC 19.020 Enunciado de los Componentes y Elementos del SMS (Ver Apéndice 5)

(a) Todo proveedor de servicios debe establecer y mantener actualizado un SMS que tenga por lo menos los siguientes componentes y sus elementos:

(1) Políticas y objetivos de seguridad operacional.

(i) Compromiso de la administración.

(ii) Obligación de rendición de cuentas sobre la seguridad operacional y responsabilidades.

(iii) Designación del personal clave de seguridad operacional.

(iv) Coordinación de la planificación de respuestas ante emergencias.

(v) Documentación SMS.

(2) Gestión de riesgos de seguridad operacional.

(i) Identificación de peligros.

(ii) Evaluación y mitigación de riesgos de seguridad operacional

(3) Aseguramiento de la seguridad operacional.

(i) Observación y medición del rendimiento en materia de seguridad operacional.

(ii) Gestión del cambio

(iii) Mejora continua del SMS.

(4) Promoción de la seguridad operacional.

(i) Instrucción y educación.

(ii) Comunicación de la seguridad operacional.

RAC 19.025 Reconocimiento del SMS de Organizaciones de Instrucción de otros Estados

Para toda organización de instrucción reconocida extranjera, a la cual se le haya aceptado debidamente un SMS por la autoridad civil del Estado responsable, la Dirección Ejecutiva de la

Agencia Hondureña de Aeronáutica Civil (AHAC) , a través del Departamento del Programa Estatal de SeguridadOperacional (SSP), podrá reconocer como bueno y válido dicho SMS para los efectos de cumplimiento con lo relativo a entrenamiento y evaluación de personal aeronáutico prescritos bajo el RAC-LPTA, previa evaluación por parte del SSP de la documentación del Estado responsable.

En caso necesario, el SSP coordinará una auditoría dirigida al organismo de instrucción de otros Estados de acuerdo con lo establecido en la presente regulación en lo que respecta a la aceptación y auditorías del SMS.

RAC 19.030 Reconocimiento del SMS de Organismos de Mantenimiento de otros Estados.

Para toda organización de mantenimiento reconocida extranjera, a la cual se le haya aceptado debidamente un SMS, por la autoridad civil del Estado responsable, la Agencia Hondureña de Aeronáutica Civil (AHAC), a través del Departamento del Programa Estatal de Seguridad Operacional (SSP), podrá reconocer como bueno y válido dicho SMS, para los efectos de cumplimiento de una organización de mantenimiento, cuando los requerimientos de certificación bajo el RAC - 145, fueran necesarios, previa evaluación por parte del SSP de la documentación del Estado responsable.

En caso necesario, el SSP coordinará una auditoría dirigida a organismo de mantenimiento de otros Estado de acuerdo con lo establecido en la presente regulación en lo que respecta a la aceptación y auditorías del SMS.

RAC 19.035 Reconocimiento del SMS de Proveedores de Servicios de Navegación Aérea de otros Estados

Para todo proveedor de servicios de navegación aérea reconocido extranjero, al cual se le haya aceptado debidamente un SMS por la autoridad civil del Estado responsable, la Agencia Hondureña de Aeronáutica Civil (AHAC), a través del Departamento del Programa Estatal de Seguridad Operacional (SSP), podrá reconocer como bueno y válido dicho SMS para los efectos de cumplimiento con lo relativo a la provisión del servicio de acuerdo al RAC-ATS, previa evaluación por parte del SSP de la documentación del Estado responsable. En caso necesario, el SSP coordinará una auditoría dirigida al proveedor de servicios de otros Estados, de acuerdo con lo establecido en la presente regulación en lo que respecta a la aceptación y auditorías del SMS.

RAC 19.040 Aplicabilidad de las Sanciones

El no cumplimiento con la implantación y mantención del SMS dentro de cualquier proveedor de servicios que le aplicase se interpretará como un peligro a la seguridad operacional y estará sujeto al régimen de sanciones establecido en el artículo 289 de la Ley de Aeronáutica Civil de Honduras.

INTENCIONALMENTE EN BLANCO

SUBPARTE D. EFECTIVIDAD

RAC 19.045 Efectividad

Este RAC-19 será de aplicación obligatoria de forma inmediata a partir del día siguiente de su publicación en el Diario Oficial La Gaceta de la República de Honduras.

RAC 19.050 Directivas Operacionales

(a) La Agencia Hondureña de Aeronáutica Civil (AHAC) puede emitir Directivas Operacionales mediante las cuales prohíba, limite o someta a determinadas condiciones una operación en interés de la seguridad operacional.

(b) Las Directivas Operacionales deben contener:

(1) El motivo de su emisión;

(2) Su ámbito de aplicación y duración;

(3) Acción requerida por parte de los proveedores de servicios.

(c) Lo requerido en las Directivas Operacionales de gestión de seguridad operacional, son complementarias y de acatamiento obligatorio a esta Regulación.

INTENCIONALMENTE EN BLANCO

SUBPARTE E. COMPONENTE I: POLITICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

RAC 19.055 Responsabilidad Funcional y Compromiso de la Dirección

(a) Todo proveedor de servicios debe definir una política de seguridad operacional de su organización, de conformidad con los requisitos nacionales, que refleje el compromiso de la organización respecto de la seguridad operacional. (Ver Apéndice 1)

(b) Toda política de seguridad operacional debe por lo menos contener:

(1) Un compromiso para implementar el SMS;
(2) Un compromiso del mejoramiento continuo del nivel de seguridad operacional;
(3) Un compromiso sobre la provisión de recursos humanos y financieros necesarios para la implantación e implementación del SMS;
(4) Un compromiso de gestionar los riesgos de seguridad operacional;
(5) Un compromiso con el cumplimiento de todo requisito de las normas nacionales e internacionales aplicables;
(6) Un compromiso de motivar a los empleados a reportar los asuntos de seguridad operacional y que estos sean de carácter no punitivo, para brindar protección a las fuentes para fomentar la presentación de la información;
(7) Un compromiso con el establecimiento de pautas claras del proceder aceptable;
(8) Una identificación de las responsabilidades de la dirección y de los empleados con respecto a la eficiencia de la seguridad operacional;
(9) Un compromiso para el establecimiento de procedimientos de presentación de informes de rendimiento en materia de seguridad operacional, tanto interno en los diferentes niveles de la organización, como externos a la revisión de la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP); y
(10) Un compromiso con la definición de los comportamientos inaceptables en lo que respecta a las actividades de aviación, las circunstancias en las que no se podrían aplicar medidas disciplinarias y claridad sobre la forma en que se establecerá una diferencia entre estos.

(c) Toda política de seguridad operacional debe:

(1) Proporcionar orientación para establecer objetivos de seguridad operacional para el SMS, los cuales deben estar relacionados con los indicadores de rendimiento en materia de seguridad operacional y planes de acción SMS;
(2) Ser comunicada con visible acuse de recibo, entendida, implantada y mantenida, en todos los niveles de la organización;
(3) Ser publicada en espacios públicos y de alto tráfico de colaboradores de la organización, así como de contratistas y visitas.
(4) Ser revisada periódicamente para asegurar que sigue siendo pertinente y apropiada a la organización;
(5) Estar definida por la dirección de la organización; y
(6) Estar aprobada y firmada por el ejecutivo responsable.

(d) Todo proveedor de servicios que posea una política de calidad se asegurará de que la misma sea coherente con las actividades del SMS y que apoye su gestión.
(e) Todo proveedor de servicios debe establecer objetivos de seguridad operacional, los cuales deben relacionarse y alinearse con los indicadores y metas de rendimiento en materia de seguridad operacional, y los planes de implementación.

RAC 19.060 Obligación de Rendición de Cuentas sobre la Seguridad Operacional

(a) Todo proveedor de servicios debe identificar al ejecutivo responsable, quién, independientemente de sus otras funciones, será el responsable último y rendirá cuentas a la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP), en nombre de laorganización, respecto a la implementación y el mantenimiento del SMS.
(b) Todo proveedor de servicios definirá claramente las líneas de obligación de rendición de cuentas sobre la seguridad operacional para toda la organización, incluida la obligación directa de rendición de cuentas sobre seguridad operacional de la dirección de la organización.
(c) Todo proveedor de servicios determinará la obligación de rendición de cuentas de todos los miembros de la dirección, independientemente de sus otras funciones, así como la de los empleados, en relación con el rendimiento en materia de seguridad operacional del SMS.
(d) Todo proveedor de servicios documentará y comunicará la información relativa a las responsabilidades funcionales, la obligación de rendición de cuentas y las atribuciones de seguridad operacional de toda la organización.
(e) Todo proveedor de servicios definirá los niveles de gestión con atribuciones para tomar decisiones sobre la tolerabilidad de los riesgos de seguridad operacional.

RAC 19.065 Responsabilidad Respecto a las Actividades Contratadas

(a) Todo proveedor de servicios debe asegurar que, el SMS de su organización interactúe de manera eficaz con los sistemas de seguridad operacional de los subcontratistas que proporcionan productos o servicios pertinentes para la seguridad operacional de sus actividades.
(b) Todo proveedor de servicios será responsable del rendimiento en materia de seguridad operacional de los productos o servicios que proporcionan los subcontratistas que no requieren la aceptación de un SMS.
(c) La interfaz entre un SMS de la organización y el sistema de seguridad operacional del proveedor de subproductos o subservicios contratados, debe incluir la identificación de peligros, la evaluación de riesgos y el desarrollo de estrategias de mitigación de riesgos, según corresponda.

(d) El proveedor de servicios debe garantizar que:

(1) El flujo de responsabilidad y autoridad de seguridad operacional entre el proveedor de servicios y el subcontratista sea establecido;
(2) El subcontratista posea un sistema de notificación de seguridad operacional proporcional a su tamaño y complejidad, que facilite la identificación temprana de peligros y averías sistémicas de interés para el proveedor de servicios;

(3) Desarrolle e implemente los indicadores de seguridad operacional/calidad para controlar el rendimiento del subcontratista, según corresponda.
(4) El proceso de promoción de la seguridad operacional del proveedor de servicios garantiza que los empleados del subcontratista cuenten con las comunicaciones de seguridad operacional correspondientes de la organización, y;
(5) Desarrolle, implemente, apruebe las políticas, responsabilidad y funciones del subcontratista pertinente para el plan de respuesta ante emergencias de proveedores de servicios.

RAC 19.070 Designación del Personal Clave de Seguridad Operacional

Todo proveedor de servicios debe designar un ejecutivo responsable y un gerente de seguridad operacional para la implantación y mantenimiento eficaz del SMS.

RAC 19.075 Designación y Responsabilidad del Ejecutivo Responsable

(a) Todo proveedor de servicios debe identificar un ejecutivo responsable quien se encargará en nombre de la organización, del cumplimiento de los requisitos de esta RAC.

(b) El proveedor de servicios debe asegurarse que el ejecutivo responsable, tome decisiones a cualquier nivel respecto a la seguridad operacional.

(c) El proveedor de servicios debe informar a la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP), la persona designada como ejecutivo responsable, el cual debe cumplir como mínimo los siguientes requisitos:

(1) Tener un nivel de autoridad dentro de la organización como presidente, director general, Gerente General, Presidente de la Junta de Directores, Socio, Propietario o en un cargo similar de relevancia en la toma de decisiones.
(2) Demostrar conocimientos obtenidos en cursos de preparación formal y/o a través de una inducción general a la designación de las tareas del ejecutivo responsable.

(d) Todo proveedor de servicios debe asegurarse que el ejecutivo responsable tenga:

(1) Pleno control de los recursos humanos necesarios para las operaciones autorizadas en su certificado y especificaciones de operaciones o según las autorizaciones otorgadas a través de la ley y los reglamentos.
(2) Pleno control de los recursos financieros necesarios para las operaciones autorizadas en su certificado y especificaciones de operaciones o según las autorizaciones otorgadas a través de la ley y los reglamentos.

(3) Control y supervisión sobre las operaciones autorizadas en su certificado y sus especificaciones de operaciones o según las autorizaciones otorgadas a través de la ley y los reglamentos.
(4) Responsabilidad directa sobre las distintas actividades designas de la organización; y
(5) Responsabilidad total en los asuntos de seguridad operacional.

RAC 19.080 Designación y Responsabilidades del Gerente de Seguridad Operacional

(Ver Apéndice 2)

(a) Todo proveedor de servicios debe designar una persona para ser gerente de seguridad operacional, quien será responsable de la implantación y mantenimiento eficaz del SMS.

(b) Todo proveedor de servicios debe someter a la Agencia Hondureña de Aeronáutica Civil, por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP), la propuesta de la persona a ser designada como gerente de seguridad operacional para su aceptación, en caso de ser para un aeródromo, la propuesta debe ser revisada en conjunto por el SSP Y CVA, si cumple al menos con las siguientes cualificaciones relacionadas directamente al tipo de proveedor de servicios al que pertenezca:

(1) Haber recibido inducción sobre las responsabilidades de su puesto antes de asumir el cargo;
(2) Tener conocimientos y experiencia operacional respecto a las funciones del tipo de proveedor de servicios;
(3) Tener conocimiento de los principios y prácticas de la gestión de la seguridad operacional;
(4) Tener experiencia previa o haber recibido entrenamiento que lo capacite sobre gestión de riesgo; y
(5) Tener experiencia previa aceptable o haber recibido entrenamiento que lo capacite para analizar los resultados o, realizar auditorías de la seguridad operacional de cualquier aspecto de las actividades de su organización.
(6) Haber recibido un curso de Sistema de Gestión de la Seguridad Operacional (SMS) aceptable para la Agencia Hondureña de Aeronáutica Civil (AHAC).

(c) Todo proveedor de servicios debe asegurarse que la persona designada como gerente se seguridad operacional cumplirá con las responsabilidades asignadas a su cargo, las cuales serán al menos las siguientes:

9

(1) Garantizar que los procesos necesarios para el SMS estén establecidos, implantados y mantenidos de la manera como está prescrito bajo esta regulación;

(2) Ser responsable de proporcionar información y asesoramiento al ejecutivo responsable sobre asuntos relacionados con la realización de operaciones seguras; y

(3) Asegurar la promoción de la seguridad operacional en todos los niveles de la organización.

(d) Todo proveedor de servicios deberá, en caso de tener vacante el cargo de gerente de seguridad operacional, y en un plazo no mayor a 60 días calendario, contratar o asignar a la persona que será delegada en ese cargo, previa aceptación del Departamento del Programa Estatal de Seguridad Operacional. De no hacerlo, se aplicará la sanción correspondiente establecida en la Ley de Aeronáutica Civil. Lo mismo aplica para los proveedores de servicios que posean operaciones en múltiples ubicaciones y que cuenten con personal designado para la administración de sus SMS, generalmente conocidos como Coordinadores u oficiales SMS.

RAC 19.085 Grupos para la Gestión de la Seguridad Operacional

(a) Todo proveedor de servicios debe, como parte de las responsabilidades funcionales y rendición de cuentas de la seguridad operacional, conformar un comité de revisión de seguridad operacional (SRB) y un grupo de acción de seguridad operacional (SAG).

(b) Todo proveedor de servicios debe conformar un comité de revisión de seguridad operacional (SRB) responsable de proporcionar la plataforma para lograr los objetivos de la asignación de recursos y evaluar la eficacia y eficiencia de las estrategias de mitigación de riesgos. El SRB debe:

(1) Estar liderado por el ejecutivo responsable;

(2) Incluir los gerentes de alto nivel de la organización, correspondientes a las áreas funcionales y los departamentos administrativos pertinentes;

(3) Recibir asesoría del gerente de seguridad operacional;

(4) Reunirse con periodicidad definida;

(5) Controlar el rendimiento en materia de seguridad operacional en comparación con la política y los objetivos de seguridad operacional de la organización;

(6) Controlar la eficacia de los procesos de gestión de la seguridad operacional de la organización;

(7) Controlar la eficacia de la supervisión de seguridad operacional de las operaciones subcontratadas;

(8) Garantizar que los recursos correspondientes estén asignados para lograr el rendimiento en materia de seguridad operacional;

(9) Propiciar los cambios del personal necesario, para maximizar la implementación del sistema dentro de la organización.

(c) Todo proveedor de servicios debe conformar un grupo de acción de seguridad operacional (SAG) responsable de la coordinación para la implementación y monitoreo de las estrategias de seguridad operacional en toda la organización. El SAG debe:

(1) Estar liderado por el gerente de seguridad operacional;

(2) Incluir los gerentes de línea y personal de primera línea;

(3) Supervisar el rendimiento en materia de seguridad operacional dentro de las áreas funcionales;

(4) Garantizar que se lleven a cabo las actividades de gestión de riesgos de seguridad operacional correspondientes;

(5) Coordinar la resolución de las estrategias de mitigación para las consecuencias de peligros identificados;

(6) Evaluar el impacto de la seguridad operacional relacionado con la introducción de cambios;

(7) Coordinar la implementación de planes de medidas correctivas de forma oportuna;

(8) Revisar la eficacia de controles y recomendaciones de seguridad operacional;

(d) No obstante, lo establecido en los párrafos (a) y (c) de esta subsección, el proveedor de servicios podrá, cuando su reducido tamaño y poca complejidad de las operaciones así lo permitan, delegar en su comité de revisión de seguridad operacional (SRB) el cumplimiento de las funciones descritas en el párrafo (c) de esta subsección, de la forma y manera aceptable para la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP).

RAC 19.090 Coordinación de la Planificación de Respuestas ante Emergencias (ERP)

(a) Todo proveedor de servicios debe elaborar y mantener actualizado un plan de respuesta ante emergencias, que sea aceptable para la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP), de la forma y manera que éste prescriba. Cuando el proveedor de servicios sea un operador de aeródromos, el plan de respuesta ante emergencias debe ser aceptado de manera conjunta por los Departamentos SSP y CVA. (Ver Apéndice 3)

(b) Todo proveedor de servicios debe asegurar que su plan de respuesta ante emergencias esta adecuadamente coordinado con los planes de respuesta ante emergencias de las organizaciones con las que debe interactuar durante la prestación de sus servicios.

(c) Todo proveedor de servicios respecto a su plan de respuesta ante emergencia debe asegurarse;

(1) Que se produzca una transición ordenada y eficiente de las operaciones normales a las operaciones ante emergencias;

(2) De la delegación de autoridad ante emergencias;

(3) De la asignación de las responsabilidades de emergencias durante las actividades coordinadas;

(4) De la autorización para el personal clave para las acciones contenidas en el plan;

(5) De la coordinación de los esfuerzos para enfrentar las emergencias;

(6) De realizar ensayos periódicos por medio de ejercicios, los cuales será en un intervalo de 6 meses;

(7) Del retorno de las actividades de emergencia a las actividades normales; y

(8) De la identificación proactiva de todos los posibles eventos/escenarios de emergencia y sus medidas de mitigación correspondientes.

(d) Todo proveedor de servicios debe asegurarse que el contenido de su plan de respuesta ante emergencias contenga al menos lo siguiente:

(1) El listado de las personas designadas que integrarán los equipos de respuesta ante emergencias y especificando quienes lo dirigirán, incluyendo datos generales, correo electrónico, cargo y número de celular.

(2) Las funciones y responsabilidades del personal asignado a los equipos de respuesta ante emergencias;

(3) La descripción de un lugar y las condiciones bajo las cuales debe operar un centro de gestión de crisis en casos de emergencia;

(4) Procedimientos para recibir solicitudes de información, especialmente durante los primeros días después de un accidente importante;

(5) Procedimientos para la designación de un portavoz para tratar con los medios de comunicación;

(6) Procedimientos para acceder a los recursos disponibles, incluidas las autorizaciones financieras para las actividades inmediatas;

(7) Procedimientos para la designación del representante de la empresa para toda investigación oficial emprendida por la Agencia Hondureña de Aeronáutica Civil (AHAC).

(8) La descripción de un plan de llamadas para el personal clave; y

(9) Listas de verificación y procedimientos pertinentes a las situaciones de emergencias específicas.

(10) Procedimiento de revisión anual del Plan de Respuesta Ante Emergencias.

RAC 19.095 Documentación SMS

(a) Todo proveedor de servicios debe elaborar y mantener actualizada la documentación sobre SMS conforme a lo prescrito en esta regulación, la cual estará contenida, toda o en parte, en un manual de gestión de la seguridad operacional (ver apéndice 6 - SMM) en la forma y manera aceptable para la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP), con el objetivo de comunicar a toda la organización su enfoque de la gestión de la seguridad operacional. Esta documentación debe al menos describir lo siguiente:

(1) Alcance e integración del sistema de gestión de la seguridad operacional;

(2) La política y objetivos de seguridad operacional;

(3) Los requisitos reguladores bajo los cuales se concibe el SMS de la organización;

(4) Los procesos y/o procedimientos del SMS deben ser al menos los siguientes:

(i) Documentación SMS;

(ii) Coordinación de la planificación de respuesta ante emergencias;

(iii) Identificación de peligros;

(iv) Evaluación y mitigación de riesgos de seguridad operacional;

(v) Observación y medición del rendimiento en materia de seguridad operacional;

(vi) Gestión del cambio;

(vii) Mejora continua del SMS;

(viii) Instrucción y educación; y

(ix) Comunicación de la seguridad operacional.

(5) Control de las actividades contratadas;

(6) Personal clave;

(7) Las obligaciones de rendición de cuentas, responsabilidades funcionales y las atribuciones relativas a los procesos y procedimientos del SMS; e

(8) Indicadores de rendimiento en materia de seguridad operacional.

(b) Todo proveedor de servicios debe mantener controlada la documentación SMS y debe asegurarse que:

(1) Las versiones actuales de los documentos pertinentes estén disponibles en todos los lugares donde se llevan a cabo las operaciones esenciales para el funcionamiento eficaz del SMS;
(2) Sea fácilmente localizable;
(3) Sea periódicamente revisada de ser necesario y aprobada por el personal autorizado; y
(4) Los documentos obsoletos sean retirados rápida y oportunamente de todos los puntos de uso o asegurarse que estos no se usen.

(c) Todo proveedor de servicios debe asegurarse de identificar, mantener y disponer de los registros del SMS, como también de que estos se encuentren legibles, identificables y trazables.
(d) Todo proveedor de servicios debe asegurarse que los registros del SMS se mantengan de forma que sean fácilmente recuperables y protegidos contra daños, deterioro y pérdida.
(e) Todo proveedor de servicios debe asegurarse de definir los tiempos de retención de los registros por un periodo aceptable por la autoridad del Estado.
(f) Todo proveedor de servicios debe permitir el acceso a los registros del SMS en la forma y manera como prescriba la autoridad del Estado.
(g) Todo proveedor de servicios debe mantener uno o varios procedimientos documentados para controlar los documentos y registros.
(h) Todo proveedor de servicios debe asegurarse que su Manual de Gestión de la Seguridad Operacional cuente con un procedimiento de revisión del mismo de por lo menos cada 24 meses.

INTENCIONALMENTE EN BLANCO

SUBPARTE F. COMPONENTE II: GESTION DE RIESGOS DE SEGURIDAD OPERACIONAL

RAC 19.100 Generalidades

Todo proveedor de servicios debe desarrollar sus procesos tomando en cuenta las características esenciales de sus operaciones y su entorno, y debe aplicar este conocimiento para identificar los peligros, analizarlos, evaluar el riesgo y establecer los controles necesarios.

RAC 19.105 Identificación de peligros (Ver Apéndice 3)

(a) Todo proveedor de servicios debe desarrollar y mantener actualizados medios de identificación de peligros de las operaciones, que combinen métodos reactivos y proactivos de datos de la seguridad operacional.

(b) Todo proveedor de servicios debe, en la identificación de peligros, considerar lo siguiente:

(1) Reporte de peligros y eventos;

(2) Recolección y almacenamiento de datos;

(3) Análisis de datos; y

(4) Distribución de información emanada de los datos de seguridad operacional.

(c) Todo proveedor de servicios en el uso del análisis reactivo se asegurará de que considera los siguientes elementos según apliquen:

(1) Reportes (obligatorios, voluntarios, confidenciales y anónimos);
(2) Identificación del peligro que causó el incidente o accidente;
(3) Las consecuencias que tuvo dicho incidente o accidente;
(4) Las evaluaciones de controles que fallaron resultando en consecuencias (si es que estaban implementados);
(5) Las mitigaciones de los controles del riesgo que fallaron resultando en consecuencias (si es que estaban implementados);

(d) Todo proveedor de servicios en el uso del análisis proactivo se asegurará de que este análisis comprende y considera los siguientes elementos, según aplique:

(1) Encuestas;

(2) Auditorías;

(3) Reportes, que pueden ser de carácter obligatorio, voluntario, confidencial y anónimo;

(4) Lluvia de ideas (sesión de búsqueda y proposición de cualquier peligro, que se pueda percibir o sospechar).

(e) Todo proveedor de servicios debe realizar un estudio para establecer si existen derivaciones con respecto a la aparición de posibles nuevos peligros o riesgos, como consecuencia de los resultados de los análisis realizados mediante uno o una combinación de los métodos señalados en los párrafos c) y d) de esta subsección, debiendo implementar sus conclusiones o recomendaciones o nuevos procedimientos.

(f) Todo proveedor de servicios debe utilizar uno o varios de los siguientes medios formales de recolección de datos de seguridad operacional que incluirán:

(1) De carácter obligatorio: cuando el proveedor de servicios exige que la información y antecedentes, sea requerida de forma mandatorio a todos sus miembros y que tiene relación con la seguridad operacional.

(2) De carácter voluntario: cuando el proveedor de servicios recibe la información con la identificación del informante.

(3) De carácter confidencial: cuando el proveedor de servicios recibe la información, la cual el informante pide dejar confidencial su identificación.

(4) De carácter anónimo: cuando el proveedor de servicios recibe la información, sin la identificación del informante.

RAC 19.110 Evaluación y mitigación de riesgos de seguridad operacional

(a) Todo proveedor de servicios debe elaborar y mantener actualizado un procesoy/o procedimiento de evaluación y mitigación de riesgos para la gestión de riesgos, que asegure el análisis de riesgos (en cuanto a la probabilidad y severidad de que se traduzcan en sucesos); su evaluación (en cuanto a su tolerabilidad); y su control (en cuanto a su mitigación y/o eliminación), de modo que permanezcan en un nivel aceptable de seguridad operacional. (Ver Apéndice 7)

(b) Todo proveedor de servicios debe definir cuáles niveles jerárquicos tendrán, en la dirección interna, la autoridad para tomar decisiones respecto de la tolerabilidad de los riesgos que afectan a la seguridad operacional.

(c) Todo proveedor de servicios debe definir e implantar los controles de seguridad operacional para cada riesgo determinado como tolerable u otro nivel de riesgo similar, de acuerdo con los criterios de tolerabilidad.

RAC 19.115 Documentación para la identificación de peligros y para la evaluación y mitigación de riesgos de seguridad operacional

Todo proveedor de servicios debe mantener uno o varios procedimientos documentados para la identificación de peligros y para la evaluación y mitigación de riesgos de seguridad operacional asociados a los peligros identificados durante el suministro de sus productos o servicios de aviación.

INTENCIONALMENTE EN BLANCO

SUBPARTE G. COMPONENTE III: ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

RAC 19.120 Observación y medición del rendimiento en materia de seguridad operacional

(a) Todo proveedor de servicios, como parte de las actividades de aseguramiento de la seguridad operacional del SMS, debe desarrollar y mantener actualizado un proceso formal para:

(1) Verificar el rendimiento en materia de seguridad operacional de la organización;

(2) Asegurarse que las medidas para el control de riesgos a la seguridad operacional desarrolladas como consecuencia de la actividad de identificación de peligros y gestión de riesgos antes enunciadas, alcancen los objetivos pretendidos.

(b) Investigar los sucesos que no requieran ser investigados por la Agencia Hondureña de Aeronáutica Civil o la Comisión de Investigación de Accidentes e Incidentes, de acuerdo con lo establecido en la Política de Cumplimiento del Departamento del Programa Estatal de Seguridad Operacional (SSP).

(c)

(1) Identificar las causas de baja eficacia del SMS, determinar las implicaciones en sus operaciones y eliminar tales causas.

(d) El rendimiento en materia de seguridad operacional del proveedor de servicios se verificará en referencia a los indicadores de rendimiento en materia de seguridad operacional del SMS, los cuales deben (Ver Apéndice 4):

(1) Estar relacionados con los objetivos de seguridad operacional de la organización;

(2) Incluir metas de rendimiento en seguridad operacional, alertas y planes de acción;

(3) Incluir una gama de indicadores de alto impacto y bajo impacto.

(e) La observación y medición del rendimiento en materia de seguridad operacional debe incluir al menos lo siguiente:

(1) Reportes de seguridad operacional;

(2) Estudios de seguridad operacional;

(3) Revisiones de seguridad operacional;

(4) Auditorías de seguridad operacional;

(5) Investigaciones internas de seguridad operacional.

Todo proveedor de servicios debe, como parte del sistema de observación y medición del rendimiento en materia de seguridad operacional, realizar evaluaciones internas o auto evaluaciones y auditorías tanto internas como externas, las cuales serán una actividad básica del SMS. Estas tomarán en consideración al menos lo siguiente:

Deben clasificarse en evaluaciones internas o auto evaluaciones y auditorías internas;

Deben ser realizadas, en el caso de las evaluaciones internas, a las actividades, procesos o procedimientos operacionales técnicos de la organización, así como las funciones específicas del SMS relacionadas a tales actividades. Deben ser efectuadas por personas del proveedor de servicios que no sean parte o que sean funcionalmente independientes de las actividades, procesos o procedimientos operacionales técnicos a ser evaluados o deben realizarse por personas u organizaciones independientes al proveedor de servicios que cumplan los requisitos establecidos por esta RAC-19 y sean aceptados para tal efecto por la autoridad del Estado, por medio del Departamento del Programa Estatal de Seguridad Operacional SSP.

Deben ser realizadas, en el caso de auto evaluaciones, a las actividades, procesos o procedimientos operacionales técnicos del proveedor de servicios, así como las funciones específicas del SMS relacionadas a tales actividades y serán conducidas por sus respectivos responsables de procesos operacionales técnicos. Estas auto evaluaciones reemplazarán a las evaluaciones internas y serán aprobadas a un proveedor de servicios solo cuando su reducido tamaño y poca complejidad de sus operaciones así lo permitan, teniendo que ser para tales propósitos aprobado por la Agencia Hondureña de Aeronáutica Civil (AHAC), por medio del Departamento del Programa Estatal de Seguridad Operacional (SSP).

Deben realizarse, en el caso de las auditorías internas, con auditores, internos o externos al proveedor de servicios. En el caso de los externos a la organización, éstos deben estar calificados y aceptados de la forma y manera prescrita por la autoridad del Estado;

Deben ser realizadas, las evaluaciones internas o auto evaluaciones y las auditorías internas, de forma periódica y sistemática, mediante el establecimiento de un plan anual de auditoría de seguridad operacional.

Deben ser conservados los registros, de todas las auditorías, al menos por 24 meses, contados a partir de la fecha de finalización de la auditoría correspondiente. En el caso de los registros de las auto evaluaciones realizadas, estos deben ser enviados al Gerente de Seguridad Operacional para actualizar la base de estadísticas y los demás procesos y procedimientos del SMS.

RAC 19.125 Gestión del cambio

1. La experiencia de los proveedores de servicios cambia debido a varios factores, los que incluyen entre otros:

a) expansión o contracción institucional;

b) mejoras empresariales que puede tener consecuencias para la seguridad operacional; estas pueden resultar en cambios a los sistemas, procesos o procedimientos internos que respaldan la entrega de productos y servicios;

c) cambios al entorno de operación de la organización;

d) cambios a las interfaces del SMS con organizaciones externas; y

e) cambios normativos externos, cambios económicos y riesgos emergentes.

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

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

a) Criticidad. Determinación de cuán crítico es el cambio. El proveedor de servicios aeronáuticos deberá considerar las consecuencias para las actividades de su organización, así como para otras organizaciones y el sistema aeronáutico.

b) Disponibilidad de expertos temáticos. Es importante que miembros clave de la comunidad aeronáutica estén involucrados en las actividades de gestión de cambios, pudiéndose incluir individuos de organizaciones externas.

c) Disponibilidad de datos e información sobre rendimiento en materia de seguridad operacional.

e) Determinación de los datos e información de que se disponen y que pueden utilizarse para proporcionar información sobre la situación y facilitar el análisis del cambio.

3. A menudo, los pequeños cambios incrementales pueden pasar desapercibidos, pero su efecto acumulativo puede ser considerable. Los cambios, tanto grandes como pequeños pueden afectar la descripción del sistema de la organización y conducir a la necesidad de su revisión. Por consiguiente, la descripción del sistema debe revisarse periódicamente para determinar su validez continua, dado que la mayoría de los proveedores de servicios experimentan cambios periódicos o incluso continuos.

El proveedor de servicios debe definir el elemento activador del proceso de cambios formal.

Los cambios que probablemente activen una gestión de cambio oficial comprenden:

a) introducción de nueva tecnología o equipo;

b) cambios en el entorno operacional;

c) cambios en el personal clave;

d) cambios significativos en los niveles de plantilla;

e) cambios en los requisitos normativos de seguridad operacional;

f) reestructuración significativa de la organización; y

g) cambios físicos (nueva instalación o base, cambios en la disposición general del aeródromo, etc.).

4. El proveedor de servicios debe considerar también las consecuencias del cambio sobre el personal. Esto podría afectar la forma en que los individuos afectados aceptan el cambio. La comunicación y participación tempranas normalmente mejorarán la forma en que se perciben e implementan los cambios.

El proceso de gestión del cambio debe incluir las actividades siguientes:

a) comprensión y definición del cambio; esto debe incluir una descripción del cambio y las razones de su implementación;

b) comprensión y definición de quiénes y qué aspectos se verán afectados; estos pueden ser individuos dentro de la organización, otros departamentos o personas u organizaciones externas. También puede haber consecuencias para los equipos, sistemas y procesos. Puede ser necesario realizar un examen de la descripción del sistema y de las interfaces de las organizaciones. Este aspecto constituye una oportunidad para determinar quién deben estar involucrados en el cambio. Los cambios podrían afectar los controles de riesgos ya implantados para mitigar otros riesgos, y por lo tanto los cambios podrían aumentar los riesgos en sectores que no son inmediatamente obvios;

c) identificación de peligros relacionados con el cambio y realización de evaluaciones de riesgos de seguridad operacional; debe identificarse los peligros directamente relacionados con el cambio. También deber examinarse las consecuencias sobre peligros y controles de riesgos de seguridad operacional existentes que puedan verse afectados por el cambio. Esta etapa debe aplicar los procesos SRM de la organización existente;

d) elaboración de un plan de acción; este debe definir lo que ha de hacerse, por quiénes y para cuándo. También debe haber un plan claro que describa la forma en que se implementará el cambio y quiénes serán responsables de las medidas que se apliquen, así como la secuencia y programación de las tareas;

e) aprobación del cambio; esto es necesario para confirmar que el cambio puede implementarse en condiciones de seguridad. El individuo con responsabilidad y autoridad generales para la implantación del cambio debe firmar el plan correspondiente; y

f) plan de seguridad; esto es para determinar las medidas de seguimiento que sean necesarias. Se debe considerar la forma en que se comunicará el cambio y si se requieren actividades adicionales (como auditorías) durante o después del mismo. Debe comprobarse todas las hipótesis o suposiciones que hubiere.

RAC 19.130 Mejora continua del SMS

El Anexo 19, Apéndice 2, 3.3 establece que… “el proveedor de servicios observará y evaluará sus procesos SMS para mantener y mejorar continuamente la eficacia general del SMS.” El mantenimiento y la mejora continua de la eficacia del SMS del proveedor de servicios aeronáuticos son apoyados por las actividades de aseguramiento de la seguridad operacional que comprende la verificación y seguimiento de las medidas y los procesos de auditoría interna. Debe reconocerse que el mantenimiento y la mejora continua del SMS son actividades permanentes, puesto que la propia organización y su entorno operacional estarán cambiando constantemente.

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

La eficacia del SMS no debe basarse solamente en los SPI; los proveedores de servicios deben proponerse la implantación de varios métodos para determinar su eficacia, medir los productos, así como los resultados de los procesos y evaluar la información recopilada con estas actividades. Tales métodos pueden incluir lo siguiente:

a) Auditorías; comprende las auditorías internas y las auditorías realizadas por otras organizaciones.

b) Evaluaciones; comprende las evaluaciones de la cultura de seguridad operacional y la eficacia del SMS.

c) Observación de sucesos: vigila la repetición de sucesos de seguridad operacional incluyendo accidentes e incidentes, así como errores y situaciones de infracción de reglamentos.

d) Estudios de seguridad operacional; incluye estudios de carácter cultural para proporcionar información útil respecto de la participación del personal en el SMS. También puede servir de indicador de la cultura de seguridad operacional de la organización.

e) Exámenes de la gestión; examinan si la organización está alcanzando sus objetivos de seguridad operacional y constituyen una oportunidad para realizar toda la información disponible sobre rendimiento en materia de seguridad operacional a efectos de identificar tendencias generales. Es importante que la administración superior examine la eficacia del SMS. Esto puede realizarse como una de las funciones del comité de seguridad operacional de más alto nivel.

f) Evaluación de los SPI y las SPT; posiblemente como parte del examen de la gestión. Considera tendencias y, cuando se dispone de datos apropiados, pueden compararse con los datos de otros proveedores de servicios, estatales o mundiales.

g) Aprovechamiento de las enseñanzas obtenidas; a partir de sistemas de notificación de seguridad operacional e investigaciones de seguridad operacional del proveedor de servicios. Estas deben conducir a la implantación de mejoras de la seguridad operacional.

En resumen, los procesos de observación del rendimiento en materia de seguridad operacional y de auditorías interna y externa contribuyen a la capacidad del proveedor de servicios de lograr una mejora continua del rendimiento en materia de seguridad operacional. La observación continua del SMS, sus controles de riesgos de seguridad operacional conexos y sistemas de apoyo garantizan al proveedor de servicios y al Estado que los procesos de gestión de la seguridad operacional están logrando sus objetivos deseados de rendimiento en materia de seguridad operacional.

RAC 19.135 Documentación para la observación y medición del rendimiento en materia de seguridad operacional, para la gestión del cambio y para la mejora continúa del SMS

Todo proveedor de servicios debe mantener uno o varios procedimientos documentados para la observación y medición del rendimiento en seguridad operacional, para la gestión del cambio y para la mejora continua del SMS.

SUBPARTE H. COMPONENTE IV: PROMOCION DE LA SEGURIDAD OPERACIONAL

RAC 19.140 Generalidades

Todo proveedor de servicios debe desarrollar y mantener instrucción formal en seguridad operacional y actividades de comunicación, para crear un ambiente donde los objetivos de seguridad operacional puedan ser alcanzados.

La promoción de la seguridad operacional alienta una cultura de seguridad operacional positiva y contribuye a alcanzar los objetivos de seguridad operacional del proveedor de servicios mediante la combinación de competencias técnicas que mejoran continuamente con la instrucción y la educación, la comunicación eficaz y la compartición de información. La administración superior proporciona el liderazgo para promover la cultura de seguridad operacional en toda la organización.

La gestión eficaz de la seguridad operacional no puede lograrse solamente siguiendo una orden o una adherencia estricta a las políticas y procedimientos. La promoción de la seguridad operacional afecta el comportamiento tanto individual como institucional y complementa las políticas, procedimientos y procesos de la organización, proporcionando un sistema de valores que respalda las actividades de seguridad operacional.

El proveedor de servicios debe establecer e implementar procesos y procedimientos que faciliten la comunicación eficaz en ambos sentidos a través de todos los niveles de la organización. Esto debe comprender una clara dirección estratégica desde los estratos más altos de la organización y la habilitación de la comunicación “jerárquica ascendente” que fomenta los comentarios abiertos y constructivos de todo el personal.

RAC 19.145 Instrucción y educación

1 De acuerdo al Anexo 19 y el Doc. 9859 “el proveedor de servicios creará y mantendrá 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”. También establece que “el alcance del programa de instrucción en seguridad operacional será apropiado para el tipo de participación que cada persona tenga en el SMS”. El gerente de seguridad operacional es responsable de garantizar que se ha implantado un adecuado programa de instrucción en seguridad operacional. Esto comprende el suministro de información de seguridad operacional apropiada y pertinente a los problemas de seguridad específicos que enfrente la organización. Contar con personal capacitado y competente para cumplir sus funciones en el marco del SMS, sin importar su nivel en la organización, es un indicio del compromiso de la administración con un SMS eficaz. El programa de instrucción debe incluir instrucción inicial, periódica o recurrente y de actualización para mantener las competencias. La instrucción inicial en seguridad operacional debe considerar, como mínimo, los siguientes aspectos:

a) políticas y objetivos de seguridad operacional de la organización;

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

c) principios básicos de la SRM;

d) sistemas de notificación de seguridad operacional;

e) procesos y procedimientos SMS de la organización; y

f) factores humanos.

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

La instrucción de actualización de seguridad operacional debe concentrarse cuando ocurran cambios en la legislación estatal, nuevas regulaciones y/o reglamentos.

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

Análisis de las necesidades de instrucción

Para la mayoría de las organizaciones, es necesario realizar evaluaciones de las necesidades de instrucción (TNA) formales para asegurar que existe una clara comprensión de la operación, las funciones de seguridad operacional del personal y la instrucción disponible. Una TNA típica se iniciará normalmente con la realización de un análisis de audiencias, que por lo general comprende las etapas siguientes:

a) Todos y cada uno de los miembros del personal del proveedor de servicios se verán afectados por la implementación del SMS, pero no de la misma manera o en el mismo grado. Se deberá identificar cada grupo de personal y las formas en que interactuarán con los procesos de gestión de la seguridad operacional, sus entradas y salidas, en particular con respecto a las funciones de seguridad operacional. Esta información debe estar disponible en las descripciones de puestos o funciones. Normalmente, comenzarán a surgir grupos de individuos con necesidades de aprendizaje similares. El proveedor de servicios debe considerar si vale la pena extender el análisis al personal de organizaciones externas interconectadas.

b) Identificar los conocimientos y las competencias necesarias para realizar cada función de seguridad operacional que requiere cada agrupamiento de personal.

c) Realizar un análisis para identificar las brechas entre las habilidades y conocimientos actuales en seguridad operacional de todo el personal y los necesarios para la realización eficaz de las funciones de seguridad operacional asignadas.

d) Identificar el enfoque más apropiado para desarrollar habilidades y conocimientos respecto de cada grupo con miras a elaborar un programa de instrucción adecuado a la participación de cada individuo o grupo en la gestión de la seguridad operacional. El programa de instrucción también debe considerar las necesidades continuas del personal en materia de conocimientos y competencias de seguridad operacional; estas necesidades se abordarán normalmente mediante un programa de instrucción periódica.

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

La organización debe determinar el grado de profundidad de la capacitación SMS que recibirá, dependiendo de su participación en el mismo, dejando claro que todos los empleados deben tener como mínimo, conocimientos básicos del SMS. La mayoría de las personas que trabajan en la organización tendrán cierta relación directa o indirecta con la seguridad operacional de la aviación y, por consiguiente, tendrán algunas funciones en el marco del SMS. Esto se aplica a todo el personal directamente involucrado en la entrega de productos y servicios y al personal que participa en los comités de seguridad operacional de la organización. Algunos miembros del personal administrativo y de apoyo tendrán funciones SMS limitadas y requerirán cierta instrucción en la materia, dado que su trabajo todavía puede tener consecuencias indirectas sobre la seguridad operacional de la aviación.

El proveedor de servicios debe identificar las funciones SMS del personal y utilizar la información para examinar el programa de instrucción en la materia y asegurar que cada individuo recibe instrucción correspondiente a su participación en el SMS. El programa de instrucción en seguridad operacional debe especificar el contenido de la misma para el personal de apoyo, el personal de operaciones, los administradores y supervisores, los gerentes superiores y el ejecutivo responsable.

Debe impartirse instrucción específica en seguridad operacional para el ejecutivo responsable y los gerentes superiores que comprenda los temas siguientes:

a) concientización específica para nuevos ejecutivos y titulares de puestos responsables con respecto a sus obligaciones de rendición de cuentas y responsabilidades;

b) importancia de cumplir los requisitos de seguridad operacional nacionales e institucionales;

c) compromiso de la administración;

d) asignación de recursos;

e) promoción de la política de seguridad operacional y del SMS;

f) promoción de la cultura de seguridad operacional positiva;

g) comunicación eficaz de seguridad operacional entre los departamentos;

h) objetivos de seguridad operacional, SPT y niveles de alerta; y i) política disciplinaria

.

El propósito principal del programa de instrucción en seguridad operacional es garantizar que el personal, a todos los niveles de la organización, mantiene su competencia para la realización de sus funciones de seguridad operacional; por consiguiente, las competencias del personal deben realizarse con carácter periódico.

RAC 19.150 Comunicación de la seguridad operacional

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

a) garantizar que el personal es plenamente consciente del SMS; esta es una buena forma de promover la política y los objetivos de seguridad operacional de la organización.

b) transmitir información crítica para la seguridad operacional; la información crítica para la seguridad operacional es información específica relacionada con problemas y riesgos de seguridad operacional que podrían exponer a la organización a ese tipo de riesgo. Podría tratarse de información recopilada de fuentes internas o externas como enseñanzas obtenidas o relacionadas con controles de riesgos de seguridad operacional. El proveedor de servicios determina el tipo de información que se considera crítica para la seguridad operacional así como la oportunidad de comunicarla.

c) crear conciencia sobre nuevos controles de riesgos de seguridad operacional y medidas correctivas; los riesgos de seguridad operacional que enfrenta el proveedor de servicios cambiarán con el tiempo, y si se trata de un nuevo riesgo de seguridad operacional que ha sido identificado o de cambios en los controles de riesgos de seguridad operacional dichos cambios deberán comunicarse al personal apropiado.

d) proporcionar información sobre procedimientos de seguridad operacional nuevos o enmendados; cuando se actualizan los procedimientos de seguridad operacional es importante que las personas apropiadas tengan conocimientos de dichos cambios.

e) promover una cultura de seguridad operacional positiva y alentar al personal a identificar y notificar peligros; la comunicación de seguridad operacional es en ambos sentidos. Es importante que todo el personal comunique los problemas de seguridad operacional a la organización a través del sistema de notificaciones de seguridad operacional.

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

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

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

Los proveedores de servicios deben asegurarse de proporcionar charlas SMS a todo el personal de contratistas que realicen obras en sus instalaciones.

Las actividades de promoción de la seguridad operacional deben llevarse a cabo durante todo el ciclo de vida del SMS, y no solo al comienzo de este.

RAC 19.155 DOCUMENTACIÓN PARA LA INSTRUCCIÓN Y EDUCACIÓN Y PARA LA COMUNICACIÓN DE LA SEGURIDAD OPERACIONAL.

Todo proveedor de servicios debe mantener uno o varios procedimientos documentados para la instrucción, educación y para la comunicación de la seguridad operacional.

.

INTENCIONALMENTE EN BLANCO

SUBPARTE I. COMPONENTES PARA LA IMPLEMENTACION Y ACEPTACION DEL SMS

RAC 19.160 ENFOQUE POR COMPONENTES PARA LA IMPLEMENTACIÓN Y LA ACEPTACION DEL SMS

Todo proveedor de servicios debe implementar el SMS en cuatro componentes. El proveedor de servicios, de acuerdo con la magnitud, complejidad y amplitud de sus operaciones, podrá adelantar o diferir el período y orden de estas componentes de manera excepcional, siempre que así este autorizado por la Agencia Hondureña de Aeronáutica Civil (AHAC), a través del Departamento del Programa Estatal de Seguridad Operacional (SSP), y siempre que no exceda el período de aceptación establecido bajo esta subsección.

RAC 19.165 Componente I. Requisitos para la implementación y aceptación Componente I

En este componente todo proveedor de servicios aeronáuticos debe satisfacer los requisitos adelante establecidos, así como establecer el marco de responsabilidades y rendición de cuentas para la implementación del SMS, que incluya los siguientes elementos:

(a) Responsabilidad funcional y compromiso de la dirección:

(1) Identificar al ejecutivo responsable y las responsabilidades de seguridad operacional de los gerentes, de conformidad con lo requerido en las subpartes RAC-19.060, RAC-19.070, RAC-19.075 y RAC-19.080.
(2) Establecer un equipo de implementación del SMS dentro de la organización, de conformidad con lo que establece RAC-19.060.
(3) Describir el sistema de su tipo de organización que al menos contenga la siguiente información:

a. Las interacciones del sistema con otros sistemas en el sistema de transporte aéreo;
b. Las funciones del sistema;
c. Las consideraciones de actuación humana requerida para la operación del sistema;
d. Los componentes hardware del sistema;
e. Los componentes software del sistema, incluyendo los procedimientos que definen las guías para la operación y el uso del sistema;
f. El entorno operacional; y
g. Los productos contratados y adquiridos.

(4) Defina el alcance y la aplicabilidad del SMS, para los operadores aéreos es necesario incluir a detalle sus flotas con sus datos.

(b) Documentación SMS

(1) Desarrolle un plan de Implementación del SMS que explique cómo la organización implementará el SMS basado en los requisitos nacionales e internacionales, la descripción del sistema y los resultados del análisis de brechas, de conformidad con lo requerido en la subsección RAC-19.095.

(c) Designación del personal clave de seguridad operacional:

(1) Identifique al Gerente de Seguridad Operacional, que será responsable de administrar el sistema en nombre del Ejecutivo Responsable, de conformidad con lo requerido en las subsecciones RAC-19.070 y RAC- 19.080.

(2) Defina la conformación y el establecimiento de la oficina de servicios de seguridad operacional.

(d) Instrucción y educación:

(1) Desarrolle un programa de instrucción inicial y recurrente en seguridad operacional que asegure la implementación y mantenimiento eficaz del SMS, de conformidad con lo requerido en la subsección RAC-19.145.

(e) Comunicación de la seguridad operacional:

(1) Desarrolle y establezca medios para las comunicaciones de seguridad operacional, de conformidad con lo requerido en la subsección RAC-19.150 (b).

RAC 19.170 Componente II. Requisitos para la implementación y aceptación del componente II

En este componente todo proveedor de servicios debe implementar los procesos de gestión fundamentales y corregir las deficiencias en los procesos de gestión de seguridad operacional existentes, así como poner en práctica los aspectos contenidos en el plan de implementación que se refieran a los siguientes elementos:

(a) Responsabilidad funcional y compromiso de la dirección:

(1) Desarrolle y establezca una política de Seguridad Operacional de conformidad con lo requerido en la subsección RAC-19.055;

(2) Desarrolle y establezca objetivos de seguridad operacional para el SMS mediante el desarrollo de normas de rendimiento en materia de seguridad operacional, de conformidad con lo requerido en la subsección RAC-19.055 (e); y

(3) Establezca los requisitos del SMS para los subcontratistas, incluyendo el establecimiento de un procedimiento para incluir requisitos de SMS en el proceso contratante y establecer los requisitos de SMS en la documentación de licitación, de conformidad con lo requerido en la subsección RAC-19.065.

(b) Obligación de rendición de cuentas sobre la seguridad operacional

(1) Defina y comunique las responsabilidades de la seguridad operacional en toda la organización, de conformidad con lo requerido en la subsección RAC-19.060;
(2) Establezca el comité de revisión de la seguridad operacional (SRB), de conformidad con lo requerido en la subsección RAC-19.085 (a);
(3) Establezca el grupo de acción de seguridad operacional (SAG), de conformidad con lo requerido en la subsección RAC-19.085 (a);
(4) Defina las funciones para el SRB y el SAG, de conformidad con lo requerido en las subsecciones RAC-19.085 (b) y (c); y
(5) Establezca líneas de comunicación entre el ejecutivo responsable, la oficina de servicios de seguridad operacional y los grupos para la gestión de la seguridad operacional.

(c) Coordinación de la planificación de respuestas ante emergencias:

(1) Identifique entidades externas que interactuarán con la organización durante situaciones de emergencia;
(2) Evalúe los ERP respectivos de las entidades externas;
(3) Establezca la coordinación entre los diferentes ERP, de conformidad con lo requerido en la subsección RAC-19.090 (b);
(4) Desarrolle un ERP, de conformidad con lo requerido en la subsección RAC-19.090; y
(5) Realice ensayos por medio de ejercicios, de conformidad con lo requerido en la subsección RAC-19.090 (c) (6).

(d) Instrucción y Educación

(1) Ejecute la instrucción correspondiente al componente II.

(e) Documentación SMS:

(1) Desarrolle un sistema de documentación de SMS para describir, mantener, recuperar y almacenar toda la información y los registros relacionados con SMS, incluyendo los siguientes:

(i) Desarrollo de un manual de SMS, de conformidad con lo requerido en la subsección RAC-19.095 (a) (Ver Apéndice 6); y

(ii) Establecimiento de un sistema de archivo de SMS para recopilar y mantener los registros actuales en relación con los procesos de SMS constantes de la organización, de conformidad con lo requerido en la subsección RAC-19.095(c), (d), (e) y (g);

(2) Desarrolle la documentación relativa a las actividades descritas en los párrafos (a), (b), (c) y (d) de la presente subsección.

RAC 19.175 Componente III. Requisitos para la implementación y la aceptación del componente III.

Todo proveedor de servicios bajo el componente III, debe establecer procesos de gestión de riesgos de la seguridad operacional y establecer las bases para recopilar datos de seguridad operacional, realizar los análisis de seguridad operacional basados en la información obtenida mediante diversos sistemas de notificación, así como poner en práctica los aspectos contenidos en el plan de implementación que se refieran a los siguientes elementos:

(a) Identificación de peligros:

(1) Establezca un procedimiento de notificación voluntaria, de conformidad con lo requerido en la subsección RAC-19.230 (h) (2);
(2) Establezca un programa/plan para la revisión sistemática de todos los procesos/equipos relacionados con la seguridad operacional que sean idóneos para la identificación de peligros, de conformidad con lo requerido en la subsección RAC- 19.230; y
(3) Establezca un procedimiento para la identificación de peligros, de conformidad con lo requerido en las subsecciones RAC-19.235 y RAC-19.245.

(b) Evaluación y mitigación de riesgos de seguridad operacional:

(1) Establezca un procedimiento de gestión de riesgos de la seguridad operacional, de conformidad con lo requerido en las subsecciones RAC-19.235, RAC-19.240 y RAC-19.245; y
(2) Desarrolle y establezca matrices de riesgos de seguridad operacional pertinentes para los procesos operacionales y de producción de la organización, de conformidad con lo requerido en la subsección RAC-19.240.

(c) Observación y medición del rendimiento en materia de seguridad operacional:

(1) Establezca un procedimiento interno de notificación e investigación de sucesos, de conformidad con lo requerido en la subsección RAC-19.120 (a) (4);
(2) Establezca la recopilación, el procesamiento y el análisis de los datos de seguridad operacional de los resultados de alto impacto, de conformidad con lo requerido en la subsección RAC-19.235 (c);
(3) Establezca indicadores y metas de rendimiento en materia de seguridad operacional de alto impacto, incluyendo los niveles de alerta, de conformidad con lo requerido en la subsección RAC-19.120 (b); y

(d) Gestión del cambio:

(1) Establezca un proceso formal para la gestión del cambio, de conformidad con lo requerido en la subsección RAC-19.125;
(2) Garantice que los procedimientos de la gestión del cambio aborden el impacto de los registros existentes de rendimiento en materia de seguridad operacional y de mitigación de riesgos antes de implementar nuevos cambios, de conformidad con lo requerido en la subsección RAC-19.125; y
(3) Establezca procedimientos para garantizar que se lleve a cabo (o se considere) la evaluación de seguridad operacional de las operaciones, los procesos y los equipos relacionados con la seguridad operacional de la aviación, según corresponda, antes de ponerlos en servicio, de conformidad con lo requerido en la subsección RAC- 19.125.

(e) Mejora continua

(1) Defina un proceso de auditoría interna y de conformidad con lo requerido en la subsección RAC-19.120 (c);
(2) Defina un proceso de auditoría externa y de conformidad con lo requerido en las sección RAC-19.120 (c);
(3) Defina un programa para la evaluación de instalaciones, equipos, documentación y procedimientos que se deben completar mediante auditorías y estudios de conformidad con lo requerido en la subsección RAC-19.130; y

(f) Instrucción y educación

(1) Ejecute la instrucción correspondiente al componente III.

(g) Documentación SMS

(1) Desarrolle la documentación relativa a las actividades descritas en los párrafos (a), (b), (c), (d), (e) y (f) de la presente subsección.

RAC 19.180 Componente IV. Requisitos para la implementación y la aceptación del componente IV.

(a) Todo proveedor de servicios bajo el componente IV debe demostrar, mediante auditoría, que tiene establecido los objetivos de la seguridad operacional asociados a su política y ha puesto en práctica los elementos contenidos en el plan de implementación que se refieran a los siguientes elementos:

(1) Responsabilidad funcional y compromiso de la dirección:

(i) Mejore la política disciplinaria con una debida consideración de los errores accidentales y las infracciones deliberadas;

(2) Identificación de Peligros:

(i) Integre los peligros identificados en los informes de investigación de sucesos con el sistema de notificación voluntaria.

(ii) Determine las interfaces de los procedimientos de identificación de peligros y gestión del riesgo con el SMS del subcontratista o cliente, según aplique, de conformidad con las subsecciones RAC-19.065 (c), (d) (2) y RAC-19.245.

(3) Observación y medición del rendimiento en materia de seguridad operacional:

(i) Desarrolle indicadores y metas de rendimiento en materia de seguridad operacional de bajo impacto, incluyendo los niveles de alerta de conformidad con la subsección RAC-19.120 (b);

(4) Mejora continua del SMS:

(i) Establezca auditorías SMS integradas y programas de revisión/estudios de SMS operacionales, de conformidad con las subsecciones RAC-19.120 (c) y (d);

(ii) Establecer otros programas de revisión/estudio de SMS operacional, donde corresponda.

(5) Instrucción y Educación:

(i) Ejecute la instrucción pertinente a el componente IV;

(6) Comunicación de seguridad operacional:

(i) Establezca mecanismos para promover la distribución y el intercambio de información de seguridad operacional de forma interna y externa, de conformidad con la subsección RAC-19.150; y

(7) Documentación SMS:

(i) Desarrolle la documentación relativa a las actividades descritas en el

párrafo (a) de la presente sección.

(b) Con el fin de dar cumplimiento a los componentes de aceptación de un SMS, la Agencia Hondureña de Aeronáutica Civil (AHAC), a través del Departamento del Programa Estatal de Seguridad Operacional (SSP), no dará la aceptación o no dará como buena y válida una auditoría de aceptación de un SMS para un proveedor de servicios cuando sea evidenciada alguna No Conformidad Mayor o se obtengan tres (3) omás No Conformidades Menores.

(c) Para el propósito de esta subparte, se entenderá una No Conformidad Mayor como el incumplimiento total de cualquier subparte de este RAC. Así mismo, se considerará una No Conformidad Menor como el incumplimiento de tres o más requisitos de cualquier subparte de este RAC.

(d) Según lo prescrito en los párrafos (b) y (c) de esta subparte, ningún proveedor de servicios que, durante una auditoría de aceptación, haya tenido una (1) No Conformidad Mayor o una cantidad igual o mayor a tres (3) No Conformidades Menores, podrá obtener el certificado de Aceptación de SMS de la AHAC, a través del SSP, que lo acredita como un proveedor de servicios que tiene implementado un SMS, excepto cuando cumpla al menos con las siguientes condiciones:

(1) Que en un plazo máximo de quince (15) días hábiles, a partir del recibo del informe formal de la auditoría de aceptación, el proveedor de servicios presente un plan de acción aceptable para la AHAC, a través del SSP, en el cual se presenten las acciones para solucionar las No Conformidades detectadas en dicha auditoría; y
(2) Que en un plazo máximo de setenta y cinco (75) días hábiles, desde la aceptación del plan de acción por parte del SSP, el proveedor de servicios presente las evidencias de la solución a las No Conformidades aceptables para la AHAC, a través del Programa Estatal de Seguridad Operacional (SSP).

(e) En el caso que un proveedor de servicios presente razones justificadas y estas sean aceptadas por el SSP, del no cumplimiento con las soluciones de las No Conformidades resultantes de una auditoría, éste podría dar un nuevo plazo de cumplimiento en adicional descrito en el párrafo (d) (2) de esta subsección.
(f) Conforme lo prescrito en los párrafos (b) y (c) de esta subsección, todo proveedor de servicios que, durante una auditoría de aceptación, no haya tenido una No Conformidad Mayor y haya tenido dos o menos (2) No Conformidades Menores, podrá obtener el certificado de Aceptación de SMS de la AHAC por medio del SSP, que lo acredita como un proveedor de servicios que tiene implementado un SMS, cuando en un plazo máximo de quince (15) días hábiles, a partir del recibo del informe final de la auditoría de aceptación, el proveedor de servicios presente un plan de acción aceptable por el SSP, en el cual se presenten las acciones para solucionar las No Conformidades detectadas en dicha auditoría.

(g) Todo proveedor de servicios que haya solicitado a la Agencia Hondureña de Aeronáutica Civil (AHAC), a través del SSP, la aceptación de un SMS que haya cumplido con todo lo prescrito bajo esta regulación, le será emitido un Certificado de Aceptación, que lo acredita como poseedor de un SMS aceptado por el SSP.

RAC 19.185 TIEMPO DE ACEPTACIÓN DE LOS COMPONENTES DEL SMS PARA TODOS LOS PROVEEDORES DE SERVICIOS:

(a) El componente I debe presentarse para aprobación del SSP en un término no mayor a 90 días calendario desde el inicio de su certificación o aprobación.
(b) El componente II debe presentarse para aprobación del SSP, a más tardar, 180 días calendario contados a partir de la aceptación del componente I.
(c) El componente III debe presentarse para aprobación del SSP, a más tardar, 180 días calendario contados a partir dela aceptación del componente II.
(d) El componente IV debe presentarse para aprobación del SSP, a más tardar, 120 días calendario contados a partir de la aceptación del componente III.

(e) En el caso que no se cumplan los tiempos establecidos en (a), (b), (c) y/o (d) se archivará el proceso de aceptación y el operador debe de iniciar nuevamente todo el proceso, salvo que el interesado presente una solicitud formal de extensión de plazos para alguna de los componentes, donde indique el motivo del retraso y una nueva fecha de cumplimiento.

(f) La solicitud mencionada en el inciso (e) será analizada y aprobada por el SSP, con las consideraciones del caso.

RAC 19.190 Plan de implementación del SMS

(a) Todo proveedor de servicios debe desarrollar un plan de implementación del SMS, que debe ser el marco en el cual la organización desarrollará las actividades para gestionarla Implementación del SMS de forma que, una vez implementado, cumpla con las necesidades de seguridad operacional de la organización; y
(b) El plan de Implementación del SMS debe ser aprobado por el ejecutivo responsable y debe cumplir al menos con las subpartes A, B, C, D, E y F de esta regulación.

RAC 19.195 Procedimiento de aceptación del plan de implementación de un SMS

(a) Todo proveedor de servicios que solicite al Departamento del Programa Estatal de Seguridad Operacional (SSP) la aceptación de un plan de Implementación de un SMS de conformidad con esta regulación debe someter su solicitud de la forma y manera aceptable por el SSP conteniendo la información por este requerida.
(b) El plan de Implementación de un SMS estará en el idioma español y en la forma y manera como sea aceptable para el SSP.

RAC 19.200 Aceptación o Negación de un plan de implementación de un SMS

(a) El proveedor de servicios debe presentar un plan de Implementación del SMS, el cual contenga la información requerida en los requisitos aplicables de esta Regulación;

(b) Si el plan de implementación del SMS presentado, no cumple con todos los elementos descritos en esta regulación, dicho plan será denegado notificándoles de la decisión.

RAC 19.205 Procedimiento de aceptación de los componentes de un SMS

(a) El SSP podrá aceptar la conclusión satisfactoria de una componente durante la Aceptación de un SMS, de un proveedor de servicios, siempre que luego de ser evaluada el componente, esta reúna los requisitos descritos en este RAC 19.
(b) El SSP no aprobará el paso de un Componente a la siguiente a menos que el proveedor de servicios haya demostrado haber cumplido con los requisitos requeridos en el componente precedente y haber sido aceptada satisfactoriamente de parte del SSP de la forma y manera prescrita por este.

RAC 19.210 Procedimiento de aceptación final de un SMS

La AHAC aceptará el SMS a un proveedor de servicios siempre que éste haya demostrado que ha cumplido con el procedimiento y los componentes de Aceptación del sistema, de conformidad con esta regulación, y haya superado satisfactoriamente una auditoría de aceptación por parte del SSP de la forma y manera aceptable por la autoridad, de conformidad con RAC 19.160.

RAC 19.215 Auditorías de seguimiento

(a) A menos que la AHAC lo aprobare de otra manera, todo proveedor de servicios debe someterse a auditorías de seguimiento con la frecuencia y en la manera que el SSP determine, a partir de la auditoría de aceptación.
(b) El SSP no dará como bueno y válido los resultados de una auditoría cuando se obtenga una (1) No Conformidad Nivel 1 o tres (3) o más No Conformidades Nivel 2.
(c) Según lo prescrito en los párrafos (a) y (b) de esta subsección, todo proveedor de servicios que, durante una auditoría de seguimiento, haya tenido una No Conformidad Nivel 1 o tres (3) o más No Conformidades Nivel 2, estará sujeto a lo prescrito en la subsección RAC-19.040 excepto cuando cumpla al menos con las siguientes condiciones:

    (1) Las No conformidades nivel 1 deben de ser rectificadas de manera inmediata a menos que el gestor disponga lo contrario, siendo que se podría dar un plazo no mayor a 72 horas para su solución. Si se refiere a un sistema o procedimiento que necesita ser documentado e implementado, el proveedor de servicios contará con un periodo no mayor a 30 días hábiles, después de recibido el informe, para iniciar con el desarrollo de la acción correctiva.
    (2) Que en un plazo máximo de quince (15) días, a partir del recibo del informe formal de la auditoría, el proveedor de servicios presente un plan de acción aceptable para el SSP, en el cual se presenten las acciones para solucionar las No Conformidades detectadas en la auditoría; y

(3) Que en un plazo máximo de setenta y cinco (75) días desde la aceptación del plan de acción de parte del SSP, el proveedor de servicios presente las evidencias de la solución a las No Conformidades aceptables para el SSP.

(d) En el caso que un proveedor de servicios presente razones justificadas y estas sean aceptadas por el SSP, del no cumplimiento con las soluciones de las No Conformidades resultantes de una auditoria, éste podría dar un nuevo plazo de cumplimiento en adicional descrito en el párrafo c) (2) de esta subsección.

(e) Según lo prescrito en los párrafos (b) y (c) de esta subsección, todo proveedor de servicios que, durante una auditoría de seguimiento, no haya tenido una No Conformidad Nivel 1 y haya tenido dos (2) o menos No Conformidades Nivel 2, podrá mantener los privilegios de su certificado que lo acredita como tal bajo el reglamento aplicable y el certificado de Aceptación de SMS del Departamento del Programa Estatal de Seguridad Operacional (SSP) que lo acredita como un proveedor de servicios que tiene implementado un SMS, cuando en un plazo máximo de quince (15) días hábiles, a partir del recibo del informe formal de la auditoría de seguimiento, el proveedor de servicios presente un plan de acción aceptable para el SSP, en el cual se presenten las acciones para solucionar las No Conformidades detectadas en dicha auditoria.

SUBPARTE J. NOTIFICACION

RAC 19.220 Sistema de notificación obligatorio

(a) Los proveedores de servicios deben de establecer un sistema de notificación obligatoria de eventos de seguridad operacional, que incluya la notificación de incidentes, con la finalidad de facilitar la obtención de datos. En el apéndice 8 se establece una lista de los sucesos que deben de ser reportados por parte del proveedor de servicios al SSP, no obstante la notificación obligatoria de estos incidentes se deberán realizar bajo el Sistema de Notificación establecido por la Comisión Investigadora de Accidentes e Incidentes de Aviación (CIAIA).

(b) Los eventos de la lista del apéndice 8 deben de ser notificados al SSP en un plazo máximo de 24 horas desde el momento en que hayan tenido acontecimiento, a menos que circunstancias excepcionales y comprobadas lo impidan.

(c) La NO notificación de incidentes a las autoridades competentes CIAIA y AHAC, establecerán motivo de aplicación de la sanción establecida en la Ley de Aeronáutica Civil.

RAC 19.225 Categorías de los sucesos

(a) Los proveedores de servicios deben de notificar los sucesos que puedan constituir un riesgo significativo para la seguridad de las operaciones y que correspondan a las siguientes categorías dentro de las notificaciones obligatorias:

(1) Sucesos relacionados con la operación de aeronaves, tales como:

(i) Sucesos relacionados con colisiones;

(ii) Sucesos relacionados con el despegue y/o aterrizaje;

(iii) sucesos relacionados con el combustible;

(iv) sucesos en vuelo;

(v) sucesos relacionados con la comunicación;

(vi) sucesos relacionados con lesiones, emergencias y otras situaciones críticas;

(vii) incapacitación de la tripulación u otros sucesos que afecten a la tripulación;

(viii) sucesos relacionados con las condiciones meteorológicas.

(2) Sucesos relacionados con las condiciones técnicas, el mantenimiento y la reparación de la aeronave, tales como:

(i) defectos estructurales;

(ii) averías del sistema;

(iii) problemas de mantenimiento o reparación;

(iv) problemas de propulsión (incluidos los motores, hélices y sistemas rotores) y problemas de las unidades de potencia auxiliar.

(3) Sucesos relacionados con servicios e instalaciones de navegación aérea, tales como:

(i) colisiones, situaciones en que casi se produzca una colisión o posible colisión;

(ii) sucesos específicos de gestión del tránsito aéreo y servicios de navegación aérea; y

(iii) sucesos operativos ATM/ANS.

(4) Sucesos relacionados con aeródromos y servicios en tierra, tales como:

(i) sucesos relacionados con actividades e instalaciones de aeródromos;

(ii) con la gestión de pasajeros, equipajes, correo y carga,

(iii) manipulación incorrecta o mantenimiento defectuoso de aeronaves en tierra.

SUBPARTE K. NOTIFICACION VOLUNTARIA

RAC 19.230 Sistema de notificación voluntaria.

El objetivo de un sistema de notificación voluntario, confidencial y no punitivo es el de buscar mejorar la seguridad operacional de la aviación mediante la recopilación de informes sobre deficiencias reales o posibles de la seguridad operacional que, de lo contrario, podrían no informarse mediante otros canales. Tales informes pueden implicar los sucesos, los peligros o las amenazas pertinentes a la seguridad operacional de la aviación. Este sistema no elimina la necesidad de la notificación obligatoria de accidentes e incidentes con aeronaves a las autoridades pertinentes, según los reglamentos de aviación existentes y lo establecido en la Subparte J de la presente regulación.

RAC 19.235 Alcance

(a) Todo proveedor de servicio debe crear un sistema de notificación voluntaria de seguridad operacional, que facilite la recopilación de:

(1) información y datos sobre sucesos que puedan no ser captados por el sistema de notificación obligatoria;
(2) otra información relacionada con la seguridad operacional que el notificante perciba como un peligro real o potencial para la seguridad aérea.

(b) Los sistemas de notificación voluntaria se deben utilizar para facilitar la recolección de datos sobre sucesos e información relacionada con la seguridad operacional:

(1) que no esté sujeta a notificación obligatoria en virtud de la Subparte H de la presente regulación.
(2) notificada por personas no relacionadas con el proveedor de servicios.

(c) Todo proveedor de servicios debe notificar oportunamente al SSP, de la manera que este lo indique, los datos de sucesos reportados por medio del sistema voluntario y confidencial de reportes, así como cualquier otra información relacionada con la seguridad que pueda implicar un riesgo real o potencial para la seguridad aérea. La AHAC, por medio del SSP puede exigir a cualquier proveedor de servicios que notifique los datos de sucesos de conformidad con RAC 19.245 (a).

(d) La AHAC, por medio del SSP, puede establecer otros sistemas de recolección y tratamiento de información sobre seguridad operacional, con la finalidad de recoger información de sucesos que puedan no ser recopilados por los sistemas de notificación mencionados en las Subpartes J y K de la presente regulación, y pueden implicar la participación:
(1) del sector de la industria área;

(2) de las organizaciones profesionales del personal de la aviación.

(e) La información recibida de notificaciones voluntarias y obligatorias puede ser integrada en un sistema único.

SUBPARTE L. TRATAMIENTO DE LA INFORMACION

RAC 19.240 Recolección y conservación de la información

(a) Cada proveedor de servicios debe designar una o varias personas para gestionar de manera independiente la recolección, evaluación, tratamiento, análisis y almacenamiento de datos sobre los sucesos notificados. La gestión de las notificaciones se debe llevar a cabo con la intención de prevenir el empleo de la información para fines distintos de seguridad, y se debe proteger adecuadamente la confidencialidad del notificante y de toda persona mencionada en relación con un suceso, con miras a fomentar una cultura justa.
(b) Previo acuerdo con la AHAC, por medio del SSP, los proveedores de servicios pequeños pueden establecer un mecanismo simplificado de recolección, evaluación, tratamiento, análisis y almacenamiento de los sucesos.

RAC 19.245 Calidad y contenido de las notificaciones de sucesos

(a) Las notificaciones de sucesos mencionados en RAC-19.250 deben contener al menos la información indicada en el apéndice 9 de la presente regulación.
(b) Las notificaciones de sucesos deben incluir una clasificación de riesgo para la seguridad operacional de acuerdo con el suceso que se trate. Dicha clasificación debe de ser examinada, si es necesario modificada, y ser refrendada por el SSP.
(c) Los proveedores de servicios deben establecer procedimientos de control de calidad de los datos para mejorar la coherencia de estos, especialmente entre la información recogida inicialmente y la notificación almacenada en la base de datos.
(d) Las bases de datos deben recurrir a formatos que sean normalizados para facilitar el intercambio de información, y deben de utilizar la taxonomía ADREP (Accident/IncidentData Reporting system).

INTENCIONALMENTE EN BLANCO

SUBPARTE M. ANALISIS DE LOS SUCESOS

RAC 19.250 Análisis de sucesos y seguimiento a nivel nacional

(a) Cada proveedor de servicios debe establecer un procedimiento para analizar los sucesos recogidos de conformidad con lo establecido en las Subpartes J y K, a fin de determinar los riesgos para la seguridad asociados a los sucesos o grupos de sucesos observados.

Nota - En función de ese análisis, cada organización debe determinar las medidas de prevención o corrección adecuadas, para la mejora de la seguridad operacional.

(b) Cuando, tras el análisis, una organización determine las eventuales medidas adecuadas para resolver las deficiencias de seguridad operacional reales o potenciales, debe:
(1) aplicar dichas medidas a su debido tiempo; y

(c) establecer un proceso de seguimiento de la aplicación y de la eficacia de las medidas.

(d) Cada proveedor de servicios debe comunicar con regularidad a su personal información sobre el análisis y el seguimiento de los diversos sucesos que son objeto de medidas preventivas o correctivas.

(e) Si un proveedor de servicios determina las deficiencias de seguridad operacional reales o potenciales como resultado de sus análisis de sucesos o grupos de sucesos notificados con arreglo a las Subpartes J y K, debe transmitir al SSP, en un plazo no mayor a 30 días naturales, contados desde la fecha de notificación del suceso por el notificante:

(1) los primeros resultados del análisis efectuado, si existen; y
(2) cualquier medida que se haya adoptado como resultado de los hallazgos.

(f) La organización debe comunicar los resultados finales, si así está previsto, tan pronto como estén disponibles y, en principio en un plazo máximo de tres meses a partir de la fecha de notificación del suceso.

(g) La AHAC, por medio del SSP, puede solicitar a las organizaciones que le transmitan los primeros resultados, o los resultados definitivos, del análisis de cualquier suceso que se le haya notificado, pero sobre el que no se haya tomado medida alguna, o sobre el que únicamente haya recibido los primeros resultados.

(h) La información obtenida a partir del análisis de los informes de sucesos será utilizada por la AHAC, por medio del SSP, para ayudar a determinar las eventuales medidas correctivas para:

(1) tomar acciones inmediatas;
(2) implementar la vigilancia basada en riesgos de seguridad operacional;
(3) definir o modificar la política y/o los objetivos de seguridad operacional;

(4) definir o modificar los SPI;
(5) definir o modificar los SPT;
(6) establecer los desencadenantes de los SPI;
(7) promover la seguridad; y
(8) realizar una evaluación adicional de los riesgos de seguridad operacional.

(i) Con el objeto de informar a la opinión pública del nivel de seguridad operacional de la aviación civil, la AHAC, por medio del SSP, publicará una memoria sobre la seguridad operacional. Dicho informe debe:

(1) contener información agregada y economizada sobre los tipos de sucesos y la información relacionada con la seguridad recogidos por sus sistemas nacionales de notificación obligatoria y voluntaria;
(2) indicar las tendencias; e
(3) indicar las medidas que se hayan adoptado.

SUBPARTE N. CONFIDENCIALIDAD Y PROTECCION DE LA FUENTES DE INFORMACION

RAC 19.255 Naturaleza y Objetivo

La confidencialidad y protección de las fuentes de información se considera esencial para el servicio de transporte aéreo. Debido a esto, el objetivo de la presente subparte es proteger el uso de información de seguridad operacional proveniente de los Sistemas de Recopilación y Procesamiento de Datos de SeguridadOperacional (SDCPS), los cuales se han desarrollado con el objetivo de mejorar la seguridad operacional.

RAC 19.260 Alcance

El alcance de esta subparte se limita en su aplicación a la información de seguridad operacional recopiladaen los SDCPS, excepto que sus disposiciones no aplican para el uso de la información recabada o generada durante el curso de las investigaciones de accidentes e incidentes de aeronaves, que se rigen de acuerdo con el RAC-13 Investigación de Accidentes e Incidentes de Aviación.

RAC 19.265 Uso apropiado de la información sobre seguridad operacional

La presente Subparte protege contra el uso inapropiado de la información de seguridad operacional tomadade los SDCPS. Sujeta a las excepciones que se estipulan en la presente regulación, esta información debede ser utilizada únicamente con el propósito de mejorar la seguridad operacional, y no para procedimientosdisciplinarios, civiles, administrativos o penales contra algún personal, ni para revelarla al público.

RAC 19.270 Principios de protección de las fuentes de información

El Principio de Protección: se considera esencial la protección de la vida, la integridad física, la seguridad de los individuos y las corporaciones, y el legado dentro del contexto de la actividad aeronáutica. Además, como parte de esta regulación, también es importante proteger la recopilación y el procesamiento de datos, así como la información de seguridad operacional con el fin de garantizar los márgenes más altos de seguridad operacional en las operaciones aéreas y actividades relacionadas.

El Principio de Confidencialidad: toda recopilación de datos y procesamiento de información de seguridad operacional, su circulación, y la actividad administrativa relacionada con estas acciones, tal como se establece en el inciso a), deben reservarse sólo para la mejora de la seguridad operacional que se expone en el presente documento.

RAC 19.275 Excepciones al principio de confidencialidad

La AHAC, por medio del SSP, debe garantizar que el proveedor de servicios que tenga un Sistema de Gestión de la Seguridad Operacional (SMS) que esté protegido por el Principio de Confidencialidad. La autoridad aeronáutica podría sólo utilizar la información de seguridad operacional para prevenir futuros accidentes o incidentes, excepto en las siguientes circunstancias:

(a) Por requerimiento expreso de una corte de justicia con la jurisdicción, y que haya determinado que la autoridad aeronáutica tiene información que podría ser necesaria para una investigación penal, o

(b) Que una autoridad competente considere que las circunstancias indican de manera razonable que el evento pudo haber sido causado por una conducta, con la intención de causar daño, o con el conocimiento de que probablemente se produciría un daño, equivalente a una conducta temeraria, negligencia grave o dolo; o

(c) Hay evidencia de que el evento ha sido causado por un acto que se considera se realizó con la intención de causar daño, o con el conocimiento de que probablemente se produciría un daño, equivalente a una conducta temeraria, negligencia grave, violación o dolo, o

(d) La revisión realizada por una autoridad apropiada determine que es necesario revelar la información sobre seguridad operacional para la correcta administración de la justicia sobre eso, y que los beneficios de esta divulgación sobrepasen el impacto adverso nacional e internacional que esta pudiera tener sobre la futura disponibilidad de la información de seguridad operacional.

(e) La información que se revela o se pone a disposición no debe incluir los nombres de los individuos. Sin embargo, una corte de justicia con competencia jurisdiccional u otra autoridad legal puede, después de considerar el impacto negativo que pueda causar la divulgación de los nombres de los individuos sobre la futura disponibilidad de la información de seguridad operacional, dictar la orden de revelar los nombres de los individuos para la correcta administración de la justicia.

RAC 19.280 Medidas de salvaguarda

El proveedor de servicios que debe mantener un Sistema de Gestión de la Seguridad Operacional (SMS) y no puede utilizar la información que sus empleados revelen con propósitos de seguridad operacional, como base para tomar medidas disciplinarias contra ellos, excepto para las condiciones definidas como inaceptables dentro de su propio Sistema de Gestión de la Seguridad Operacional (SMS).

RAC 19.285 Medidas de salvaguarda concerniente a la información sobre terceros

El proveedor de servicios que debe mantener un Sistema de Gestión de la Seguridad Operacional (SMS) no debe tomar medidas que podrían afectar de forma adversa las condiciones de trabajo de sus empleados, como represalia por la información que estos revelen sobre supuestas acciones u omisiones que cometa otra persona, siempre y cuando se haya revelado de buena fe y por motivos de seguridad operacional.

RAC 19.290 Excepciones a la protección de la recopilación y el procesamiento de datos

La recopilación, procesamiento y análisis de datos, y el uso del proceso de información de seguridad operacional proporcionado por un Sistema de Gestión de la Seguridad Operacional (SMS), el cual es mantenido por un proveedor de servicios, obligado o no a mantener este sistema, están protegidos por el Principio de Confidencialidad y esa información no se puede revelar o poner a disposición, excepto en los siguientes casos:

(a) Por requerimiento expreso de una corte de justicia con la jurisdicción, y que haya determinado que la autoridad aeronáutica tiene información que podría ser necesaria para

una investigación penal, o

(b) Que una autoridad competente considere que las circunstancias indican de manera razonable que el evento pudo haberse originado con la intención de causar daño, o con el conocimiento de la posibilidad de que este evento ocurriera, y es equivalente a una conducta temeraria, negligencia grave, violación o dolo, o

(c) Hay evidencia de que el evento ha sido causado por un acto que se considera se realizó con laintención de causar daño, o con el conocimiento de la posibilidad de que este ocurriera, y es equivalente a una conducta temeraria, negligencia grave o un acto doloso, o

(d) La revisión realizada por una autoridad apropiada determina que es necesario revelar la información sobre seguridad operacional para la correcta administración de la justicia y que su divulgación sobrepasa al impacto adverso nacional e internacional que esta pudiera tener sobre la futura disponibilidad de la información de seguridad operacional.

(e) La información que se da a conocer o se pone a disposición no debe incluir los nombres de los individuos. Sin embargo, una corte de justicia con competencia jurisdiccional u otra autoridad legal puede, después de considerar el impacto negativo que pueda causar la divulgación de los nombres de los individuos sobre la futura disponibilidad de la información de seguridad operacional, dictar la orden de revelar los nombres de los individuos para la correcta administración de la justicia.

RAC 19.295 Registrador de datos de vuelo

Sujeta a las excepciones del RAC 19.310, las cuales aplican por igual aquí, la información de seguridad operacional recopilada a partir de los registros de datos de vuelo no se debe utilizar para tomar medidas disciplinarias o iniciar procedimientos legales contra el explotador aéreo, su tripulación, sus empleados, cualquier persona relacionada con el explotador, o un tercero, como resultado de acciones que generen información relacionada con la seguridad operacional, excepto para las condiciones definidas como inaceptables dentro de su propio Sistema de Gestión de la Seguridad Operacional (SMS).

RAC 19.300 Acuerdos tomados con el proveedor de servicios

Con el fin de promover la seguridad operacional, la AHAC, por medio del SSP, tiene la facultad de concertar acuerdos con el explotador aéreo, el proveedor de servicios, o el fabricante de equipo aeronáutico, respecto a la recopilación, análisis, uso y difusión de información de seguridad operacional.

RAC 19.305 Protección de la información contenida en los acuerdos

La información de seguridad operacional que resulte de los acuerdos mencionados en el RAC 19.325 de esta regulación, y que se proporcione a la autoridad aeronáutica, no debe utilizarse para tomar medidas o iniciar procedimientos legales contra el explotador aéreo, su tripulación, sus empleados, o un tercero, dado que esta información es relevante para salvaguardar la seguridad operacional y está protegida por el Principio de Confidencialidad.

RAC 19.310 Excepciones a la confidencialidad de los acuerdos

La información proporcionada a la autoridad aeronáutica competente y que resulte de los acuerdos mencionados en el RAC 19.325 de esta regulación, está regulada por el Principio de Confidencialidad y no se puede revelar ni poner a disposición, excepto:

(a) Por requerimiento expreso de una corte de justicia con la jurisdicción, y que haya determinado que la autoridad aeronáutica tiene información que podría ser necesaria para una investigación penal, o

(b) Que una autoridad competente considere que las circunstancias indican de manera razonable que el evento pudo haberse originado con la intención de causar daño, o con el conocimiento dela posibilidad de que este evento ocurriera, y es equivalente a una conducta temeraria, negligencia grave o un acto doloso, o

(c) Hay evidencia de que el evento ha sido causado por un acto que, se considera se realizó con la intención de causar daño, o con el conocimiento de la posibilidad de que este ocurriera, y es equivalente a una conducta temeraria, negligencia grave, violación o un acto doloso, o

(d) La revisión realizada por una autoridad apropiada determina que es necesario revelar la información sobre seguridad operacional para la correcta administración de la justicia, y que su divulgación sobrepasa al impacto adverso nacional e internacional que esta pudiera tener sobre la futura disponibilidad de la información de seguridad operacional.

(e) La información que se da a conocer o se pone a disposición no debe incluir los nombres de los individuos. Sin embargo, una corte de justicia con competencia jurisdiccional u otra autoridad legal puede, después de considerar el impacto negativo que pueda causar la divulgación de los nombres de los individuos sobre la futura disponibilidad de la información de seguridad operacional, dictar la orden de revelar los nombres de los individuos para la correcta administración de la justicia.

RAC 19.315 Confidencialidad de los informes voluntarios

De acuerdo con el Departamento del Programa Estatal de Seguridad Operacional (SSP), en el caso de un informe voluntario,este debe de ser regulado por el Principio de Confidencialidad.

RAC 19.320 Excepciones a la confidencialidad de los informes voluntarios

La información proporcionada conforme a un programa de informes voluntarios, tal como el que se describeen el RAC 10.325, está protegida por el Principio de Confidencialidad y esa información no puede revelarseo ponerse a disposición, excepto en los siguientes casos:

(a) Por requerimiento expreso de una corte de justicia con la jurisdicción, y que haya determinado que la autoridad aeronáutica tiene información que podría ser necesaria para una investigación penal, o

(b) Que una autoridad competente considere que las circunstancias indican de manera razonable que el evento pudo haberse originado con la intención de causar daño, o con el conocimiento de la posibilidad de que este evento ocurriría, y es equivalente a una conducta temeraria, negligencia grave o un acto doloso, o

(c) Hay evidencia de que el evento ha sido causado por un acto que se considera se realizó con

la intención de causar daño, o con el conocimiento de la posibilidad de que este ocurriera, y es equivalente a una conducta temeraria, negligencia grave, violación o un acto doloso, o

(d) La revisión realizada por una autoridad apropiada determina que es necesario revelar la información sobre seguridad operacional para la correcta administración de la justicia, y que su divulgación sobrepasa al impacto adverso nacional e internacional que ésta pudiera tener sobre la futura disponibilidad de la información de seguridad operacional.

(e) La información que se da a conocer o se pone a disposición no debe incluir los nombres de los individuos. Sin embargo, una corte de justicia con competencia jurisdiccional u otra autoridad legal puede, después de considerar el impacto negativo que pueda causar la divulgación de losnombres de los individuos sobre la futura disponibilidad de la información de seguridad operacional, dictar la orden de revelar los nombres de los individuos para la correcta administración de la justicia.

(f) Por requerimiento expreso de una corte de justicia con la jurisdicción, y que haya determinado que la autoridad aeronáutica tiene información que podría ser necesaria para una investigación penal, o

(g) Que una autoridad competente considere que las circunstancias indican de manera razonable que el evento pudo haberse originado con la intención de causar daño, o con el conocimiento de la posibilidad de que este evento ocurriría, y es equivalente a una conducta temeraria, negligencia grave o un acto doloso, o

(h) Hay evidencia de que el evento ha sido causado por un acto que se considera se realizó con laintención de causar daño, o con el conocimiento de la posibilidad de que este ocurriera, y es equivalente a una conducta temeraria, negligencia grave, violación o un acto doloso, o

(i) La revisión realizada por una autoridad apropiada determina que es necesario revelar la información sobre seguridad operacional para la correcta administración de la justicia, y que su divulgación sobrepasa al impacto adverso nacional e internacional que ésta pudiera tener sobrela futura disponibilidad de la información de seguridad operacional.

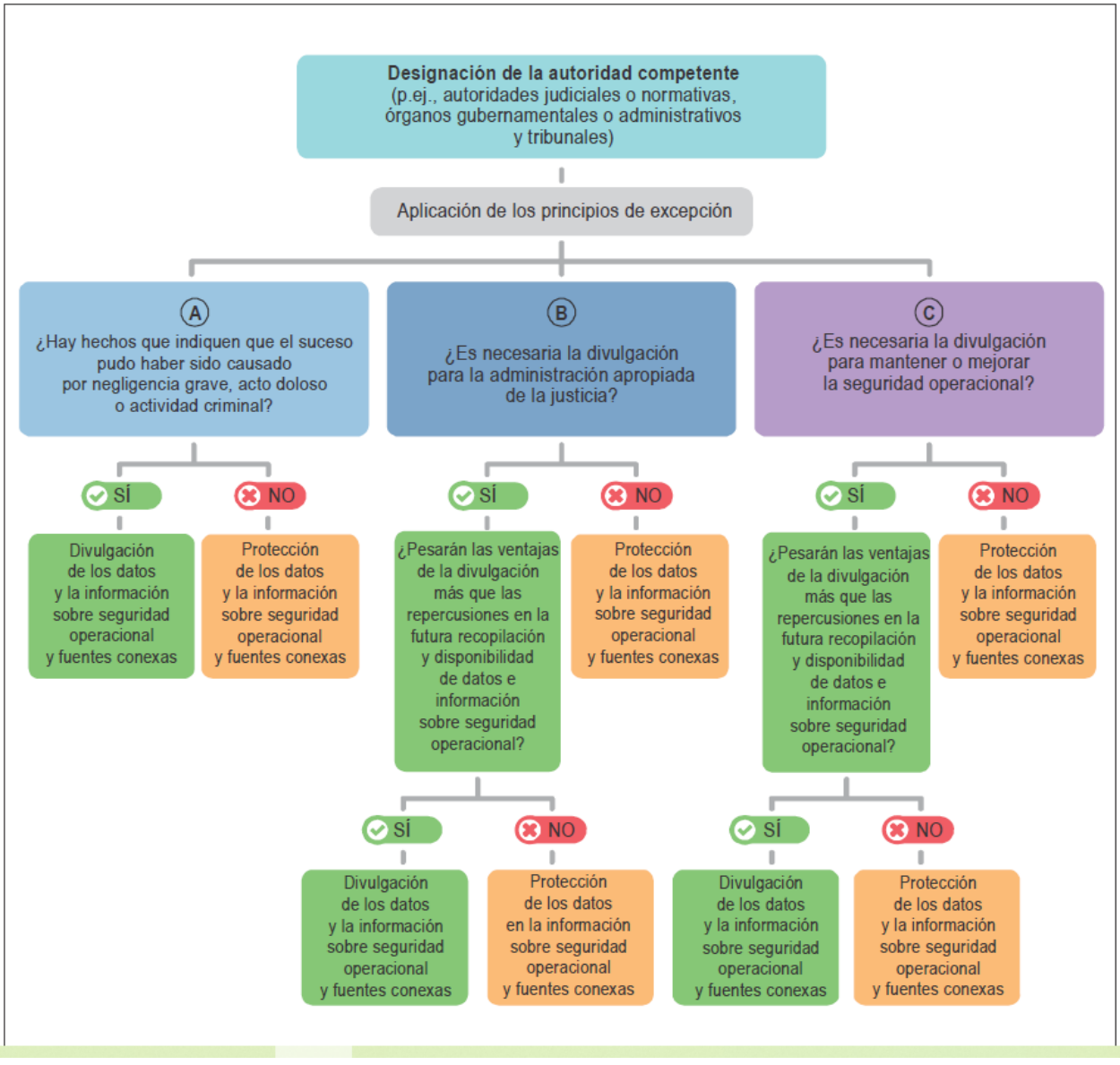
(j) La información que se da a conocer o se pone a disposición no debe incluir los nombres de losindividuos. Sin embargo, una corte de justicia con competencia jurisdiccional u otra autoridad legal puede, después de considerar el impacto negativo que pueda causar la divulgación de losnombres de los individuos sobre la futura disponibilidad de la información de seguridadoperacional, dictar la orden de revelar los nombres de los individuos para la correctaadministración de la justicia.

RAC 19.325 Uso de la información de seguridad operacional

Basada en el Principio de Confidencialidad, la AHAC está autorizada para utilizar la información de seguridad operacional o cualquier información obtenida de manera voluntaria bajo el Departamento del Programa Estatal de Seguridad Operacional (SSP), la cual considere apropiada o necesaria para salvaguardar la seguridad operacional.

RAC 19.330 Difusión de información de seguridad operacional entre los Estados contratantes de laOACI

La información de seguridad operacional obtenida de forma voluntaria bajo el Departamento del Programa Estatal de Seguridad Operacional (SSP) puede difundirse entre los Estados Contratantes con el fin de mejorar la seguridad operacional, pero sin identificar a los proveedores de servicios, o a los individuos relacionados con la actividad aeronáutica, y debe estar regulada por el Principio de Confidencialidad.



Directrices para la aplicación de los principios de excepción

La incorrecta evaluación de reclamaciones concurrentes para obtener acceso a datos o información sobre seguridad operacional puede tener consecuencias adversas para las actividades presentes y futuras en dos formas. La divulgación al público de ciertos datos o información puede percibirse como una violación de la privacidad de los individuos o de las expectativas de confidencialidad de organizaciones relacionadas con dichos datos e información. El uso de ciertos datos o información como parte de un argumento en apoyo de sanciones contra individuos u organizaciones involucrados puede considerarse también como una violación de principios básicos de equidad. La futura disponibilidad de datos e información sobre seguridad operacional puede verse afectada por el comportamiento humano predecible de retener información debido a la percepción de una posible amenaza basada en su divulgación o uso incriminatorio. Esto puede tener un impacto evidente en las funciones de recopilación y análisis de datos de la gestión de la seguridad operacional.

INTENCIONALMENTE EN BLANCO

Apéndice 1

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 el funcionario ejecutivo, principal director ejecutivo/o lo que corresponda para la organización.

Nuestro compromiso es para:

(1) 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;
(2) garantizar que la gestión de la seguridad operacional sea una de las responsabilidades principales de todos los gerentes y empleados;
(3) 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;
(4) 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;
(5) 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;
(6) cumplir con y, cuando sea posible, superar los requisitos y las normas reglamentarias y legislativas;
(7) garantizar que estén disponibles suficientes recursos humanos y financieros
(8) cualificados y capacitados para implementar las estrategias y los procesos de seguridad operacional;
(9) 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;

(10) 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;
(11) 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
(12) 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.
(13) Esta política de seguridad operacional será comunicada y divulgada a todos los colaboradores de la organización, de la misma manera será desplegada en las áreas de visitas y de alto tráfico de personas.
(14) Esta política de seguridad operacional será revisada de manera periódica en período no mayor a 12 meses o cuando las circunstancias lo requieran.
(15) Fecha.

(Firmado)_____

Director ejecutivo/o quien corresponda

Apéndice 2

Designación de personal clave de seguridad operacional

1. Propósito General

La designación de una o varias personas para la función de gerente de seguridad operacional es fundamental para la implementación y funcionamiento eficaces del SMS. El gerente de seguridad operacional puede identificarse con diferentes nombres en las organizaciones, pero para el propósito de esta RAC, se utilizará el término “gerente de seguridad operacional” con referencia a la función, y no necesariamente al individuo. La persona que realiza la función de gerente de seguridad operacional es responsable ante el ejecutivo responsable del rendimiento del SMS y de la prestación de los servicios de seguridad operacional a los demás departamentos de la organización.

2. Funciones Claves

El gerente de seguridad operacional asesora al ejecutivo responsable y a los gerentes de línea respecto de asuntos de gestión de la seguridad operacional, y es responsable de coordinar y comunicar los problemas de seguridad operacional dentro de la organización, así como con los miembros externos de la comunidad aeronáutica. Entre las funciones de gerente de seguridad operacional figuran las siguientes:

a) gestionar el plan de implementación del SMS en nombre del ejecutivo responsable (después de la implantación inicial);

b) realizar o facilitar la identificación de peligros y el análisis de riesgos de seguridad operacional;

c) controlar las medidas correctivas y evaluar sus resultados;

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

e) mantener registros y documentación de seguridad operacional;

f) planificar y facilitar la capacitación en seguridad operacional del personal;

g) proporcionar asesoramiento independiente sobre asuntos de seguridad operacional;

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

i) coordinar y comunicarse (en nombre del ejecutivo responsable) con la AHAC y otras entidades estatales, según sea necesario, sobre temas relacionados con la seguridad operacional.

3. En la mayoría de las organizaciones, se designa a un individuo como gerente de seguridad operacional. Dependiendo de la envergadura, características y complejidad de la organización, la función de gerente de seguridad operacional puede ser de carácter exclusivo o puede combinarse con otras tareas. Además, algunas organizaciones pueden tener que adjudicar la función a un grupo de personas. La institución debe asegurarse de que la opción escogida no resulte en conflictos de intereses. Siempre que sea posible, el gerente de seguridad operacional no debería involucrarse directamente en la entrega de productos o servicios, pero debería tener conocimientos prácticos de los mismos. La designación también debería considerar posibles conflictos de intereses con otras tareas y funciones. Dichos conflictos podrían incluir:

a) competencia para el logro de financiación (p. ej., si el gerente financiero es el gerente de seguridad operacional);

b) prioridades conflictivas para la obtención de recursos; y

c) los casos en que el gerente tiene una función operacional y puede evaluar la eficacia respecto del
d) SMS de las actividades operacionales en que está involucrado.

En los casos en que la función se asigne a un grupo de personas (p. ej., cuando los proveedores de servicios amplían su SMS para abarcar múltiples actividades) debería designarse una persona como gerente de seguridad operacional “principal”, a efectos de mantener una línea de notificación directa e inequívoca hacia el ejecutivo responsable.

Entre las competencias del gerente de seguridad operacional figuran las siguientes:

a) experiencia en gestión de la seguridad operacional/calidad;

b) experiencia operacional relacionada con el producto o servicio proporcionado por la organización;

c) antecedentes técnicos para comprender los sistemas que respaldan las operaciones o los productos a servicios proporcionados;

d) habilidades para relacionarse con las personas;

e) habilidades analíticas y de solución de problemas;

f) habilidades de gestión de proyectos;

g) habilidades de comunicación oral y escrita; y

h) comprensión de los factores humanos

Dependiendo de la envergadura, características y complejidad de la organización, puede ser necesario contar con personal adicional para respaldar al gerente de seguridad operacional. El gerente de seguridad operacional y el personal de apoyo son responsables de asegurar la rápida recopilación y análisis de datos de seguridad operacional y la apropiada distribución dentro de la organización de la información sobre seguridad operacional conexa de modo que puedan adoptarse decisiones sobre riesgos de seguridad operacional y medidas de control, según sea necesario.

Los proveedores de servicios deberían establecer comités de seguridad operacional apropiados que respalden las funciones SMS en toda la organización. Esto debería comprender la determinación de quienes deberían integrar el comité de seguridad operacional y la frecuencia de las reuniones de éste.

El comité de seguridad operacional de mayor nivel, denominado a veces consejo de revisión de seguridad operacional (SRB), está integrado por el ejecutivo responsable y los administradores superiores participando como asesor el gerente de seguridad operacional. El SRB tiene carácter estratégico y trata de asuntos de alto nivel relacionados con las políticas de seguridad operacional, asignación de recursos y rendimiento de la organización. El SRB controla:

a. la eficacia del SMS;

b. la adopción oportuna de cualquier medida de control de riesgos de seguridad operacional que sean necesarias;

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

d. la eficacia general de las estrategias de mitigación de riesgos de seguridad operacional;

e. la eficacia de los procesos de gestión de la seguridad operacional de la organización que respaldan:

    1) la prioridad institucional declarada de la gestión de la seguridad operacional; y

    2) la promoción de la seguridad operacional en toda la organización.

Una vez que el comité de seguridad operacional de mayor nivel ha elaborado una dirección estratégica, la implementación de las estrategias de seguridad operacional debe coordinarse en toda la organización. Esto puede lograrse mediante la creación de grupos de acción de seguridad operacional (SAG) que están más concentrados en las operaciones. Los SAG se componen normalmente de gerentes y personal de primera línea y están presididos por un gerente de línea designado. Los SAG son entidades tácticas que abordan problemas de implementación específicos según la dirección del SRM. Los SAG:

a. 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 SRM apropiadas;

b. revisan los datos de seguridad operacional disponibles e identifican la implementación de estrategias apropiadas de control de riesgo de seguridad operacional y garantizan que se proporcionan comentarios de los empleados;

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

d. coordinan la implementación de medidas correctivas relacionadas con los controles de seguridad operacional y garantizan que dichas medidas se tomen rápidamente; y

e. revisan la eficacia de los controles de riesgo de seguridad operacional específicos.

Apéndice 3

Coordinación de la planificación de respuesta ante emergencias

(a) Por definición, una emergencia es una situación o un suceso repentino e imprevisto que requiere medidas inmediatas. La coordinación de la planificación de respuestas ante emergencias se refiere a la planificación de actividades que tiene lugar dentro de un período de tiempo limitado durante una situación de emergencia operacional aeronáutica imprevista. Un plan de respuestas ante emergencias (ERP) es un componente integral del proceso SRM de proveedor de servicio para enfrentar emergencias, crisis o sucesos relacionados con la aviación. Cuando existe la posibilidad de que las operaciones o actividades aeronáuticas de un proveedor de servicios se vean comprometidas por emergencias como casos de salud pública o pandemias, estos escenarios también deberían abordarse en su ERP según corresponda. El ERP debe abordar también emergencias previsibles que se identifiquen en el SMS y comprender medidas, procesos y controles de mitigación para gestionar eficazmente las emergencias relacionadas con la aviación.

(b) El objetivo general del ERP es la continuación de las operaciones en condiciones de seguridad y el retorno a las operaciones normales tan pronto como sea posible. Esto debe garantizar que exista una transición ordenada y eficiente de operaciones normales a operaciones de emergencia, incluida la asignación de responsabilidades de emergencia y la delegación de la autoridad. Se incluye también el período de tiempo necesario para restablecer las operaciones “normales” después de una emergencia. El ERP determina las medidas que debe adoptar el personal responsable durante una emergencia. La mayoría de estos casos exigirá acciones coordinadas entre diferentes organizaciones, posiblemente con otros proveedores de servicios y con otras organizaciones externas como las de servicios de emergencia no relacionados con la aviación. El ERP debe ser de fácil acceso para el personal clave apropiado, así como para las organizaciones externas de coordinación.

(c) La coordinación de la planificación de respuesta ante emergencias se aplica solamente a aquellos proveedores de servicios que deben establecer y mantener un ERP. En el Anexo 19 no se exige la creación o elaboración de un ERP; la planificación de respuestas ante emergencias se aplica solamente a proveedores de servicios específicos según se establece en los Anexos pertinentes de la OACI (en los diversos Anexos pueden utilizarse términos diferentes para las disposiciones relativas al tratamiento de situaciones de emergencia). Esta coordinación debería ejercerse como parte del ensayo periódico del ERP.

Una respuesta satisfactoria ante una emergencia comienza con la planificación eficaz. Un ERP representa la base de un enfoque sistemático para gestionar los asuntos de la organización durante las consecuencias de un evento no planificado importante, en el peor de los casos, un accidente importante.

Documentación del SMS

La documentación del SMS debe incluir un “manual SMS”, de alto nivel, en el que se describa las políticas, procesos y procedimientos SMS del proveedor de servicios a efectos de facilitar la administración, comunicación y mantenimientos internos del SMS por parte de la organización. Ello debe contribuir a que el personal comprenda la forma en que funciona el SMS de la organización y cómo se satisfarán las políticas y objetivos de seguridad operacional. La documentación debe incluir una descripción del sistema que proporcione los límites del SMS. También debe ayudar a aclarar la relación entre las diversas políticas, procedimientos, procesos y prácticas y definir como estos se relacionan con la política y objetivos de seguridad operacional del proveedor de servicios. La documentación debe adaptarse y redactarse para abordar las actividades cotidianas de gestión de la seguridad operacional de forma que puedan ser fácilmente comprensibles por todo el personal de la organización.

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

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

a) la política y los objetivos de seguridad operacional;

b) referencias a cualesquiera requisitos SMS normativos aplicables;

c) una descripción del sistema;

d) obligaciones de rendición de cuentas en materia de seguridad operacional y personal clave de seguridad operacional;

e) procesos y procedimientos de sistemas de notificación voluntaria y obligatoria de seguridad operacional;

f) procesos y procedimientos de identificación de peligros y evaluación de riesgos de seguridad operacional;

g) procedimientos de investigación de seguridad operacional;

h) procedimientos para establecer y observar los indicadores de rendimiento en materia de seguridad operacional;

i) procesos y procedimientos de instrucción en SMS y comunicaciones;

j) procesos y procedimientos de comunicación de seguridad operacional;

k) procedimientos de auditoría interna;

l) gestión de procedimientos de cambio;

m) procedimientos de gestión de la documentación SMS; y

n) cuando corresponda, coordinación de la planificación de respuestas ante emergencias.

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

a) registros de informes de peligros e informes sobre peligros/seguridad operacional;

b) SPI y gráficos relacionados;

c) registro de evaluaciones de seguridad operacional completadas;

d) registros de revisión o auditoría internas del SMS;

e) registros de auditoría interna;

f) registros de instrucción en SMS/seguridad operacional;

g) actas de reuniones del comité del SMS/ seguridad operacional;

h) plan de implementación del SMS (durante el período de implementación inicial); y

i) análisis de brechas para respaldar el plan de implementación.

COMPONENTE 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

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

El proceso de SRM identifica sistemáticamente los peligros que existen en el contexto de la entrega de sus productos o servicios. Puede que los peligros sean resultado de los sistemas que son deficientes en su diseño, función técnica, interfaz humana o interacciones con otros procesos y sistemas. También pueden resultar de una falla de los procesos o sistemas existentes para adaptar los cambios en el entorno de operación del proveedor de servicios. A menudo, un análisis cuidadoso de estos factores puede identificar posibles peligros en cualquier punto de la operación o del ciclo de vida de la actividad.

Es fundamental comprender el sistema y su entorno operacional para lograr un alto rendimiento en materia de seguridad operacional. Contribuirá a ello contar con una descripción detallada del sistema y sus interfaces. Se pueden descubrir peligros durante el ciclo de vida operacional a partir de fuentes internas y externas. Deberán revisarse continuamente las evaluaciones y mitigaciones de riesgos de seguridad operacional para asegurar que permanecen vigentes.

Identificación de peligros

La identificación de peligros es la primera etapa del proceso SRM. El proveedor de servicios debe desarrollar y mantener un proceso formal para identificar peligros que puedan tener consecuencias en la seguridad operacional de la aviación en todos los sectores de operación y actividades. Esto comprende equipo, instalaciones y sistemas. La identificación y el control de los peligros relacionados con la seguridad operacional de la aviación son beneficiosos para la seguridad de la operación de que se trate. También es importante considerar los peligros que puedan existir como resultado de las interfaces del SMS con organizaciones externas.

Fuentes para la identificación de peligros

Existen varias fuentes para la identificación de peligros, tanto internas como externas a la organización. Entre algunas fuentes internas figuran:

a) Observación normal de las operaciones; se aplican técnicas de observación para el seguimiento de las operaciones y actividades cotidianas como las auditorías de la seguridad de las operaciones en línea (LOSA).

b) Sistemas automáticos de observación; se utilizan sistemas automáticos de registro para observar parámetros que puedan analizarse, como el análisis de datos de vuelo (FDM).

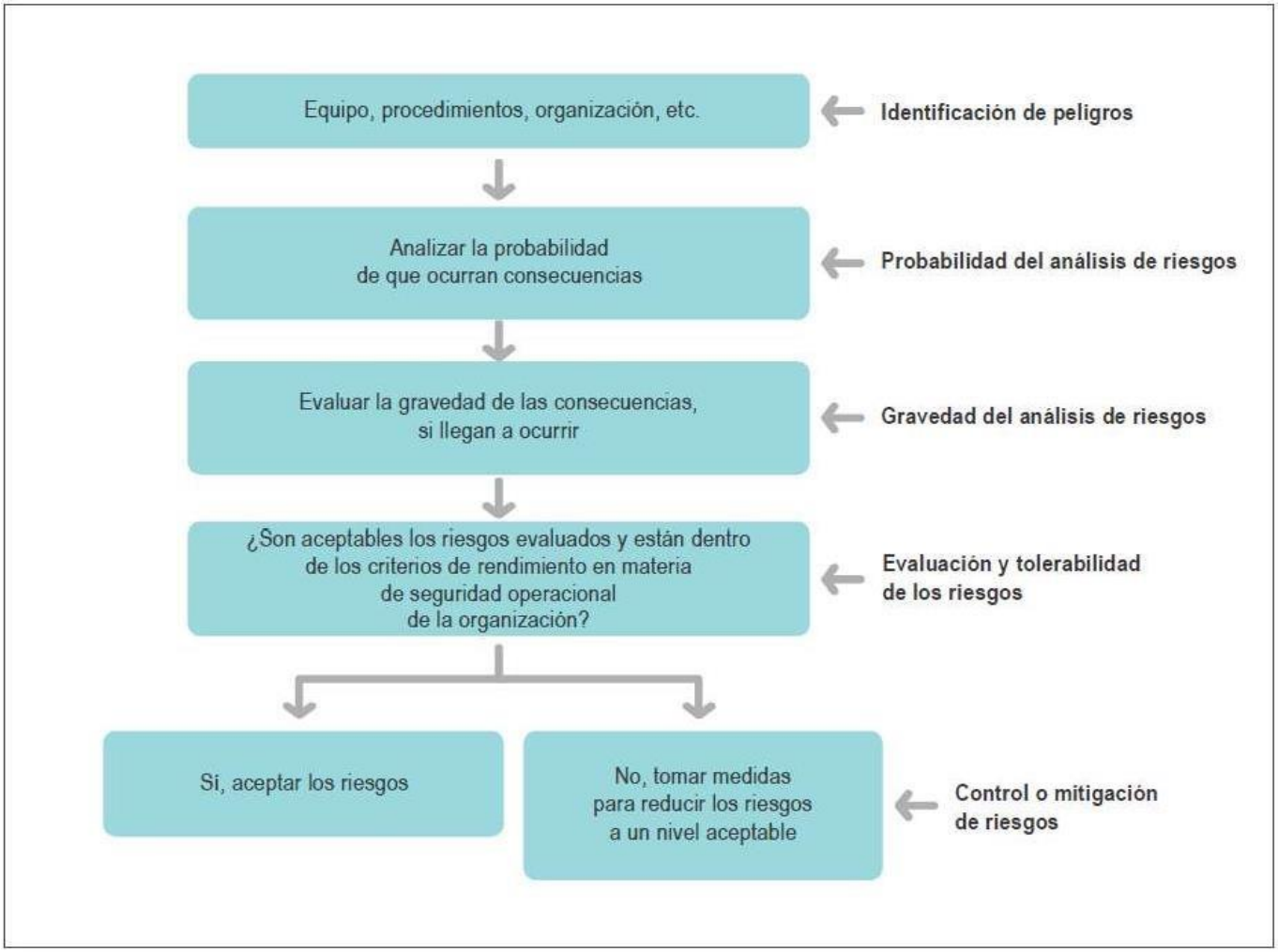


Figura 9-1 Proceso de identificación de peligros y gestión de riesgos

c) Sistemas de notificación voluntaria y obligatoria de seguridad operacional; esto brinda a todos, incluyendo el personal de organizaciones externas, oportunidades para notificar a la organización peligros y otros problemas de seguridad operacional.

d) Auditorías; pueden utilizarse para identificar peligros en la tarea o proceso que se está auditando. Estos también deberían coordinarse con los cambios que hubiere en la organización para identificar peligros relacionados con la implementación de dichos cambios.

e) Comentarios procedentes de la instrucción; una instrucción interactiva (en ambos sentidos) puede facilitar la identificación de nuevos peligros por parte de los participantes.

f) Investigaciones de la seguridad operacional del proveedor de servicios; peligros identificados en investigaciones internas de la seguridad operacional y notificaciones de seguimiento sobre accidentes/incidentes.

.

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

a) Informes de accidentes de aviación; informes de accidentes que pueden estar relacionados con accidentes en el mismo Estado o con un tipo similar de aeronave, región o entorno operacional.

b) Sistemas estatales de notificación obligatoria y voluntaria de seguridad operacional; algunos Estados proporcionan resúmenes de las notificaciones de seguridad operacional recibidas de los proveedores de servicios.

c) Auditorías estatales de vigilancia y auditorías de terceras partes; las auditorías externas pueden a veces estar en condiciones de identificar peligros que pueden haberse documentado como no identificados o captados en forma menos evidente dentro de una constatación de auditoría.

d) Asociaciones comerciales y sistemas de intercambio de información; muchas asociaciones comerciales y grupos industriales pueden compartir datos que pueden incluir peligros identificados.

Apéndice 4

Indicadores y metas de rendimiento en materia de seguridad operacional (SPI)

Indicadores cualitativos y cuantitativos

Los SPI se utilizan para ayudar a la administración a saber si es probable o no que la organización logre su objetivo de seguridad operacional; pueden ser cualitativos o cuantitativos. Los indicadores cuantitativos se refieren a la medición por cantidades, más que por calidades, mientras que los indicadores cualitativos son descriptivos y miden por calidad. Los indicadores cuantitativos son preferibles a los cualitativos porque se los puede contar y comparar más fácilmente. La elección del indicador depende de la disponibilidad de datos confiables que se puedan medir cuantitativamente. Importa plantearse si la evidencia necesaria debe estar en forma de datos comparables y generalizables (cuantitativos) o en forma de imágenes descriptivas de la situación de seguridad operacional (cualitativa). Cada opción, cualitativa o cuantitativa, entraña diferentes tipos de SPI que pueden lograrse de mejor manera mediante un proceso reflectivo de selección de SPI. Una combinación de enfoques resulta útil en muchas situaciones y puede resolver muchos de los problemas que pueden surgir de la adopción de un enfoque único. Un ejemplo de indicador cualitativo para un Estado podría ser el grado de madurez de los SMS de sus proveedores de servicios en un sector particular, o la evaluación de la cultura de seguridad operacional para un proveedor de servicios.

Los indicadores cuantitativos pueden expresarse como un número (x incursiones) o como una tasa (x incursiones por n movimientos). En algunos casos, una expresión numérica será suficiente. No obstante, el solo uso de números puede crear una impresión distorsionada de la situación real de la seguridad operacional si el nivel de actividad fluctúa. Por ejemplo, si el control del tránsito aéreo registra tres fallas de altitud en julio y seis en agosto, puede haber una gran preocupación por el deterioro significativo del rendimiento en materia de seguridad operacional. Pero agosto puede haber tenido el doble de movimientos que julio, lo que significa que el incumplimiento de la altitud por movimiento, o sea la tasa, ha disminuido y no aumentado. Esto puede o no cambiar el nivel de escrutinio, pero provee otra información valiosa que puede ser vital para la toma de decisiones de seguridad operacional basadas en datos.

Por este motivo, cuando corresponda, los SPI deberían reflejarse en términos de una tasa relativa para medir el nivel de rendimiento, independientemente del nivel de actividad. Esto proporciona una medida del rendimiento normalizada, es decir, si la actividad aumenta o disminuye. En otro ejemplo, un SPI podría medir el número de incursiones en las pistas. Pero si hubo menos salidas en el periodo considerado, el resultado podía ser engañoso. Una medida más precisa y valiosa del rendimiento sería la cantidad de incursiones en las pistas en relación con el número de movimientos, p. ej., x incursiones por 1000 movimientos.

Indicadores de resultados (lagging en inglés) y avanzados (leading en inglés)

Las dos categorías más comunes utilizados por los Estados y proveedores de servicios para clasificar sus SPI son los indicadores de resultados y los indicadores avanzados. Los SPI de resultados miden sucesos que ya han ocurrido. También se les conoce como “SPI basados en resultados” y normalmente (pero no siempre) son los resultados negativos que la organización intenta evitar. Los indicadores avanzados miden procesos e insumos que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como “SPI de actividad o proceso”, ya que observan y miden las condiciones que tienen el potencial de convertirse en un resultado específico, o contribuir a éste.

Los SPI de resultados ayudan a la organización a comprender lo que ha sucedido en el pasado y son útiles para determinar tendencias a largo plazo. Se pueden utilizar como indicadores de alto nivel o como una indicación de tipos específicos de sucesos o ubicaciones, como “tipos de accidentes por tipo de aeronave” o “tipos de incidentes específicos por región”. Debido a que los indicadores de resultados miden los resultados de seguridad operacional, pueden medir la efectividad de las medidas de mitigación de la seguridad operacional. También resultan eficaces para validar el rendimiento de seguridad operacional general del sistema. Por ejemplo, la vigilancia del “número de colisiones en rampa por número de movimientos entre vehículos después de un rediseño de las marcas de la rampa” se obtiene una medida de la eficacia de las nuevas marcas (suponiendo que nada más haya cambiado). La reducción en las colisiones valida una mejora en el rendimiento en materia de seguridad operacional general del sistema de rampa, que puede atribuirse al cambio en cuestión.

Las tendencias en los SPI de resultados pueden analizarse para determinar las condiciones existentes en el sistema que deberían abordarse. Utilizando el ejemplo anterior, una tendencia creciente en el número de colisiones de rampa por cantidad de movimientos pudo haber sido lo que llevo a la identificación de marcas de rampa por debajo de la norma como una mitigación.

Los SPI de resultados se dividen en dos tipos:

a) *Baja probabilidad/alta gravedad*: resultados tales como accidentes o incidentes graves. La baja frecuencia de los resultados de alta gravedad significa que la agregación de datos (a nivel de segmento industrial o nivel regional) puede dar como resultado un análisis más significativo. Un ejemplo de este tipo de SPI de resultados serían los daños a los aviones y al motor debidos a choques con aves.

b) *Alta probabilidad/baja gravedad*: resultados que no se manifestaron necesariamente en un accidente o incidente grave. A veces también se los denomina indicadores de sucesos precursores. Los SPI para resultados de alta probabilidad/baja gravedad se utiliza principalmente para vigilar problemas de seguridad específicos y medir la eficacia de las mitigaciones de riesgos de seguridad existentes. Un ejemplo de este tipo de SPI precursor sería “detecciones de aves en el radar”, que indica el nivel de actividad de las aves en lugar de la cantidad real de choques con las mismas.

Las medidas de seguridad operacional de la aviación han estado históricamente sesgadas hacia los SPI que reflejan resultados de “baja probabilidad/alta gravedad”. Esto es comprensible ya que los accidentes e incidentes graves son eventos de alto perfil y son fáciles de contar. Sin embargo, desde una perspectiva de gestión de rendimiento en materia de la seguridad operacional, existen inconvenientes en una dependencia excesiva de accidentes e incidentes graves como un indicador fiable del rendimiento en materia de seguridad operacional.

Por ejemplo, los accidentes e incidentes graves son poco frecuentes (puede haber un solo accidente en un año, o ninguno) lo que hace difícil la realización de análisis estadísticos para identificar tendencias. Esto no indica necesariamente que el sistema es seguro. Una consecuencia de confiar en este tipo de datos es un falso sentido de confianza potencial en que el rendimiento en materia de seguridad operacional de una organización o sistema es eficaz, cuando de hecho puede estar peligrosamente cerca de un accidente.

Los indicadores avanzados son medidas que se centran en los procesos y aportes que se implementan para mejorar o mantener la seguridad operacional. Estos también se conocen como “SPI de actividad o proceso” dado que vigilan y miden las condiciones que tienen el potencial de convertirse en un resultado específico o contribuir al mismo.

Los ejemplos de SPI avanzados que impulsan al desarrollo de capacidades organizativas para la gestión proactivo del rendimiento en materia de seguridad operacional comprenden cosas tales como “porcentaje del personal que ha completado con éxito la instrucción de seguridad operacional a tiempo” o “la frecuencia de las actividades de ahuyentamiento de aves”.

Los SPI avanzados también pueden informar a la organización sobre cómo su operación se enfrenta al cambio, incluyendo los cambios en su entorno operacional. La atención se centrará en anticipar puntos débiles y vulnerabilidades como resultado del cambio o la supervisión del rendimiento después de un cambio. Un ejemplo de SPI para vigilar un cambio en las operaciones sería “el porcentaje de sitios que han implementado el procedimiento X”.

Para una indicación más precisa y útil del rendimiento en materia de la seguridad operacional, los SPI de resultados, que miden tanto eventos de “baja probabilidad/alta gravedad” como eventos de “alta probabilidad/baja gravedad”, deben combinarse con los SPI avanzados. En la Figura 5-1 se ilustra el concepto de indicadores avanzados y de resultados que proporciona una imagen más completa y realista del rendimiento de la organización en materia de seguridad operacional.

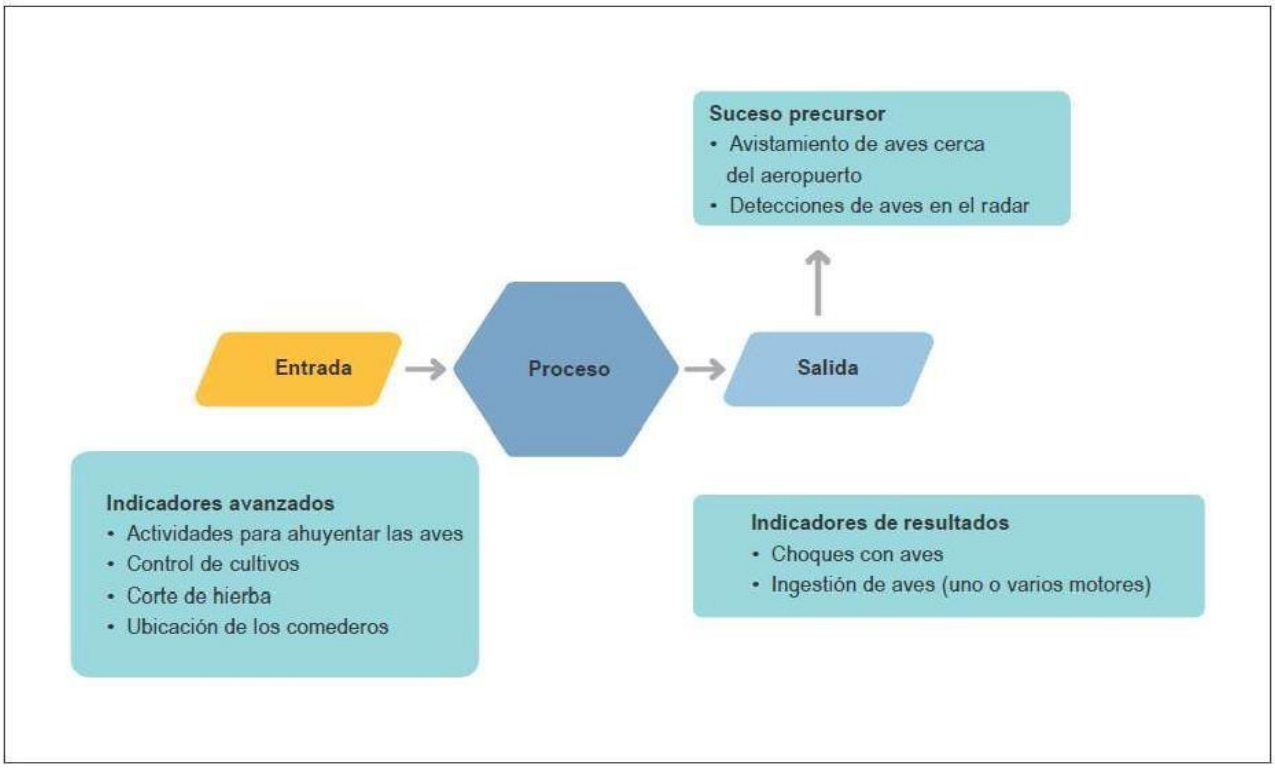


Figura 5-1 Fases del concepto de indicador avanzado y de indicador de resultados

Selección y definición de los SPI

Los SPI son los parámetros que le proporcionan a la organización una visión de su desempeño de seguridad operacional: dónde ha estado, dónde está ahora y hacia dónde se dirige, en relación con la seguridad operacional. Esta imagen actúa como una base sólida y defendible sobre la cual se toman decisiones de seguridad operacional basadas en datos de la organización. Estas decisiones, a su vez, afectan positivamente el rendimiento en materia de seguridad operacional de la organización. Por lo tanto, la identificación de los SPI debe ser realista, pertinente y estar vinculada a los objetivos de seguridad operacional, independientemente de su carácter simple o complejo.

Es probable que la selección inicial de los SPI se limite a la observación y medición de parámetros que representan sucesos o procesos que son fáciles o convenientes de captar (datos de seguridad operacional que pueden estar fácilmente disponibles). Idealmente, los SPI deberían enfocarse en parámetros que son indicadores importantes del rendimiento en materia de seguridad operacional, en lugar de aquellos que son fáciles de alcanzar.

Los SPI deberían ser:

(a) relacionados con el objetivo de seguridad operacional que pretenden indicar;

(b) seleccionados o desarrollados en base a datos disponibles y mediciones fiables;

(c) apropiadamente específicos y cuantificables; y

(d) realistas, teniendo en cuenta las posibilidades y limitaciones de la organización.

Normalmente, se requiere una combinación de SPI para proporcionar una indicación clara del rendimiento en materia de seguridad operacional. Debería haber un vínculo claro entre los SPI de resultados y los avanzados. Lo ideal sería definir los SPI de resultados antes de determinar los SPI avanzados. La definición de un SPI precursor vinculado a un suceso o condición más grave (SPI de resultados) asegura que existe una clara correlación entre ambos. Todos los SPI, tanto de resultados como avanzados, son igualmente válidos y valiosos. En la Figura 5-2 se ilustra un ejemplo de estos enlaces.

Es importante seleccionar los SPI que se relacionan con los objetivos de seguridad operacional de la organización. Tener SPI que estén bien definidos y alineados facilitará la identificación de las metas de rendimiento en materia de seguridad operacional (SPT), lo que mostrara el progreso hacia el logro de los objetivos de seguridad operacional. Esto le permite a la organización asignar recursos con el mayor efecto de seguridad operacional al saber exactamente lo que se requiere y cuándo y cómo actuar para lograr el rendimiento en materia de seguridad operacional previsto. Por ejemplo, un Estado tiene el objetivo de seguridad operacional de “reducir el número de salidas de pista en un 50% en tres años” y un SPI bien alineado de “número de salidas de pista por millón de salidas en todos los aeródromos”.

Si el número de salidas de pista disminuye inicialmente cuando comienza la observación, pero empieza a subir nuevamente después de doce meses, el Estado podría optar por reasignar recursos fuera de un área donde, de acuerdo con los SPI, el objetivo de seguridad operacional se está logrando fácilmente y hacia la reducción de las salidas de pista para aliviar la tendencia no deseada.

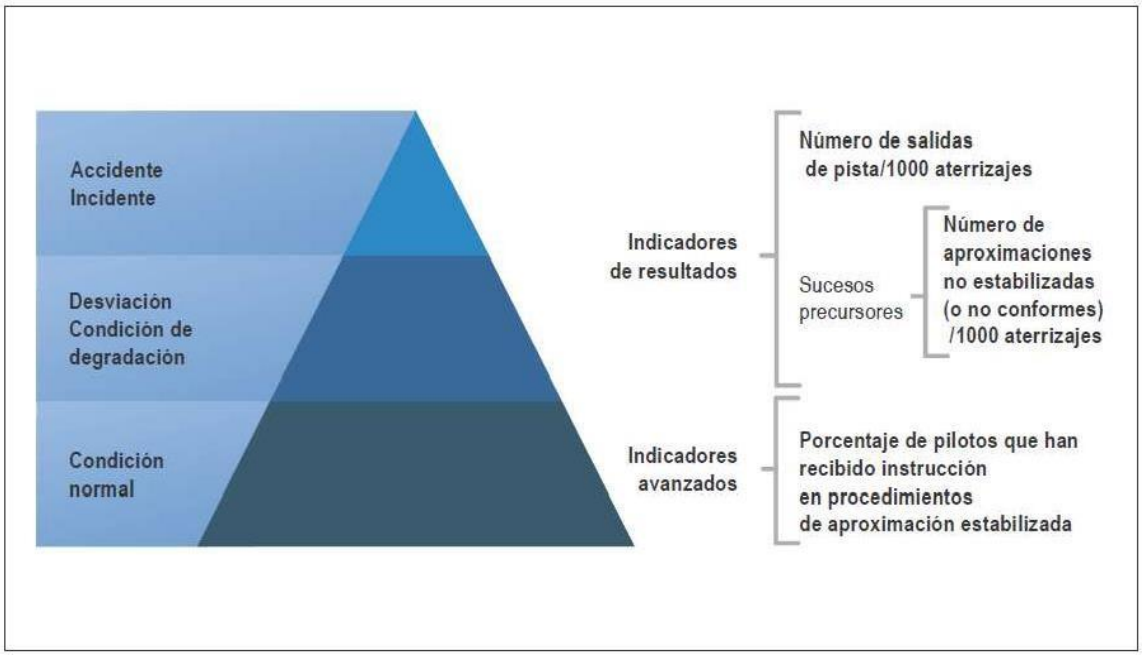


Figura 5-2 Ejemplos de enlaces entre los indicadores de resultado y los avanzados

Definición de los SPI

El contenido de cada SPI debería incluir:

(a) una descripción de lo que mide el SPI;

(b) el propósito del SPI (lo que se pretende gestionar y a quién se desea informar);

(c) las unidades de medida y cualquier requisito para su cálculo;

(d) quién es responsable de recopilar, validar, controlar, informar y actuar sobre el SPI (puede tratarse de personal de diferentes partes de la organización);

(e) dónde o cómo deben recopilarse los datos; y

(f) las frecuencias de las notificaciones, la recopilación, la observación y el análisis de los datos del SPI.

Los SPI y las notificaciones de seguridad operacional

Los cambios en las prácticas operacionales pueden llevar a notificaciones insuficientes hasta que su impacto sea totalmente aceptado por los posibles notificadores. Esto se conoce como “sesgo de la notificación”. Los cambios en las disposiciones relacionadas con la protección de la información de seguridad operacional, y las fuentes relacionadas, también podrían llevar a un exceso de notificaciones. En ambos casos, el sesgo de las notificaciones puede distorsionar la intención y la precisión de los datos utilizados para el SPI. Si se emplean juiciosamente, las notificaciones de seguridad operacional aún pueden proporcionar datos valiosos para la gestión del rendimiento en materia de seguridad operacional.

Establecimiento de metas de rendimiento en materia de seguridad operacional

Las metas de rendimiento en materia de seguridad operacional (SPT) definen los logros deseados de rendimiento en la materia a corto y mediano plazo. Actúan como “hitos” que proporcionan la confianza de que la organización está en el camino correcto para lograr sus objetivos de seguridad operacional y proporcionan una forma mensurable de verificar la eficacia de las actividades de gestión del rendimiento en materia de seguridad operacional.

La configuración de las SPT debe tener en cuenta factores como el nivel predominante del riesgo de seguridad operacional, la tolerabilidad de los riesgos de seguridad operacional y las expectativas con respecto a la seguridad operacional del sector de la aviación en particular. La configuración de las SPT debería determinarse después de considerar lo que puede lograrse realmente para el sector de aviación conexo y el rendimiento reciente de la SPI en particular, cuando se dispone de datos históricos de tendencia.

Si la combinación de los objetivos de seguridad operacional, los SPI y las SPT es de tipo SMART (específica, medible, alcanzable, realista y oportuna), permitirá a la organización demostrar de manera más efectiva su desempeño de seguridad operacional. Hay múltiples enfoques para lograr los objetivos de la gestión del rendimiento en materia de seguridad operacional, especialmente la configuración de las SPT. Un enfoque entraña el establecimiento general de objetivos de seguridad operacional de alto nivel con SPI alineados para luego identificar niveles razonables de mejoras después de haberse establecido una línea base de rendimiento de seguridad operacional. Estos niveles de mejoras pueden basarse en objetivos específicos (p. ej., porcentaje de disminución) o en el logro de una tendencia positiva. Otro enfoque que se puede utilizar cuando los objetivos de seguridad operacional son SMART es hacer que las metas de seguridad operacional actúen como hitos para lograrlos objetivos de seguridad operacional. Cualquiera de estos enfoques es válido y puede haber otros que la organización encuentre efectivos para demostrar su rendimiento en materia de seguridad operacional. Se pueden aplicar diferentes enfoques en combinación según corresponda a las circunstancias específicas.

Establecimiento de metas con objetivos de seguridad operacional de alto nivel

Las metas se establecen con el acuerdo de la administración superior respecto de los objetivos de seguridad operacional de alto nivel. Luego, la organización identifica los SPI apropiados que mostraran una mejora en el rendimiento en materia de seguridad operacional con respecto a los objetivos de seguridad operacional acordados. Los SPI se medirán utilizando fuentes de datos existentes, pero también pueden requerir la recopilación de datos adicionales. Luego, la organización comienza a reunir, analizar y presentar los SPI. Las tendencias comenzarán a surgir, proporcionando una visión general de los resultados de seguridad operacional de la organización y si se dirige hacia sus objetivos de seguridad operacional o se aparta de los mismos. En este punto, la organización puede identificar SPT razonables y alcanzables para cada SPI.

Establecimiento de metas con objetivos de seguridad SMART

Los objetivos de seguridad operacional pueden ser difíciles de comunicar y de alcanzar; al dividirlos en objetivos de seguridad operacional concretos más pequeños, el proceso de alcanzarlos es más fácil de administrar. De esta forma, las metas forman un vínculo crucial entre la estrategia y las operaciones cotidianas. Las organizaciones deberían identificar áreas claves que impulsen el desempeño de seguridad operacional y establezcan una forma de medirlas. Una vez que la organización tiene una idea de cuál es su nivel de rendimiento actual mediante el establecimiento de una línea base de rendimiento en materia de seguridad operacional, puede comenzar a configurar las SPT para proporcionar a todos en el Estado un claro sentido de lo que deberían aspirar a lograr. La organización también puede utilizar la evaluación comparativa para ayudar a establecer metas de rendimiento. Esto implica usar información de rendimiento de organizaciones similares que ya han estado midiendo su desempeño para tener una idea de cómo les está yendo a otros en la comunidad.

En la Figura 5-3 se ilustra un ejemplo de la relación entre los objetivos de seguridad operacional, los SPI y las SPT. En este ejemplo, la organización registró 100 salidas de pista por millón de movimientos en 2018. Se ha determinado que esto es demasiado y se ha establecido un objetivo para reducir el número de salidas de pista en un 50% para 2022. Para observar, medir e informar sus progresos, la organización ha elegido como SPI las “salidas de pista por millón de movimientos por año”. La organización es consciente de que el progreso será más inmediato y eficaz si se establecen metas específicas que se correspondan con el objetivo de seguridad operacional. Por lo tanto, ha establecido un objetivo de seguridad operacional que equivale a una reducción promedio de 12,5% anual durante el período de notificación (cuatro años). Como se muestra en la representación gráfica, se espera que el progreso sea mayor en los primeros años y menor en los años posteriores. Esto está representado por una proyección curva hacia su objetivo. En la Figura 5-3:

(a) el objetivo de seguridad operacional SMART es “una reducción del 50% en la tasa de salidas de pista para 2022”;

(b) el SPI seleccionado es el “número de salidas de pista por millón de movimientos por año”; y

(c) las metas de seguridad operacional relacionadas con este objetivo representan los hitos para

(d) alcanzar el objetivo de seguridad operacional SMART y corresponde a una reducción de alrededor del 12% anual hasta 2022;

(1) la SPT 1a es “inferior a 78 salidas de pistas por millón de movimientos en 2019”;

(2) la SPT 1b es “inferior a 64 salidas de pista por millón de movimientos en 2020”;

(3) la SPT 1c es “inferior a 55 salidas de pista por millón de movimientos en 2021”.

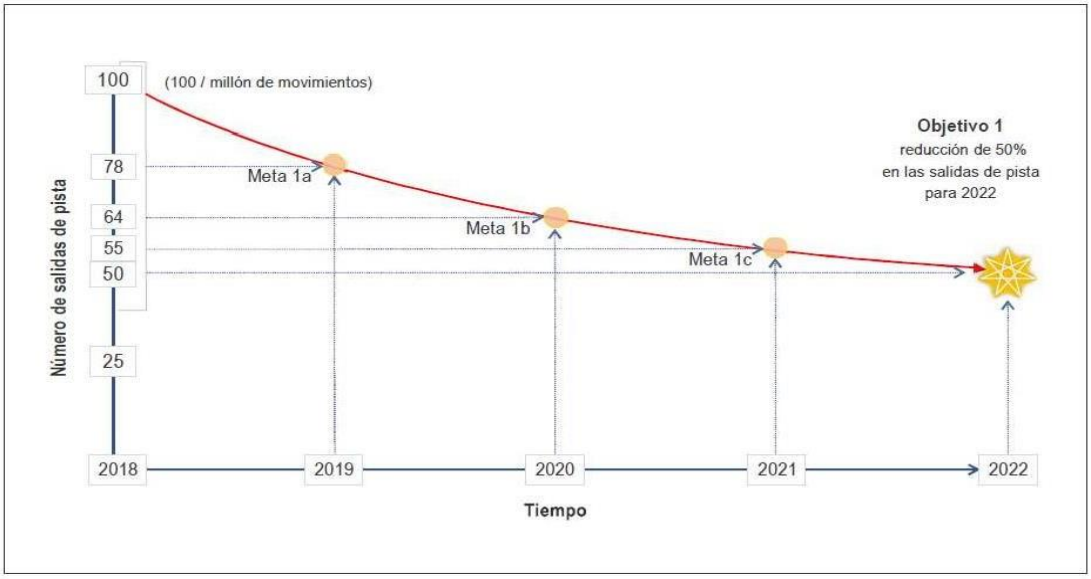


Figura 5-3 Ejemplo de SPT con objetivos de seguridad operacional SMART

Consideraciones adicionales para la selección de SPI y SPT

Al seleccionar SPI y SPT, debería también considerarse lo siguiente:

(a) *Gestión de la carga de trabajo*. La creación de una cantidad viable de SPI puede ayudar al personal a gestionar su carga de trabajo de control y notificación. Lo mismo es cierto respecto de la complejidad de los SPI o la disponibilidad de los datos necesarios. Es mejor ponerse de acuerdo sobre lo que es factible, y luego priorizar la selección de los SPI sobre esta base. Si un SPI deja de contribuir al rendimiento de seguridad operacional, o ha recibido una prioridad menor, debería considerarse la interrupción de su aplicación en favor de un indicador más útil ode mayor prioridad.

(b) *Extensión óptima de los SPI*. Una combinación de SPI que abarque las áreas de interés ayudará a obtener una visión más profunda del rendimiento general de la organización en materia de seguridad operacional y a tomar decisiones basadas en datos.

(c) *Claridad de los SPI.* Al seleccionar un SPI, debería quedar en claro lo que se está midiendo y cuan a menudo se hace. Los SPI con definiciones claras ayudan a comprenderlos resultados, evitar mal entendidos y permitir comparaciones valiosas con el tiempo.

(d) *Fomento de comportamientos deseados*. Las SPT pueden modificar comportamientos y contribuir a resultados deseados. Esto es especialmente importante si el logro de la meta se relaciona con recompensas institucionales, como la remuneración de la administración. Las SPT deberían fomentar comportamientos institucionales e individuales positivos que resulten deliberadamente en decisiones justificables y mejoras del rendimiento en materia de seguridad operacional. Al seleccionar SPI y SPT es igualmente importante tener en cuenta posibles comportamientos no deseados.

(e) *Elección de medidas valiosas*. Es fundamental seleccionar SPI útiles, y no solo aquella cuya medición sea fácil. La organización debería decidir cuáles son los parámetros de seguridad operacional más útiles, o sea los que orienten a la organización a la mejora de sus decisiones, gestión del rendimiento en materia de seguridad operacional, y logro de sus objetivos de seguridad operacional.

(f) *Logro de las SPT*. Esta es una consideración particularmente importante y está relacionada con los comportamientos de seguridad operacional deseados. El logro de las SPT convenidas no siempre indicaría mejoras del rendimiento. La organización debería distinguir entre el mero logro de las SPT y su mejoramiento real y demostrable del rendimiento. Es imperativo que la organización considere el contexto en el que se alcanzó la meta, en vez de considerarla aisladamente. El reconocimiento de la mejora general del rendimiento, más que un logro individual de SPT fomentará comportamientos institucionales deseables y el intercambio de información de seguridad operacional que está en el centro de la SRM y del aseguramiento de la seguridad operacional. Esto podría mejorar las relaciones entre el Estado y el proveedor de servicios y su disposición a compartir datos e ideas de seguridad operacional.

Advertencias para el establecimiento de SPT

No siempre es necesario o apropiado definir las SPT dado que podrían haber SPI más fáciles de controlar en cuanto a tendencias que al uso de una meta determinada. Las notificaciones de la seguridad operacional son un ejemplo de cuándo una meta podría llevar a que las personas no notificaran (si la meta es no superar un número) o notificaran asuntos triviales a efectos de satisfacerla (si la meta consiste en alcanzar un determinado número). También podrían haber SPI que se utilizaran mejor para definir bien una dirección hacia la mejora continua del rendimiento en materia de seguridad operacional (es decir reducir el número desucesos) en vez de utilizarse para definir una meta absoluta, que puede resultar difícil de determinar. En la determinación de SPT apropiadas debería también considerarse lo siguiente:

(a) Posibilidad de comportamiento indeseable; si los administradores o las organizaciones se concentran demasiado en alcanzar valores numéricos como indicadores de éxito podrían no lograr la mejora prevista del rendimiento en materia de seguridad operacional.

(b) Objetivos operacionales; concentrarse demasiado en el logro de objetivos operacionales (salidasen hora, reducción de costos generales) sin equilibrar las SPT puede llevar al “logro de metas operaciones” aunque no necesariamente a una mejora del rendimiento en materia de seguridadoperacional.

(c) Concentración en la cantidad más que en la calidad; esto puede alentar al personal o a los departamentos a alcanzar la meta, pero, al hacerlo, podría entregarse un producto o servicio debaja calidad.

(d) Limitación de innovaciones; aunque no se haya previsto, el haber alcanzado una meta puede llevar al relajamiento y a pensar que no se necesitan más mejoras, cayéndose así en complacencia.

(e) Conflicto institucional; las metas pueden crear conflictos entre departamentos y organizacionescuando discuten sobre quién recae la responsabilidad en vez de tratar de trabajar en conjunto.

Medición del rendimiento en materia de seguridad operacional

La medición correcta del rendimiento en materia de seguridad operacional involucra decidir la mejor forma de medir el logro de los objetivos en la materia. Las organizaciones deberían tomarse el tiempo de elaborar su conciencia estratégica de lo que impulsa la mejora de la seguridad operacional para alcanzar los objetivos.

Uso de SPI y SPT

Los SPI y las SPT pueden utilizarse en diferentes formas para demostrar el rendimiento en materia de seguridad operacional. Es fundamental que las organizaciones adapten, seleccionen y apliquen varias herramientas y enfoques de medición dependiendo de sus circunstancias específicas y del carácter de lo que se está midiendo. Por ejemplo, en algunos casos, las organizaciones podrían adoptar SPI que tengan SPT conexas. En otras situaciones, puede ser preferible concentrarse en el logro de una tendencia positivaen los SPI, sin valores específicos para metas. El paquete de las métricas de rendimiento seleccionadas normalmente incluirá una combinación de ambos enfoques.

Observación del rendimiento en materia de seguridad operacional

Una vez que la organización ha identificado las metas basadas en los SPI que en su opinión producirán los resultados previstos, debe cerciorarse de que las partes interesadas actúan en consecuencia mediante la asignación de claras responsabilidades para su realización. La definición de SPT para la AHAC, sector y proveedor de servicios contribuye al logro del ALoSP para el Estado mediante la asignación de un claro proceso de rendición de cuentas.

Deberían establecerse mecanismos para la observación y medición del rendimiento de la organización en materia de seguridad operacional a efectos de identificar los cambios que puedan ser necesarios si el progreso alcanzado no es el esperado y reforzar el compromiso de la organización para satisfacer sus objetivos de seguridad operacional.

Rendimiento básico en materia de seguridad operacional

La comprensión de la forma en que los planes de la organización avanzan hacia sus objetivos de seguridad operacional exige saber dónde se encuentra en relación con la misma. Una vez establecida y funcionando la estructura de rendimiento en materia de seguridad operacional de la organización (objetivos, indicadores, metas, activadores de seguridad operacional), es posible conocer su rendimiento básico en la materia a través de un período de control y observación. El rendimiento básico en materia de seguridad operacional es el desempeño de seguridad operacional al inicio del proceso de medición de dicho rendimiento, el puntode referencia a partir del cual pueda medirse el progreso. En el ejemplo de las Figuras 5-2 y 5- 3, el rendimiento básico en materia de seguridad operacional para ese objetivo determinado “100 salidas de pistas por millón de movimientos durante el año (2018)”. A partir de esta base sólida, pueden registrarse indicadores y metas precisas y significativas.

Perfeccionamiento de los SPI y los SPT

Los SPI y las SPT conexas deben revisarse para determinar si están proporcionando la información necesaria para el seguimiento de los progresos alcanzados hacia los objetivos de seguridad operacional y garantizar que las metas son realistas y pueden alcanzarse.
La gestión de rendimiento en materia de seguridad operacional es una actividad continua. Los riesgos de seguridad operacional o la disponibilidad de datos cambian con el tiempo. Los SPI iniciales pueden elaborarse utilizando recursos limitados de información de seguridad operacional. Más adelante, pueden establecerse más canales de notificación, puede disponerse de más datos de seguridad operacional y las capacidades de análisis de seguridad de la organización probablemente alcancen mayor madurez. Puede resultar apropiado para las organizaciones elaborar SPI iniciales sencillos (más amplios). A medida que acopian más datos y logran una mayor capacidad de gestión de la seguridad operacional, las organizaciones pueden considerar el perfeccionamiento del alcance de los SPI y las SPT para corresponder mejor a los objetivos de seguridad operacional deseados.

Las organizaciones pequeñas y de poca complejidad pueden optar por refinar sus SPI y SPT o seleccionar indicadores genéricos (pero específicos) que se apliquen a la mayoría de los sistemas aeronáuticos. Algunos ejemplos de indicadores genéricos serían:

(a) sucesos que incluyan daño estructural al equipo;

(b) sucesos que indiquen circunstancias en que casi haya ocurrido un accidente;

(c) sucesos en que personalde operaciones o miembros de la comunidad aeronáutica experimentaron lesiones mortales o graves;

(d) sucesos en que miembros del personal de operaciones resultaron incapacitados o no pudieron realizar sus tareas en condiciones de seguridad;

(e) proporción de notificaciones voluntarias de sucesos; y

(f) proporción de notificaciones obligatorias de sucesos.

Las organizaciones más grandes y complejas pueden optar por instituir una gama más amplia o profunda deSPI y SPT e integrar indicadores genéricos como los indicados anteriormente con otros específicos de cadaactividad. Por ejemplo, un gran aeropuerto que preste servicios a importantes líneas aéreas y esté situado bajo un espacio aéreo complejo podría considerar la combinación de algunos de los SPI genéricos con SPIde mayor alcance para representar aspectos específicos de su operación. La observación de éstos puede exigir mayores esfuerzos, pero probablemente producirá resultados superiores en materia de seguridad operacional. Existe una clara correlación entre la complejidad relativa de los SPI y SPT y la escala y complejidad de las operaciones del Estado o de los proveedores de servicios. Esta complejidad relativa debería reflejarse en el indicador y en la meta establecida. Los responsables del establecimiento de la gestión del rendimiento en materia de seguridad operacional deberían tener conciencia de esto.

El conjunto de SPI y SPT seleccionados por una organización debería revisarse periódicamente para asegurar su validez continua como indicaciones del rendimiento de la organización en materia de seguridadoperacional.

Entre las razones para continuar, suspender o modificar SPI y SPT figuran las siguientes:

(a) los SPI notifican continuamente el mismo valor (como 0% o 100%); es improbable que estos SPI proporcionen información útil para la toma de decisiones por la administración superior;

(b) SPI con comportamientos similares se consideran como duplicados;

(c) la SPT para un SPI implantada para medir la introducción de un programa o mejoras previstas se ha alcanzado;

(d) otra preocupación de seguridad operacional pasa a tener mayor prioridad en cuanto a control y medición;

(e) obtener una mejor comprensión de una preocupación determinada de seguridad operacional afinando las características específicas de un SPI (es decir reducir el “ruido” para aclarar la “señal”); y

(f) los objetivos de seguridad operacional han cambiado y, en consecuencia, los SPI deben actualizarse para seguir siendo pertinentes.

Actividades de seguridad operacional

Corresponde presentar una breve perspectiva de las funciones de activadores para ayudar su posible función en el contexto de la gestión del rendimiento en materia de seguridad operacional por parte de una organización.

Un elemento activador es un nivel establecido o valor de criterio que activa (inicia) una evaluación, decisión, ajuste o medida correctiva relacionada con el indicador en cuestión. Un método para establecer criterios de activadores fuera de límites para las SPT es el uso del principio de desviación estándar de la población (STDEVP). Este método permite obtener el valor de desviación estándar (SD) sobre la base de los datos históricos precedentes de un determinado indicador de la seguridad operacional. El valor SD más el valor promedio (media) del conjunto de datos históricos constituye el valor básico de activación para el siguiente período de control. El principio de SD (función estadística básica) establece los criterios de nivel de los activadores sobre la base del desempeño histórico real del indicador determinado (conjunto de datos), incluyendo su carácter volátil (fluctuaciones de los puntos de datos). Un conjunto de datos históricos más volátiles resultará normalmente en un mayor valor de nivel de activador (más generoso) para el siguiente período de control. Los activadores proporcionan advertencias tempranas que permiten que los encargados de tomar decisiones de seguridad operacional lo hagan sobre la base de una mayor información mejorando, así, el rendimiento en materia de seguridad operacional. En la Figura 5-4 se presenta un ejemplo de niveles de activadores basados en desviaciones estándar (SD). En el ejemplo, podría ser necesario adoptar decisiones basadas en datos y medidas de mitigación de seguridad operacional cuando la tendencia va más allá de +1SD o +2SD a partir de la media del período precedente. A menudo los niveles de activadores (en este caso +1SD, +2SD o mayores que +2SD) corresponderán los niveles de la gestión de decisiones y a la urgencia de tomar medidas.

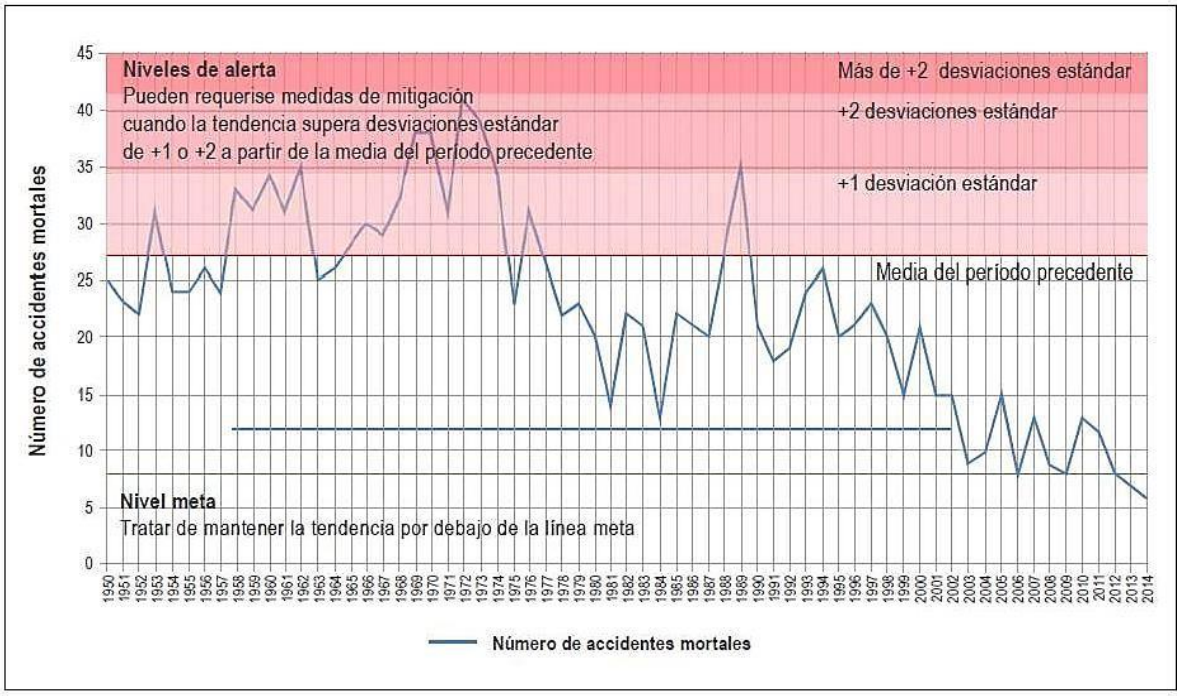


Figura 5-4 Ejemplo de representación de niveles de activadores (alertas) deseguridad operacional

Una vez definidos las SPT y los valores de activadores (si se utilizan), podrá hacerse el seguimiento de su SPI conexo para determinar sus respectivos estados de rendimiento. También podría compilarse o combinarse un resumen consolidado del resultado general del comportamiento de las SPT y activadores enel paquete total de SPI para un período de control determinado. Pueden asignarse valores cualitativos (satisfactorio/insatisfactorio) a cada logro de SPT y cada nivel de activador que no se haya traspasado. Alternativamente, pueden utilizarse valores numéricos (puntos) para obtener una medición cuantitativa del rendimiento general del paquete de SPI.

Cabe señalar que los valores de activación sirven para activar (iniciar) una evaluación, decisión, ajuste o medida correctiva relativa a un indicador particular. La activación de un SPI no es necesariamentecatastrófica ni indicativa de falla. Constituye meramente un signo de que la actividad ha ido más allá del límite predeterminado. El activador tiene por objeto llamar la atención de quienes adoptan decisiones para que ahora puedan tomar, o no, medidas correctivas dependiendo de las circunstancias.

Advertencia sobre los indicadores

La identificación de niveles fiables para activadores presenta retos. Los activadores y sus niveles conexos funcionan mejor cuando se dispone de amplios datos de seguridad operacional y de capacidades de gestión de estos. Esto puede imponer una carga de trabajo adicional en la organización. La noción de activador se diseñó para la SRM de sistemas puramente técnicos (p. ej., vigilancia de los motores de aeronave). En este caso, grandes volúmenes de datos cuantitativos apoyan la identificación de activadores precisos y niveles de activación. La noción de activadores es menos pertinente a la SRM de sistemas socio técnicos. Los sistemas socio técnicos son sistemas en los que las personas interactúan activamente con procesos y tecnologías para alcanzar los objetivos de prestación de servicios o de producción del sistema. Tanto los SSP como SMS son sistemas socio técnicos. La utilización de activadores menos fiables y significativos en los sistemas socio técnicos se debe a las limitaciones de las medidas fiables cuando hay seres humanos involucrados.

Por lo tanto, se necesita un enfoque más flexible para que los activadores tengan sentido. No se requiere que los proveedores de servicios definan niveles de activadores para cada SPI. No obstante, hay beneficios para aquellas organizaciones en que los datos para un SPI son muy específicos, hay datos suficientes y estos son suficientemente fiables.

La Figura 5-5 es una ampliación del ejemplo anterior, “reducción del 50% en las salidas de pista para 2022”. En este escenario, se trata ahora del año 2020. La organización ha estado acopiando datos de seguridad operacional (SPI – “ninguna salida de pista/millón de movimientos/año”) y ha trabajado con las partes interesadas para reducir esos casos.
La SPT para 2019 (<78 salidas de pista/millón de movimientos en el año) ha sido alcanzada. No obstante, el SPI muestra que, no solo no se ha alcanzado la SPT para 2020 (<64 salidas de pista/millón de movimientos en el año), sino que el número de salidas de pista ha superado el nivel de activación en dos períodos de notificación consecutivos. Los encargados de tomar decisiones han sido alertados respecto al deterioro del rendimiento en materia de seguridad operacional y ahora pueden tomar decisiones sobre la base de los datos en cuanto a la adopción de ulteriores medidas.

Estas decisiones basadas en datos estarán dirigidas a devolver al rendimiento en materia de seguridad operacional a la zona aceptable y dirigirlo hacia el logro de su objetivo de seguridad.

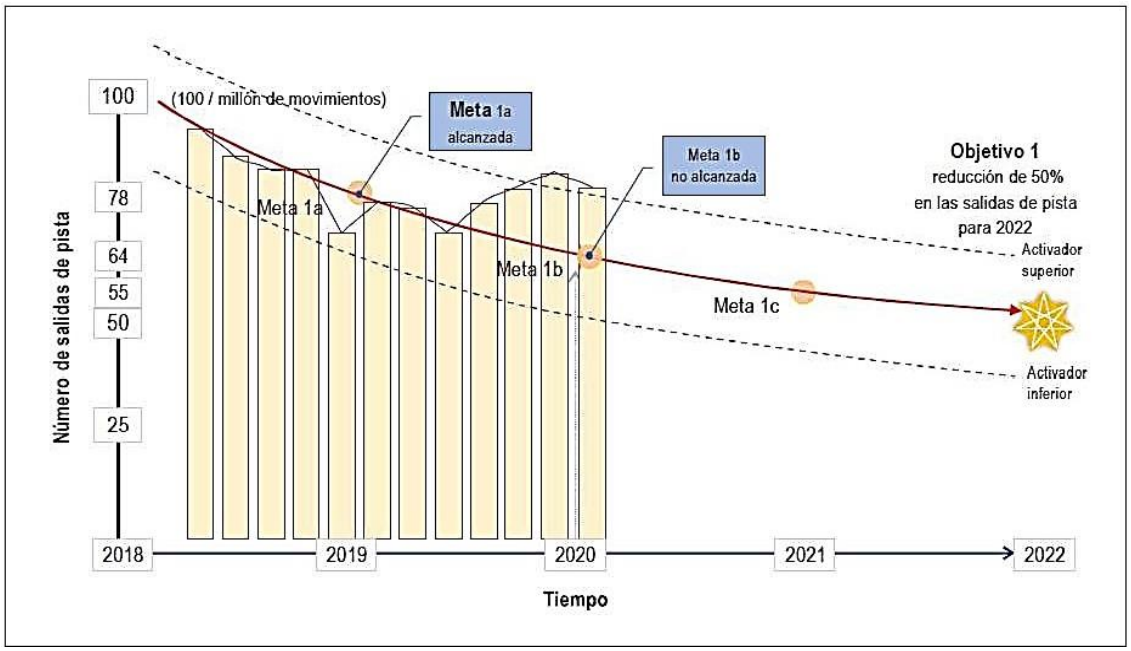


Figura 5-5 Ejemplo de establecimiento de activadores de seguridad operacional

De hecho, el resultado más importante de establecer una estructura de gestión del rendimiento en materia de seguridad operacional es la presentación de información a los encargados de tomar decisiones en la organización para que puedan hacerlo sobre la base de datos e información de seguridad operacional actuales y fiables. La finalidad debería ser siempre la adopción de decisiones con arreglo a la política de seguridad operacional y tendiente al logro de objetivos en esa materia.

En relación con la gestión del rendimiento en materia de seguridad operacional, la toma de decisiones basada en datos se dirige a adoptar decisiones eficaces bien fundamentadas sobre la base de los resultados de los SPI controlados y medidos, o de otras notificaciones y análisis de datos e información de seguridad operacional. El uso de datos de seguridad operacional válidos y pertinentes combinados con información que proporcione contexto apoya la toma de decisiones en la organización acorde con sus objetivos y metas de seguridad operacional.

La información de contexto también puede comprender otras prioridades de partes interesadas, deficiencias conocidas en los datos y otros datos complementarios para evaluarlos aspectos a favor y en contra,las oportunidades, limitaciones y riesgos relacionados con la decisión. El contar con información rápidamente disponible y de fácil interpretación contribuye a mitigar sesgos, influencias y errores humanos en el proceso de toma de decisiones.

INTENCIONALMENTE EN BLANCO

APÉNDICE 5

GESTIÓN ESTATAL DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

Los Estados deben identificar posibles riesgos de seguridad operacional en el sistema aeronáutico. El Estado debe aumentar sus métodos tradicionales de analizar las causas de un accidente o incidente mediante procesos proactivos para alcanzar dicho objetivo. Los procesos proactivos permiten al Estado identificar y abordar elementos precursores y contribuyentes de accidentes, así como gestionar estratégicamente los recursos de seguridad operacional para maximizar las mejoras en la materia. Los Estados deberían:

a) exigir que sus proveedores de servicios implementen SMS para gestionar y mejorar la seguridad de sus actividades relacionadas con la aviación;

b) establecer medios para determinar si la SRM de los proveedores de servicios es aceptable; y c) examinar el SMS del proveedor de servicios y asegurar que permanece siendo eficaz.

El componente estatal de la SRM comprende la implementación de SMS por los proveedores de servicios, incluyendo procesos de identificación de peligros y gestión de riesgos de seguridad operacional conexos.

Los Estados deben aplicar también los principios de la SRM a sus propias actividades. Estas comprenden la elaboración de reglamentos y la priorización de actividades de vigilancia basadas en riesgos evaluados.

Con frecuencia, los proveedores de servicios y reglamentadores no prestan la debida atención a los riesgos de seguridad operacional inducidos a través de interfaces con otras entidades. La interfaz entre el SSP y los SMS puede plantear un reto particular para los Estados y proveedores de servicios. El Estado debería considerar destacar la importancia de la gestión de riesgos de la interfaz SMS a través de sus reglamentos y orientación de apoyo. Entre los ejemplos de riesgos de interfaz figuran los siguientes:

a) Dependencia — la organización A depende de la organización B para proporcionar bienes o servicios. La organización B no tiene en claro las expectativas y la dependencia de la organización A y no proporciona dichos elementos.

b) Control — las organizaciones en interfaz a menudo tienen un control mínimo de la calidad o eficacia de las organizaciones involucradas.

En estos dos ejemplos, la gestión de los riesgos de interfaz puede poner de relieve el riesgo, aclarar las expectativas mutuas y mitigar las consecuencias no deseadas mediante verificaciones mutuamente convenidas de los límites pertinentes.

Obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones

En el Doc. 9734, Parte A, figura orientación sobre obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones (CE-6).

Las obligaciones de otorgamiento de licencias, certificaciones, autorizaciones y aprobaciones son componentes importantes de la estrategia estatal de control de riesgo de seguridad operacional. Estas brindan al Estado garantías de que los proveedores de servicios y otras organizaciones representativas de la industria pertinentes han alcanzado las normas requeridas para operar dentro del sistema aeronáutico en condiciones de seguridad. Algunos Estados han establecido reglamentos de explotación comunes para facilitar el reconocimiento o aceptación de licencias, certificados, autorizaciones y aprobaciones expedidas por otros Estados. Dichos arreglos no eximen al Estado del cumplimiento de sus obligaciones en el marco del Convenio de Chicago.

Obligaciones del sistema de gestión de la seguridad operacional

Requisitos normativos del SMS

En el Anexo 19 se especifica el marco para la implantación y mantenimiento de un SMS. Independientemente de la envergadura y complejidad del proveedor de servicios, se aplican todos los elementos de dicho marco para el SMS. La implementación debería adaptarse a la organización en cuestión y sus actividades.

El marco de la OACI para el SMS está integrado por los siguientes cuatro componentes y doce elementos:

Componentes y elementos del marco de la OACI para el SMS

COMPONENTE	*ELEMENTO*
1. Políticas y objetivos de seguridad	1.1 Compromiso de la administración
Operacional	1.2 Obligacion de rendicion de eventos sobre la seguridad operacional Y responsabilidades
	1.3 Designación del personal clave de seguridad operacional
	1.4 Coordinación de la planificación de respuestas ante emergencias
	1.5 Documentación SMS
2. Gestión de riesgos de seguridad	2.1 Identificación de peligros
Operacional	2.2 Evaluacion y Mitigacion de riesgos de seguridad operacional
3. Aseguramiento de la seguridad operacional	3.1 Observación y medición del rendimiento en materia de seguridad operacional
	3.2 Gestión del cambio
	3.3 Mejora continua del SMS
4. Promoción de la seguridad operacional	4.1 Instrucción y educación
	4.2 Comunicación de la seguridad operacional

Nota – El período de implementación indicado es una aproximación. El período de implementación real depende del alcance de las medidas necesarias para cada elemento asignado y la envergadura/complejidad de la organización.

Apéndice 6

Guía sobre el desarrollo de un manual de SMS

1. Generalidades

Esta sección 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.

Al usar el formato sugerido y los elementos del contenido en este apéndice 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 de SMS de la organización.

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 puede someterse al respaldo o aprobación de la AHAC como evidencia de la aceptación del SMS, a través del Programa Estatal de Seguridad Operacional (SSP).

Nota. — 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

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

(a) encabezado de sección;

(b) objetivo;

(c) criterios;

(d) documentos de referencia cruzada.

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

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

(a) Control de documentos;
(b) Requisitos reglamentarios del SMS;
(c) Alcance e integración del sistema de gestión de la seguridad operacional;
(d) Política de seguridad operacional;
(e) Objetivo de Seguridad Operacional;
(f) Responsabilidades de la seguridad operacional y personal clave;
(g) Notificación de seguridad operacional y medidas correctivas;
(h) Identificación de peligros y evaluaciones de riesgo;
(i) Control y medición del rendimiento en materia de seguridad operacional;
(j) Investigaciones relacionadas con la seguridad operacional y medidas correctivas;
(k) Capacitación y comunicación de seguridad operacional;
(l) Mejora continua y auditoría de SMS;
(m) Gestión de los registros de SMS;
(n) Gestión de cambio;
(o) Plan de respuesta ante emergencias/contingencias.

1. Control de documentos

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 actual de documento.

(a) Copia impresa o medio electrónico controlado y lista de distribución.

(b) La correlación entre el manual de SMS y otros manuales existentes, como el manual de control de mantenimiento (MCM) o el manual de operaciones.
(c) El proceso de revisión periódica del manual y sus formularios/documentos

relacionados para garantizar su sustentabilidad, suficiencia y eficacia constantes.

(d) El proceso de administración, aprobación y aceptación reglamentaria del manual.

Documentos de referencia cruzada

Manual de la calidad, manual de ingeniería.

2. Requisitos Reglamentarios

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

(a) 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.
(b) Donde corresponda, elaborar o explicar la importancia y las implicaciones de los reglamentos para la organización.
(c) Establecer una correlación con otros requisitos o normas relacionados con la seguridad operacional, donde corresponda.

Referencias de reglamentos/requisitos de SMS, referencias de documentos de guía de SMS.

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

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.

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

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

(b) 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.

(c) 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.
(d) Donde haya otros sistemas de control/gestión relacionados dentro de la organización, como QMS, OSHE e, identifique su integración pertinente (donde corresponda) dentro del SMS de la aviación.

4. Política de seguridad operacional

La política de seguridad operacional debería ser respaldada visiblemente por la administración superior y por el ejecutivo responsable. El "respaldo visible" se refiere a que el apoyo activo de la política de seguridad operacional por parte de la administración sea visible para el resto de la organización. Esto puede hacerse a través de cualesquiera medios de comunicación y la correspondencia de las actividades con la política de seguridad operacional.

(a) La política de seguridad operacional debe ser adecuada para la envergadura y complejidad de la organización.
(b) La política de seguridad operacional señala las intenciones de la organización, sus principios de gestión y el compromiso con la mejora continua en la seguridadoperacional de la aviación.
(c) El ejecutivo responsable aprueba y firma la política de seguridad operacional.
(d) El ejecutivo responsable y el resto de los gerentes promueven la política de seguridad operacional.
(e) La política de seguridad operacional se revisa periódicamente.
(f) El personal en todos los niveles participa en el establecimiento y mantenimiento del sistema de gestión de la seguridad operacional.
(g) La política de seguridad operacional se comunica a todos los empleados con la intención de crear conciencia de sus obligaciones de seguridad operacional individuales.

5. Objetivos de seguridad operacional

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.

(a) Se hayan establecido los objetivos de seguridad operacional.

(b) 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.

(c) Existe un proceso formal para desarrollar un conjunto coherente de objetivos de seguridad operacional.

(d) Los objetivos de seguridad operacional se difunden y distribuyen.

(e) Se han asignado recursos para lograr los objetivos.

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

6. Funciones y responsabilidades

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

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.
Se asignó un gerente (oficina) de seguridad operacional correspondiente, un comité de seguridad operacional o grupos de acción de seguridad operacional, según corresponda.
Las autoridades y responsabilidades de seguridad operacional del personal en todos los niveles de la organización están definidos y documentados.
Todo el personal comprende sus autoridades y responsabilidades en relación con los procesos, las decisiones y las medidas de la gestión de seguridad operacional.
Se dispone de un diagrama de responsabilidades institucionales del SMS.

7. Notificación de seguridad operacional

Un sistema de notificación debe incluir medidas reactivas (informes de accidentes/incidentes) 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.

La organización tiene un procedimiento que proporciona la captura de sucesos internos, como accidentes, incidentes y otros sucesos pertinentes para el SMS.
Se debe hacer una distinción entre los informes obligatorios (accidentes, incidentes graves, defectos importantes) que se deben notificar a la AHAC y otros informes de sucesos de rutina, que permanecen dentro de la organización.
También existe un sistema de notificación de peligros/sucesos voluntaria y confidencial, que incorpora la protección de identidad/datos adecuada, según corresponda.
Los procesos de notificación respectivos son simples, accesibles y proporcionales a la envergadura de la organización.
Los informes de alto impacto y las recomendaciones asociadas se abordan y revisan según el nivel de gestión correspondiente.
Los informes se recopilan en una base de datos adecuada para facilitar el análisis necesario.

8. Identificación de peligros y evaluación de riesgos

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.

(a) Los peligros identificados se evalúan, priorizan y procesan para la evaluación de riesgos, según corresponda.
(b) Existe un proceso estructurado para la evaluación de riesgos que implica la evaluación de gravedad, probabilidad, tolerabilidad y controles preventivos.
(c) 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.
(d) El proceso de evaluación de riesgos usa hojas de cálculo, formularios o software correspondientes a la complejidad de la organización y las operaciones involucradas.
(e) El nivel de gestión correspondiente aprueba las evaluaciones de seguridad operacional completadas.
(f) Existe un proceso para evaluar la eficacia de las medidas correctivas, preventivas y de recuperación que se han desarrollado.
(g) Existe un proceso para la revisión periódica de las evaluaciones de seguridad operacional completadas y la documentación de sus resultados.

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

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.

(a) El proceso formal para desarrollar y mantener un conjunto de indicadores de rendimiento en materia de seguridad operacional y sus objetivos eficaces asociados.
(b) 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.
(c) El proceso de control del rendimiento de estos SPI, incluido el procedimiento demedidas correctivas, cada vez que se activen tendencias inaceptables o anormales.
(d) Cualquier otro criterio o proceso de control y medición del rendimiento en materiade seguridad operacional o de SMS complementario.

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

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.

(a) Procedimientos para garantizar que se investiguen de forma interna los accidentes e incidentes notificados.

(b) Divulgación interna de los informes de investigación completados al igual que a la AHAC, según corresponda.

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

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

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

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

(g) 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.

11. Capacitación y comunicación de seguridad operacional

Describir el tipo de SMS y otra capacitación relacionada con la seguridad operacionalque 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.

(a) Se documenta el programa de capacitación, la idoneidad y los requisitos.
(b) Existe un proceso de validación que mide la eficacia de la capacitación.
(c) La capacitación incluye capacitación inicial, recurrente y de actualización, donde corresponda.
(d) La capacitación de SMS de la organización es parte del programa de capacitación general de la organización.
(e) Se incorpora la toma de conciencia de SMS en el programa de empleo o adoctrinamiento.
(f) Los procesos/canales de comunicación de la seguridad operacional dentro de la organización.

12. Mejora continua y auditoría de SMS

Describir el proceso para la revisión y mejora continuas del SMS.

(a) El proceso para una auditoría/revisiones internas regulares del SMS de la organización para garantizar su continua sustentabilidad, suficiencia y eficacia.
(b) 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.

13. Gestión de los registros de SMS

Describir el método de almacenamiento de todos los registros y documentos relacionados con SMS.

(a) 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.
(b) 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.
(c) 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.

14. Gestión de cambio

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.

(a) Procedimientos para garantizar que los cambios institucionales y operacionales sustanciales consideran cualquier impacto que puedan tener en los riesgos existentes de la seguridad operacional.
(b) 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.
(c) Procedimientos para la revisión de evaluaciones de seguridad operacional existentes cada vez que se apliquen cambios al proceso o equipo asociado.

15. Plan de respuesta ante emergencias/contingencia

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.

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

(b) Existe un proceso de notificación que incluye una lista de llamadas de emergencia y un proceso de movilización interno.

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

(d) La organización tiene procedimientos para las operaciones del modo de emergencia, donde corresponda.

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

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

(g) Existen responsabilidades de investigación de accidentes definidas dentro de la organización.

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

(i) Existe una capacitación de preparación y respuesta ante emergencias para el personal afectado.

(j) 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.

(k) Existe un procedimiento para registrar las actividades durante una respuesta ante emergencias.

INTENCIONALMENTE EN BLANCO

Apéndice 7

Matrices gestión de riesgo seguridad operacional

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

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

b) ¿Qué otros equipos o componentes del mismo tipo presentan problemas similares?

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

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

Tener en cuenta los posibles factores subyacentes a estas preguntas contribuirá a evaluar la probabilidad de las consecuencias del peligro en cualquier escenario previsible.

Un suceso se considera previsible si cualquier persona razonable podría haber esperado que sucediera dicho tipo de suceso en las mismas circunstancias. Es imposible identificar todos los peligros concebibles o teóricamente probables. Por lo tanto, se requiere un buen juicio para determinar un nivel de detalle apropiado en la identificación de los peligros. Los proveedores de servicios deben actuar con la debida diligencia al identificar peligros importantes y razonablemente previsibles en relación con su producto o servicio.

Nota. — Con respecto al diseño de productos, se tiene la intención de que el término "previsible "corresponda a su uso en los reglamentos, políticas y orientaciones sobre aeronavegabilidad.

La Tabla 1 presenta una clasificación típica de la probabilidad de riesgos de seguridad operacional. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un evento o condición inseguros, la descripción de cada categoría y una asignación de valor a cada una. Este ejemplo utiliza términos cualitativos; también pueden definirse términos cuantitativos a efectos de una evaluación más precisa. Esto dependerá de la disponibilidad de datos de seguridad operacional apropiados y del grado de desarrollo de la organización y la operación.

Tabla 1 – Tabla de probabilidad de riesgo de seguridad operacional

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 que haya ocurrido)	2
Sumamente improbable	Es casi inconcebible que el suceso ocurra	1

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

Gravedad del riesgo de seguridad operacional

Una vez completada la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional teniendo en cuenta las posibles consecuencias relacionadas con el peligro. La gravedad del riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La clasificación de la gravedad debe tener en cuenta:

a) muertes o lesiones graves que podrían ocurrir como resultado de:

1) encontrarse en la aeronave;

2) tener contacto directo con cualquier parte de la aeronave incluyendo las que se hayan desprendido de la misma; o

3) exposición directa al chorro de los reactores; y daños:

1) daños o fallas estructurales sufridos por la aeronave que:

i) afecten adversamente la resistencia estructural, performance o características de vuelo de la aeronave;

ii) requerirían normalmente importantes reparaciones o sustituciones del componente afectado;

2) daños sufridos por el equipo de ATS o aeródromo que:

i) afecten adversamente la gestión de la separación de aeronaves; o

ii) afecten adversamente la capacidad de aterrizaje.

La evaluación de la gravedad debe considerar todas las posibles consecuencias relacionadas con un peligro, teniendo en cuenta la peor condición previsible. En la Tabla 2 se presenta una clasificación típica de la gravedad del riesgo de seguridad operacional. Comprende cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada una de ellas. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla es solo un ejemplo.

Tabla 2. Ejemplo de gravedad del riesgo de seguridad operacional

Gravedad	*Significado*	*Valor*
Catastrófico	• Aeronave o equipo destruidos • Varias muertes	A
Peligroso	• Gran reducción de los márgenes de seguridad operacional, estrés físico o una carga de trabajo tal que ya no se pueda confiar en que el personal de operaciones realice sus tareas con precisión o por completo • Lesiones graves • Daños importantes al equipo	B
Grave	• Reducción importante de los márgenes de seguridad operacional, reducción en la capacidad del personal de operaciones para tolerar condiciones de operación adversas, como resultado de un aumento en la carga de trabajo o como resultado de condiciones que afecten su eficiencia	C

Gravedad	*Significado*	*Valor*
	• Incidente grave • Lesiones a las personas	
Leve	• Molestias • Limitaciones operacionales • Uso de procedimientos de emergencia • Incidente leve	D
Insignificante	• Pocas consecuencias	E

Tolerabilidad del riesgo de seguridad operacional

El índice de riesgo de seguridad operacional se crea mediante la combinación de resultados de las evaluaciones de probabilidad y gravedad. En el ejemplo anterior, se trata de un designador alfanumérico. Las respectivas combinaciones de gravedad/probabilidad se presentan en la matriz de evaluación de riesgos de seguridad operacional de la Tabla 3. Dicha matriz se aplica para determinar la tolerabilidad del riesgo de seguridad operacional. Considérese, por ejemplo, una situación en que la probabilidad del riesgo de seguridad operacional se ha evaluado como ocasional (4), y la gravedad del riesgo de seguridad operacional se ha evaluado como peligrosa (B), la combinación de ambas es el índice de riesgo de seguridad operacional (4B).

Tabla 3. Ejemplo de matriz de riesgos de seguridad operacional

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

Nota. — En la determinación de la tolerabilidad del riesgo de seguridad operacional, debe tener en cuenta la calidad y la fiabilidad de los datos utilizados para la identificación del peligro y la probabilidad del riesgo de seguridad operacional.

El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a la matriz de tolerabilidad del riesgo de seguridad operacional que describe — en forma narrativa — los criterios de tolerabilidad para la organización particular. La Tabla 4 es un ejemplo de tabla de tolerabilidad del riesgo de seguridad operacional. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B corresponde a la categoría de "intolerable". En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por lo tanto, la organización debe tomar medidas de control de riesgos para reducir:

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

b) la gravedad de las consecuencias relacionadas con el peligro, es decir, reducir el componente de gravedad del índice de riesgo a un nivel aceptable; o

c) tanto la gravedad como la probabilidad para que el riesgo pueda gestionarse a un nivel aceptable.

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 resultan inaceptables bajo todo punto de vista. La probabilidad o gravedad de las consecuencias de los peligros tienen tal magnitud, y sus posibles daños representan tal amenaza para la seguridad operacional, que se requiere una medida de mitigación inmediata o la cancelación de la operación.

Tabla 4. Ejemplo de tabla de tolerabilidad del riesgo de seguridad operacional

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

Evaluación de riesgos relacionados con factores humanos

La consideración de los factores humanos tiene particular importancia en la SRM puesto que las personas pueden ser tanto una fuente como una solución de los riesgos de seguridad operacional, a saber:

a. contribuyendo a un accidente o incidente mediante una actuación variable debido a limitaciones humanas;

b. previendo y adoptando medidas apropiadas para evitar una situación peligrosa: y

c. resolviendo problemas, tomando decisiones y adoptando medidas para mitigar los riesgos.

Por consiguiente, es importante involucrar a personas con adecuada experiencia en factores humanos en la identificación, evaluación y mitigación de los riesgos.

La SRM requiere que se aborden todos los aspectos de los riesgos de seguridad operacional, incluyendo los relacionados con las personas. La evaluación de los riesgos asociados con el desempeño humano es más compleja que la de los factores de riesgo relacionados con la tecnología y el entorno dado que:

a) el desempeño humano es muy variable, con una amplia gama de influencias interactuantes tanto internas como externas al individuo. Muchos de los efectos de la interacción entre estas influencias son difíciles o imposibles de predecir; y

b) las consecuencias del variable desempeño humano serán diferentes según la tarea que se realice y el contexto de la misma.

Lo señalado anteriormente complica la forma en que se determina la probabilidad y la gravedad del riesgo. Por consiguiente, la experiencia en factores humanos es muy valiosa para identificar y evaluar los riesgos de seguridad operacional. [La gestión de la fatiga aplicando procesos SMS se aborda en el *Manual para la supervisión de los enfoques de gestión de la fatiga* (Doc 9966)].

Estrategias de mitigación de riesgos de seguridad operacional

La mitigación de riesgos de seguridad operacional se conoce a menudo como control de riesgos de seguridad operacional. Los riesgos de seguridad operacional deben gestionarse a un nivel aceptable mitigándolos mediante la aplicación de adecuados controles de riesgos de seguridad operacional. Esto debe equilibrarse con respecto al tiempo, costos y dificultades de adoptar medidas para reducir o eliminar el riesgo. El nivel de riesgo de seguridad operacional puede disminuirse mediante la reducción de la gravedad de las posibles consecuencias, la probabilidad de que el suceso ocurra o la reducción de la exposición a ese riesgo de seguridad operacional. Es más sencillo y más común reducir dicha probabilidad que reducir la gravedad.

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

a) *Evitar*: Se cancela o evita la operación o actividad debido a que los riesgos de seguridad operacional superan los beneficios de continuarla, eliminado así el riesgo de seguridad operacional en su totalidad.

b) *Reducir*: Se reduce la frecuencia de la operación o actividad o se adoptan medidas para reducir la magnitud de las consecuencias del riesgo.

c) *Segregar*: Se toman medidas para aislar los efectos de las consecuencias del riesgo o se introduce capas redundantes de protección contra los riesgos.

La consideración de los factores humanos es parte integral de la identificación de mitigaciones eficaces porque se requiere que las personas apliquen la mitigación o las medidas correctivas o contribuyan a las mismas. Por ejemplo, las mitigaciones pueden incluir el uso de procesos o procedimientos. Sin aportes de las personas que los utilizarán en situaciones del "mundo real" o de individuos con experiencia en factores humanos, los procesos o procedimientos elaborados pueden no ser adecuados al propósito en cuestión y resultar en consecuencias imprevistas. Además, debe considerarse las limitaciones de la actuación humana como parte de toda mitigación de riesgos de seguridad operacional, desarrollando estrategias de captación de errores para tener en cuenta la variabilidad de dicha actuación. En última instancia, esta importante perspectiva de factores humanos tendrá como resultado mitigaciones más completas y eficaces.

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

a) *Eficacia*. El grado en que las alternativas reducen o eliminan los riesgos de seguridad operacional. La eficacia puede determinarse en términos de las defensas técnicas, de instrucción y normativas que puedan reducir o eliminar los riesgos.

b) *Costo/beneficio*. El grado en que las ventajas percibidas de la mitigación superan los costos.

c) *Practicidad*. El grado en que la mitigación puede implementarse y cuán apropiada resulta en términos de recursos tecnológicos, financieros y administrativos disponibles, así como de legislación, voluntad política, realidades operacionales, etc.

d. *Aceptabilidad*. El grado en que la alternativa resulta aceptable para las personas que se espera la apliquen.

e. *Cumplimiento*. El grado en que pueda vigilarse el cumplimiento de nuevas reglas, reglamentos o procedimientos operacionales.

f. Duración. El grado en que la mitigación pueda ser sostenible y eficaz.

g. Riesgos de seguridad operacional residuales. El grado de riesgo de seguridad operacional que permanece después de la implementación de la mitigación inicial y que pueda requerir medidas adicionales de control de riesgos.

h) *Consecuencias involuntarias*. La introducción de nuevos peligros y riesgos de seguridad operacional conexos relacionados con la implementación de una alternativa de mitigación.

i) *Tiempo*. El tiempo requerido para implantar la alternativa de mitigación de riesgo de seguridad operacional.

Las medidas correctivas deben tener en cuenta las defensas que existan y su capacidad o incapacidad de alcanzar un nivel aceptable de riesgo de seguridad operacional. Esto puede resultar en una revisión de evaluaciones de riesgos anteriores que puedan haber sido afectadas por la medida correctiva. Las mitigaciones y controles de riesgos de seguridad operacional deberán verificarse o auditarse para asegurar que son eficaces. Otra forma de observar la eficacia de las mitigaciones es aplicando los SPI.

Documentación de la gestión de riesgos de la seguridad operacional

Las actividades de gestión de riesgos de seguridad operacional deben documentarse, incluyendo toda su posición subyacente a la evaluación de la probabilidad y la gravedad, las decisiones adoptadas, y toda medida de mitigación de riesgos emprendidas. Esto puede realizarse utilizando una hoja de cálculo o una tabla. Algunas organizaciones pueden utilizar una base de datos u otro soporte lógico donde puedan almacenarse y analizarse grandes volúmenes de datos de seguridad operacional o de información sobre seguridad operacional.

El mantenimiento de un registro de peligros identificados minimiza la probabilidad de que la organización pierda de vista sus peligros conocidos. Cuando se identifican nuevos peligros, pueden compararse con los peligros conocidos que figuran en el registro para ver si ya han sido registrados y qué medidas se adoptaron para mitigarlos. Los registros de peligros se presentan normalmente en forma de tablas y típicamente incluyen lo siguiente: el peligro, posibles consecuencias, evaluación de riesgos conexos, fecha de identificación, categoría del peligro, breve descripción, cuándo y dónde se aplica, quién o quiénes lo han identificado y qué medidas se adoptaron para mitigar los riesgos.

Las herramientas y procesos de toma de decisiones sobre riesgos de seguridad operacional pueden utilizarse para mejorar la repetición y justificación de las decisiones tomadas por los encargados de adoptar decisiones de seguridad operacional en la organización. En la Figura 2-6 se proporciona un ejemplo de ayuda para tomar decisiones sobre riesgos de seguridad operacional.

Análisis de costo-beneficios

El análisis de costo-beneficios o rentabilidad se realiza normalmente durante las actividades de mitigación de riesgos de seguridad operacional. Se asocia comúnmente con la gestión empresarial, como una evaluación de impactos normativos o procesos de gestión de proyectos. No obstante, puede que haya situaciones donde una evaluación de riesgos de seguridad operacional tenga consecuencias financieras de importancia. En tales situaciones, puede justificarse un análisis de costo-beneficios o un proceso de rentabilidad complementarios para respaldar la evaluación de los riesgos de seguridad operacional. Esto asegurará que el análisis de rentabilidad o la justificación de medidas de control de riesgos recomendadas han tenido en cuenta las repercusiones financieras conexas.

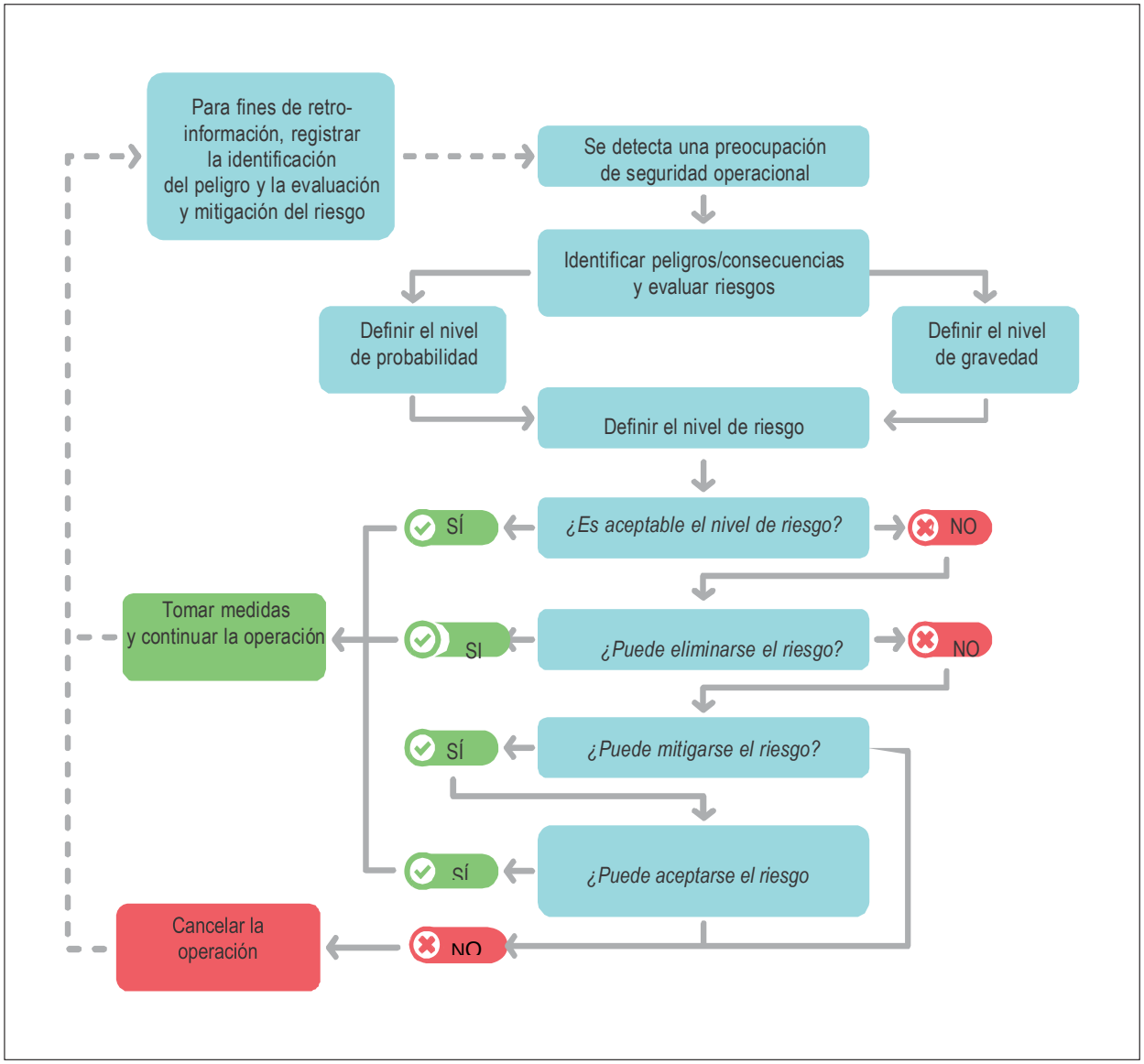


Figura 2-6. Ayuda para tomar decisiones sobre riesgos de seguridad operacional

INTENCIONALMENTE EN BLANCO

Apéndice 8

Lista de clasificación de sucesos operacionales

A continuación, se establece la lista detallada de clasificación de los sucesos obligatorios que se deben notificar al SSP por parte de los SMS de los proveedores de servicios.

A. Sucesos Operacionales

1. **Operaciones aéreas.**

1.1. **Preparación del vuelo**:

1.1.1 . Uso de datos incorrectos o introducción errónea de datos en los equipos usados para la navegación o los cálculos de las actuaciones de la aeronave que han puesto, o que podrían haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.

1.1.2 Transporte o intento de transporte de mercancías peligrosas en violación de las normas aplicables, incluidos el etiquetado, el embalaje y la manipulación incorrectos de mercancías peligrosas.

1.2. **Preparación de la aeronave:**

1.2.1 Tipo de combustible incorrecto o combustible contaminado.
1.2.2 Falta de tratamiento de deshielo o antihielo, o tratamiento incorrecto o inadecuado.

En los casos que las aeronaves sean operadas en estas condiciones

1.3. **Despegue y aterrizaje:**

1.3.1. Excursión de calle de rodaje o de la pista.
1.3.2. Incursión real o potencial en calle de rodaje o de la pista.
1.3.3. Incursión en el área de aproximación final y de despegue (FATO – Final Approach and Take-offÁrea).
1.3.4. Cualquier despegue abortado.
1.3.5. Incapacidad de lograr las actuaciones requeridas o previstas durante el despegue, lamaniobra de ida al aire, o el aterrizaje.
1.3.6. Despegue, aproximación o aterrizaje, o intento de despegue, aproximación o aterrizaje conparámetros de configuración incorrectos.
1.3.7. Golpe en la cola, palas de las hélices, punta alar o góndola de motor durante el despegue o el aterrizaje.
1.3.8. Continuación de la aproximación contra los criterios de aproximación estabilizada del operador aéreo.
1.3.9. Continuación con una aproximación por instrumentos por debajo de los mínimos publicados con referencias visuales inadecuadas.
1.3.10. Aterrizaje preventivo o forzoso.

1.3.11. Aterrizaje corto o aterrizaje largo.

1.3.12. Aterrizaje duro.

1.4. **Cualquier fase del vuelo**

1.4.1. Pérdida de control.
1.4.2. Posición anormal, superación de la actitud de cabeceo normal, ángulo de alabeo o velocidad aerodinámica inadecuados para las condiciones de vuelo.
1.4.3. Desvío del nivel de vuelo autorizado.
1.4.4. Activación de cualquier protección de la envolvente de vuelo, incluidos el aviso de entrada enpérdida, avisadores integrados en la palanca de control (stick shaker/stick pusher) y protecciones automáticas.
1.4.5. La desviación no intencionada de la trayectoria prevista o asignada del doble de la performance de navegación requerida o de 10 millas náuticas, lo que sea menor.
1.4.6. Superación de las limitaciones del manual de vuelo de la aeronave.
1.4.7. Operación con reglaje altimétrico incorrecto.
1.4.8. Sucesos relacionados con el impacto del chorro de un reactor o de una hélice que han puesto,o que podrían haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
1.4.9. Interpretación incorrecta de los automatismos o de cualquier información de la cabina de vuelofacilitada a la tripulación de vuelo que han puesto, o que podrían haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.

1.5. **Otros tipos de sucesos**

1.5.1. Suelta no intencionada de carga o de otros equipos transportados externamente.
1.5.2. Pérdida de conciencia situacional (incluidos la conciencia del entorno, los sistemas y su modo de operación, la desorientación espacial y el horizonte temporal).
1.5.3. Cualquier suceso en el que el desempeño humano haya contribuido, o podría habercontribuido, de forma directa a un accidente o a un incidente grave.

1.6. **Sucesos Técnicos**

1.6.1. Estructuras y sistemas
1.6.2. Desprendimiento de cualquier parte de la estructura de la aeronave en vuelo.
1.6.3. Pérdida de cualquier sistema.
1.6.3. Pérdida de la redundancia de cualquier sistema.
1.6.4. Fuga de un líquido que provoque un peligro de incendio o la posible contaminación peligrosa de la estructura, los sistemas o los equipos de la aeronave, o que han puesto, o que podrían haber puesto en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
1.6.5. Mal funcionamiento o defectos del sistema de combustible que hayan tenido repercusiones significativas sobre el abastecimiento y/o la distribución del combustible.
1.6.6. Mal funcionamiento o defecto de cualquier sistema de aviso que dé lugar a indicaciones engañosas para la tripulación.
1.6.7. Funcionamiento anormal de los controles de vuelo, como controles

de vuelo asimétrico o atascado [por ejemplo: dispositivos hipersustentadores (flaps/slats), aumento de la resistencia aerodinámica (spoilers), dispositivos de control de actitud (alerones, timones de profundidad y de dirección).

1.7 Sistemas de propulsión (incluidos motores, hélices y rotores) y unidades de potencia auxiliar (APU)

1.7.1. Fallo o mal funcionamiento significativo de cualquier pieza o control de una hélice, rotor o grupo moto propulsor.

1.7.2 Daño o fallo en el rotor principal o rotor de cola, la transmisión y/o los sistemas equivalentes.

1.7.3 Apagado o parada en vuelo de cualquier motor o del APU cuando este sea requerido. Por ejemplo: operaciones de alcance extendido de las aeronaves bimotor (ETOPS), lista de equipo mínimo (MEL).

1.7.4 Superación de los límites de funcionamiento del motor, incluidos el exceso de velocidad o la incapacidad de controlar la velocidad de cualquier componente rotatorio de alta velocidad (por ejemplo: APU, arrancador neumático, sistema de refrigeración de aire, turbina de motor, hélice o rotor).

1.7.5 Fallo o mal funcionamiento de cualquier pieza de un motor, grupo moto propulsor, APU o transmisión que provoque uno o más de los sucesos siguientes:

a. no respuesta de las reversas de empuje al ser accionadas;

b. incapacidad de controlar la potencia, el empuje o las revoluciones por minuto;

c. no contención de componentes o restos.

2. Interacción con los servicios de navegación aérea (ANS) y la gestión del tránsito aéreo (ATM)

2.1. Autorización ATC insegura.
2.2. Pérdida prolongada de comunicación con el ATS (servicio de tránsito aéreo) o la dependencia ATM.
2.3. Instrucciones contradictorias de dependencias ATS diferentes que puedan dar lugar a una pérdida de separación.
2.4. Mal interpretación de una comunicación por radio que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
2.5. Desviación intencionada de una instrucción ATC que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
2.6.

3. Emergencias y otras situaciones críticas

3.1. Cualquier suceso que dé lugar a una declaración de emergencia (llamada MAYDAY o PAN).

3.2. Cualquier combustión, fusión, humos, emanaciones, arco eléctrico, sobre calentamiento,incendio o explosión.

3.3. Aire contaminado en la cabina de vuelo o en el compartimento de pasajeros que ha puesto, o quepodría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.

3.4. Falta de aplicación del procedimiento correcto para situaciones no habituales o anormales porparte de la tripulación de vuelo o de cabina para gestionar una situación de emergencia.

3.5. Uso de un procedimiento de emergencia o para situaciones anormales que afecte a las prestaciones en vuelo o de aterrizaje.

3.6. Fallo de un sistema o equipo de emergencia o rescate que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.

3.7. Presión de cabina incontrolable.

3.8. Cantidad críticamente baja de combustible o cantidad de combustible en destino inferior a la cantidad de combustible de reserva final exigida.

3.9. Cualquier uso por parte de la tripulación de su sistema de oxígeno.

3.10. Incapacitación de un miembro de la tripulación de vuelo o de cabina que tenga como consecuencia la reducción de esta por debajo del número mínimo de tripulación certificada.

3.11. Fatiga de la tripulación que repercute o pueda repercutir en su capacidad de llevar a cabo de forma segura sus funciones en vuelo.

4. Entorno exterior y meteorología

4.1. Una colisión o cuasi colisión, en tierra o en el aire, con otra aeronave, el terreno o un obstáculo(Un obstáculo puede ser un vehículo).
4.2. Avisos de resolución (RA) del sistema anticolisión de a bordo (ACAS).
4.3. Activación de un aviso de un sistema de prevención de colisiones contra el terreno, tal como el sistema de alerta de proximidad al suelo (GPWS) o el sistema de advertencia y alarma de terreno (TAWS).
4.4. Colisión con fauna, incluida la colisión con aves.
4.5. Daños provocados por objetos extraños o restos (FOD).
4.6. Encuentro inesperado con malas condiciones de la superficie de la pista.
4.7. Encuentro con turbulencias de estela.
4.8. Interferencia con la aeronave mediante armas de fuego, fuegos artificiales, cometas, luces láser de alta potencia, sistemas de aeronave pilotada a distancia, aeromodelos o por medios similares.
4.9. Impacto de rayo que haya resultado en daños a la aeronave o la pérdida o malfuncionamiento de un sistema de la aeronave.
4.10. Encuentro con granizo que haya resultado en daños a la aeronave o la pérdida o malfuncionamiento de un sistema de la aeronave.
4.11. Encuentro con turbulencia severa o cualquier encuentro que resulte en lesiones a los ocupantes o que requiera una comprobación por encuentro con turbulencia («Turbulence check») de la aeronave.
4.12. Encuentro con cizalladura o cortante de viento (windshear) o tormenta que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
4.13. Encuentro con condiciones de engelamiento que resulte en dificultades de manejo, daños a la aeronave o la pérdida o malfuncionamiento de un sistema de la aeronave.
4.14. Encuentro con cenizas volcánicas.

B. Sucesos relacionados con las condiciones técnicas, el mantenimiento y la reparación de lasaeronaves.

1. Fabricación

1.1. Los productos, componentes o equipos entregados por la organización de producción condesviaciones respecto de los datos de diseño aplicables que pudieran dar lugar a una situaciónpotencial de inseguridad identificada por el titular del certificado de tipo o de la homologación del diseño.

2. Diseño

2.2. Cualquier fallo, malfuncionamiento, defecto u otro suceso relacionado con un producto, componente o equipo que ha dado lugar o que podría dar lugar a una situación de inseguridad.

3. Mantenimiento y gestión de la aeronavegabilidad continuada

3.1. Daños estructurales graves (por ejemplo: grietas, deformación permanente, exfoliación, desunión, desgaste excesivo, o corrosión) detectados durante el mantenimiento de la aeronave o componente.
3.2. Fuga o contaminación grave de líquidos (por ejemplo: fluido hidráulico, combustible, aceite, gasolina u otros líquidos).
3.3. Fallo o mal funcionamiento de cualquier parte de un motor o grupo moto propulsora y/o transmisión que provoque uno o más de los sucesos siguientes:

a) falta de contención de componentes o restos;

b) fallo en la estructura de soporte del motor.

3.4. Daño, fallo o defecto de la hélice que pueda provocar la separación en vuelo de esta o de gran parte de esta y/o mal funcionamiento del control de la hélice.
3.5. Daño, fallo o defecto del acoplamiento de las palas de los rotores o de la caja de transmisión del rotor principal que pueda provocar la separación en vuelo del conjunto del rotor y/o malfuncionamiento del control del rotor.
3.6. Malfuncionamiento significativo de un sistema o equipo crítico de seguridad, incluido el sistema o equipo de emergencia durante la prueba de mantenimiento, o fallo en la activación de estos sistemas tras el mantenimiento.
3.7. Montaje o instalación incorrectos de componentes de la aeronave detectados durante una inspección o procedimiento de prueba no destinado a ese propósito específico.
3.8. Evaluación incorrecta de un defecto grave, o incumplimiento grave de los procedimientos de la lista de equipo mínimo (MEL) y del libro de registro técnico de la aeronave (ATL).
3.9. Daño grave del sistema de interconexión de cableado eléctrico (EWIS).
3.10. Cualquier defecto que provoque la retirada de una pieza crítica de vida límite antes de la plena terminación de la vida límite de la pieza.
3.11. El uso de productos, componentes o materiales de origen desconocido o sospechoso, o de componentes críticos no aptos para el servicio.
3.12. Datos o procedimientos de mantenimiento aplicables engañosos, incorrectos o insuficientes, incluidos los de carácter lingüístico, que puedan inducir a errores de mantenimiento significativos.
3.13. Control o aplicación incorrectos de las limitaciones de mantenimiento o del mantenimiento programado de la aeronave.
3.14. Puesta en servicio tras mantenimiento de una aeronave con una no-conformidad que ponga en peligro la seguridad del vuelo.
3.15. Daños graves causados a una aeronave durante las actividades de mantenimiento debido a un mantenimiento incorrecto o al uso de equipos de apoyo en tierra inadecuados o no aptos para el servicio que exigen intervenciones de mantenimiento adicionales.
3.16. Sucesos de combustión, fusión, humos, emanaciones, arcos eléctricos, sobre calentamiento o incendio detectados.
3.17. Cualquier suceso en el que el desempeño humano, incluida la fatiga del personal, haya contribuido de forma directa, o podría haber contribuido, a un accidente o a un incidente grave.
3.18. Un malfuncionamiento significativo, un problema de fiabilidad o recurrente de calidad de grabación que afecte a un sistema registrador de vuelo (tal como un registrador de datos de vuelo, un sistema registrador por enlace de datos o un sistema registrador de voz en cabina de vuelo) o la falta de información necesaria para garantizar la aptitud para el servicio de un sistema registrador de vuelo.

C. Sucesos relacionados con los servicios e instalaciones de navegación aérea.

1. Sucesos relacionados con las aeronaves

1.1 Una colisión o cuasi colisión, en tierra o en el aire, entre una aeronave y otra aeronave, el terreno o un obstáculo, incluido un cuasi impacto con el terreno sin pérdida de control (cuasi CFIT).

1.2 Reducción de la separación mínima establecida.

1.3 Avisos de resolución (RA) del sistema de anticolisión de abordo (ACAS).

1.4 Colisión con fauna, incluida la colisión con aves.

1.5 Excursión de calle de rodaje o de pista.

1.6 Incursión real o potencial en calle de rodaje o pista.

1.7 Incursión en área de aproximación final y despegue (FATO).

1.8 Desviación de la aeronave de la autorización dada por el control de tránsito aéreo (ATC).

1.9 Desviación de la aeronave de la normativa aplicable en materia de gestión del tránsito aéreo (ATM):

a) desviación de la aeronave de los procedimientos aplicables publicados en materia de ATM;
b) violación del espacio aéreo, incluida la penetración sin autorización de espacio aéreo;

1.10 Sucesos relacionados con la confusión de indicativos de llamada.

2. Degradación o pérdida total de servicios o funciones

2.1. Incapacidad de prestar servicios de ATM o de ejercer funciones de ATM: incapacidad de prestar servicios de tránsito aéreo o de ejercer funciones de servicios de tránsito aéreo;
2.2. incapacidad de prestar servicios de gestión del espacio aéreo o de ejercer funciones de gestión del tránsito aéreo;
2.3. incapacidad de prestar servicios de gestión de la afluencia del tránsito aéreo y de capacidad o de ejercer las funciones de gestión de la afluencia de tránsito aéreo y de capacidad.
2.4. Información incompleta o significativamente incorrecta, errónea, inadecuada o engañosa de un servicio de apoyo, incluida la relacionada con las malas condiciones de la superficie de la pista.
2.5. Fallos de los servicios de comunicación.
2.6. Fallos de los sistemas de vigilancia.
2.7. Fallo de la función o del servicio de procesamiento y distribución de datos.
2.8. Fallos en los servicios de navegación.
2.9. Fallo de seguridad física del sistema ATM que ha tenido, o que podría haber tenido, un impacto negativo directo en la prestación segura del servicio.
2.10. Sobrecarga significativa del sector o de la posición ATS que provoque el deterioro potencial de la prestación del servicio.
2.11. La recepción o interpretación incorrecta de comunicaciones importantes, incluida la debida a la falta de comprensión del idioma utilizado, cuando ello ha tenido, o podía haber tenido, un impacto negativo directo sobre la prestación segura del servicio.
2.12. Pérdida prolongada de comunicación con una aeronave o con otra dependencia ATS.

3. Otros sucesos

3.1. Declaración de emergencia (llamada «MAYDAY» o «PAN»).
3.2. Interferencia externa significativa con los servicios de navegación aérea, como, por ejemplo, las emisiones en frecuencia modulada (FM) de estaciones de radio que interfieren con el sistema de aterrizaje por instrumentos (ILS), el radiofaro omnidireccional de muy alta frecuencia (VOR) y las comunicaciones.
3.3. Interferencia con una aeronave, una dependencia ATS o una transmisión de radiocomunicación mediante, entre otras, armas de fuego, fuegos artificiales, cometas, luces láser, luces láser de alta potencia, sistemas de aeronave pilotada a distancia, aeromodelos, o medios similares.
3.4. Vaciado de combustible en vuelo (Fuel dumping).
3.5. Amenaza de bomba o secuestro.
3.6. La fatiga que repercuta, o que pueda repercutir, en la capacidad de ejercer de forma segura las funciones de navegación o tránsito aéreo
3.7. Cualquier suceso en el que el desempeño humano haya contribuido de forma directa, o podría haber contribuido, a un accidente o a un incidente grave

D. Sucesos relacionados con los aeródromos y los servicios en tierra

1. Gestión de la seguridad operacional de un aeródromo

1.1. Sucesos relacionados con aeronaves y obstáculos

1.1.1. Una colisión o cuasi colisión, en tierra, entre una aeronave y otra aeronave, el terreno o un obstáculo.
1.1.2. Colisión con fauna, incluida la colisión con aves.
1.1.3. Excursión en calle de rodaje o de pista.
1.1.4. Incursión real o potencial en calle de rodaje o pista.
1.1.5. Operación de una aeronave o vehículo haciendo caso omiso de una autorización, instrucción o restricción en el área de movimiento de un aeródromo (por ejemplo: uso de pista o calle de rodaje incorrecta o parte restringida de un aeródromo).
1.1.6. Objeto extraño en el área de movimiento que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
1.1.7. Presencia de obstáculos en el aeródromo o en las proximidades del aeródromo no indicados en el AIP (publicación de información aeronáutica) o mediante NOTAM (avisos a navegantes) y/o que no están marcados o iluminados adecuadamente.
1.1.8. Retroceso asistido (push-back), retroceso autónomo con motor (power-back), o rodajes interferidos por un vehículo, equipo o persona.
1.1.9. Pasajeros o personas no autorizadas dejados sin supervisión en la zona de estacionamiento de aeronaves.
1.1.10. Impacto del chorro de un reactor, o de la corriente de aire de un rotor principal o ráfaga de una hélice.
1.1.11. Declaración de emergencia (llamada «MAYDAY» o «PAN»).

1.2. Degradación o pérdida total de servicios o funciones

1.2.1. Pérdida o fallo de comunicación entre:

a) el aeródromo, un vehículo u otro personal de tierra y la dependencia de servicios de tránsito aéreo o la unidad del servicio de gestión de la zona de plataforma;

b) la unidad del servicio de gestión de la zona de plataforma y una aeronave, vehículo o ladependencia de servicios de tránsito aéreo.

1.2.2. Fallo, mal funcionamiento o defecto significativos de un equipo o sistema del aeródromo que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona;

1.2.3. Deficiencias significativas en la iluminación, señalización visual o carteles de aeródromo.

1.2.4. Fallo del sistema de alerta de emergencia del

aeródromo.

1.2.5. Servicios de rescate y de lucha contra incendios no disponibles conforme a los requisitos aplicables.

1.3. Otros sucesos

1.3.1. Incendio, humo o explosiones en las instalaciones y equipo del aeródromo y sus proximidades, que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
1.3.2. Sucesos relacionados con la seguridad física del aeródromo (por ejemplo: entrada ilícita, sabotaje, amenaza de bomba).
1.3.3. No comunicación de un cambio significativo en las condiciones de operación del aeródromo que ha puesto, o que podría haber puesto, en peligro la aeronave, a sus ocupantes o a cualquier otra persona.
1.3.4. Derrame significativo durante los repostajes de combustible.
1.3.5. Carga de un tipo de carburante u otros líquidos esenciales contaminados o incorrectos (incluidos oxígeno, nitrógeno, aceite y agua potable).
1.3.6. Incapacidad de solventar malas condiciones de la superficie de la pista.
1.3.7. Cualquier suceso en el que el desempeño humano haya contribuido de forma directa, o podría haber contribuido, a un accidente o a un incidente grave.

2. Asistencia en tierra de una aeronave

2.1. Equipo de embarque retirado suponiendo un peligro para los ocupantes de la aeronave.
2.2. Transporte, intento de transporte o manipulación de mercancías peligrosas que han puesto en peligro, o que podrían haber puesto en peligro, la seguridad de la operación, o haber dado lugar a una situación de inseguridad (por ejemplo: incidente o accidente imputable a mercancías peligrosas según la definición de las Instrucciones Técnicas de la OACI.)
2.3. Incumplimiento de los procedimientos requeridos de asistencia y mantenimiento en tierra de las aeronaves, especialmente de los procedimientos reabastecimiento, o carga, incluidos el posicionamiento incorrecto o la retirada de equipos.
2.4. Derrame significativo durante los reabastecimientos de combustible. Fallo, malfuncionamiento o defecto de equipos de tierra utilizados para la asistencia en tierra que tengan o puedan tener como consecuencia daños a la aeronave, como, por ejemplo: barra de arrastre o unidad de potencia en tierra (GPU).
2.5. Daños a la aeronave provocados por equipos o vehículos de asistencia en tierra, incluidos los daños no declarados con anterioridad.
2.6. Cualquier suceso en el que el desempeño humano haya contribuido de forma directa, o podría haber contribuido, a un accidente o a un incidente grave.

E. Sucesos relacionados con aeronaves y obstáculos

1.1. Operaciones aéreas

1.1.1 Pérdida no intencionada de control.
1.1.2 Suceso en el que el piloto del planeador no pudo soltar el cable del torno o el cable de remolque y tuvo que emplear procedimientos de emergencia para hacerlo.
1.1.3 Cualquier suelta del cable del cabrestante o de remolque que ha puesto, o que podría haber puesto, en peligro el planeador, a sus ocupantes o a cualquier otra persona.
1.1.4 En el caso de un motovelero, un fallo de motor durante el despegue.
1.1.5 Cualquier vuelo que haya sido efectuado con un planeador no apto para la navegación aérea, o para el cual la preparación de vuelo no ha sido completada, que ha puesto, o podría haber puesto, en peligro el planeador, a sus ocupantes o a cualquier otra persona.

1.2. Sucesos técnicos

1.2.1. Fuerte vibración anormal, como, por ejemplo, flapeo (aleteo) del alerón, del timón de profundidad, o de la hélice).
1.2.2. Cualquier control de vuelo que no funcione correctamente o esté desconectado.
1.2.3. Fallo o deterioro sustancial de la estructura del planeador.
1.2.4 Pérdida en vuelo de cualquier parte de la estructura o instalación del planeador.

1.3. Interacción con los servicios de navegación aérea y la gestión del Tránsito aéreo

1.3.1. Interacción con los servicios de navegación aérea (por ejemplo: servicios prestados de manera incorrecta, comunicaciones contradictorias o desviación de la autorización) que ha puesto, o podría haber puesto, en peligro el planeador, a sus ocupantes o a cualquier otra persona.
1.3.2. Violaciones de espacio aéreo

1.4. Emergencias y otras situaciones críticas

1.4.1. Cualquier suceso que dé lugar a una llamada de emergencia.
1.4.2. Cualquier situación en la que no quede disponible ninguna zona de aterrizaje seguro.
1.4.3. Incendio, explosión, humo, gases o emanaciones tóxicas en el planeador.
1.4.4. Incapacitación del piloto que imposibilite la realización de cualquier trabajo

1.5. Entorno exterior y meteorología

1.5.1. Una colisión en tierra o en el aire, con otra aeronave, el terreno o un obstáculo.
1.5.2. Una cuasi colisión, en tierra o en el aire, con una aeronave o un obstáculo.
1.5.3. Interferencia con el planeador mediante armas de fuego, fuegos artificiales, cometas, luces láser, luces láser de alta potencia, sistemas de aeronave pilotada a distancia, aeromodelos, o por medios similares.
1.5.4. Impacto de rayo que provoque daños en el planeador

2. Vehículos más ligeros que el aire (globos y dirigibles)

2.1. Operaciones aéreas

2.1.1. Cualquier vuelo que haya sido efectuado con un vehículo más ligero que el aire no apto para la navegación aérea, o para el cual la preparación de vuelo no ha sido completada, que ha puesto, o podría haber puesto en peligro el vehículo más ligero que el aire, a sus ocupantes o cualquier otra persona.
2.2.1. Apagado permanente no intencionado de la llama del piloto.

2.2. Sucesos técnicos

2.2.1. Fallo de cualquiera de los siguientes componentes o controles: tubo de inmersión del cilindro de combustible, polea de la envoltura, cable de control, cable de amarre, fuga en el sellado de la válvula del quemador, mosquetón, daño en el tubo de combustible, válvula de gas de elevación, envoltura o globo compensador, soplador, válvula limitadora de la presión (globo de gas), cabrestante (globos de gas cautivos).
2.2.2. Fuga importante o pérdida de gas de elevación (por ejemplo: porosidad, válvulas de gas de elevación desasentadas).

2.3. Interacción con los servicios de navegación aérea y la gestión del tránsito aéreo

2.3.1. Interacción con los servicios de navegación aérea (por ejemplo: servicios prestados de una manera incorrecta, comunicaciones contradictorias o desviación de la autorización) que ha puesto, o podría haber puesto, en peligro el vehículo más ligero que el aire, a sus ocupantes o a cualquier otra persona.

2.3.2. Violación de espacio aéreo

2.4. Emergencias y otras situaciones críticas

2.4.1. Cualquier suceso que dé lugar a una llamada de emergencia.

2.4.2. Incendio, explosión, humo o emanaciones tóxicas en el vehículo más ligero que el aire (aparte de las normales por el funcionamiento del quemador).
2.4.3. Ocupantes del vehículo más ligero que el aire despedido de la canastilla o barquilla.
2.4.5. Incapacitación del piloto que imposibilite la realización de cualquier trabajo.
2.4.6. Elevación o arrastre no intencionados del personal de tierra, con resultado de muerte o lesiones de una persona.

2.5. Entorno exterior y meteorología

2.5.1. Una colisión o cuasi colisión, en tierra o en el aire, con una aeronave, el terreno o un obstáculo que ha puesto, o podría haber puesto, en peligro el vehículo más ligero que el aire, a sus ocupantes o a cualquier otra persona.
2.5.2. Interferencia con el vehículo más ligero que el aire mediante armas de fuego, fuegos artificiales, cometas, luces láser, luces láser de alta potencia, sistemas de aeronave pilotada a distancia, aeromodelos, o por medios similares.
2.5.3. Encuentro inesperado con malas condiciones meteorológicas que han puesto, o que podrían haber puesto, en peligro el vehículo más ligero que el aire, a sus ocupantes o a cualquier otra persona.

INTENCIONALMENTE EN BLANCO

Apéndice 9

Lista de requisitos aplicables a los sistemas obligatorios y voluntarios de notificación de sucesos

A. Campos de datos obligatorios comunes

A la hora de registrar todo suceso de notificación obligatoria y, en la medida de lo posible, todo suceso de notificación voluntaria en sus respectivas bases de datos, las organizaciones deben velar por que en las notificaciones de sucesos registradas figure como mínimo la siguiente información:

1. Título.

2. Datos de registros – Entidades responsables – Número de expediente – Estatus del suceso

3. Fecha – Hora UTC

4. Lugar del suceso.

5. Clasificación – categoría de suceso.

6. Tipo de suceso.

B. Campos de datos relacionados con las aeronaves

A la hora de registrar todo suceso de notificación obligatoria y, en la medida de lo posible, todo suceso de notificación voluntaria en sus respectivas bases de datos, las organizaciones deben velar por que en las notificaciones de sucesos registradas figure como mínimo la siguiente información, en caso de que haya estado implicada en el suceso una aeronave:

1. Identificación de la aeronave:

    a. Estado de matrícula.
    b. Marca/Modelo/Serie.
    c. Número de serie de la aeronave.
    d. Matrícula de la aeronave.
    e. Indicativo de llamada por radio.

2. Operación de la aeronave:

    a. Operador.

b. Tipo de operación.

3. Historial del vuelo:

a. Último punto de partida.

b. Destino previsto.

c. Fase de vuelo.

4. Condiciones meteorológicas

a. Relevancia de las condiciones meteorológicas al momento del evento.

C. Campos de datos relacionados con los servicios de navegación aérea

A la hora de registrar todo suceso de notificación obligatoria y, en la medida de lo posible, todo suceso de notificación voluntaria en sus respectivas bases de datos, las organizaciones velarán por que en las notificaciones de sucesos registradas figure como mínimo la siguiente información, en caso de que haya estado implicado en el suceso un servicio de navegación aérea o el entorno operativo circundante:

1. Relación con el Servicio de tránsito aéreo (ATS, «Air Traffic Services»)

a. Contribución ATS al evento.

b. Servicio afectado (repercusiones en el servicio ATS).

2. Denominación de la dependencia de los servicios de tránsito aéreo.

D. Campos de datos relacionados con una infracción de las mínimas de separación/pérdida de separación y violación del espacio aéreo

A la hora de registrar todo suceso de notificación obligatoria y, en la medida de lo posible, todo suceso de notificación voluntaria en sus respectivas bases de datos, las organizaciones velarán por que en las notificaciones de sucesos registradas figure como mínimo la siguiente información, en caso de que haya estado implicada en el suceso una infracción de las mínimas de separación/pérdida de separación o una violación del espacio aéreo:

1. Espacio aéreo

a. Tipo de espacio aéreo.

b. Clase de espacio aéreo.

c. Denominación FIR/UIR.

E. Campos de datos relacionados con los aeródromos

A la hora de registrar todo suceso de notificación obligatoria y, en la medida de lo posible, todo suceso de notificación voluntaria en sus respectivas bases de datos, las organizaciones velarán por que en las notificaciones de sucesos registradas figure como mínimo la siguiente información, en caso de que haya estado implicado en el suceso un servicio aeroportuario o el entorno operativo circundante:

1. Indicadores de localización (indicador OACI del aeropuerto).

2. Situación dentro del aeródromo.

F. Campos de datos relacionados con daños a la aeronave o lesiones producidas a las personas

A la hora de registrar todo suceso de notificación obligatoria en sus respectivas bases de datos, las organizaciones velarán por que en las notificaciones de sucesos registradas figure como mínimo la siguiente información, en caso de haberse producido daños a una aeronave o lesiones a una persona:

1. Gravedad

a. Daños más importantes.

b. Gravedad de las lesiones.

2. Lesiones producidas a personas:

a. número de lesiones en tierra (mortales, graves, leves).

b. número de lesiones en las aeronaves (mortales, graves, leves).

INTENCIONALMENTE EN BLANCO