



REPÚBLICA DEL PARAGUAY
DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL

**REGLAMENTO DEL SISTEMA DE GESTIÓN
DE LA SEGURIDAD OPERACIONAL (SMS)**

Primera edición
(Aprobado por Resolución N°180/2009)

Marzo 2009

INTENCIONALMENTE EN BLANCO

INTENCIONALMENTE EN BLANCO

DOCUMENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

ÍNDICE

CAPITULO 1.

GENERALIDADES

| | | |
|-----|--|---|
| 1.1 | Concepto de seguridad operacional | 1 |
| 1.2 | Requisitos de la OACI | 1 |
| 1.3 | Nivel aceptable de seguridad operacional | 2 |
| 1.4 | Partes interesadas en la seguridad operacional | 4 |

CAPÍTULO 2.

ALCANCE Y APLICABILIDAD

| | | |
|-----|----------------------------|---|
| 2.1 | Ámbito | 6 |
| 2.2 | Finalidad | 6 |
| 2.3 | Aplicabilidad y Aceptación | 6 |
| 2.4 | Destinatarios | 7 |

CAPÍTULO 3.

IDENTIFICACIÓN DE LOS PELIGROS Y GESTIÓN DE RIESGOS

| | | |
|------|---|----|
| 3.1 | Generalidades | 8 |
| 3.2 | Ciclo de seguridad operacional | 8 |
| 3.3 | Identificación de peligros | 10 |
| 3.4 | Evaluación de riesgos | 11 |
| 3.5 | Probabilidad de consecuencias perjudiciales | 13 |
| 3.6 | Gravedad de las consecuencias del suceso | 14 |
| 3.7 | Aceptabilidad de los riesgos | 14 |
| 3.8 | Mitigación de riesgos | 17 |
| 3.9 | Comunicación de riesgos | 19 |
| 3.10 | Proceso de implementación | 20 |

CAPÍTULO 4.

COMPONENTES DE UN SMS

| | | |
|-----|---------------|----|
| 4.1 | Generalidades | 26 |
|-----|---------------|----|

| | | |
|--------------------------------------|---|-----------|
| 4.2 | Política y objetivos de seguridad | 26 |
| 4.3 | Estructura y responsabilidad organizacional | 26 |
| 4.4 | Plan para la implementación de un SMS | 27 |
| 4.5 | Coordinación del plan de respuesta a la emergencia | 28 |
| 4.6 | Documentación | 29 |
| 4.7 | Gestión del riesgo de la seguridad | 29 |
| | | |
| CAPÍTULO 5. | | |
| ASEGURAMIENTO DE LA SEGURIDAD | | |
| 5.1 | Generalidades | 31 |
| 5.2 | Monitoreo y medición de la performance de la seguridad | 31 |
| 5.3 | Gestión del cambio | 31 |
| 5.4 | Mejora continua del SMS | 31 |
| | | |
| CAPÍTULO 6. | | |
| PROMOCION DE LA SEGURIDAD | | |
| 6.1 | Generalidades | 33 |
| 6.2 | Entrenamiento de seguridad | 33 |
| 6.3 | Comunicación de seguridad | 33 |
| | | |
| CAPÍTULO 7. | | |
| | POLITICA DE CALIDAD | 34 |
| | | |
| CAPÍTULO 8. | | |
| | IMPLEMENTACIÓN DEL SMS POR FASES | 35 |
| | | |
| CAPÍTULO 9. | | |
| | PROMOCIÓN DE LA SEGURIDAD OPERACIONAL | 37 |
| | | |
| CAPÍTULO 10. | | |
| | GESTIÓN DE LA INFORMACIÓN DE SEGURIDAD OPERACIONAL | 40 |

*** **

CAPITULO 1 GENERALIDADES

1.1 Concepto de seguridad operacional

1.1.1 Para entender la gestión de la seguridad operacional es necesario considerar qué quiere decir “seguridad operacional”. Dependiendo de la perspectiva que se adopte, el concepto de seguridad operacional de la aviación puede tener diferentes connotaciones, tales como:

- a) ningún accidente (o incidente grave), opinión que sostiene ampliamente el público viajero;
- b) ausencia de peligro o riesgos, es decir, de aquellos factores que causan o que probablemente causen perjuicios;
- c) actitud de los empleados con respecto a actos y condiciones inseguras (que reflejan una cultura “segura” de la empresa);
- d) grado en que los riesgos inherentes a la aviación son “*aceptables*”;
- e) proceso de identificación de peligros y gestión de riesgos; y
- f) control de pérdida accidental (de personas y bienes, y daños al medio ambiente).

1.1.2 Si bien la eliminación de accidentes (y de incidentes graves) sería deseable, una seguridad operacional del cien por cien es un objetivo inalcanzable. Ocurrirán fallas y errores a pesar de los mejores esfuerzos para evitarlos. Ninguna actividad humana ni ningún sistema hecho por el hombre se pueden garantizar como que es absolutamente seguro, es decir, libre de riesgos. La seguridad operacional es una noción relativa, por lo que en un sistema “seguro” los riesgos inherentes son aceptables.

1.1.3 Cada vez más, la seguridad operacional se percibe como una gestión de riesgos. Por lo tanto, para los fines de este documento se considera que tiene el siguiente significado:

Seguridad operacional es el estado en que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel aceptable, o por debajo del mismo, por medio de un proceso continuo de identificación de peligros y gestión de riesgos.

1.2 Requisitos de la OACI

1.2.1 La seguridad operacional ha sido siempre la consideración primordial en las actividades de la aviación. Esto se refleja en los fines y objetivos de la OACI declarados en el Artículo 44 del *Convenio sobre Aviación Civil Internacional* (Doc 7300), conocido como el Convenio de Chicago, en el que se encomienda a la OACI lograr el desarrollo seguro y ordenado de la aviación civil internacional en todo el mundo.

1.2.2 Al establecer los requisitos que deben cumplir los Estados para la gestión de la seguridad operacional, la OACI hace la distinción entre programas de seguridad operacional y sistemas de gestión de la seguridad operacional (SMS):

- Un **programa de seguridad operacional** es un conjunto integrado de reglamentos y actividades encaminados a mejorar la seguridad operacional. Un programa de

seguridad operacional tendrá un alcance amplio, e incluirá muchas actividades de seguridad operacional dirigidas a alcanzar los objetivos del programa. El programa de seguridad operacional de un Estado comprende los reglamentos y las instrucciones para la realización de operaciones seguras desde el punto de vista de los explotadores de aeronaves y de quienes proveen servicios de tránsito aéreo (ATS), aeródromos y mantenimiento de aeronaves. El programa de seguridad operacional puede incluir disposiciones para diversas actividades, tales como notificación de incidentes, investigaciones de seguridad operacional, auditorias de la seguridad operacional y promoción de la seguridad operacional. Poner en práctica las actividades conducentes a la seguridad operacional de modo integrado exige un SMS coherente.

• Un **sistema de gestión de la seguridad operacional (SMS)** es un enfoque sistemático para la gestión de la seguridad operacional, que incluye la estructura orgánica, las líneas de responsabilidad, las políticas y los procedimientos necesarios para ese fin. Por lo tanto, de conformidad con las disposiciones de los Anexos 6, 11 y 14, los Estados exigirán que cada explotador, organismo de mantenimiento, proveedor de servicios ATS y explotador de aeródromo certificado ponga en práctica un SMS aprobado por el Estado. Como mínimo, los SMS deberán:

- a) identificar los peligros para la seguridad operacional;
- b) asegurar que se aplican las medidas correctivas necesarias para mitigar los riesgos y peligros; y
- c) prever una supervisión permanente y una evaluación periódica del nivel de seguridad operacional logrado.

1.2.3 El SMS de una organización deberá definir claramente las líneas de responsabilidad por la seguridad operacional, e incluirá una responsabilidad directa del personal administrativo superior con respecto a la seguridad operacional.

1.2.4 La DINAC, en cumplimiento de las normas y métodos recomendados (SARPS) de la OACI, ha establecido los requerimientos desde el 31 de julio de 2006, requiriendo que todos los proveedores de servicios ATS, aeródromos, explotadores de aeronaves y organizaciones de mantenimiento de aeronaves implementen un SMS y cumplir con las disposiciones de los Anexos 6, 11 y 14. La DINAC auditará los SMS de los proveedores de servicios ATS, aeródromos, explotadores de aeronaves.

1.3 Nivel aceptable de seguridad operacional

1.3.1 En todo sistema, es necesario fijar y medir los resultados en términos de eficacia a fin de determinar si el sistema funciona de conformidad con las expectativas e identificar el punto en que es necesario aplicar medidas para mejorar los niveles de eficacia y responder así a esas expectativas.

1.3.2 La introducción del concepto de *nivel aceptable de seguridad operacional* responde a la necesidad de complementar el enfoque prevaleciente para la gestión de la seguridad operacional basado en el cumplimiento de la reglamentación, con un enfoque basado en la

eficacia. El nivel aceptable de seguridad operacional expresa los objetivos (o las expectativas) de seguridad operacional de una autoridad de vigilancia, un explotador o un proveedor de servicios. Desde la perspectiva de la relación entre autoridades de vigilancia y explotadores o proveedores de servicios, proporciona un objetivo en términos de la eficacia de la seguridad operacional que los explotadores o proveedores de servicios deberán alcanzar cuando desempeñan sus funciones básicas, como un mínimo aceptable para la autoridad de vigilancia. Es una referencia con respecto a la cual la autoridad de vigilancia puede medir la eficacia de la seguridad operacional. Para determinar un nivel aceptable de seguridad operacional es necesario considerar factores tales como el nivel de riesgo pertinente, los costos y beneficios de las mejoras del sistema y las expectativas del público respecto a la seguridad operacional en la industria de la aviación.

1.3.3 En la práctica, el concepto de nivel aceptable de seguridad operacional se expresa mediante dos medidas o parámetros (indicadores de eficacia de la seguridad operacional y objetivos de eficacia de la seguridad operacional) y se aplica por medio de varios requisitos de seguridad operacional. Seguidamente se explica el empleo de estas expresiones en este documento.

- Los ***indicadores de eficacia de la seguridad operacional*** son una medida de la eficacia de la seguridad operacional de una organización de aviación o de un sector de la industria. Los indicadores de seguridad operacional deberían ser fáciles de medir y estar vinculados con los principales componentes del programa de seguridad operacional de un Estado o con el SMS de un explotador o un proveedor de servicios. Por lo tanto, los indicadores de seguridad operacional serán diferentes según los diversos segmentos de la industria de la aviación, tales como explotadores de aeronaves, explotadores de aeródromo o proveedores ATS.
- Los ***objetivos de eficacia de la seguridad operacional*** (a veces llamados metas) se determinan considerando cuáles son los niveles de eficacia de la seguridad operacional que son deseables y realistas para los explotadores y proveedores de servicios considerados individualmente. Los objetivos de seguridad operacional deberían ser medibles, aceptables para las partes interesadas y compatibles con nuestro programa de seguridad operacional.
- Los ***requisitos de seguridad operacional*** son necesarios para alcanzar los indicadores y los objetivos de eficacia de la seguridad operacional. Entre estos requisitos se incluyen los procedimientos operacionales, la tecnología y los sistemas o programas con respecto a los cuales pueden especificarse las medidas de fiabilidad, disponibilidad, eficacia y precisión.

1.3.4 La relación entre nivel aceptable de seguridad operacional, indicadores de eficacia de la seguridad operacional, objetivos de eficacia de la seguridad operacional y requisitos de seguridad operacional es la siguiente: *nivel aceptable de seguridad operacional* es el concepto general; *indicadores de eficacia de la seguridad operacional* son las medidas o parámetros que se emplean para determinar si se ha logrado el nivel aceptable de seguridad operacional; los *objetivos de seguridad operacional* son los objetivos cuantificados pertinentes al nivel aceptable de seguridad operacional; y los

requisitos de seguridad operacional son los medios necesarios para lograr los objetivos de la seguridad operacional.

1.3.5 Los indicadores de seguridad operacional y los objetivos de seguridad operacional pueden ser diferentes (p. ej., el indicador es 0,5 accidentes mortales por 100 000 horas para los explotadores de línea aérea y el objetivo es una reducción del 40% del índice de accidentes mortales para las operaciones de líneas aéreas) o pueden ser iguales (p. ej., el indicador es 0,5 accidentes mortales por 100 000 horas para los explotadores de línea aérea y el objetivo es 0,5 accidentes mortales por 100 000 horas, como máximo, para los explotadores de línea aérea).

1.3.6 Raramente habrá un nivel nacional aceptable de seguridad operacional. Con mayor frecuencia, dentro de cada Estado habrá diferentes niveles aceptables de seguridad operacional establecidos de común acuerdo entre la autoridad encargada de la vigilancia reglamentaria y los diversos explotadores y proveedores de servicios. Cada nivel aceptable de seguridad operacional establecido de común acuerdo debería ser acorde con la complejidad del contexto operacional de cada explotador o proveedor de servicios.

1.3.7 El hecho de establecer niveles aceptables de seguridad operacional para el programa de seguridad operacional no reemplaza los requisitos legales, reglamentarios o de otro tipo, ni exime a los Estados de sus obligaciones respecto al *Convenio sobre Aviación Civil Internacional* (Doc 7300) y las disposiciones conexas. Del mismo modo, el hecho de establecer niveles aceptables de seguridad operacional para el SMS no exime a los explotadores o proveedores de servicios de sus obligaciones en el marco de los reglamentos nacionales ni de las dimanantes del *Convenio sobre Aviación Civil Internacional*.

1.4 PARTES INTERESADAS EN LA SEGURIDAD OPERACIONAL

1.4.1 Dado el costo total de los accidentes de aviación, muchos grupos de diversa índole tienen un gran interés en mejorar la gestión de la seguridad operacional. Los principales interesados en la seguridad operacional son los siguientes:

- a) profesionales de la aviación [p. ej., tripulación de vuelo, tripulación de cabina, controladores de tránsito aéreo (ATCO) y mecánicos de mantenimiento de aeronaves;
- b) propietarios y explotadores de aeronaves;
- c) fabricantes (especialmente los fabricantes de células y motores);
- d) autoridades de reglamentación de la aviación (p. ej., CAA, EASA y ASECNA);
- e) asociaciones del sector de la aviación (p. ej., IATA, ATA y ACI);
- f) proveedores ATS regionales (p. ej., EUROCONTROL);
- g) asociaciones profesionales y sindicatos (p. ej., IFALPA e IFATCA);
- h) organizaciones internacionales de aviación (p. ej., OACI);
- i) organismos de investigación (p. ej., NTSB de los Estados Unidos); y
- j) el público viajero.

1.4.2 Los principales sucesos relacionados con la seguridad operacional invariablemente involucran a otros grupos que no siempre comparten un objetivo común en el adelanto de la seguridad operacional en la aviación, por ejemplo:

- a) parientes cercanos, víctimas o personas lesionadas en un accidente;

- b) empresas de seguro;
- c) sector de viajes y turismo;
- d) instituciones educacionales y de instrucción en seguridad de la aviación;
- e) otros departamentos y organismos gubernamentales;
- f) funcionarios gubernamentales elegidos por sufragio;
- g) inversores;
- h) peritos forenses y policías;
- i) medios de comunicación;
- j) el público en general;
- k) abogados y consultores; y
- l) diversos grupos de intereses especiales.

*** **

CAPITULO 2

ALCANCE Y APLICABILIDAD

2.1 **Ámbito**

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

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

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

DINAC R145: Aeronavegabilidad - Talleres Aeronáuticos de Reparaciones
DINAC-R11, Servicios de Tránsito Aéreo

DINAC-R14, Aeródromos

Anexo 6 — *Operación de aeronaves, Parte I — transporte aéreo internacional — Aeroplanos, y Parte III — Operaciones internacionales — Helicópteros,*

Anexo 11 — Servicios de tránsito aéreo, y

Anexo 14 — *Aeródromos, Volumen I — Diseño y Operación de Aeródromos, de la Organización de Aviación Civil Internacional.*

2.1.3 Este Documento se orienta a la seguridad de la aviación relacionada con los procesos y actividades antes que a la seguridad ocupacional, protección de ambiente, o calidad de los servicios al cliente.

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

2.1.5 Este Documento establece los requisitos mínimos aceptables; y que el proveedor de servicio puede establecer requisitos más estrictos establecidos por la autoridad de aviación civil.

2.2 **Finalidad**

2.2.1 La finalidad de este documento es ayudar a aquellos que trabajan en, con y asisten donde están los proveedores de servicios de tránsito aéreo, operadores de aeródromos certificados, organismos de mantenimiento y operadores de aeronaves, en cumplimiento de los requisitos establecidos en los Anexos 6, 11 y 14 de la OACI con respecto a la implantación de Sistema de Gestión de la Seguridad Operacional (SMS).

2.2.2 En el contexto de este documento el término “proveedor de servicio” debe ser entendido para referirse a cualquier organización que suministra servicios relacionados a la aviación civil. El término incluye a operadores de aeronaves, organizaciones de

mantenimiento, proveedores de servicios de tránsito aéreo y operadores de aeródromos, lo que sea aplicable.

2.3 Aplicabilidad y Aceptación

2.3.1 A partir del 5 de marzo de 2013, todo operador o proveedor de servicio ATS, de aeródromos certificados, organizaciones de mantenimiento y Operador de Aeronaves, deberán poseer un sistema de gestión de la seguridad operacional (SMS) que sea aceptable para la Autoridad de Aviación Civil del Paraguay, que como mínimo:

- 2.3.1.1 identifique los riesgos de seguridad;
- 2.3.1.2 asegure la implementación de las acciones necesarias para mantener un nivel aceptable de seguridad;
- 2.3.1.3 provea un monitoreo continuo y una regular valoración del nivel de seguridad obtenido; y
- 2.3.1.4 establezca una mejora continua en todos los niveles de seguridad.

2.3.2 A fin de ser aceptable para la Autoridad de Aviación Civil del Paraguay, el SMS del proveedor de servicio debe reunir los requisitos establecidos en este reglamento.

2.4 Destinatarios

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

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

- a) funcionarios responsables de la reglamentación del sistema de aviación;
- b) administradores de organizaciones operacionales, tales como explotadores, proveedores ATS, aeródromos y organismos de mantenimiento; y
- c) profesionales de la seguridad operacional, tales como jefes y asesores de los servicios de seguridad operacional.

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

*** **

CAPITULO 3

IDENTIFICACIÓN DE LOS PELIGROS Y GESTIÓN DE RIESGOS

3.1 GENERALIDADES

3.1.1 La seguridad operacional es una condición en la que el riesgo de lesiones o daños está limitado a un nivel aceptable. Los peligros para la seguridad operacional que crean riesgo pueden llegar a ser evidentes después de una perturbación obvia de la seguridad operacional, como en el caso de un accidente o incidente, o también pueden ser identificados preventivamente por medio de programas formales de gestión de la seguridad operacional — antes de que ocurra realmente un suceso. Una vez identificado un peligro para la seguridad operacional, se pueden evaluar los riesgos relacionados con el mismo. Con una comprensión clara de la naturaleza de los riesgos, se puede determinar la “aceptabilidad” de los mismos; respecto a los que no son aceptables, se deben adoptar medidas.

3.1.2 La gestión de la seguridad operacional está centrada en ese enfoque sistemático de la identificación de peligros y la gestión de riesgos — a fin de reducir al mínimo la pérdida de vidas humanas, los daños a los bienes y las pérdidas financieras y para el medio ambiente y la sociedad.

3.2 CICLO DE SEGURIDAD OPERACIONAL

3.2.1 Dado el número de factores que pueden afectar a la seguridad operacional y las posibles relaciones entre los mismos, es necesario un SMS eficaz. En la Figura 3-1 se da un ejemplo del tipo de proceso sistemático que se necesita, y lo que sigue es una breve descripción del ciclo de seguridad operacional.

3.2.2 La identificación de peligros es el primer paso crítico en la gestión de la seguridad operacional. Para esto, se necesitan pruebas del peligro, que pueden obtenerse de varias maneras y de diversas fuentes, por ejemplo:

- a) sistemas de notificación de peligros e incidentes;
- b) investigación y seguimiento de peligros e incidentes notificados;
- c) análisis de tendencias;
- d) retorno de información de la instrucción;
- e) análisis de datos de vuelo;
- f) encuestas sobre seguridad operacional y auditoria de la vigilancia de la seguridad operacional;
- g) supervisión de las operaciones normales;

- h) investigación de accidentes e incidentes graves por el Estado; y
- i) sistemas de intercambio de información.

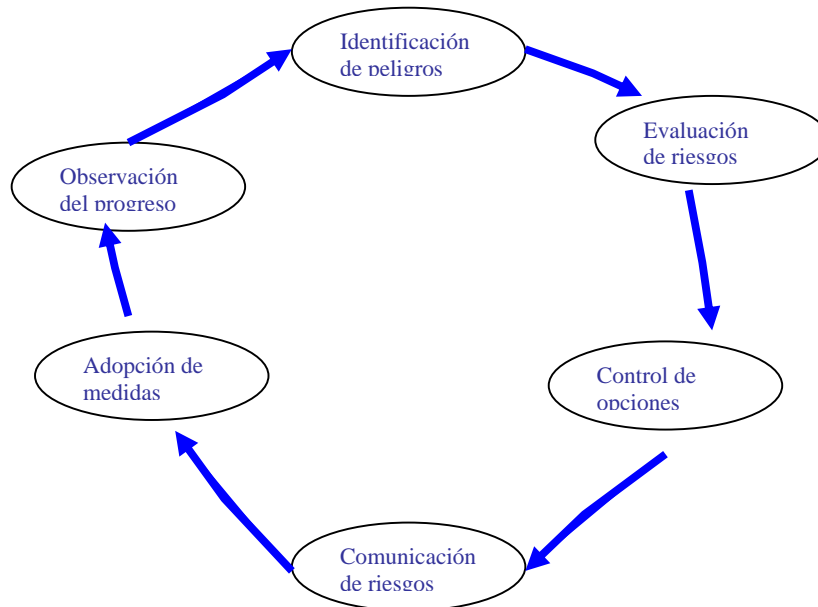


Figura 3.1 Ciclo de seguridad operacional

3.2.3 Se debe evaluar cada peligro detectado y dársele la prioridad correspondiente. Esta evaluación requiere la compilación y el análisis de todos los datos disponibles. Estos datos se evalúan para determinar la amplitud del peligro: ¿Es “único” o es sistémico? Puede ser necesaria una base de datos para facilitar el almacenamiento y la búsqueda y extracción de datos. Para analizar los datos se necesitan herramientas apropiadas.

3.2.4 Una vez comprobada una deficiencia en la seguridad operacional, se deben tomar decisiones en cuanto a la medida más apropiada para evitar o eliminar el peligro o reducir los riesgos relacionados con el mismo. La solución debe tener en cuenta las condiciones locales, dado que una solución no es necesariamente buena para todas las situaciones. Debe tenerse cuidado de que la solución no introduzca nuevos peligros. Este es el proceso de gestión de riesgos.

3.2.5 Una vez que se ha puesto en práctica la medida de seguridad operacional apropiada, se debe vigilar su eficacia para asegurarse de que se ha logrado el resultado deseado, por ejemplo:

- a) se ha eliminado el peligro (o por lo menos se ha reducido la probabilidad o la gravedad de los riesgos relacionados con el mismo);

- b) la medida adoptada permite enfrentar satisfactoriamente el peligro; y
- c) no se han introducido nuevos peligros en el sistema.

3.2.6 Si el resultado no es satisfactorio, debe repetirse todo el proceso.

3.3 IDENTIFICACIÓN DE PELIGROS

3.3.1 Dado que un peligro puede crear una situación o condición que encierra la posibilidad de causar consecuencias perjudiciales, el ámbito de los peligros en la aviación es grande, como lo indican los ejemplos siguientes:

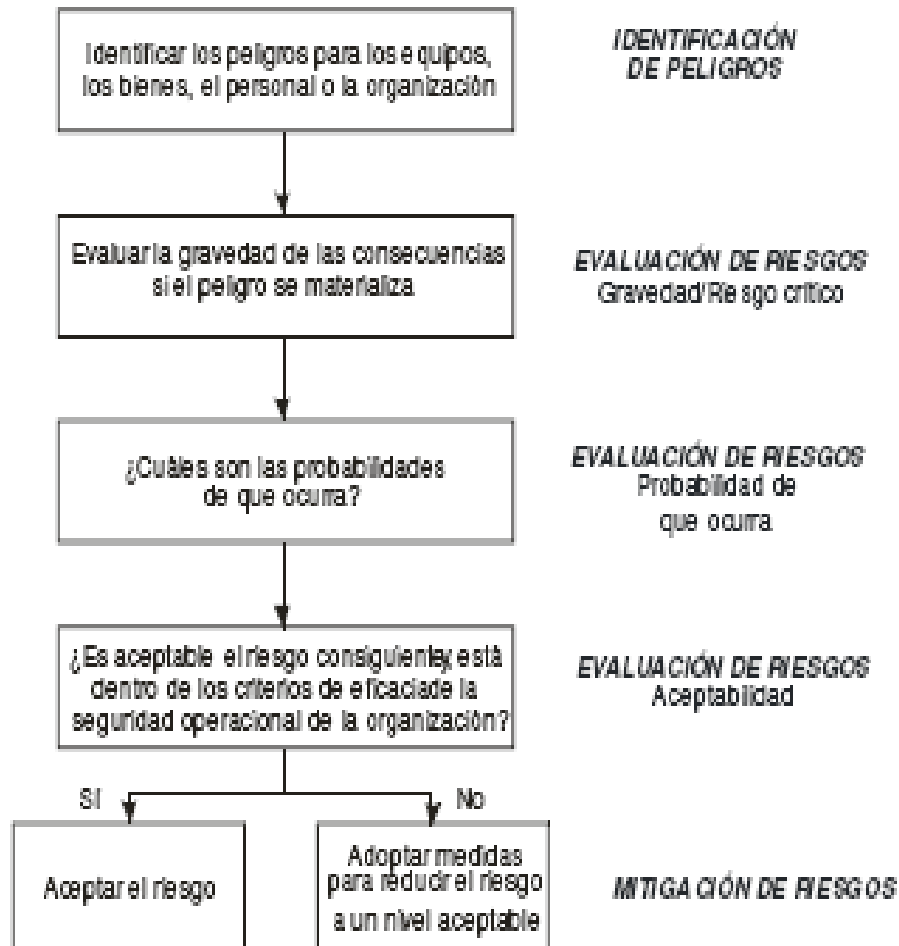


Figura 3.2. Proceso de gestión de riesgos

- a) **factores de diseño**, incluido el diseño de equipos y de tareas;
- b) **procedimientos y prácticas operacionales**, incluidas su documentación y las listas de verificación, y su validación en condiciones de operación;
- c) **comunicaciones**, incluidos el medio, la terminología y el lenguaje;
- d) **factores de personal**, tales como políticas de la empresa para la contratación, instrucción y remuneración;
- e) **factores de organización**, tales como compatibilidad de producción y objetivos de seguridad operacional, asignación de recursos, presión en las operaciones y cultura de seguridad operacional de la empresa;
- f) **factores del entorno de trabajo**, tales como ruido ambiente y vibraciones, temperatura, iluminación y ropa y equipos de protección disponibles;
- g) **factores de vigilancia reglamentaria**, incluida la aplicabilidad y fuerza de los reglamentos, la certificación de equipo, personal y procesamientos, y las auditorias de supervisión adecuadas; y
- h) **defensas**, incluidos factores tales como la provisión de sistemas adecuados de detección y alarma, tolerancia de errores por los equipos y medida en que los equipos están reforzados contra fallas.

3.4 EVALUACIÓN DE RIESGOS

3.4.1 Una vez confirmada la presencia de peligros para la seguridad operacional, es necesario algún tipo de análisis para evaluar el potencial de perjuicios o daños. Típicamente, esta evaluación del peligro supone tres consideraciones:

- a) la **probabilidad** de que el peligro produzca un suceso peligroso (es decir, la probabilidad de consecuencias perjudiciales en caso de que se permita que las condiciones inseguras subyacentes persistan);
- b) la **gravedad** de las posibles consecuencias perjudiciales, o el resultado de un suceso peligroso; y
- c) el índice de **exposición** a los peligros. La probabilidad de consecuencias perjudiciales aumenta con la mayor exposición a condiciones inseguras, por lo que la exposición debe considerarse como otra dimensión de probabilidad. Sin embargo, algunos métodos para definir la probabilidad también pueden incluir el elemento de exposición, por ejemplo, un índice de 1 en 10 000 horas.

3.4.2 El **riesgo** es el potencial evaluado de las consecuencias perjudiciales que pueden resultar de un peligro. Es la probabilidad de que se realice el potencial de peligro para causar perjuicios.

3.4.3 La **evaluación de riesgos** supone considerar tanto la probabilidad como la gravedad de toda consecuencia perjudicial; en otras palabras, se determina el potencial de pérdidas. Cuando se lleva a cabo la evaluación de riesgos es importante distinguir entre *peligros* (el potencial de causar perjuicios) y *riesgos* (la probabilidad de que el perjuicio ocurra dentro de un período determinado). Una matriz de evaluación de riesgos (como la que se presenta en la Tabla 3-1 y en el Adjunto D) es un instrumento útil para poner en orden de prioridad los peligros que requieren más atención.

3.4.4 Hay muchos modos, algunos más formales que otros, de enfocar los aspectos analíticos de la evaluación de riesgos. En el caso de algunos riesgos, el número de variables y el disponer de datos apropiados y modelos matemáticos pueden conducir a resultados verosímiles con métodos cuantitativos (que requieren el análisis matemático de datos específicos). Sin embargo, pocos peligros en la aviación se prestan a análisis verosímiles con sólo métodos numéricos. Típicamente, estos análisis se complementan cualitativamente por medio de análisis críticos y lógicos de los hechos conocidos y sus relaciones.

3.4.5 La literatura sobre los tipos de análisis empleados en la evaluación de riesgos es considerable. Para las evaluaciones de riesgos examinadas no se necesitan métodos complejos; una comprensión básica de unos pocos métodos será suficiente.

3.4.6 Cualesquiera sean los métodos empleados, los riesgos pueden expresarse de varias formas, por ejemplo:

- a) número de muertos, pérdida de ingresos o pérdida de parte del mercado (es decir, cifras absolutas);
- b) índice de pérdidas (p. ej., número de muertos por 1.000.000 de pasajeros – kilómetros efectuados;
- c) probabilidad de accidentes graves (p. ej., 1 cada 50 años);
- d) gravedad de los resultados (p. ej., lesiones graves); y
- e) valor en dólares de las pérdidas previstas en comparación con el ingreso anual de las operaciones (p. ej., US\$ 1 millón de pérdidas por US\$ 200 millones de ingresos).

3.4.7 Todos los factores citados en este ejemplo o cualquiera de ellos pueden ser válidos y subrayar la naturaleza de la multicausalidad. Sin embargo, la forma en que se defina la cuestión de seguridad operacional afectará la decisión adoptada para reducir o eliminar los peligros. Al evaluar los riesgos, se deben evaluar todas las perspectivas potencialmente válidas y seguir únicamente las más apropiadas.

Nota: Ver Adjunto “A”, ejemplo de formulario para Identificación y Mitigación de Riesgos

3.5 Probabilidad de consecuencias perjudiciales

3.5.1 Independientemente de los métodos analíticos empleados, debe evaluarse la probabilidad de causar perjuicios o daños. Esta probabilidad dependerá de las respuestas a preguntas como:

- a) ¿Hay antecedentes de sucesos similares, o este es un caso aislado?
- b) ¿Qué otro equipo o componentes del mismo tipo pueden tener defectos similares?
- c) ¿Cuántos miembros del personal de operaciones o de mantenimiento siguen, o deben seguir, los procedimientos en cuestión?
- d) ¿Durante qué porcentaje de tiempo se usa el equipo o el procedimiento sospechoso?
- e) ¿Existen implicaciones de organización, gestión o reglamentación que podrían reflejar amenazas más grandes para el público?

3.5.2 Basándose en estas consideraciones, se puede evaluar la probabilidad de que un suceso ocurra, como en los ejemplos que siguen (ver Adjunto B):

a) **Probablemente no ocurra.** Las fallas que “probablemente no ocurran” incluyen los sucesos aislados, y riesgos en que el índice de exposición es muy bajo o el tamaño de la muestra es pequeño. La complejidad de las circunstancias necesarias para crear una situación de accidente puede ser tal que es poco probable que vuelva a producirse la misma cadena de sucesos. Por ejemplo, no es probable que sistemas independientes fallen concurrentemente. Sin embargo, aun cuando la posibilidad sólo sea remota, las consecuencias de fallas concurrentes podrían justificar el seguimiento.

Nota. — Existe una tendencia natural a atribuir sucesos poco probables a “coincidencias”. Es necesario proceder con cautela en esto. Si bien la coincidencia puede ser estadísticamente factible, no debería emplearse como un pretexto para no hacer el análisis debido.

b) **Puede ocurrir.** Las fallas que “pueden ocurrir” provienen de peligros con una probabilidad razonable de que puedan presentarse modelos de comportamiento humano similares en condiciones de trabajos similares, o de que existen los mismos defectos físicos en otras partes del sistema.

c) **Probablemente ocurrirá.** Esos sucesos reflejan un tipo (o tipo posible) de fallas físicas que aún no han sido rectificadas. Dado el diseño o el mantenimiento del equipo, su fortaleza en las condiciones de funcionamiento conocidas, etc., continuar las operaciones probablemente conducirá a una falla. Del mismo modo, dada la prueba empírica sobre algunos aspectos de la actuación humana, puede preverse con cierta certidumbre que individuos normales, actuando en condiciones de trabajo similares, probablemente

cometan los mismos errores o estén sujetos a obtener los mismos resultados indeseables de esa actuación.

3.6 Gravedad de las consecuencias del suceso

3.6.1 Una vez determinada la probabilidad del suceso (ver Adjunto C), se debe evaluar la naturaleza de las consecuencias perjudiciales en caso de que el suceso ocurra realmente. Las consecuencias posibles rigen el grado de urgencia de la medida de seguridad operacional requerida. Si hay un riesgo considerable de consecuencias muy graves, o si el riesgo de lesiones graves o de daños a los bienes o al medio ambiente es elevado, se justifican medidas de seguimiento urgentes. Al evaluar la gravedad de las consecuencias del suceso, podrían hacerse los siguientes tipos de preguntas:

- a) ¿Cuántas **vidas peligran**? (*Empleados, pasajeros, personas que se encuentren en el lugar y el público en general*).
- b) ¿Cuál es la extensión probable de los **daños a los bienes o financieros**? (*Pérdidas directas para el explotador, daños a la infraestructura aeronáutica, daños indirectos a terceros, repercusiones financieras y repercusiones económicas para el Estado*).
- c) ¿Qué probabilidades hay de **repercusiones en el medio ambiente**? (*Derramamiento de combustible u otro producto peligroso y daño físico del hábitat natural*).
- d) ¿Qué probabilidades hay de **repercusiones políticas** y de **interés de los medios de comunicación**?

3.7. Aceptabilidad de los riesgos

3.7.1 A partir de la evaluación de riesgos, se puede dar a estos un orden de prioridad con relación a otros peligros para la seguridad operacional no resueltos. Esto es crítico cuando se deben adoptar decisiones racionales para asignar recursos limitados teniendo en cuenta los peligros que presentan los riesgos más grandes para la organización.

3.7.2 Dar a los riesgos un orden de prioridad exige una base racional para dar a cada uno su importancia con respecto a otros riesgos. Para definir qué constituye un riesgo *aceptable* y qué constituye un riesgo *inaceptable* se necesitan criterios o normas. Considerando la probabilidad de un resultado indeseable en comparación con la gravedad potencial de ese resultado, un riesgo puede clasificarse dentro de una matriz de evaluación. (Ver Adjunto E)

3.7.3 En la versión de matriz de evaluación de riesgos que se muestra como ejemplo:

- a) la **gravedad** del riesgo se clasifica como *catastrófica, peligrosa, importante, poco importante* o *insignificante* y en cada caso un descriptor indica la posible gravedad de las consecuencias;

b) la **probabilidad** del suceso también se clasifica por medio de cinco niveles diferentes de definición cualitativa y se presentan descriptores para las diferentes probabilidades del suceso; y

c) los **valores** pueden asignarse numéricamente, para considerar la importancia relativa de cada nivel de gravedad y probabilidad. Se puede obtener una evaluación compuesta del riesgo, para ayudar a comparar los riesgos, multiplicando los valores de gravedad y probabilidad.

3.7.4 Cuando se ha empleado una matriz de riesgos para asignar valores a los riesgos, pueden asignarse diversos valores a fin de clasificar los riesgos como aceptables, indeseables o inaceptable. Estos términos se explican seguidamente:

- **Acceptable** significa que no es necesario tomar más medidas (a menos que se pueda reducir más el riesgo con poco costo o esfuerzo).
- **Indeseable (o tolerable)** significa que las personas afectadas están preparadas para soportar el riesgo a fin de obtener ciertos beneficios, en la inteligencia de que el riesgo se mitiga lo mejor posible.
- **Inaceptable** significa que las operaciones en las condiciones actuales deben cesar hasta que el riesgo se reduzca por lo menos al nivel *tolerable*.

3.7.5 Un enfoque menos numérico para determinar la *aceptabilidad* de riesgos particulares incluye considerar factores como los que siguen:

- Gestión.** ¿Es el riesgo compatible con la política y las normas de seguridad operacional de la organización?
- Capacidad para afrontar los costos.** ¿Impide la naturaleza del riesgo una solución eficaz con relación a los costos?
- Legalidad.** ¿Está el riesgo dentro de las normas de reglamentación y de la capacidad para hacerlas cumplir?
- Cultura.** ¿Cómo ven este riesgo el personal de la organización y otros interesados?
- Mercado.** ¿Se comprometen la capacidad de competir y el buen funcionamiento de la empresa con respecto a otro si no se reduce o elimina este riesgo?
- Política.** ¿Habrá que pagar un precio político por no reducir o eliminar este riesgo?
- Público.** ¿Cuánta influencia tendrán los medios de información o los grupos de interés especial en la opinión del público respecto a este riesgo?

3.8 MITIGACIÓN DE RIESGOS

3.8.1 Por lo que respecta a los riesgos, no existe una seguridad operacional absoluta. Los riesgos tienen que ser mantenidos en el nivel “más bajo prácticamente posible” (**ALARP**). Esto quiere decir que el riesgo debe equilibrarse con el tiempo, el costo y la dificultad de adoptar medidas para reducir o eliminar el riesgo.

3.8.2 Cuando se considera que la *aceptabilidad del riesgo es indeseable o inaceptable*, es necesario introducir medidas de control — cuanto más elevado el riesgo, mayor será la urgencia. El nivel de riesgo puede disminuirse sea reduciendo la gravedad de las posibles consecuencias, sea reduciendo la probabilidad de que ocurra, sea reduciendo la exposición a ese riesgo.

3.8.3 La solución óptima variará, dependiendo de las circunstancias y exigencias locales. Para formular medidas de seguridad operacional apropiadas, es necesario comprender si las defensas existentes son adecuadas.

Análisis de las defensas

3.8.4 En todo sistema de seguridad operacional, las defensas para proteger a las personas, los bienes o al medio ambiente son un componente importante. Estas defensas pueden emplearse para:

- a) reducir la probabilidad de que ocurran sucesos indeseables; y
- b) reducir la gravedad de las consecuencias relacionadas con los sucesos indeseables.

3.8.4.1 Las defensas pueden clasificarse en los dos tipos que siguen:

- a) **Defensas físicas**. Estas defensas incluyen objetos que desalientan o impiden actos inapropiados, o que mitigan las consecuencias de los sucesos (p. ej., interruptor del indicador de posición del tren de aterrizaje, cubiertas de conmutadores, equipo de protección de datos, equipo de supervivencia, advertencias y alarmas).
- b) **Defensas administrativas**. Estas defensas incluyen los procedimientos y prácticas que mitigan la probabilidad de un accidente (p. ej., reglamentos de seguridad operacional, supervisión e inspección y destreza personal).

3.8.4.2 Antes de seleccionar las estrategias de mitigación de riesgos apropiadas es importante comprender *por qué* el sistema de defensas existente era inadecuado. Cabe hacer las preguntas siguientes:

- a) ¿Había defensas para protegerse contra esos peligros?
- b) ¿Funcionaron las defensas como estaba previsto?

- c) ¿Eran prácticas las defensas para usarlas en condiciones de trabajo reales?
- d) ¿Conocía el personal afectado los riesgos y las defensas existentes?
- e) ¿Son necesarias medidas adicionales de mitigación de riesgos?

Estrategias de mitigación de riesgos

3.8.4.3 Hay una variedad de estrategias para la mitigación de riesgos, por ejemplo:

- a) **Evitar la exposición.** Se evita la tarea, práctica, operación o actividad que entraña riesgos porque el riesgo excede los beneficios.
- b) **Reducir las pérdidas.** Se inician actividades para reducir la frecuencia de los sucesos peligrosos o la magnitud de las consecuencias.
- c) **Separar la exposición** (separación o duplicación). Se toman medidas para aislar los efectos del riesgo o crear redundancia para protegerse de los riesgos, es decir, reducir la gravedad del riesgo (por ejemplo, protegiéndose de daños indirectos en el caso de una falla de material o previendo sistemas de reserva para reducir la probabilidad de una falla total del sistema).

Evaluación de las opciones para mitigar riesgos

3.8.4.4 Cuando se evalúan las opciones para mitigar los riesgos, no todas ofrecen el mismo potencial. Es necesario evaluar la eficacia de cada opción antes de adoptar una decisión. Es importante considerar toda la gama de medidas de control posibles y también considerar la compensación entre las diversas medidas para encontrar una solución óptima. Cada opción propuesta para mitigar los riesgos debería ser examinada desde perspectivas como las que siguen:

- a) **Eficacia.** ¿Reducirá o eliminará los riesgos identificados? ¿En qué medida mitigan los riesgos otras opciones? La eficacia puede considerarse como una continuidad:
 - 1) **Nivel uno** (medidas de ingeniería). La medida de seguridad operacional **elimina** el riesgo; por ejemplo, previendo interruptores de seguridad para impedir la activación del inversor de empuje durante el vuelo.
 - 2) **Nivel dos** (medidas de control). La medida de seguridad operacional acepta el riesgo pero ajusta el sistema para **mitigar** el riesgo reduciéndolo a un nivel manejable; por ejemplo, imponiendo condiciones de utilización más restrictivas.
 - 3) **Nivel tres** (medidas de personal). Las medidas adoptadas aceptan que el peligro no se puede eliminar (nivel uno) ni controlar (nivel dos), de modo que el personal debe aprender a **enfrentarlo**; por ejemplo, agregando una advertencia, una lista de verificación revisada e instrucción adicional.

- b) **Costo-beneficio.** ¿Superan los costos los beneficios percibidos? El potencial de beneficios, ¿será proporcional a las repercusiones del cambio que se necesita?
- c) **Práctica.** ¿Es **factible** y apropiado en términos de tecnología disponible, factibilidad financiera y administrativa, legislación y reglamentos, voluntad política, etc.?
- d) **Reto.** ¿Puede la medida para mitigar el riesgo resistir el análisis crítico de todos los interesados (empleados, personal directivo, partes interesadas y administraciones de los Estados, etc.)?
- e) **Aceptación** de cada interesado. ¿Cuánta aceptación (o resistencia) puede esperarse de las partes interesadas? (Las conversaciones con los interesados durante la fase de *evaluación de riesgo* pueden indicar cuál es la opción que prefieren para mitigar los riesgos).
- f) **Cumplimiento obligatorio.** Si se ponen en vigor nuevas reglas (reglamentos, etc.), ¿se pueden hacer cumplir?
- g) **Duración.** ¿Resistirá la medida la prueba del tiempo? ¿Será de beneficio temporal o será útil a largo plazo?
- h) **Riesgos residuales.** Una vez puesta en vigor la medida para mitigar los riesgos, ¿cuáles serán los riesgos residuales con relación al peligro original? ¿Cuál es la capacidad para mitigar los riesgos residuales?
- i) **Nuevos problemas.** ¿Qué nuevos problemas, o nuevos riesgos (quizá peores), introducirá el cambio propuesto?

3.8.4.5 Obviamente, debe darse preferencia a las medidas correctivas que eliminarán completamente el riesgo. Lamentablemente, esas soluciones frecuentemente son las más caras. En el otro extremo del espectro, cuando los recursos o la voluntad de la organización son insuficientes, el problema a menudo se remite al departamento de instrucción para enseñar al personal a hacer frente a los riesgos. En esos casos, la administración quizá esté evitando decisiones difíciles delegando la responsabilidad de los riesgos a los subordinados.

3.9 COMUNICACIÓN DE RIESGOS

3.9.1 La comunicación de riesgos incluye todo intercambio de información acerca de los riesgos, es decir, toda comunicación pública o privada que informa a otros acerca de la existencia, naturaleza, forma, gravedad o aceptabilidad de los riesgos. La necesidad de información por parte de los grupos que siguen puede exigir una atención especial:

- a) La administración debe estar informada de todos los riesgos que presentan un potencial de pérdidas para la organización.
- b) Quienes están expuestos a los riesgos identificados deben estar informados de la gravedad de los mismos y de la probabilidad de que ocurran.

- c) Quienes identificaron el peligro necesitan retorno de información sobre la medida propuesta.
- d) Quienes están afectados por los cambios previstos deben estar informados tanto de los peligros como de los fundamentos de las medidas adoptadas.
- e) Las autoridades de reglamentación, los proveedores, las asociaciones de la industria, el público en general, etc., posiblemente necesiten información respecto a riesgos específicos.
- f) Los interesados pueden ayudar a quienes deben adoptar decisiones si los riesgos se comunican anticipadamente de un modo equitativo, objetivo y comprensible. Una comunicación eficaz de los riesgos (y los planes para solucionarlos) da mayor valor al proceso de gestión de riesgos.

3.9.2 El no comunicar la experiencia adquirida respecto a la seguridad operacional de un modo claro y oportuno debilitará la credibilidad de la administración para promover una cultura de seguridad operacional positiva. Para que los mensajes respecto a la seguridad operacional inspiren confianza, deben estar en consonancia con los hechos, con declaraciones anteriores de la administración y con los mensajes de otras autoridades. Estos mensajes deben estar formulados en términos que los interesados entiendan.

3.10 PROCESO DE IMPLEMENTACIÓN

3.10.1 La evaluación de riesgos debe ser desarrollado de conformidad a los siguientes procesos:

- 1) desarrollo de una completa descripción del sistema a ser evaluado y el ambiente en la cual el sistema operará;
- 2) identificación de peligros;
- 3) estimación de la probabilidad de que un peligro ocurra;
- 4) estimación de la severidad de las consecuencias de un peligro;
- 5) evaluación del riesgo;
- 6) mitigación del riesgo; y
- 7) desarrollo de los documentos de evaluación de la seguridad operacional.

3.10.2 Para cada peligro identificado, los índices de riesgos deben ser calculados en cuanto a su severidad y probabilidad de la siguiente manera:

ADJUNTO A -IDENTIFICACIÓN DE LOS PELIGROS Y MITIGACIÓN DE LOS RIESGOS

| Nº | Tipo de operación o actividad | Peligro genérico | Descripción del o de los riesgos | Medidas actuales para reducir el o los riesgos e índice de riesgo actual | Acciones ulteriores para reducir el riesgo e índice del riesgo resultante | Responsabilidad |
|----|-------------------------------|------------------|----------------------------------|--|---|-----------------|
| | | | | <i>Índice de riesgo: Tolerabilidad del riesgo</i> | <i>Índice de riesgo: Tolerabilidad del riesgo:</i> | |

ADJUNTO “B” - PROBABILIDAD DEL RIESGO

| Probabilidad del evento | | | |
|----------------------------------|---|---|----------|
| Definición Cualitativa | Significado | | Valor |
| Frecuente | 1 a 10^{-3} por cantidad de operación | <i>Probable que ocurra muchas veces (ha ocurrido frecuentemente)</i> | 5 |
| Ocasional | 10^{-3} a 10^{-5}, por cantidad de operación | <i>Probable que ocurra algunas veces (ha ocurrido infrecuentemente)</i> | 4 |
| Remoto | 10^{-5} a 10^{-7} por cantidad de operación | <i>Poco probable, pero es posible que ocurra (ocurre raramente)</i> | 3 |
| Improbable | 10^{-7} a 10^{-9} por cantidad de operación | <i>Muy improbable que ocurra (no se conoce que haya ocurrido)</i> | 2 |
| Extremadamente improbable | $<10^{-9}$ por cantidad de operación | <i>Casi inconcebible que el evento ocurra</i> | 1 |

ADJUNTO “C” - SEVERIDAD DE LOS RIESGOS

| Severidad de los eventos | | |
|-----------------------------|---|-------|
| Definiciones de la aviación | Significado | Valor |
| Catastrófico | <ul style="list-style-type: none"> • <i>Destrucción de equipamiento</i> • <i>Muertes múltiples</i> | A |
| Peligroso | <ul style="list-style-type: none"> • <i>Una reducción importante de los márgenes de seguridad, daño físico o una carga de trabajo tal que los operadores no pueden desempeñar sus tareas en forma precisa y completa.</i> • <i>Lesiones serias o muertes de una cantidad de gente.</i> • <i>Daños mayores al equipamiento.</i> | B |
| Mayor | <ul style="list-style-type: none"> • <i>Una reducción significativa de los márgenes de seguridad, una reducción en la habilidad del operador en responder a condiciones operativas adversas como resultado del incremento de la carga de trabajo, o como resultado de condiciones que impiden su eficiencia.</i> • <i>Incidente serio.</i> • <i>Lesiones a las personas.</i> | C |
| Menor | <ul style="list-style-type: none"> • <i>Interferencia.</i> • <i>Limitaciones operativas.</i> • <i>Utilización de procedimientos de emergencia.</i> • <i>Incidentes menores.</i> | D |
| Insignificante | <ul style="list-style-type: none"> • <i>Consecuencias leves</i> | E |

ADJUNTO “D” -MATRIZ DE EVALUACIÓN DEL RIESGO

| Probabilidad del riesgo | Severidad del riesgo | | | | |
|-------------------------------|----------------------|----------------|------------|------------|---------------------|
| | Catastrófico A | Peligroso B | Mayor C | Menor D | Insignificante E |
| 5 – Frecuente | 5A | 5B | 5C | 5D | 5E |
| 4 – Ocasional | 4A | 4B | 4C | 4D | 4E |
| 3 – Remoto | 3A | 3B | 3C | 3D | 3E |
| 2 – Improbable | 2A | 2B | 2C | 2D | 2E |
| 1 – Extremadamente improbable | 1A | 1B | 1C | 1D | 1E |

ADJUNTO “E”**-TOLERABILIDAD DEL RIESGO**

| Índice de evaluación del riesgo | Criterio sugerido |
|--|---|
| 5A, 5B, 5C, 4A, 4B, 3A | Inaceptable bajo las circunstancias existentes |
| 5D,5E, 4C, 3B, 3C, 2A, 2B | El control/mitigación del riesgo requiere una decisión de la dirección |
| 4D, 4E, 3D, 2C, 1A, 1B | Aceptable después de revisar la operación |
| 3E, 2D, 2E, 1C, 1D, 1E | Aceptable |

CAPITULO 4

COMPONENTES DE UN SMS

4. Generalidades

4.1 El proveedor de servicio establecerá, mantendrá y agregará a un sistema de gestión de seguridad (SMS) que sea apropiado al tamaño, naturaleza y complejidad de las operaciones autorizadas a ser realizadas acorde al certificado de operación y los peligros y riesgos de seguridad relacionado a las operaciones.

4.2 Política y objetivos de seguridad

4.2.1 Requisitos Generales

4.2.2 Un proveedor de servicio deberá definir la política de seguridad de la organización.

4.2.3 La política de seguridad deberá ser firmado por la máxima autoridad de la organización.

4.2.4 La política de seguridad deberá estar acorde con los requerimientos nacionales e internacionales, y reflejar el compromiso de la organización con respecto a la seguridad.

4.2.5 La política de seguridad deberá ser comunicado, con apoyo visible, en toda la organización.

4.2.6 La política de seguridad deberá incluir una clara declaración acerca de la provisión de los recursos humanos y financieros para su implementación.

4.2.7 La política de seguridad deberá incluir los siguientes objetivos:

4.2.7.1 compromiso para implementar un SMS;

4.2.7.2 compromiso para la mejora continua del nivel de seguridad;

4.2.7.3 compromiso para la gestión del riesgo de la seguridad;

4.2.7.4 compromiso para alentar a los empleados para reportar los temas de seguridad;

4.2.7.5 establecer claros estándares para un desempeño aceptable; y

4.2.7.6 identificación de las responsabilidades del gerenciamiento y de los empleados con respecto al desempeño de la seguridad.

4.3 Estructura y responsabilidad organizacional

4.3.1 Un proveedor de servicio deberá identificar el Ejecutivo Responsable (Accountable Executive) que asuma la responsabilidad por el servicio del proveedor para el cumplimiento de los requerimientos de este reglamento y notificar a la Autoridad de Aviación Civil el nombre de la persona.

4.3.2 El Ejecutivo Responsable (Accountant Executive) deberá ser la persona responsable y punto focal para el desarrollo y mantenimiento del sistema de gestión de la seguridad (SMS).

4.3.3 El Ejecutivo Responsable deberá:

4.3.3.1 tener un control total de los recursos humanos requeridos para la operación autorizada de conformidad con el certificado otorgado para las operaciones.

- 4.3.3.2 tener un control total de los recursos financieros requeridos para las operaciones autorizadas de conformidad con el certificado otorgado para las operaciones.
- 4.3.3.3 tener plena autoridad sobre las operaciones autorizadas de conformidad al certificado otorgado para las operaciones.
- 4.3.3.4 tener directa responsabilidad para conducir los asuntos de la organización; y
- 4.3.3.5 plena responsabilidad por todos los asuntos de seguridad.
- 4.3.4 Un proveedor de servicio establecerá una estructura de seguridad necesaria para la implementación y mantenimiento del SMS de la organización.
- 4.3.5 Un proveedor de servicio identificará las responsabilidades de todos los integrantes de las gerencias, además de otras responsabilidades.
- 4.3.6 Las posiciones relacionadas con la seguridad, responsabilidades y autoridades deben ser definidos, documentados y comunicados a toda la organización.
- 4.3.7 Un proveedor de servicio identificará un gerente de Seguridad para ser el miembro de la gestión quien será el responsable individual y punto focal para la implementación y mantenimiento de un SMS efectivo.
- 4.3.8 El gerente de Seguridad deberá:
 - 4.3.8.1 asegurar los procesos requeridos para que un SMS sea establecido, implementado y mantenido;
 - 4.3.8.4 reportar al Ejecutivo Responsable respecto al desarrollo del SMS y cualquier necesidad de mejoramiento;
 - 4.3.8.4 asegurar la promoción de la seguridad en toda la organización.

4.4 **Plan para la implementación de un SMS**

- 4.4.1 Un proveedor de servicio deberá desarrollar y mantener un plan de implementación de un sistema de gestión de la seguridad (SMS).
- 4.4.4 El plan de implementación debe definir la aproximación que la organización adoptará para la gestión de seguridad de una manera que se cumpla con las necesidades de seguridad de la organización.
- 4.4.4 El plan de implementación SMS deberá incluir lo siguiente:
 - 4.4.4.1 Política y objetivos de seguridad;
 - 4.4.4.2 Responsabilidad y compromiso de seguridad;
 - 4.4.4.3 Descripción del sistema;
 - 4.4.4.4 Análisis del faltante (Gap analysis);
 - 4.4.4.5 Componentes del SMS;
 - 4.4.4.6 Medición de la performance de seguridad;
 - 4.4.4.7 Política de reporte de seguridad;

- 4.4.4.8 Comunicación de seguridad
- 4.4.4.9 Medios para involucramiento de los empleados
- 4.4.4.10 Revisión por la Dirección de la performance de la seguridad
- 4.4.5 El plan de implementación de un SMS deberá ser apoyada por la máxima autoridad de la organización.
- 4.4.6 Un proveedor de servicio, como parte del desarrollo de un plan para implementación de un SMS, deberá contemplar la descripción del sistema.
- 4.4.7 La descripción del sistema deberá incluir lo siguiente:
 - 4.4.7.1 Las interacciones del sistema con otros sistemas del transporte aéreo;
 - 4.4.7.4 Las funciones del sistema;
 - 4.4.7.4 Consideraciones sobre factores humanos requeridos para la operación del sistema;
 - 4.4.7.4 Los componentes del hardware del sistema;
 - 4.4.7.5 Los componentes del software del sistema;
 - 4.4.7.4 Procedimientos relacionados que definen las guías para la operación y uso del sistema;
 - 4.4.7.4 Entorno operacional;
 - 4.4.7.8 Productos o servicios contratados o adquiridos.

4.5 Coordinación del plan de respuesta a la emergencia

- 4.5.1 Un proveedor de servicios deberá desarrollar y mantener, o coordinar, según corresponda, un plan de respuesta a la emergencia (PRE) que asegure:
 - 4.5.1.1 Transición ordenada y eficiente desde una situación normal a una operación de emergencia;
 - 4.5.1.4 Designación de una autoridad para emergencia;
 - 4.5.1.4 Asignación de responsabilidades para emergencia;
 - 4.5.1.4 Coordinación de esfuerzos para manejo de emergencia; y
 - 4.5.1.5 Segura continuación de las operaciones, o retornar a la operación normal tan pronto como sea posible.

4.6 Documentación

- 4.6.1 Un proveedor de servicio deberá desarrollar y mantener una documentación sobre SMS, en papel o formato electrónico, para describir lo siguiente:
 - 4.6.1.1 Políticas de seguridad;
 - 4.6.1.4 Objetivos de seguridad;
 - 4.6.1.4 Requisitos, procedimientos y procesos del SMS;

- 4.6.1.4 Responsabilidades y autoridades para procedimientos y procesos; y
- 4.6.1.5 Producciones del SMS
- 4.6.4 Un proveedor de servicio deberá, como parte de la documentación SMS, desarrollar y mantener un documento de gestión de la seguridad, para comunicar el interés de la seguridad en toda la organización.
- 4.6.4 El Documento de Gestión de la Seguridad (MGS) documentará todos los aspectos de un SMS; y su contenido incluirá lo siguiente:
 - 4.6.4.1 Alcance del sistema de gestión de la seguridad;
 - 4.6.4.4 Política y objetivos de seguridad;
 - 4.6.4.4 Responsabilidades sobre seguridad;
 - 4.6.4.4 Personal clave de seguridad;
 - 4.6.4.5 Procedimiento de control de documentos;
 - 4.6.4.4 Plan de respuesta a emergencias;
 - 4.6.4.4 Esquema para identificación de peligros y gestión de riesgos;
 - 4.6.4.8 Vigilancia de la performance de la seguridad;
 - 4.6.4.9 Gestión del cambio;
 - 4.6.4.10 Auditoria de la seguridad;
 - 4.6.4.11 Promoción de la seguridad

4.7 Gestión del riesgo de la seguridad

4.7.1 Generalidades

- 4.7.1.1 Un proveedor de servicio deberá desarrollar y mantener un sistema de recolección y procesamiento de datos de seguridad (SRPDS) que brinde la identificación y análisis de peligros, evaluación y control de riesgos.
- 4.7.1.2 Un sistema de recolección y procesamiento de datos (SRPDS) de un proveedor de servicio deberá incluir métodos reactivos, proactivos y predictivos para la recolección de datos de seguridad.

4.7.2 Identificación del peligro

- 4.7.2.1 Un proveedor de servicio desarrollará y mantendrá un medio formal de recolección, registro, acción y generación de retroalimentación cerca de los peligros en las operaciones, que combinen métodos reactivos, proactivos y predictivos de recolección de datos de seguridad.
- 4.7.2.2 El proceso de identificación de los peligros incluirá los siguientes pasos:
 - 1) reportes de peligros, incidentes y temas de seguridad;
 - 2) recolección y almacenamiento de datos de seguridad;
 - 3) análisis de los datos de seguridad; y

4) distribución de la información sobre la seguridad obtenida de los datos de seguridad.

4.8 **Gestión de riesgos**

4.8.1 Un proveedor de servicio deberá desarrollar y mantener formalmente un proceso de gestión de riesgo que asegure el análisis, evaluación y control de riesgos en un nivel aceptable.

4.8.2 Los riesgos en cada peligro identificado a través de los procesos de identificación de peligros descrito en el numeral 4.4 de este documento debe ser analizado en términos de probabilidad y severidad del incidente, y evaluado su tolerabilidad.

4.8.3 La organización definirá con la autoridad aeronáutica los niveles de gestión para tomar decisiones sobre la tolerabilidad del riesgo de seguridad.

4.8.4 La organización definirá los controles de seguridad para cada riesgo evaluado como intolerable.

*** **

CAPÍTULO 5. ASEGURAMIENTO DE LA SEGURIDAD

5.1 Generalidades

- 5.1.1 Un proveedor de servicio desarrollará y mantendrá procesos de aseguramiento de la seguridad para asegurar que los controles de riesgos de seguridad desarrollados como parte de las actividades de identificación de los peligros y gestión de riesgos, mencionado en el numeral 4, logran cumplir con sus objetivos propuestos.
- 5.1.4 Los procesos de aseguramiento de seguridad serán aplicados a un SMS si las actividades y/u operaciones son cumplidas internamente o externamente.
- 5.1.4 El procedimiento de reporte de seguridad establecerá las condiciones de inmunidad de acciones disciplinarias que serían consideradas.

5.2 Monitoreo y medición de la performance de la seguridad

- 5.2.1 Un proveedor de servicio, como parte de las actividades del aseguramiento de la seguridad de un SMS, desarrollará y mantendrá los medios necesarios para verificar la performance de la seguridad de la Organización en comparación con las políticas y objetivos de seguridad aprobados, y validar la efectividad de los controles de riesgos de seguridad implementados.
- 5.2.2 Los medios de medición y vigilancia de la performance de seguridad incluirán lo siguiente:
 - 1. Reporte de seguridad;
 - 2. Auditoria de seguridad;
 - 3. Relevamiento de seguridad;
 - 4. Revisión de seguridad;
 - 5. Estudios de seguridad;
 - 6. Investigaciones sobre seguridad interna.

5.3 Gestión del cambio

- 5.3.1 Un proveedor de servicio, como parte de las actividades de aseguramiento de la seguridad del SMS; deberá desarrollar y mantener un proceso formal para gestión del cambio.
- 5.3.2 El proceso formal para la gestión del cambio deberá:
 - 5.3.2.1 identificar los cambios dentro de la Organización que podría afectar los procesos y servicios establecidos;
 - 5.3.2.2 describir los arreglos que asegure la performance de seguridad antes de implementar los cambios;
 - 5.3.2.3 eliminar o modificar los controles de riesgos de seguridad que no son requeridos debido a los cambios en el entorno operacional.

5.4 Mejora continua del SMS

- 5.4.1 Un proveedor de servicio, como parte de las actividades del aseguramiento de la seguridad del SMS, desarrollará y mantendrá procesos formales para identificar las

causas de un performance por debajo de nivel deseado del SMS, determinar las implicancias en sus operaciones, y eliminar tales causas a fin de asegurar la mejora continua del SMS.

5.4.2 La mejora continua del SMS de un proveedor de servicio incluirá:

5.4.2.1 evaluaciones preactiva y reactiva de facilidades, equipo, documentación y procedimientos, para verificar la efectividad de las estrategias para el control de riesgos de seguridad; y

5.4.2.2 evaluación preactiva de la performance individual para verificar el cumplimiento de las responsabilidades de seguridad.

*** **

CAPÍTULO 6. PROMOCIÓN DE LA SEGURIDAD

6.1 Generalidades

6.1.1 Los proveedores de servicios desarrollarán y mantendrán formalmente actividades de comunicación y entrenamiento sobre seguridad a fin de crear un ambiente en donde los objetivos de seguridad de la Organización puedan ser logrados.

6.2 Entrenamiento de Seguridad

6.2.1 Un proveedor de servicio, como parte de sus actividades de la promoción de la seguridad, desarrollará y mantendrá un programa de entrenamiento de la seguridad a fin de asegurar que el personal este entrenado y sea competente para asumir responsabilidades del SMS.

6.2.2 El factor principal del entrenamiento de la seguridad deberá ser apropiado a cada persona involucrada en el SMS.

6.2.3 El ejecutivo responsable (The Accountable Executive) recibirá entrenamiento de conocimiento sobre seguridad, considerando:

9.2.3.1 Responsabilidad y compromiso SMS;

9.2.3.4 Política de seguridad;

9.2.3.4 Objetivos del SMS; y

9.2.3.4 Aseguramiento de la seguridad.

6.3 Comunicación de Seguridad

6.3.1 Un proveedor de servicio, como parte de sus actividades de la promoción de la seguridad, deberá desarrollar y mantener medios formales de comunicación de la seguridad para:

6.3.1.1 asegurar que todo el personal tenga pleno conocimiento del SMS;

6.3.1.4 transmitir información crítica de seguridad;

6.3.1.4 explicar porqué se toman determinadas acciones de seguridad; y

6.3.1.4 explicar porqué los procedimientos de seguridad son incluidos o modificados.

6.3.2 Los medios formales de comunicación de seguridad debería incluir:

9.3.2.1 Políticas y procedimientos de seguridad;

9.3.2.4 Carta de noticias; y

9.3.2.4 Boletines

*** **

CAPÍTULO 7.
POLÍTICA DE CALIDAD

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

*** **

CAPÍTULO 8. IMPLEMENTACIÓN DEL SMS

- 8.1 Este documento propone una implementación SMS por fases de parte de un proveedor de servicios, que comprende 4 fases.
- 8.2 **La Fase 1:** proveerá una guía de cómo serán cumplidos los requerimientos SMS e integrado a las actividades de trabajo de la organización; así como un marco de responsabilidades para la implementación del SMS:
- 8.2.1 identificar al ejecutivo responsable y las responsabilidades de los gerentes;
 - 8.2.2 identificar la persona (o grupo de planificación) responsable de la organización por la implementación del SMS;
 - 8.2.3 describir el sistema (Operador Aéreo, proveedor de servicio ATC, organización de mantenimiento aprobado, operador de aeródromo certificado);
 - 8.2.4 conducir análisis del faltante (Gap Analysis) de los recursos existentes de la organización comparado con los requerimientos nacionales e internacionales para establecer un SMS;
 - 8.2.5 desarrollar un plan de implementación SMS que describa como la organización implementará el SMS de conformidad a los requerimientos nacionales básicos y las normas internacionales, la descripción del sistema y los resultados del análisis del faltante;
 - 8.2.6 desarrollar documentaciones relevantes a la política y objetivos de la seguridad; y
 - 8.2.7 desarrollar y establecer medios para la comunicación de seguridad.
- 8.3 **La Fase 2:** debería llevar a la práctica los elementos del plan de implementación SMS que se refieren al proceso reactivo de la gestión de riesgo de la seguridad:
- 8.3.1 investigación y análisis;
 - 8.3.2 identificación de peligros y gestión de riesgos.
 - 8.3.3 entrenamiento relacionado a:
 - 8.3.3.1 componentes del plan de implementación SMS; y
 - 8.3.3.2 gestión de riesgos de seguridad (procesos reactivos)
 - 8.3.4 documentaciones relacionadas a:
 - 8.3.4.1 componentes del plan implementación de SMS;
 - 8.3.4.2 gestión de riesgos de seguridad (procesos reactivos).
- 8.4 **La Fase 3:** pondrá en práctica los elementos del plan de implementación SMS que se refieren al proceso proactivo de la gestión de riesgos de la seguridad:
- 8.4.1 investigación y análisis;
 - 8.4.2 identificación de peligros y gestión de riesgos;

- 8.4.3 entrenamiento relacionado a:
 - 8.4.3.1 componentes del plan de implementación SMS; y
 - 8.4.3.2 gestión de riesgos de seguridad (procesos preactivos).

- 8.4.4 documentaciones relacionadas a:
 - 11.4.4.1 componentes del plan de implementación SMS; y
 - 11.4.4.2 gestión de riesgos de seguridad (procesos preactivos).

- 8.5 La Fase 4 pondrá en práctica el aseguramiento de la seguridad operacional:
 - 8.5.1 desarrollo del nivel aceptable de seguridad;
 - 8.5.2 desarrollo de indicadores y metas de seguridad;
 - 8.5.3 mejora continua del SMS;
 - 8.5.4 entrenamiento relativo al aseguramiento de la seguridad operacional; y
 - 8.5.5 documentaciones relativos al aseguramiento de la seguridad operacional.

*** **

CAPÍTULO 9

9.1 PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

15.1.1 Un programa permanente de promoción de la seguridad operacional asegurará que los empleados se beneficien de la experiencia adquirida en seguridad operacional y continúen comprendiendo el SMS de la organización. La promoción de la seguridad operacional está estrechamente vinculada con la instrucción y la difusión de información sobre seguridad operacional: se refiere a aquellas actividades que la organización lleva a cabo a fin de asegurar que el personal comprenda por qué se introducen procedimientos de gestión de la seguridad operacional, qué significa gestión de la seguridad operacional, por qué se adoptan medidas particulares de seguridad operacional, etc. La promoción de la seguridad operacional es el mecanismo por medio del cual los conocimientos obtenidos en las investigaciones de sucesos y otras actividades relacionadas con la seguridad operacional se ponen a disposición de todo el personal afectado. También es un medio para fomentar el desarrollo de una cultura de seguridad operacional positiva y asegurar que, una vez establecida, dicha cultura se mantenga.

9.1.2 La publicación de políticas, procedimientos y boletines de seguridad operacional por sí solas no producirá necesariamente el desarrollo de una cultura de seguridad operacional positiva. Si bien es importante que los miembros del personal estén bien informados, también es importante que vean pruebas de la dedicación de la administración a la seguridad operacional. Por lo tanto, las actitudes y los actos de la administración serán un factor importante en la promoción de prácticas de trabajo seguras y en el desarrollo de una cultura de seguridad operacional positiva.

9.1.3 Las actividades de promoción de la seguridad operacional son particularmente importantes durante las etapas iniciales de la implantación de un SMS. Sin embargo, la promoción de la seguridad operacional también desempeña un papel importante en el mantenimiento de la seguridad operacional, dado que es el medio por el cual se tiene conocimiento de los problemas de seguridad operacional dentro de la organización. Estos problemas pueden corregirse por medio de programas de instrucción para el personal o mediante mecanismos menos formales.

9.1.4 A fin de proponer soluciones para identificar peligros, el personal debe tener conciencia de aquellos que ya se han identificado y de las medidas correctivas que se han implantado. Por lo tanto, las actividades de promoción de la seguridad operacional y los programas de instrucción deberían tratar de las razones que justifican la introducción de nuevos procedimientos. Cuando los conocimientos adquiridos también sean importantes para otros Estados, explotadores o proveedores de servicios, se debería considerar la posibilidad de dar a la información una difusión más amplia.

Métodos de promoción

9.1.5 Si un mensaje de seguridad operacional debe ser aprendido y retenido, quien lo recibe debe estar, en primer lugar, positivamente motivado. A menos que esto sea así, se desperdiciarán muchos esfuerzos bien intencionados. La propaganda que meramente exhorta a

la gente a evitar cometer errores, tener más cuidado, etc. es ineficaz porque no contiene nada concreto con lo que las personas puedan ver una relación. A veces, se ha comparado este enfoque con las pegatinas en los parabrisas de los automóviles.

9.1.6 Los temas de seguridad operacional para campañas de promoción se deberían seleccionar teniendo en cuenta su potencial para controlar y reducir las pérdidas. Por lo tanto, la selección debería basarse en la experiencia de accidentes o cuasi colisiones pasadas, asuntos identificados mediante análisis de peligros y observaciones de auditorías de la seguridad operacional. Además, se debería alentar a los empleados a que presenten sugerencias para campañas de promoción.

9.1.7 Todos los métodos de difusión — orales y escritos, carteles, vídeos, presentaciones de diapositivas, etc. — para ser eficaces requieren talento, habilidad y experiencia. Una difusión deficiente puede ser peor que ninguna. Por consiguiente, es aconsejable el aporte de profesionales cuando se difunde información para una audiencia crítica.

9.1.8 Una vez que se ha tomado la decisión de difundir información de seguridad operacional, se deberían tener en consideración varios factores importantes, entre ellos:

- a) *La audiencia.* El mensaje debe estar expresado en términos y en un lenguaje que reflejen el conocimiento de la audiencia a la que está dirigido.
- b) *La respuesta.* ¿Qué se espera lograr?
- c) *El medio.* Si bien los textos impresos pueden ser el medio más fácil y barato, probablemente sea el menos eficaz.
- d) *El estilo de presentación.* Esto puede suponer el uso de humor, gráficos, fotografías y otras técnicas para atraer la atención.

9.1.9 Idealmente, un programa de promoción de la seguridad operacional se basará en varios métodos de comunicación diferentes. Para este fin, generalmente se emplean los métodos indicados seguidamente:

- a) *Presentaciones orales.* Quizá este sea el método más eficaz, especialmente si se complementa con una presentación visual; sin embargo, es el más caro porque reunir la audiencia, las ayudas y el equipo requiere tiempo y esfuerzo. Algunos Estados emplean especialistas en seguridad operacional que visitan las organizaciones y dan conferencias y seminarios.
- b) *Textos escritos.* Este es el método más popular porque es rápido y económico. Sin embargo, la proliferación de textos impresos tiende a saturar nuestra capacidad para absorberlos. Los textos impresos de promoción de la seguridad operacional compiten con cantidades considerables de otros textos impresos para atraer nuestra atención y en la era digital resulta aún más difícil lograrlo. Sería conveniente la orientación o asistencia profesional para asegurarse de que el mensaje se transmite de modo eficaz.

c) *Vídeos*. Los vídeos ofrecen las ventajas de imágenes dinámicas y sonidos para reforzar eficientemente determinados mensajes de seguridad operacional. Sin embargo, los vídeos presentan dos limitaciones importantes: gastos de producción y necesidad de equipo especial para presentarlos. No obstante, los vídeos pueden ser eficaces para difundir determinados mensajes a través de una estructura orgánica muy dispersa, con lo que se reduce al mínimo la necesidad de que el personal viaje. Hoy en día, los vídeos pueden distribuirse electrónicamente mediante discos compactos (CD) y muchos de ellos pueden obtenerse en el mercado y aparecen en listas de los sitios Internet sobre seguridad operacional.

d) *Presentaciones*. Cuando un mensaje debe aparecer en una gran reunión, como una conferencia, un kiosco de presentación es una buena técnica de autoinformación. Se necesitan imaginación y experiencia en presentaciones para hacer llegar no sólo el mensaje si no también la imagen de la organización. Los inconvenientes de una presentación son el gasto y, a menos que esté atendido por una persona, el hecho de que en cierta medida un kiosco resulta estático y poco interesante. Es necesario contar con orientación o asistencia profesional para asegurarse de que el mensaje se transmite de un modo eficaz.

e) *Sitios Web*. Muchos de los métodos de promoción mencionados antes pueden ser poco atractivos para las generaciones que han crecido con computadoras personales, juegos digitales y acceso a la Internet. El enorme crecimiento de la Internet ofrece un gran potencial para mejorar la promoción de la seguridad operacional. Aun las pequeñas organizaciones pueden establecer y mantener un sitio Web para difundir información sobre seguridad operacional.

f) *Conferencias, simposios, seminarios, talleres, etc.* Estas reuniones proporcionan foros ideales para fomentar la conciencia de la seguridad operacional. La organización, la autoridad de reglamentación, las asociaciones del sector, los institutos de seguridad operacional, las universidades, los fabricantes, etc. pueden patrocinar este tipo de reuniones. El valor de estos foros a menudo va más allá de la promoción de la seguridad operacional porque ayudan a establecer relaciones con otras personas que trabajan en el campo de la seguridad operacional.

9.1.10 Cuando se prevé organizar un programa de promoción importante, es prudente pedir asesoramiento a especialistas en comunicaciones experimentados y a representantes bien informados de los grupos a quienes está dirigida la información.

*** **

CAPÍTULO 10.

GESTIÓN DE LA INFORMACIÓN DE SEGURIDAD OPERACIONAL

10.1 Generalidades

10.1.1 La calidad de los datos es vital para la gestión de la seguridad operacional. Una gestión eficaz de la seguridad operacional depende de los datos. La información recogida de informes operacionales y de mantenimiento, informes de seguridad operacional, auditorias, evaluaciones de métodos de trabajo, etc. generan muchos datos, aunque no todos son pertinentes para la gestión de la seguridad operacional. Se recoge y almacena tanta información relacionada con la seguridad operacional que existe el riesgo de abrumar a los administradores responsables, con lo que se compromete la utilidad de los datos. La buena gestión de las bases de datos de la organización es fundamental para las funciones de una gestión eficaz de la seguridad operacional (tales como observación de tendencias, evaluación de riesgos, análisis de costo-beneficio e investigación de sucesos).

10.1.2 El argumento de que el cambio es necesario para la seguridad operacional debe basarse en el análisis de datos consolidados y de calidad. El establecimiento y mantenimiento de una base de datos de seguridad operacional crea un instrumento indispensable para los administradores de la organización, los jefes de seguridad operacional y las autoridades de reglamentación que vigilan los aspectos de seguridad operacional del sistema. Lamentablemente, los datos de muchas bases carecen de la calidad necesaria para ser fiables y tenerlos en cuenta para ajustar las prioridades en materia de seguridad operacional, evaluar la eficacia de las medidas de mitigación de riesgos e iniciar investigaciones relacionadas con la seguridad operacional. Es necesario comprender los datos, las bases de datos y el uso de los instrumentos apropiados para poder tomar decisiones válidas a tiempo.

10.1.3 Cada vez con más frecuencia, se usan programas de computadora para facilitar las tareas de registro, almacenamiento, análisis y presentación de información de seguridad operacional. Ahora es posible y fácil realizar análisis complicados con la información de las bases de datos. Actualmente existe en el mercado una amplia gama de bases de datos para computadoras personales, de costos relativamente bajos y capaces de responder a las necesidades de una organización en materia de gestión de datos. Estos sistemas independientes presentan la ventaja de no emplear el sistema de la computadora central de la organización, con lo que aumenta la seguridad de los datos.

10.2 Bases de datos

10.2.1 Los proveedores de servicios deberán establecer una base de datos sobre accidentes e incidentes para facilitar el análisis efectivo de la información sobre seguridad operacional, incluida la proveniente de sus sistemas de notificación de incidentes. Los sistemas de bases de datos deberían emplear formatos normalizados para facilitar el intercambio de datos.

“Las bases de datos contienen mucha información sobre la seguridad operacional; sin embargo, sin los instrumentos y la capacidad necesaria para tener acceso a los datos y analizarlos, esa información es inútil.”

*** **