CAPITULO PRIMERO

I. SEGURIDAD OPERACIONAL EN MANTENIMIENTO

A. GENERALIDADES

La Seguridad Operacional es una condición en la que el riesgo de lesiones o daños está limitado a un nivel aceptable. Los peligros que crean riesgo pueden llegar a ser evidentes después de una perturbación de la seguridad operacional, como en el caso de un accidente o incidente, que pueden ser identificados preventivamente por medio de programas formales de gestión de la Seguridad Operacional antes de que ocurra realmente un suceso.

Una vez reconocido un peligro para la Seguridad Operacional, se pueden valorar los riesgos concernientes con el mismo. Con una comprensión clara de la naturaleza de los riesgos, se puede determinar el grado de “aceptabilidad” de los mismos; respecto a los que no son aceptables.

El Sistema de 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, el medio ambiente y la comunidad.

B. CONCEPTO DE SEGURIDAD OPERACIONAL

El Sistema de Administración de Seguridad (SMS), es un Sistema que sirve para garantizar la operación segura de la aeronave mediante una gestión de riesgo de seguridad operacional eficaz. El estado donde la posibilidad de dañar a las personas o las propiedades se reduce y mantiene mismo nivel o debajo de un nivel aceptable mediante el proceso seguido de identificación de peligros y gestión de riesgo de la seguridad operacional, pero hay que considerar:

- La eliminación de todos los accidentes e incidentes serios
- Las fallas seguirán ocurriendo, a pesar de los más logrados esfuerzos de prevención.

- No hay actividad humana, o sistema diseñado por el ser humano, que este totalmente libre de riesgos y errores.
- Los riesgos y errores son aceptables en un sistema implícitamente seguro **siempre que estén bajo control**
- Actitud de los empleados con respecto a actos y condiciones inseguras (que reflejan una cultura “segura” de la empresa).
- Grado en que los riesgos inherentes a la aviación son “aceptables”.
- Proceso de identificación de peligros y gestión de riesgos.

Ninguna actividad o sistema hecho por el hombre puede garantizar que es absolutamente seguro, es decir, libre de riesgos. Ocurrirán fallas y errores a pesar de los mejores esfuerzos para evitarlos. Por lo tanto:

1. Seguridad Operacional

La seguridad Operacional es cero accidentes o incidentes graves de aviación, libre de peligros es decir libre de aquellos factores que causan o que tienen el potencial de causar daño, actitudes de los empleados de las organizaciones de aviación, frente a actos o condiciones de inseguridad, prevención de errores, cumplimiento de los reglamentos.

La finalidad del Sistema de Administración de Seguridad (SMS), buscar contener o mitigar proactivamente los riesgos antes de que produzcan accidentes e incidentes de aviación

En el momento en que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel admisible, o por debajo del mismo, por medio de una causa continuo de identificación de peligros y gestión de riesgos.

C. ENFOQUES RESPECTO A LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

Desde el 1 de enero del 2009, los estados exigirán, como parte de su programa de seguridad, que cada organización de mantenimiento aplique un Sistema de Administración de Seguridad aceptable por el estado.

Por el aumento de las actividades de la aviación, los métodos tradicionales para reducir los riesgos a un nivel aceptable no son suficientes. Por consiguiente, están apareciendo nuevos métodos para comprender y llevar a cabo la gestión de seguridad operacional la cual puede considerarse desde dos puntos de vista desiguales:

1. Enfoque Tradicional

Históricamente, la seguridad operacional de la aviación se concentraba en el cumplimiento de requisitos reglamentarios cada vez más complejos. Este enfoque funcionó bien hasta fines del decenio de 1970, cuando la tasa de accidentes acusó un aumento pronunciado. Los accidentes continuaban ocurriendo a pesar de todos los reglamentos.

2. Enfoque Moderno

A fin de mantener los riesgos para la seguridad operacional en un nivel aceptable con niveles de actividad más elevados, las prácticas modernas de gestión de la seguridad operacional están **dejando** de actuar por reacción para actuar de un modo más **preventivo** con un marco sólido de leyes y requisitos reglamentarios basados en las normativas de la OACI, Cabe destacar que este enfoque complementa o se agrega a las obligaciones de los Estados y otras organizaciones de cumplir los manuales de la OACI y los reglamentos propios.

D. RESPONSABILIDAD ESPECIAL DE LA ADMINISTRACIÓN

La responsabilidad de la seguridad operacional y de la gestión eficaz de la seguridad operacional la comparten las organizaciones e instituciones de un amplio espectro que incluye organizaciones internacionales, autoridades de reglamentación de la aviación civil y militar de los Estados, propietarios y explotadores de aeronaves, proveedores de servicios para los servicios de navegación aérea y aeródromos, grandes fabricantes de aeronaves y grupos motores, organismos de mantenimiento, asociaciones industriales y profesionales, e instituciones de enseñanza e instrucción en aeronáutica.

CAPITULO SEGUNDO

I. COMPRENSIÓN DE LA SEGURIDAD OPERACIONAL

Para comprender la seguridad operacional analizaremos algunos conceptos.

A. CONCEPTO DE RIESGO

La seguridad operacional absoluta no existe, se define en términos de riesgo. Antes de determinar si un sistema es seguro o no, primero es necesario determinar qué es un nivel de riesgo aceptable para el sistema.

El riesgo tiene dos dimensiones: la **probabilidad** de que el hecho peligroso se produzca y la **gravedad** de sus posibles consecuencias.

Los riesgos se perciben según las tres grandes categorías que siguen:

- Riesgos que son tan elevados que son inaceptables.
- Riesgos que son tan bajos que son aceptables.
- Riesgos que están entre lo aceptable e inaceptable.

Si el riesgo no satisface los criterios de aceptabilidad predeterminados, siempre se puede procurar reducirlo a un nivel que sea aceptable empleando procedimientos apropiados para mitigarlo. Si el riesgo no se puede reducir para llevarlo a un nivel aceptable o más bajo, se podrá considerar que es tolerable si:

- El riesgo es menor que el límite inaceptable predeterminado.
- El riesgo ha sido reducido al nivel más bajo prácticamente posible; y
- Los beneficios del sistema o de los cambios propuestos son suficientes como para justificar que se acepte el riesgo.

Nota.- Antes de clasificar un riesgo como tolerable, deben satisfacerse los tres criterios anteriores.

B. ACCIDENTES E INCIDENTES

Un **accidente** es un suceso durante la utilización de una aeronave debido al cual:

- Una persona sufre lesiones mortales o graves;
- La aeronave sufre daños considerables que significan roturas estructurales o que exigen una reparación importante; o
- La aeronave desaparece o no se puede llegar a ella.

Un **incidente** es un suceso relacionado con la utilización de una aeronave, distinto a un accidente, y que afecta o que puede afectar a la seguridad de las operaciones. Un incidente grave es un incidente en el que intervienen circunstancias que indican que casi ocurrió un accidente.

En las definiciones de la OACI se emplea el término “suceso” para indicar un accidente y un incidente. Desde la perspectiva de la gestión de la seguridad operacional, es peligroso concentrarse en la diferencia entre accidentes e incidentes empleando definiciones que pueden ser arbitrarias y limitativas.

Cada día ocurren muchos incidentes que pueden ser notificados, o no, a la autoridad encargada de las investigaciones, pero que casi llegan a ser accidentes y que a menudo ponen de manifiesto riesgos importantes. Puesto que no hay lesionados o los daños son pequeños o inexistentes, quizá esos incidentes no sean objeto de investigación. Esto es lamentable, porque la investigación de un incidente puede producir mejores resultados para la identificación de peligros que la investigación de un accidente. La diferencia entre un accidente y un incidente puede ser simplemente un elemento de causalidad.

C. CAUSAS DE LOS ACCIDENTES

La evidencia más clara de una perturbación grave de la seguridad operacional de un sistema es un accidente. Debido a que los accidentes y los

incidentes están estrechamente relacionados es fundamental comprender las causas que los originan para reducir la probabilidad de que ocurran.

1. Enfoque Tradicional de Causalidad

Después de un gran accidente, cabe hacer las siguientes preguntas:

- ¿Cómo y por qué personal competente cometió los errores necesarios para que sucediera el accidente?
- ¿Podría volver a ocurrir algo como esto?

Tradicionalmente, los investigadores han examinado una cadena de sucesos o circunstancias que en definitiva llevaron a alguien a hacer algo improcedente que provocó el accidente. Este comportamiento improcedente puede haber sido un error de juicio (como una desviación de los SOP), un error debido a una falta de atención o una violación deliberada de las normas.

Con la dirección tradicional, la indagación se concentraba más a menudo en encontrar al culpable del accidente (y castigarlo). En el mejor de los casos, las actividades de gestión de la seguridad operacional se concentraban en encontrar las formas de reducir el riesgo de cometer actos inseguros. Sin embargo, parecería que los errores o violaciones que provocan accidentes ocurren aleatoriamente. Al no haber un modelo que seguir, esas actividades de gestión de la seguridad operacional para reducir o eliminar sucesos aleatorios pueden ser inútiles.

Las observaciones de datos de accidentes frecuentemente revelan que la situación anterior al accidente estaba “madura para un accidente”. Las personas a quienes preocupa la seguridad operacional pueden haber estado diciendo que era sólo una cuestión de tiempo antes de que estas circunstancias condujeran a un accidente. Cuando el accidente ocurre, a menudo se encuentra que miembros del personal que gozan de buena salud, calificados, experimentados, motivados y

bien equipados cometieron errores que produjeron el accidente. Ellos (y sus colegas) pueden haber cometido estos errores o haber empleado prácticas inseguras muchas veces antes, sin que hubiera consecuencias perjudiciales. Además, algunas de las condiciones inseguras en las que operaban pueden haber existido durante años, sin que tampoco causaran un accidente. En otras palabras, hay un elemento de causalidad.

Algunas veces estas condiciones inseguras eran la consecuencia de decisiones de la administración; ésta reconocía los riesgos, pero otras prioridades requerían hacer concesiones. En realidad, el personal de operaciones a menudo trabaja en un contexto definido por factores de organización y de gestión que están fuera de su control. Estos empleados son sólo una parte de un sistema más grande.

Para tener éxito, los sistemas de gestión de la seguridad operacional (SMS) necesitan que la causalidad de los accidentes se entienda de otro modo, de un modo que depende de examinar el contexto total (es decir, el sistema) en que trabaja la gente.

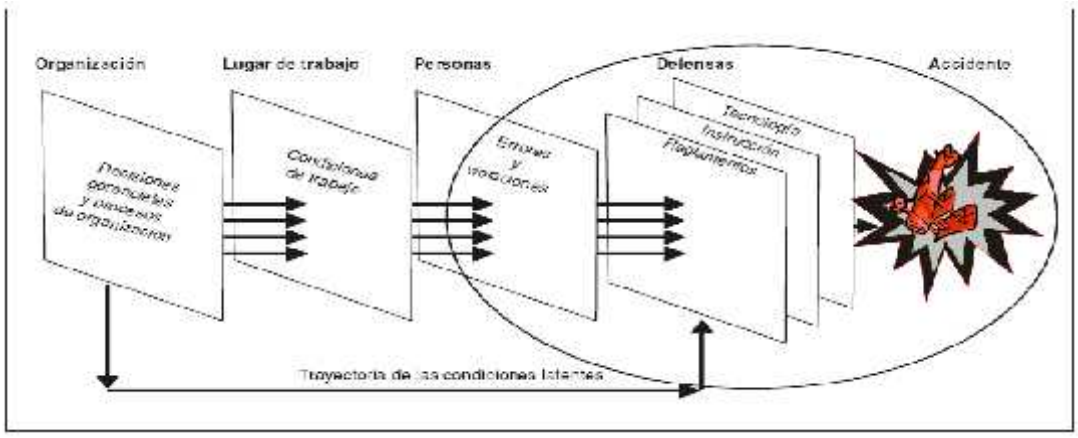
2. Enfoque moderno de causalidad

De conformidad con el pensamiento moderno, los accidentes se producen cuando cierto número de factores permiten que ocurran, cada uno es necesario, pero por sí mismo no es suficiente para quebrar las defensas del sistema. Las fallas de grandes equipos, y los errores del personal de operaciones, raramente son la causa de que se quiebren las defensas de la seguridad operacional. A menudo, estos trastornos son la consecuencia de errores humanos en la toma de decisiones. Estos casos pueden deberse a fallas activas en el nivel de las operaciones o a condiciones latentes propicias para facilitar la quiebra de las defensas de seguridad operacional inherentes del sistema. La mayoría de los accidentes incluyen tanto condiciones activas como ocultas.

En la Figura se presenta un modelo de causalidad de accidente que ayuda a comprender la interrelación de los factores de organización y de gestión (es decir, factores sistémicos) en la causalidad de los accidentes. En el sistema de la aviación hay varias “defensas” contra un desempeño improcedente o malas decisiones en todos los niveles del sistema (es decir, en el lugar de trabajo, en los niveles de supervisión y en la administración superior). Este modelo muestra que si bien los factores de organización, incluidas las decisiones de la administración, pueden crear condiciones latentes que pueden conducir a un accidente, estos factores también contribuyen a la defensa del sistema de administración de seguridad, Charles Darwin dijo:

“No es el más fuerte ni el más inteligente el que sobrevive, sino aquel que más se adapta a los cambios”.

Modelo de Causalidad de Accidente



Fuente: Modelo de james Reason

Las culpas y las infracciones que tienen un efecto perjudicial inmediato pueden considerarse como **actos inseguros**; estos actos generalmente están relacionados con personal de operaciones (pilotos, controladores de tránsito aéreo, técnicos de mantenimiento de aeronaves, etc.). Estos actos inseguros pueden penetrar las diversas defensas existentes para proteger el sistema de aviación creadas por la administración de la

empresa, las autoridades de reglamentación, etc. y dar como resultado un suceso.

3. Modelo de Causalidad de los Accidentes

Los hechos inseguros pueden ser el resultado de errores ordinarios o pueden ser el resultado de violaciones deliberadas de las prácticas y los procedimientos prescritos. El modelo reconoce que en el lugar de trabajo hay muchas condiciones que conducen al error o violaciones y que pueden afectar a la conducta individual o de equipo.

Estos actos inseguros se cometen en un contexto operacional que incluye **condiciones inseguras latentes**. Una condición latente es el resultado de una acción o decisión adoptada mucho antes de un accidente. Sus consecuencias pueden permanecer latentes durante mucho tiempo. Individualmente, estas condiciones latentes generalmente no son perjudiciales, puesto que, en primer lugar, no se perciben como fallas.

Los ambientes inseguros escondidas sólo pueden llegar a ser evidentes una vez que se han quebrado las defensas del sistema. Estas condiciones pueden haber estado presentes en el sistema mucho antes de un accidente y generalmente las crean quienes toman decisiones o las autoridades de reglamentación y otras personas que están muy lejos, en tiempo y espacio, del suceso.

El personal que ejecuta las operaciones puede heredar defectos del sistema, tales como los que crean un diseño deficiente del equipo o de las tareas, objetivos incompatibles, servicio a tiempo o bien seguridad operacional, defectos de organización, comunicaciones internas deficientes, o malas decisiones de la gerencia.

Las acciones de gestión de la seguridad operacional que son fuertes procuran identificar y mitigar estas condiciones inseguras escondidas en todo el sistema, en vez de realizar actividades localizadas para

reducir a un mínimo los actos inseguros de los sujetos. Esos actos inseguros sólo pueden ser señales de problemas de seguridad operacional.

Aún en las organizaciones mejor dirigidas, la mayoría de las condiciones inseguras latentes comienzan en quienes toman decisiones. Este personal directivo también está sujeto a limitaciones y predisposiciones humanas normales, así como también a limitaciones de tiempo, presupuestarias, políticas y de otro tipo muy reales.

Dado que algunas de estas decisiones inseguras no pueden evitarse, deben adoptarse medidas para detectarlas y reducir sus consecuencias perjudiciales.

La manera en que los supervisores y la organización en su totalidad desempeñan sus funciones establece las situaciones en que se produce un error o una violación. Por ejemplo, ¿es eficaz la administración con respecto a establecer objetivos de trabajo realizables, organizar tareas y recursos, manejar los asuntos cotidianos, y comunicar interna y externamente?

Las medidas falibles adoptadas por la administración de la empresa y las autoridades de reglamentación muy a menudo son la consecuencia de recursos inadecuados. Sin embargo, evitar los costos de reforzar la seguridad operacional del sistema puede facilitar accidentes que resultan tan caros como la bancarrota del explotador.

4. Incidentes: Precursores de Accidentes

Libremente del modelo de causalidad de accidentes empleado, periódicamente habrá habido precursores evidentes antes del accidente. Con mucha frecuencia, estos precursores sólo llegan a ser evidentes con la retrospección. Las condiciones inseguras latentes pueden haber existido en el momento del suceso.

Identificar y validar estas condiciones inseguras exige un análisis de riesgos, objetivo y a fondo.

Aunque emplear investigaciones de accidentes para identificar peligros es importante, es un método para mejorar la seguridad operacional que obedece a la reacción y es costoso.

D. CONTEXTO DE ACCIDENTES E INCIDENTES

Los accidentes e incidentes ocurren dentro de un conjunto definido de circunstancias y condiciones. Entre los principales factores que crean el contexto de los accidentes e incidentes de aviación se encuentran: diseño de los equipos, infraestructura de apoyo, factores humanos y culturales, cultura de seguridad operacional de la empresa y costos.

1. Diseño de los Equipos

El diseño de los equipos (y de las tareas) es fundamental para la realización de operaciones de aviación seguras.

Desde la perspectiva del operador del equipo, este debe “funcionar como lo anuncia el fabricante”. El diseño ergonómico debe reducir al mínimo el riesgo y las consecuencias de los errores.

El diseñador también necesita tener en cuenta la perspectiva del encargado del mantenimiento del equipo. Debe haber espacio suficiente para permitir el acceso para efectuar el mantenimiento necesario en condiciones de trabajo típicas y con las limitaciones normales en cuanto a fuerza y alcance humanos. El diseño debe incorporar también la función de dar información adecuada para advertir si se ha efectuado un ensamblaje incorrecto.

Aunque la mayor automatización ha reducido el potencial para que ocurran muchos tipos de accidentes, muchos jefes de seguridad

operacional ahora enfrentan nuevos retos creados por esa automatización.

2. Infraestructura de Apoyo

Desde el punto de vista de un explotador de aeronaves o un proveedor de servicios, es esencial disponer de infraestructura de apoyo adecuada para la realización de operaciones seguras.

3. Factores Humanos

El historial de accidentes demuestra repetidamente que de cada cuatro accidentes en tres, por lo menos, ha habido errores de actuación de individuos aparentemente sanos y con las calificaciones apropiadas. La prisa por adoptar nuevas tecnologías hace que a menudo se pasen por alto a las personas que deben usar los equipos.

El elemento humano es la parte más flexible y adaptable del sistema de aviación, pero es también el más vulnerable a las influencias que pueden perjudicar su actuación.

Dado que la mayoría de los accidentes resultan de una actuación humana que no llega a ser óptima, **ha habido una tendencia a atribuirlos simplemente al error humano lo cual permite ocultar los factores subyacentes que se deben sacar a la luz para evitar accidentes**. Por tal razón, la expresión “error humano” no es muy útil para la gestión de la seguridad operacional. Si bien puede indicar dónde ocurrió la falla en el sistema, no proporciona orientación en cuanto a por qué ocurrió.

4. Factores Culturales

La cultura influye en los valores, las creencias y los comportamientos que compartimos con otros miembros de los diversos grupos sociales a que pertenecemos. La cultura sirve para vincularnos como miembros de

grupos y proporciona claves sobre la forma de comportarse tanto en situaciones normales como inhabituales.

Las organizaciones no son inmunes a las consideraciones culturales. El comportamiento de la organización está sujeto a estas influencias en cada uno de sus niveles. Los tres niveles de cultura que siguen son importantes para las iniciativas de gestión de la seguridad operacional:

a. Cultura Nacional.

Esta cultura conoce e identifica las características y los sistemas de valores propios de las diversas naciones. Por ejemplo, las personas de diferentes nacionalidades son diferentes en cuanto a la forma en que responden a la autoridad, enfrentan la incertidumbre y la ambigüedad y expresan su individualidad. No todos los individuos están atentos a las necesidades colectivas del grupo (equipo u organización) del mismo modo. En las culturas colectivistas, se acepta la condición desigual y la deferencia a los líderes. Esos factores pueden afectar la disposición de los individuos a objetar decisiones o acciones lo que es una consideración importante. La distribución de tareas mezclando culturas nacionales también puede afectar a la actuación del equipo cuando se crean malentendidos.

b. Cultura Profesional.

Esta cultura reconoce e identifica el comportamiento y las características de los diversos grupos profesionales (p. ej., el comportamiento típico de los pilotos con respecto al de los controladores de tránsito aéreo, o al de los técnicos de mantenimiento de aeronaves). Por medio de la selección, educación e instrucción del personal, la experiencia en el trabajo, etc.

c. Cultura de la Organización.

Esta cultura reconoce e identifica el comportamiento y los valores de cada organización (p. ej., el comportamiento de los miembros de una empresa en comparación con los de otra empresa, o del gobierno en comparación con los del sector privado). Las organizaciones protegen las culturas nacionales y profesionales. En una línea aérea, por ejemplo, los pilotos pueden provenir de sectores profesionales diferentes (p. ej., tener una experiencia militar o civil, de operaciones complementarias o en zonas remotas o de una gran empresa de transporte aéreo).

Generalmente, el personal en la industria de la aviación tiene un sentido de pertenencia. Su comportamiento diario está influenciado por los valores de la organización a la que pertenecen.

El ámbito más amplio para crear y alimentar una cultura de seguridad operacional está en el nivel de organización. Esto se conoce generalmente como **cultura de seguridad operacional de la empresa**.

5. Cultura de Seguridad Operacional de la Empresa

Como se dijo antes, muchos factores crean el contexto para el comportamiento humano en el lugar de trabajo. La cultura de la organización o de la empresa establece los límites del comportamiento humano aceptable en el lugar de trabajo, estableciendo las normas de conducta y los límites. De este modo, la cultura de la organización o de la empresa constituye una piedra angular para la toma de decisiones de la administración y de los empleados.

La cultura de seguridad operacional es un subproducto natural de la cultura de la empresa. La actitud de la empresa hacia la seguridad operacional influye en el enfoque colectivo de los empleados; al

respecto la cultura de seguridad operacional resulta afectada por factores tales como:

- Medidas y prioridades de la administración.
- Políticas y procedimientos.
- Prácticas de supervisión.
- Planificación y objetivos de la seguridad operacional.
- Medidas en respuesta a comportamientos inseguros.
- Instrucción y motivación del personal.
- Participación o adhesión de los empleados.

6. Cultura de Seguridad Operacional Positiva

Si bien el cumplimiento de los reglamentos de seguridad operacional es necesario para la seguridad de las operaciones, el pensamiento contemporáneo necesita mucho más que eso. Las organizaciones que cumplen simplemente con las normas mínimas establecidas por los reglamentos no están en condiciones para identificar los problemas de seguridad operacional que surgen.

Un modo eficaz de promover una actividad segura es que el explotador desarrolle una cultura de seguridad operacional positiva. Dicho simplemente, **todo el personal debe ser responsable y tener en cuenta las repercusiones de la seguridad operacional en todo lo que hace**. Esta manera de pensar debe estar tan arraigada y que verdaderamente llegue a ser una “cultura”. Todas las decisiones, sean del consejo de administración, de un conductor en la plataforma o de un técnico de mantenimiento deben tomarse teniendo en cuenta las repercusiones sobre la seguridad operacional.

Una cultura de seguridad operacional positiva debe tener su origen en los niveles superiores y descansa en un elevado grado de confianza y respeto entre los trabajadores y la administración. Los trabajadores deben creer y sentir que tendrán apoyo en cualquier decisión que tomen en favor de la seguridad operacional. También deben entender

que las violaciones deliberadas de la seguridad operacional que ponen en peligro las operaciones no serán toleradas.

7. Culpa y Sanción

Una vez que una investigación ha identificado la causa de un suceso, generalmente se sabe quién lo "causó". Tradicionalmente, en ese caso se podría asignar la culpa (y el castigo). Si bien el contexto jurídico varía ampliamente entre los Estados, muchos Estados todavía concentran sus investigaciones en determinar la culpa y la correspondiente responsabilidad.

Para ellos, la sanción sigue siendo uno de los principales instrumentos de seguridad operacional.

Filosóficamente, la sanción es atractiva desde varios puntos de vista, tales como:

- Dar justo castigo por un abuso de confianza.
- Proteger a la sociedad de reincidentes.
- Modificar el comportamiento individual.
- Servir de ejemplo a otros.

El castigo puede tener efecto cuando la gente transgrede las "reglas" deliberadamente.

Puede decirse que las sanciones quizá disuadan al trasgresor (o a otros en circunstancias similares).

Si un accidente fue el resultado de un error de juicio o de técnica, es casi imposible castigar eficazmente ese error. Se podrían hacer cambios en los procesos de selección o de instrucción, o se podría hacer que el sistema tolere más esos errores. Si en esos casos se opta por el castigo, dos resultados son casi seguros: primero, no se recibirán más informes de ese tipo de errores; segundo, puesto que nada se ha

hecho para cambiar la situación, podría esperarse que el mismo accidente ocurra otra vez.

Los errores ahora se consideran como los resultados de alguna situación o circunstancia, no necesariamente como su causa. Como resultado, los administradores están comenzando a buscar las condiciones inseguras que facilitan esos errores y están comenzando a pensar que **la detección sistemática de puntos débiles y deficiencias en la seguridad operacional de las organizaciones es más beneficioso para la gestión de la seguridad operacional que castigar a los individuos.** (Esto no quiere decir que estas organizaciones no deban tomar medidas contra los individuos que no mejoran después de haber recibido orientación o instrucción adicional).

E. ERROR HUMANO

El error humano se cita como una causa o factor que contribuye en la mayoría de los sucesos de aviación. A menudo, personal competente comete errores, aunque claramente nadie había planeado tener un accidente. Los errores no son un tipo de conducta aberrante; son un subproducto natural de todo quehacer humano. El error debe ser aceptado como un componente normal de cualquier sistema en que hay interacción de seres humanos y tecnología. “Errar es humano”.

F. CONSIDERACIONES SOBRE COSTOS

La seguridad operacional y las ganancias no se excluyen mutuamente. En realidad, las buenas organizaciones se dan cuenta que los gastos para la corrección de condiciones inseguras son una inversión para la rentabilidad a largo plazo. Las pérdidas cuestan dinero. A medida que se gasta dinero en medidas de reducción de riesgos, se reducen las pérdidas costosas. Sin embargo, cuando se gasta más y más dinero en la reducción de riesgos, las ganancias que se logran reduciendo las pérdidas pueden no guardar proporción con los gastos efectuados. Las empresas deben encontrar un

equilibrio entre los costos de las pérdidas y los gastos en las medidas de reducción de riesgos.

1. Costos de los Accidentes

a. Costos Directos

Estos son los costos obvios, que son bastante fáciles de determinar. Estos costos se relacionan principalmente con los daños materiales e incluyen rectificación, reemplazo o indemnización por lesiones, equipos de aeronave y daños a los bienes. Los costos elevados de un accidente pueden reducirse mediante la cobertura de seguro. (Algunas organizaciones grandes se auto aseguran reservando fondos para cubrir sus riesgos).

b. Costos Indirectos

Si bien el seguro puede cubrir los costos de accidentes especificados, hay muchos costos que no están asegurados y generalmente ascienden a mucho más que los costos directos que resultan de un accidente. Tales costos algunas veces no son obvios y a menudo aparecen más tarde. Entre los ejemplos de costos no asegurados que pueden resultar de un accidente cabe señalar los que siguen:

- Pérdida de negocios y daños a la reputación de la organización.
- Pérdida del uso del equipo.
- Pérdida de productividad del personal.
- Investigación y limpieza.
- Cobertura deducible
- Acción judicial y reclamaciones por daños.
- Multas y emplazamientos**.**

2. Costos de los Incidentes

Los incidentes de aviación graves, pueden ocasionar muchos de estos costos indirectos o que no están asegurados. Entre los factores típicos de costos que se originan en este tipo de incidentes pueden incluirse:

- Demoras y cancelaciones de los vuelos.
- Empleo de otros medios de transporte para los pasajeros, alojamiento, quejas, etc.
- Cambio y traslado de la tripulación.
- Pérdida de ingresos y de reputación.
- Recuperación, reparación y ensayo en vuelo de la aeronave.
- Investigación del incidente.

CAPITULO TERCERO

I. ELEMENTOS BÁSICOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL.

A. PRINCIPIOS DE GESTIÓN DE LA SEGURIDAD OPERACIONAL.

1. Función Básica de Gestión

En las estructuras de aviación que tienen éxito, la gestión de la seguridad operacional es una función básica de la empresa. Una gestión eficaz de la seguridad operacional exige un equilibro realista entre seguridad operacional y objetivos de producción. Si se aplican correctamente, las medidas de gestión de la seguridad operacional no sólo aumentara la seguridad operacional sino que también mejorara la eficacia de las operaciones de una organización.

La experiencia y las lecciones extraídas de la investigación de accidentes de aviación han subrayado la importancia de llevar a cabo una gestión de la seguridad operacional de modo sistemático, preventivo y explícito. Estos términos se explican a continuación:

a. Sistemático

Significa que las actividades de gestión de la seguridad operacional se realizarán de conformidad con un plan determinado y se aplicarán por igual en toda la organización.

b. Preventivo

Significa la adopción del enfoque que pone énfasis en la prevención, por medio de la detección de peligros y la introducción de medidas para mitigar los riesgos antes de que ocurra un suceso que afecte negativamente a la eficacia de la seguridad operacional.

c. Explícito

Significa que todas las actividades de gestión de la seguridad operacional deberán estar documentadas, ser visibles y ser realizadas independientemente de otras actividades de gestión.

Abordar la seguridad operacional de un modo sistemático, preventivo y explícito asegura que, a largo plazo, la seguridad operacional llegue a ser parte integral de las actividades cotidianas de la organización y que las actividades de la organización relacionadas con la seguridad operacional estén dirigidas a áreas en que los beneficios serán mayores.

2. Enfoque Sistémico

La seguridad operacional no puede lograrse simplemente implantando reglas o directivas respecto a los procedimientos que habrá de seguir el personal de operaciones.

La gestión de la seguridad operacional comprende la mayoría de las actividades de la organización. Por esta razón, la gestión de la seguridad operacional debe comenzar en la administración superior y los efectos de esta gestión en la seguridad operacional deben examinarse en todos los niveles de la organización.

3. Seguridad de Sistemas

La búsqueda de una mejor seguridad operacional hizo necesario considerar la seguridad operacional de la aviación como algo más que el avión y sus pilotos. La aviación es un sistema total que incluye todo lo que se necesita para una operación de vuelo seguro. El “sistema” incluye aeropuerto, control de tránsito aéreo, mantenimiento, tripulación de cabina, servicios de apoyo en tierra, despacho, etc. Una buena gestión de la seguridad operacional debe encarar todas las partes del sistema.

B. FACTORES QUE AFECTAN A LA SEGURIDAD DE LOS SISTEMAS

Los factores que afectan a la seguridad dentro de un sistema definido son los siguientes:

1. Fallas Activas y Condiciones Latentes

Las fallas activas generalmente son el resultado de fallas del equipo o errores cometidos por el personal de operaciones. Las condiciones latentes, sin embargo, siempre encierran un elemento humano y pueden ser el resultado de defectos de diseño no detectados. Por ejemplo, existen condiciones latentes cuando la cultura de la organización alienta que se tome un atajo en vez de seguir siempre los procedimientos aprobados. La consecuencia directa de una condición relacionada con el camino más corto se manifestaría en el nivel operacional con la inobservancia de los procedimientos correctos. Sin embargo, si hay una aceptación general de este tipo de comportamiento entre el personal de operaciones y la administración no tiene conocimiento de esto o no adopta medidas, existe una condición latente en el sistema a nivel de la administración.

2. Defectos de los Equipos

La probabilidad de una falla del sistema se determina analizando las tasas de fallas de los componentes de los equipos. Las causas de las fallas de los componentes pueden ser eléctricas, mecánicas y defectos del soporte lógico.

Se necesita un análisis de seguridad operacional para considerar tanto la probabilidad de fallas durante las operaciones normales como los efectos de no disponer continuamente de algún elemento en otros aspectos del sistema.

3. Error humano

La culpa ocurre cuando el resultado de una tarea desarrollada por un ser humano no es el resultado previsto. La actuación humana puede basarse en la pericia, en las reglas o en el conocimiento. Los errores pueden ser la consecuencia de lapsos de memoria, descuidos al hacer lo que se deseaba o el resultado de equivocaciones que son errores conscientes de juicio.

4. Diseño de sistemas

Las complejas interacciones de los factores humanos, materiales y ambientales en las operaciones, la eliminación completa de los riesgos es un objetivo inalcanzable. Aun en organizaciones con los mejores programas de instrucción y una cultura de seguridad operacional positiva, los operadores humanos pueden cometer errores ocasionalmente. El equipo mejor diseñado y mantenido en alguna ocasión fallará. Los diseñadores de sistemas deben, por lo tanto, tener en cuenta que los errores y fallas son inevitables. Es importante diseñar e implantar los sistemas de manera que, en la mayor medida posible, los errores y fallas de los equipos no resulten en un accidente.

Esto demanda un análisis para identificar los posibles puntos débiles en los aspectos de procedimiento del sistema, teniendo en cuenta el hecho de que los accidentes raramente, obedecen a una sola causa. Por consiguiente, el análisis debe considerar las combinaciones de sucesos y circunstancias a fin de identificar las secuencias que encierran la posibilidad de que la seguridad operacional resulte implicada.

La necesidad de una serie de defensas en vez de una sola capa de defensa se debe a la posibilidad de que las defensas quizá no siempre trabajen perfectamente. Este principio de diseño se llama “defensas en profundidad”.

Para que un accidente ocurra en un sistema bien diseñado, deben crearse brechas en todas las capas de defensa del sistema en el momento crítico en que esa defensa debería haber sido capaz de detectar un error o falla anterior.

C. POLÍTICAS DE LA SEGURIDAD OPERACIONAL

Dentro las políticas de seguridad operacional podemos mencionar.

1. Estrategias de la Seguridad Operacional

Es un método el cual realiza una serie de observaciones en la normalidad de la operación de Mantenimiento, detectando amenazas, errores o estados en el ambiente de trabajo.

Los periodos de la observación se dividen en 4 fases:

Recolección de datos, Verificación de datos, Gestión de datos Conclusión de la observación.

Reportes voluntarios, encuestas y auditorias de seguridad, basadas en la noción que los riesgos pueden ser minimizados de forma activa, Buscado de forma activa los riesgos de seguridad existentes, tomando las acciones necesarias para reducir los riesgos que afecten la seguridad.

a. Un **enfoque de la empresa** para la seguridad operacional. El enfoque de la empresa se funda en la cultura de seguridad operacional de la organización y comprende las políticas, los objetivos y metas de la organización y, lo que es más importante, el compromiso de la administración superior respecto a la seguridad operacional.

b. Instrumentos de organización eficaces para mantener niveles de seguridad operacional. Se necesitan instrumentos de organización eficaces para llevar a cabo las actividades y procesos necesarios para fomentar la seguridad operacional. Los principales puntos de

atención son los peligros y sus posibles efectos en las actividades críticas para la seguridad operacional.

c. Un sistema formal de vigilancia de la seguridad operacional. Esto es necesario para confirmar el continuo cumplimiento por la organización de sus políticas, objetivos, metas y normas de seguridad operacional. Para un explotador o un proveedor de servicios, a menudo se emplea la expresión supervisión de la eficacia de la seguridad operacional para abarcar estas actividades en el marco de su sistema de gestión de la seguridad operacional (SMS).

2. Estrategias de Gestión de la Seguridad Operacional

La estrategia que una organización adopta para su SMS reflejará su cultura de seguridad operacional y puede situarse en una gama que va desde la pura reacción, respondiendo únicamente a los accidentes, hasta estrategias que son muy activas en su búsqueda para detectar problemas de seguridad operacional. En el proceso tradicional, o de reacción, predominan las reparaciones retrospectivas (es decir, cerrar la puerta después que se escapó el gato). Con un enfoque más moderno o preventivo, la reforma futura tiene el papel más importante (es decir, hacer que la puerta no pueda quedar abierta o que el gato no quiera escaparse). Dependiendo de la estrategia adoptada, deben emplearse diferentes métodos y herramientas.

3. Estrategia de Seguridad Operacional por Reacción: Investigar Accidentes y Notificar Incidentes

Esta estrategia es útil para las situaciones en que se trata de fallas de la tecnología o de sucesos poco comunes. La utilidad del enfoque de reacción para la gestión de la seguridad operacional depende de la medida en que la investigación va más allá de las causas determinantes, para incluir un examen de todos los factores que intervinieron.

4. Estrategia de seguridad operacional preventiva:

Buscar activamente información proveniente de diversas fuentes que puede indicar la gestación de problemas de seguridad operacional

Las organizaciones que siguen una estrategia preventiva para la gestión de la seguridad operacional estiman que el riesgo de accidentes puede reducirse al mínimo detectando los puntos vulnerables antes de que fallen y adoptando las medidas necesarias para reducir esos riesgos.

D. ACTIVIDADES CLAVE DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

Las organizaciones que tienen más éxito en la gestión de seguridad operacional ponen en práctica varias actividades comunes. Seguidamente se describen algunas de las actividades específicas:

1. Organización.

Están organizadas para establecer una cultura de seguridad operacional y reducir sus pérdidas por accidentes.

2. Evaluaciones de la Seguridad Operacional.

Analizan sistemáticamente los cambios propuestos para el equipo o los procedimientos a fin de detectar y mitigar los puntos débiles antes de implantar cambios.

3. Notificación de Sucesos.

Han establecido procedimientos formales para notificar los sucesos relacionados con la seguridad operacional y otras condiciones inseguras.

4. **Mecanismos de Detección de Peligros**.

Emplean mecanismos de reacción y preventivos para detectar los peligros relacionados con la seguridad operacional en toda la organización, tales como notificación voluntaria de incidentes, encuestas de seguridad operacional, auditorías de la seguridad operacional y evaluaciones de seguridad operacional.

5. **Investigación y Análisis**.

Hacen el seguimiento de los sucesos notificados y de las condiciones inseguras, si es necesario, inician investigaciones y análisis competentes de la seguridad operacional.

6. **Supervisión de la Eficacia**.

Procuran activamente el retorno de información necesario para cerrar el ciclo del proceso de gestión de la seguridad operacional empleando técnicas tales como observación de tendencias y auditorías internas de la seguridad operacional.

7. **Promoción de la Seguridad Operacional**.

Difunden activamente los resultados de las investigaciones y los análisis de seguridad operacional, compartiendo la experiencia adquirida en la materia tanto dentro de la organización como fuera de ella, si se justifica.

8. **Vigilancia de la Seguridad Operacional**.

Tanto el Estado (que reglamenta) como la organización objeto de reglamentación tienen sistemas para supervisar y evaluar la eficacia de la seguridad operacional.

E. PROCESO DE GESTIÓN DE LA SEGURIDAD OPERACIONAL

La gestión de la seguridad operacional se basa en pruebas, porque requiere el análisis de datos para detectar peligros. Empleando técnicas de

evaluación de riesgos, se establecen prioridades para reducir las posibles consecuencias de los peligros. Una vez identificadas, se elaboran estrategias para reducir o eliminar los peligros y se aplican con responsabilidades claramente establecidas. La situación se reevalúa continuamente y se aplican medidas adicionales cuando es necesario.

1. **Recolección de Datos**.

   El primer paso en el proceso de gestión de la seguridad operacional es adquirir los datos de seguridad operacional pertinentes que son las pruebas necesarias para determinar la eficacia de la seguridad operacional o detectar condiciones inseguras latentes (peligros para la seguridad operacional). Los datos pueden obtenerse de cualquier parte del sistema: el equipo empleado, las personas que participan en la operación, los procedimientos de trabajo, las interacciones entre el elemento humano, el equipo y los procedimientos, etc.

2. **Análisis de Datos**.

   Los peligros para la seguridad operacional pueden detectarse analizando toda la información pertinente. Pueden determinarse las condiciones en que los peligros presentan riesgos reales, sus posibles consecuencias y la probabilidad de que ocurran; en otras palabras, ¿qué puede ocurrir? ¿Cómo? ¿Cuándo? Este análisis puede ser cualitativo y también cuantitativo.

3. **Prioridad de las Condiciones Inseguras**.

   Un proceso de evaluación de riesgos determina la gravedad de los peligros. Aquellos que presentan los riesgos más grandes se consideran para medidas de seguridad operacional. Esto puede exigir un análisis de costo-beneficio.

4. **Elaboración de Estrategias**.

   Comenzando por los riesgos de mayor prioridad, pueden considerarse varias opciones de gestión de riesgos, como las que siguen:

a. **Distribuir** el riesgo lo más amplio posible. (Esta es la base del seguro).

b. **Eliminar** el riesgo completamente (si es necesario deteniendo esa operación o práctica).

c. **Aceptar** el riesgo y continuar las operaciones sin hacer cambios.

d. **Mitigar** el riesgo aplicando medidas para reducir el riesgo o, por lo menos, hacer que sea más fácil enfrentarlo. Cuando se escoge una estrategia de gestión de riesgos, es necesario evitar introducir nuevos riesgos que resulten en un nivel de seguridad operacional inaceptable.

5. Aprobación de Estrategias.

Una vez analizados los riesgos y habiéndose decidido cuál es el plan de acción apropiado, se necesita la aprobación de la administración. En este paso el reto es la formulación de un argumento convincente (y quizá caro) para efectuar cambios

6. Asignación de Responsabilidades y Aplicación de Estrategias.

Una vez adoptada la decisión de proceder, se deben estudiar los detalles de la aplicación. Esto incluye asignación de recursos y de responsabilidades, orden cronológico, revisiones de los procedimientos operacionales, etc.

7. Reevaluación de la Situación.

La ejecución raramente tiene tanto éxito como se prevé inicialmente. Es necesario el retorno de información para cerrar el ciclo formulándose las siguientes preguntas ¿Qué nuevos problemas se han creado? ¿Responde la nueva estrategia de reducción de riesgos a las expectativas de eficacia? ¿Qué modificaciones al sistema o al proceso podrían ser necesarias?

8. Recolección de Datos Adicionales.

Dependiendo de la etapa de reevaluación, podría ser necesario obtener nueva información y repetir el ciclo para perfeccionar la medida de seguridad operacional.

La gestión de la seguridad operacional exige capacidad analítica que quizá la administración no ponga habitualmente en práctica. Cuanto más complejo el análisis, más importante es la necesidad de aplicar los instrumentos analíticos más apropiados. El proceso de cerrar el ciclo de gestión de la seguridad operacional también requiere el retorno de información para que la administración pueda comprobar la validez de sus decisiones y evaluar la eficacia de su aplicación.

CAPITULO CUARTO

I. GESTIÓN DE RIESGOS

La gestión de riesgos sirve para concentrar las actividades de seguridad operacional en aquellos peligros que presentan más riesgos

A. ANTECEDENTES

El riesgo es un subproducto de desarrollar actividades. No todos los riesgos pueden eliminarse, ni todas las medidas imaginables de mitigación de riesgos son económicamente factibles. Los riesgos y los costos inherentes a la aviación requieren un proceso racional de toma de decisiones. Diariamente, las decisiones se toman en tiempo real, comparando la probabilidad y la gravedad de las consecuencias perjudiciales que encierra un riesgo con la ganancia que se espera de tomar el riesgo.

B. DEFINICIÓN

Gestión de riesgos se define como la identificación, análisis y eliminación (o mitigación a un nivel aceptable o tolerable) de los peligros, y los consiguientes riesgos, que amenazan la viabilidad de una organización.

En otras palabras, la gestión de riesgos facilita el equilibrio entre los riesgos evaluados y la mitigación viable de los riesgos. La gestión de riesgos es un componente integrante de la gestión de la seguridad operacional que supone un proceso lógico de análisis objetivo, particularmente en la evaluación de los riesgos.

La gestión de riesgos comprende tres elementos esenciales: identificación de riesgos, evaluación de riesgos y mitigación de riesgos. Los conceptos de la gestión de riesgos se aplican por igual en la toma de decisiones de operaciones de vuelo, control de tránsito aéreo, mantenimiento, gestión de aeropuertos y administración del Estado.

C. IDENTIFICACIÓN DE PELIGROS

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:

1. **Factores de diseño**, incluido el diseño de equipos y de tareas.
2. **Procedimientos y prácticas operacionales**, incluidas su documentación y las listas de verificación, y su validación en condiciones de operación.
3. **Comunicaciones,** incluidos el medio, la terminología y el lenguaje.
4. **Factores de personal,** tales como políticas de la empresa para la contratación, instrucción y remuneración.
5. **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.
6. **Factores del entorno de trabajo,** tales como ruido ambiente y vibraciones, temperatura, iluminación y ropa y equipos de protección disponibles.
7. **Factores de vigilancia reglamentaria,** incluida la aplicabilidad y fuerza de los reglamentos, la certificación de equipo, personal y procesamientos, y las auditorías de supervisión adecuadas.
8. **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.

Los peligros pueden reconocerse en los sucesos reales relacionados con la seguridad operacional (accidentes o incidentes), o pueden identificarse preventivamente mediante procesos dirigidos a identificar peligros antes de que produzca un suceso. En la práctica, tanto las medidas de reacción como los procesos preventivos son un medio eficaz para identificar peligros.

Los sucesos relacionados con la seguridad operacional deberían investigarse para identificar los peligros para el sistema. Esto supone investigar todos los

factores, incluidos los factores humanos y los de organización que tienen un papel en el suceso.

En un sistema de gestión de la seguridad operacional maduro, la identificación de peligros debería provenir de diversas fuentes, como un proceso permanente. Las evaluaciones de la seguridad operacional prevén un proceso estructurado y sistémico de identificación de peligros cuando:

- Hay un aumento inexplicable de sucesos relacionados con la seguridad operacional o de infracciones a la seguridad operacional.
- Se planean cambios importantes en las actividades, incluidos cambios en el personal clave u otros cambios importantes en los equipos o sistemas.
- La organización es objeto de un cambio importante, como el crecimiento
- Se prevén fusiones o adquisiciones de empresas, o la reducción de la empresa

D. EVALUACIÓN DE RIESGO

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:

1. La **probabilidad** de que se produzca un suceso peligroso (es decir, la probabilidad de consecuencias perjudiciales en caso de que se permita que las condiciones inseguras persistan).

DEFINICIÓN CUALITATIVA	SIGNIFICADO	VALOR
Frecuente	Probable que ocurra muchas veces (ha ocurrido frecuentemente)	5
ocasional	Probable que ocurra algunas veces (ha ocurrido Infrecuentemente)	4
Remoto	Improbable, pero es posible que ocurra (ocurre raramente)	3
Improbable	Muy improbable que ocurra (no se conoce que haya ocurrido)	2
Extremadamente improbable	Casi inconcebible que el evento ocurra	1

2. La **gravedad** de las posibles consecuencias perjudiciales, o el resultado de un suceso peligroso.
3. 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.
4. 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.
5. 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).

Para las evaluaciones de riesgos examinadas en este manual, no se necesitan métodos complejos; una comprensión básica de unos pocos métodos será suficiente.

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

- Número de muertos, pérdida de ingresos o pérdida de parte del mercado (es decir, cifras absolutas).
- Índice de pérdidas.
- Probabilidad de accidentes graves (p. ej., 1 cada 50 años).
- Gravedad de los resultados (p. ej., lesiones graves).
- Valor monetario de las pérdidas previstas en comparación con el ingreso anual de las operaciones.

1. Aceptabilidad de los Riesgos

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.

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.

Pueden asignarse diversos valores a fin de clasificar los riesgos como aceptables, indeseables o inaceptable. Estos términos se explican seguidamente:

a. Aceptable

Significa que no es necesario tomar más medidas (a menos que se pueda reducir más el riesgo con poco costo o esfuerzo).

b. Indeseable (o Tolerable)

Significa que las personas afectadas están preparadas para soportar el riesgo a fin de obtener ciertos beneficios, en el entendido de que el riesgo se mitiga lo mejor posible.

c. Inaceptable

Significa que las operaciones en las condiciones actuales deben cesar hasta que el riesgo se reduzca por lo menos al nivel tolerable.

E. MITIGACIÓN DE RIESGO

Por lo que respecta a los riesgos, no existe una seguridad operacional absoluta. Los riesgos tienen que ser mantenidos en el nivel “más bajo 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.

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.

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.

1. Análisis de las Defensas

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:

- Reducir la probabilidad de que ocurran sucesos indeseables.
- Reducir la gravedad de las consecuencias relacionadas con los sucesos indeseables.

Las defensas pueden clasificarse en dos tipos:

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, SOP, supervisión e inspección y destreza personal). 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:

- ¿Había defensas para protegerse contra esos peligros?
- ¿Funcionaron las defensas como estaba previsto?
- ¿Eran prácticas las defensas para usarlas en condiciones de trabajo reales?
- ¿Conocía el personal afectado los riesgos y las defensas existentes?
- ¿Son necesarias medidas adicionales de mitigación de riesgos?

2. Estrategias de Mitigación de Riesgos

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 implica 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).

3. Generación de Ideas

Generar las ideas necesarias a fin de crear las medidas apropiadas para mitigar el riesgo constituye un reto. Elaborar medidas para mitigar los riesgos frecuentemente exige creatividad, ingenio y, por sobre todo, una mente abierta para considerar todas las soluciones posibles. El pensamiento de quienes están cerca del problema (y que generalmente tienen más experiencia) a menudo está afectado por métodos habituales y tendencias naturales. Una participación amplia, que incluye representantes de los diversos organismos, tiende a ayudar a superar las posturas rígidas. Pensar más allá de los parámetros establecidos por la experiencia y los conocimientos personales es fundamental para resolver eficazmente los problemas en un mundo complejo. Habría que considerar cuidadosamente todas las ideas nuevas antes de rechazar cualquiera de ellas.

4. Evaluación de las Opciones para Mitigar Riesgos

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 riesgos pueden indicar cuál es la opción que prefieren para mitigar los riesgos).

f. Cumplimiento Obligatorio.

Si se ponen en vigor nuevas reglas (SOP, reglamentos, etc.), ¿se pueden hacer cumplir?

g. Duración.

¿Resistirá la medida la prueba del tiempo? ¿Será de beneficio temporario 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?

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.

F. COMUNICACIÓN DE RIESGO

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:

- La administración debe estar informada de todos los riesgos que presentan un potencial de pérdidas para la organización.
- Quienes están expuestos a los riesgos identificados deben estar informados de la gravedad de los mismos y de la probabilidad de que ocurran.
- Quienes identificaron el peligro necesitan retorno de información sobre la medida propuesta.
- Quienes están afectados por los cambios previstos deben estar informados tanto de los peligros como de los fundamentos de las medidas adoptadas.
- Las autoridades de reglamentación, los proveedores, las asociaciones de la industria, el público en general, etc., posiblemente necesiten información respecto a riesgos específicos.
- 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.

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.

CAPITULO QUINTO

I. MANTENIMIENTO DE AERONAVES

A. SEGURIDAD OPERACIONAL EN EL MANTENIMIENTO

Inclusive hace poco tiempo, se prestaba menos atención a reducir sistemáticamente los riesgos originados en las actividades de mantenimiento de las aeronaves que a los originados en las operaciones de vuelo. Sin embargo, cada año se mencionan errores de mantenimiento e inspección como un factor en varios accidentes e incidentes graves en todo el mundo.

La seguridad de vuelo depende de la aeronavegabilidad de la aeronave. Por lo tanto, la gestión de la seguridad operacional en cuanto a mantenimiento, inspección, reparación y revisión es vital para la seguridad de vuelo. Los organismos de mantenimiento deben aplicar a la gestión de la seguridad operacional el mismo enfoque disciplinado que el que se necesita para las operaciones de vuelo.

Las condiciones para las fallas relacionadas con el mantenimiento pueden existir mucho antes de la falla. Por ejemplo, una grieta debida a la fatiga que no ha sido detectada puede tomar años hasta que llegue a producir una falla. A diferencia de las tripulaciones de vuelo que reciben información sobre sus errores en casi tiempo real, el personal de mantenimiento generalmente recibe muy poca información sobre su trabajo, hasta que ocurre una falla. Durante este período de retraso, los trabajadores de mantenimiento pueden continuar creando las mismas condiciones inseguras latentes.

Como consecuencia, el área de mantenimiento incorpora una combinación de defensas de seguridad operacional que incluyen aspectos como certificación de los organismos de mantenimiento, otorgamiento de licencias de mecánico de mantenimiento de aeronaves, directrices de aeronavegabilidad, SOP detallados, fichas de trabajo, inspección del trabajo, aprobaciones y registros de trabajo completado.

El potencial de riesgo pueden crearlo las condiciones en las cuales se realiza el mantenimiento, incluidas variantes tales como problemas de organización, condiciones del lugar de trabajo y problemas de actuación humana pertinentes al mantenimiento de aeronaves.

En el contexto del mantenimiento de aeronaves, a menudo se considera que la expresión “seguridad operacional” tiene dos connotaciones.

La primera es el énfasis en la seguridad e higiene en el lugar de trabajo para la protección de los técnicos de mantenimiento de aeronaves, las instalaciones y el equipo.

La segunda es el proceso para asegurarse de que los técnicos de mantenimiento proveen aeronaves en condiciones de aeronavegabilidad para las operaciones de vuelo. Aunque ambas connotaciones pueden estar estrechamente vinculadas, este capítulo se concentra en la segunda, haciendo pocas referencias a las cuestiones de seguridad y salud en el lugar de trabajo.

B. GESTIÓN DE LA SEGURIDAD OPERACIONAL EN EL MANTENIMIENTO

Dada la naturaleza de la función de mantenimiento, del entorno de trabajo para los técnicos de mantenimiento y de los numerosos problemas de factores humanos que pueden comprometer la actuación que se espera de ellos, es necesario un enfoque sistemático para la seguridad operacional, es decir, un sistema de gestión de la seguridad operacional (SMS). El sistema reconoce las interdependencias e interacciones en la organización, por lo que es necesario integrar los esfuerzos respecto a la seguridad operacional en todas las actividades. Los SMS que tienen éxito son los que se crean sobre la base de las tres piedras angulares que siguen:

1. Enfoque de la Empresa Respecto a la Seguridad Operacional

El modo en que la empresa enfoca la seguridad operacional da el parámetro en que la organización desarrolla su filosofía y su cultura de seguridad operacional. A la hora de decidir el enfoque que la organización desea adoptar respecto a la gestión de la seguridad operacional, pueden ser importantes los siguientes factores:

- Tamaño de la organización del mantenimiento (los grandes explotadores tienden a necesitar más estructura).
- Naturaleza de las operaciones (p. ej., operaciones internacionales o regulares durante las 24 horas, o bien interiores o no regulares).
- Naturaleza de la organización (p. ej., departamento de una línea aérea o empresa independiente).
- Madures de la organización y de su fuerza de trabajo (p. ej., estabilidad y experiencia empresarial).
- Relaciones laborales (p. ej., historia reciente y complejidad).
- Cultura actual de la empresa (en comparación con la cultura de seguridad operacional deseada).
- Amplitud del trabajo de mantenimiento (p. ej., mantenimiento ordinario o revisión completa de las aeronaves o de los principales sistemas).

a. Organización para la seguridad operacional

Los canales de comunicación dependen de la confianza y del respeto establecido en las relaciones de trabajo cotidianas.

Para un explotador de aeronaves, el jefe de seguridad operacional (SM) debe tener responsabilidades y líneas de rendición de cuentas claramente definidas con respecto a la gestión de la seguridad operacional en el mantenimiento. La organización del mantenimiento puede hacer que sea necesario que un especialista

técnico trabaje con el SM. Como mínimo, el SM necesitará asesoramiento especializado del departamento de mantenimiento.

El comité de seguridad operacional de la empresa debería incluir representantes del departamento de mantenimiento. En los grandes explotadores, podría justificarse un subcomité especializado para las cuestiones de seguridad operacional en el mantenimiento.

b. Gestión de Documentación y Registros

Los departamentos de mantenimiento dependen mucho de los sistemas para adquirir, almacenar, buscar y consultar la información que se necesita para la gestión de la seguridad operacional; entre las razones para ello cabe mencionar:

- Se deben mantener actualizadas las bibliotecas técnicas (respecto a cosas tales como instrucciones técnicas, certificaciones de tipo, directrices de aeronavegabilidad y boletines de servicio).
- Se deben registrar con detalles los defectos de mantenimiento y el trabajo completado.
- Se deben conservar los datos sobre la supervisión de la performance y de los sistemas para analizar las tendencias.
- Se deben documentar y distribuir formalmente las políticas, los objetivos y las metas de la empresa respecto a la seguridad operacional.
- Se deben conservar los registros sobre instrucción, calificaciones y actualización del personal.
- Se debe conservar la información sobre la historia y la vida útil de los componentes.

c. Asignación de Recursos

Hasta el mejor SMS será inútil si no se tienen los recursos adecuados. Para protegerse de las pérdidas debidas a un accidente, será necesario hacer gastos. Por ejemplo, habrá que asignar recursos para:

- Personal con conocimientos especializados para diseñar e implantar el sistema de seguridad operacional en mantenimiento.
- Instrucción en gestión de la seguridad operacional para todo el personal.
- Sistema de gestión de la información para almacenar los datos de seguridad operacional y especialistas para analizar los datos.

d. Cultura de Seguridad Operacional

En una organización de mantenimiento una cultura de seguridad operacional deficiente puede hacer que los métodos de trabajo que no son seguros no se corrijan; creando posiblemente condiciones inseguras latentes que quizá no causen un problema durante años. El éxito de la administración en fomentar una cultura de seguridad operacional positiva en el departamento de mantenimiento dependerá en gran medida de la forma en que se abordan los aspectos mencionados y la forma en que se aplica el SMS.

2. Principales Instrumentos para la Gestión de la Seguridad Operacional en el Mantenimiento

El funcionamiento eficaz de un SMS para el mantenimiento se funda en la toma de decisiones basada en los riesgos. Por ejemplo, los ciclos de mantenimiento se fundan en las probabilidades de que los sistemas y los componentes no fallen durante el ciclo. A menudo, los componentes se reemplazan porque han llegado al límite de su vida útil, aun cuando

siguen siendo funcionalmente útiles. Si se toman como base el conocimiento y la experiencia, los riesgos de fallas imprevistas se pueden reducir a niveles aceptables.

Entre los principales instrumentos para el funcionamiento de un SMS en el mantenimiento son:

- SOP claramente definidos y aplicados.
- Asignación de recursos en función de los riesgos.
- Sistemas de notificación de peligros e incidentes.
- Programas de análisis de datos de vuelo.
- Observación de las tendencias y análisis de seguridad operacional (incluidos los análisis de costo-beneficio).
- Investigación competente de los sucesos relacionados con el mantenimiento;
- Instrucción en gestión de la seguridad operacional.
- Sistemas de comunicación y de retorno de información (inclusive intercambio de información y promoción de la seguridad operacional).

3. Vigilancia de la Seguridad Operacional y Evaluación de Programas

La vigilancia de la seguridad operacional supone un control periódico (si no continuo) de todos los aspectos de las operaciones de una organización. En la superficie, la vigilancia de la seguridad operacional de una organización demuestra el cumplimiento de reglas, reglamentos, normas, procedimientos, etc.

La supervisión proporciona otro método para la identificación preventiva de los peligros, la validación de la eficacia de las medidas de seguridad operacional adoptadas y la evaluación continua de la eficacia de la seguridad operacional.

La evaluación del programa debería proporcionar respuestas satisfactorias a preguntas como las que siguen:

- ¿En qué medida la administración ha tenido éxito en el establecimiento de una cultura de seguridad operacional positiva?
- ¿Cuáles son las tendencias en notificación de peligros e incidentes? (¿Por especialidades técnicas, por flotas de aeronaves u otras?)
- ¿Se identifican y resuelven los peligros?
- ¿Se han previsto recursos adecuados para el SMS en el mantenimiento?

C. GESTIÓN DE LAS DESVIACIONES.

El sistema de mantenimiento incluye no sólo los técnicos de mantenimiento en los talleres, sino también a todos los otros técnicos, ingenieros, planificadores, administradores, encargados de suministros y otras personas que participan en el proceso de mantenimiento. En un sistema tan amplio, las desviaciones de los procedimientos y los errores son inevitables

Es más probable que los accidentes e incidentes de mantenimiento sean atribuibles a las acciones de los seres humanos que a las fallas mecánicas. A menudo, en esos sucesos ha habido una desviación de las prácticas y los procedimientos establecidos. Hasta las fallas mecánicas pueden reflejar errores en la observación (o notificación) de defectos de menor importancia antes de que lleguen a ser una falla.

Entre los factores que ayudan a evitar los errores de mantenimiento podemos citar los siguientes:

- Información necesaria para realizar el trabajo.
- Equipo y herramientas necesarias.
- Limitaciones de diseño de las aeronaves.
- Requisitos de los trabajos o tareas.
- Necesidad de competencias o conocimientos técnicos.
- Factores que afectan a la actuación de los individuos
- Factores del medio ambiente o del lugar de trabajo.
- Factores de la organización, tales como ambiente de la empresa.
- Liderazgo y supervisión.

Las organizaciones de mantenimiento seguras fomentan la notificación consiente de errores de mantenimiento, especialmente de aquellos que ponen en peligro la aeronavegabilidad, de manera que puedan adoptarse medidas eficaces. Esto requiere una cultura en que el personal se siente cómodo cuando notifica errores al supervisor.

Existen nuevos sistemas para la gestión de las desviaciones de los procedimientos (y los errores) en el mantenimiento de aeronaves, estos presentan las siguientes características:

- Fomentan la notificación sin inhibiciones de sucesos que de otro modo no sería necesario notificar.
- Proporcionan instrucción para el personal sobre el objetivo del SMS en el mantenimiento y los procedimientos para usar dicho sistema, que incluye una clara definición de las políticas disciplinarias de los diversos departamentos (p. ej., las medidas disciplinarias sólo serían necesarias para los casos de incumplimiento temerario o deliberado de las instrucciones promulgadas sobre los procedimientos).
- Realizan investigaciones competentes de seguridad operacional sobre los errores notificados.
- Procuran aplicar medidas de seguridad operacional apropiadas en el seguimiento de las deficiencias detectadas en la seguridad operacional.
- Proporcionan retorno de información a los trabajadores.
- Proporcionan datos apropiados para los análisis de tendencias.

1. Clasificación de las Responsabilidades del (SMS)

Las responsabilidades del SMS son:

a. Gerente General

El Gerente es responsable del funcionamiento y operatividad del SMS destinado los recursos administrativos y financieros requeridos para tal fin sus responsabilidades son:

Dar total cumplimiento de los RAC y demás normativa aeronáutica aplicable.

Designar el personal para la implementación del SMS.

Apoyar la coordinación del plan de respuesta a emergencias.

Apoyar en la identificación de peligros

b. Gerencia de Talento Humano

Es su responsabilidad apoyar en la implementación del (SMS) y en las diferentes actividades de divulgación además ser líder en el cambio de paradigmas frente a la seguridad operacional

Funciones:

Generará una estrategia para lograr un cambio organizacional frente a la cultura de la seguridad operacional y recepcionar los reportes de seguridad operacional.

c. Gerencia Administrativa y Financiera

Su responsabilidad es apoyar la implementación de SMS y brindar gestión de los recursos económicos requeridos, para lograrlo tiene a cargo las siguientes responsabilidades, además ser líder en el cambio de paradigmas frente a la seguridad operacional.

Funciones:

Autorizar las solicitudes de compras de insumos y requerimientos para el SMS.

Realizar revisiones al desempeño del SMS.

Recepcionar los reportes de seguridad operacional.

d. Director Control Calidad

Es su responsabilidad apoyar y estimular al personal de inspección en el desarrollo de los reportes operacionales que se identifiquen o presenten en las diferentes actividades de mantenimiento que se desarrollen, además ser líder en el cambio de paradigmas frente a la seguridad operacional.

Funciones:

Recepcionar los reportes de seguridad operacional, retroalimentar al personal técnico en el desarrollo del SMS.

e. Coordinador de Gestión Calidad

Es responsable de coordinar la gestión de calidad y SMS realizar toda la gestión de los requerimientos para el buen funcionamiento del sistema y para lograrlo sus responsabilidades son:

Realizar gestión de riesgo

Realizar evaluación de riesgo

Realizar monitoreo de la performance de seguridad

Gestión de cambio

Comunicación en seguridad.

Funciones:

Realizar el programa de riesgo de seguridad operacional

Realizar gestión de la comunicación

Diseñar medidas de prevención, control o eliminación de peligros

Ser líder en el cambio de paradigmas frente a la seguridad operacional

f. Director de Mantenimiento

Es su responsabilidad apoyar y estimular al personal técnico en el desarrollo de los reportes operacionales que se identifiquen o presenten en las diferentes actividades de mantenimiento que se desarrollen, además ser líder en el cambio de paradigmas frente a la seguridad operacional.

Funciones:

Recepcionar los reportes de seguridad operacional

Retroalimentar al personal técnico en el desarrollo del SMS.

g. Inspector de Control de Calidad

Es su responsabilidad apoyar y realizar un monitoreo constante a los peligros identificados dentro de las actividades desarrolladas así como el de reportar y hacer seguimiento a los incidentes operacionales.

Funciones:

Realizar promoción de la política de seguridad operacional

Ser líder en el cambio de paradigmas frente a la seguridad operacional.

2. Ayuda en caso de decisiones erróneas en el mantenimiento (MEDA)

Un instrumento para controlar las desviaciones de los procedimientos en el mantenimiento es el método de ayuda en caso de decisiones erróneas en el mantenimiento (MEDA) elaborado por la empresa Boeing Company.

MEDA ofrece al supervisor de los trabajadores (y al SM) un método estructurado para analizar y buscar y descubrir los factores que conducen a errores de mantenimiento y para recomendar estrategias de prevención de error.

En el proceso MEDA hay cinco pasos básicos:

a. Suceso.

Después de un suceso, compete a la organización de mantenimiento seleccionar los aspectos debidos a error que deben investigarse.

b. Decisión.

Después de resolver el problema y de que la aeronave vuelva a prestar servicios, el explotador decide si el suceso estaba relacionado con el mantenimiento. En caso afirmativo, el explotador lleva a cabo una investigación MEDA.

c. Investigación.

El explotador lleva a cabo una investigación siguiendo un formulario estructurado (diseñado específicamente para MEDA). El investigador toma nota de la información general respecto al avión, de cuándo se hizo el mantenimiento y cuándo ocurrió el suceso, del suceso que originó la investigación, del error que causó el suceso, de los factores que influyeron para que ocurriera el error y las estrategias de prevención posibles.

d. Estrategias de Prevención.

La administración examina, establece prioridades e implanta estrategias de prevención (mejoras en los procedimientos) que después sigue, a fin de evitar o reducir la probabilidad de que ocurran errores similares en el futuro.

e. Retorno de información.

Se informa a los trabajadores de mantenimiento de modo que los técnicos de mantenimiento sepan que se han hecho cambios en el sistema de mantenimiento como resultado del proceso MEDA. La administración es responsable de afirmar la eficacia de la participación de los empleados y de validar la contribución de éstos al proceso MEDA compartiendo los resultados de la investigación con ellos.