NO RESTRINGIDO

COMUNICADO DE SEGURIDAD

SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL: GUÍAS PARA LOS OPERADORES AÉREOS

SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL: GUÍAS PARA LOS OPERADORES AÉREOS
Este documento recopila material de guía, publicado principalmente por OACI y el SM ICG, acerca de las actividades que ha de realizar el operador aéreo en el ámbito del Sistema de Gestión de la Seguridad operacional. El objetivo es proporcionar material de guía para la elaboración del Capítulo 3 del Manual de Operaciones por parte del operador aéreo en lo referente al Sistema de Gestión de la Seguridad Operacional.

Ámbito de Aplicación	
Aeronavegabilidad:	No afecta directamente
Operaciones:	Afecta
Licencias al Personal:	No afecta directamente
Navegación Aérea:	No afecta directamente
Aeropuertos:	No afecta directamente
Otros:	No afecta directamente

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

REGISTRO DE EDICIONES

EDICIÓN	Fecha de EDICIÓN	Fecha de APLICABILIDAD	MOTIVO DE LA EDICIÓN/REVISIÓN DEL DOCUMENTO
1.0	02/01/2014	02/01/2014	Este material de guía se emite para ayudar a los operadores aéreos en la implementación de su Sistema de Gestión de la Seguridad Operacional.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Índice de Contenidos

0. DOCUMENTOS DE REFERENCIA. 4

1. ANTECEDENTES 5

2. OBJETIVO DEL COMUNICADO 5

3. LISTA DE ACRÓNIMOS....6

4. INTRODUCCIÓN: GESTIÓN DEL RIESGO FRENTE A ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL....7

5. IDENTIFICACIÓN DE LOS PELIGROS....8

6. EVALUACIÓN Y MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL 15

6.1 ANÁLISIS EN TÉRMINOS DE PROBABILIDAD Y SEVERIDAD DE OCURRENCIA 15
6.2 EVALUACIÓN EN TÉRMINOS DE TOLERABILIDAD DEL RIESGO DE SEGURIDAD OPERACIONAL 20
6.3 CONTROL, EN TÉRMINOS DE MITIGACIÓN, DE LOS RIESGOS A UN NIVEL ACEPTABLE....23
6.4 OTRAS METODOLOGÍAS PARA LA EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL....25

7. OBSERVACIÓN Y MEDICIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL37

7.1 CÓMO MEDIR: TIPOS DE INDICADORES DE RENDIMIENTO DE SEGURIDAD OPERACIONAL....39

8. PLAN DE ACCIÓN DE SEGURIDAD OPERACIONAL 43

9. GESTIÓN DEL CAMBIO 44

ANEXO A. EJEMPLOS DE LA COMPONENTE GESTIÓN DE RIESGOS 46

1. CASO 1: OPERACIÓN EN UN AEROPUERTO EN OBRAS DE CONSTRUCCIÓN 46
2. CASO 2: INICIACIÓN DE OPERACIONES EN PISTAS DE PEDREGULLO 49

ANEXO B. EJEMPLOS DE INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL – MATERIAL OACI....52

ANEXO C. EJEMPLOS DE INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL – MATERIAL SM ICG 54

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

0. DOCUMENTOS DE REFERENCIA.

REFERENCIAS GENERALES			
CÓDIGO	TIPO DOCUMENTO	TÍTULO	Edición
Anexo 19	Anexo de OACI	Anexo 19 al Convenio sobre Aviación Civil Internacional. Gestión de la Seguridad Operacional	1ª*
9859	Doc. OACI 9859	Safety Management Manual (SMM)	3ª*
-	Guía del SM ICG	Risk Based Decision Making Principle	
	Guía del SM ICG	Measuring Safety Performance. Guidelines for Service Provider	

* Se aplica la Última Edición en vigor

REFERENCIAS ESPECÍFICAS			
CÓDIGO	TIPO DOCUMENTO	TÍTULO	Edición
N/A	N/A	N/A	*

* Se aplica la Última Edición en vigor

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

1. ANTECEDENTES

Esta guía recopila, en un único documento, material de guía publicado por OACI y por el grupo SM ICG principalmente.

2. OBJETIVO DEL COMUNICADO

El objetivo de este comunicado es proporcionar, en un único documento, ayuda al operador aéreo en su proceso de implantación de un sistema de gestión de la seguridad operacional.

Tras la publicación del Reglamento (UE) Nº 965/2012 de la Comisión de 5 de octubre de 2012 por el que se establecen requisitos técnicos y procedimientos administrativos en relación con las operaciones aéreas en virtud del Reglamento (CE) Nº 216/2008 del Parlamento Europeo y del Consejo, los operadores aéreos que realizan transporte aéreo comercial han de establecer un Sistema de Gestión de acuerdo con el requisito ORO.GEN.200. Dicho requisito establece en la letra a) 3):

> *la determinación de los peligros para la seguridad aérea derivados de las actividades del operador, su evaluación y la gestión de los riesgos asociados, incluida la adopción de medidas para mitigar los riesgos y verificar su eficacia;*

Este documento, que complementa a la **Guía de Evaluación del MO-A (3-11) Avión** publicada recientemente por la Agencia Estatal de Seguridad Aérea, pretende ayudar al operador aéreo en el cumplimiento con el mencionado requisito.

En particular este material guía se centra en dos de las cuatro componentes del Sistema de Gestión de la Seguridad operacional que engloban las actividades cotidianas del operador en el ámbito del Sistema de Gestión de la Seguridad operacional. Estas dos componentes son: la Gestión del riesgo de seguridad operacional y el Aseguramiento de la seguridad operacional.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

3. LISTA DE ACRÓNIMOS

ACRÓNIMO	DESCRIPCIÓN
SIGLA	DESCRIPCIÓN
DESATI	Dirección de Evaluación de la Seguridad y Auditoría Técnica Interna
EASA	Agencia Europea de Seguridad Aérea
ECAST	European Commercial Aviation Safety Team
EHEST	European Helicopter Safety Team
FAA	Federal Aviation Administration
SM ICG	Safety Management International Collaboration Group
MO	Manual de Operaciones
OACI	Organización de Aviación Civil Internacional

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

4. INTRODUCCIÓN: GESTIÓN DEL RIESGO FRENTE A ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

La función o el componente de "*Gestión del Riesgo de seguridad operacional*" es esencialmente una función asociada a la planificación de las operaciones. Antes de comenzar la operación o ante un cambio en el entorno operacional o funcional:

a) se describe el sistema; es decir, se identifican los componentes y las condiciones del contexto operativo del operador y las interacciones previstas entre tales componentes y condiciones;

b) se completa la identificación inicial de peligros y la evaluación de los riesgos de seguridad operacional de las consecuencias que surjan de los peligros, en base a las interacciones previstas entre los componentes y condiciones; y

c) se implementan mitigaciones contra las consecuencias que surjan de los peligros identificados.

Tras lo cual, se inician las operaciones cotidianas por parte del operador aéreo, bajo el supuesto que las mitigaciones o controles en vigor son garantía suficiente de seguridad en la operación.

La función de "*Aseguramiento de la seguridad operacional*" es una actividad íntimamente asociada a la operación. Se inicia en el momento que se inician las operaciones, para asegurar – por medio de la monitorización continua de las operaciones – que las mitigaciones o los controles funcionan de acuerdo a lo previsto y que logran sus objetivos previstos. Como consecuencia de la monitorización continua de las operaciones, el "Aseguramiento de la seguridad operacional" también permite la identificación de otros peligros que pudieron no haber sido identificados inicialmente, así como de otros debidos a la introducción de cambios en el entorno operacional, lo que a su vez lleva a la puesta en marcha de mitigaciones adicionales.

Como se observa en la siguiente figura ambas funciones o componentes están relacionadas entre sí:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

5. IDENTIFICACIÓN DE LOS PELIGROS

Para la elaboración de esta sección se ha hecho uso del Capítulo 6 del documento "Risk Based Decision Making Principles", del SM ICG.

En el ámbito del grupo SM ICG se define un peligro como *una condición que puede causar o contribuir a un incidente o accidente de la aeronave*. Por otro lado, el SMM de la OACI recoge la definición de peligro utilizada por los profesionales de la seguridad operacional: *una condición u objeto con el potencial de matar, causar lesiones al personal, dañar el equipo o las estructuras, perder material o reducir la capacidad de realizar funciones prescritas*. No obstante, el SMM añade, que para propósitos de la gestión de riesgos de seguridad operacional de la aviación, el término peligro debe enfocarse en aquellas condiciones que pueden causar o contribuir con una operación insegura de la aeronave o del equipo, los productos y servicios relacionados con la seguridad operacional de la aviación.

Durante la fase de identificación del peligro, el analista[1] de seguridad operacional del operador analiza los datos para identificar y documentar los peligros potenciales, así como los efectos o consecuencias correspondientes. El nivel de detalle requerido en el proceso de identificación de peligros depende de la complejidad del proceso de la aviación que se considere.

Consideraciones sobre la identificación de peligros

Para garantizar que la identificación de los peligros es efectiva, se deberían considerar varios elementos. En primer lugar, se debería desarrollar un proceso sistemático para identificar los peligros en el sistema. Hay numerosos métodos que podrían utilizarse, sin embargo, todos deben incluir los tres elementos siguientes:

a) Los analistas en seguridad operacional deberían poseer experiencia técnica y/o de gestión.

b) Los analistas de seguridad operacional deberían recibir formación o tener experiencia en diversas técnicas de análisis de peligros.

c) Debería existir o desarrollarse una(s) herramienta(s) de análisis de peligros.

En segundo lugar, el analista de seguridad operacional debería identificar las fuentes de datos necesarias para identificar los peligros. Por último, el analista de seguridad operacional debería seleccionar la técnica o herramienta más apropiada para los datos disponibles y el tipo de sistema de aviación que se está evaluando.

Fuentes potenciales de peligros

Durante la identificación del peligro, se deberían considerar todas las posibles fuentes de peligros. Dependiendo de la naturaleza y el tamaño del sistema en consideración, estos pueden incluir:

a) Equipamiento a bordo y en tierra (hardware y software);

[1] Un analista de seguridad operacional, en el contexto del SM ICG, no es necesariamente un experto en análisis de datos. Un analista puede ser un experto en un sector particular de la aviación o un panel de seguridad operacional formado por un grupo de expertos o analistas en seguridad operacional. Es una buena práctica, normalmente, minimizar la toma de decisiones críticas por un único punto sino por medio de una revisión por un grupo técnicamente diverso.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

b) Entorno operativo (incluidas las condiciones ambientales, las deficiencias de infraestructura de los aeropuertos, el espacio aéreo, el diseño de los aeropuertos y el diseño de las rutas aéreas);

c) Rendimiento humano;

d) Interfaz hombre-máquina;

e) Procedimientos Operacionales;

f) Indicadores de Seguridad Operacional,

g) Procedimientos de Mantenimiento;

h) Interfaces externas (por ejemplo, servicios de outsourcing);

i) Procedimientos de la organización; y

j) Cambios en la organización.

Teniendo en cuenta las distintas fuentes de peligros identificadas por el grupo SM ICG, AESA ha determinado cómo podrían utilizarse las distintas fuentes de datos de las que dispone un operador aéreo para identificar distintos peligros:

- Sistema de Análisis de los Datos de Vuelo (FDM): Equipamiento a bordo, Rendimiento humano, Entorno operativo, Interfaz hombre-máquina; Procedimientos Operacionales;
- ASR (Air Safety Reports): Equipamiento a bordo y en tierra, Rendimiento humano, Entorno operativo, Interfaz hombre-máquina; Procedimientos Operacionales, Procedimientos de Mantenimiento y de la Organización
- Sistema de Notificación de Sucesos: Procedimientos de Mantenimiento y de la Organización, Entorno operativo, Interfaz hombre-máquina; Procedimientos Operacionales;
- Encuestas de seguridad operacional: Equipamiento a bordo y en tierra, Rendimiento humano, Entorno operativo, Interfaz hombre-máquina; Procedimientos Operacionales, Procedimientos de Mantenimiento y de la Organización
- Auditorías de seguridad operacional: Equipamiento a bordo y en tierra, Rendimiento humano, Entorno operativo, Interfaz hombre-máquina; Procedimientos Operacionales, Procedimientos de Mantenimiento y de la Organización, Interfaces externas, cambios en la organización

Desencadenantes de la identificación de peligros

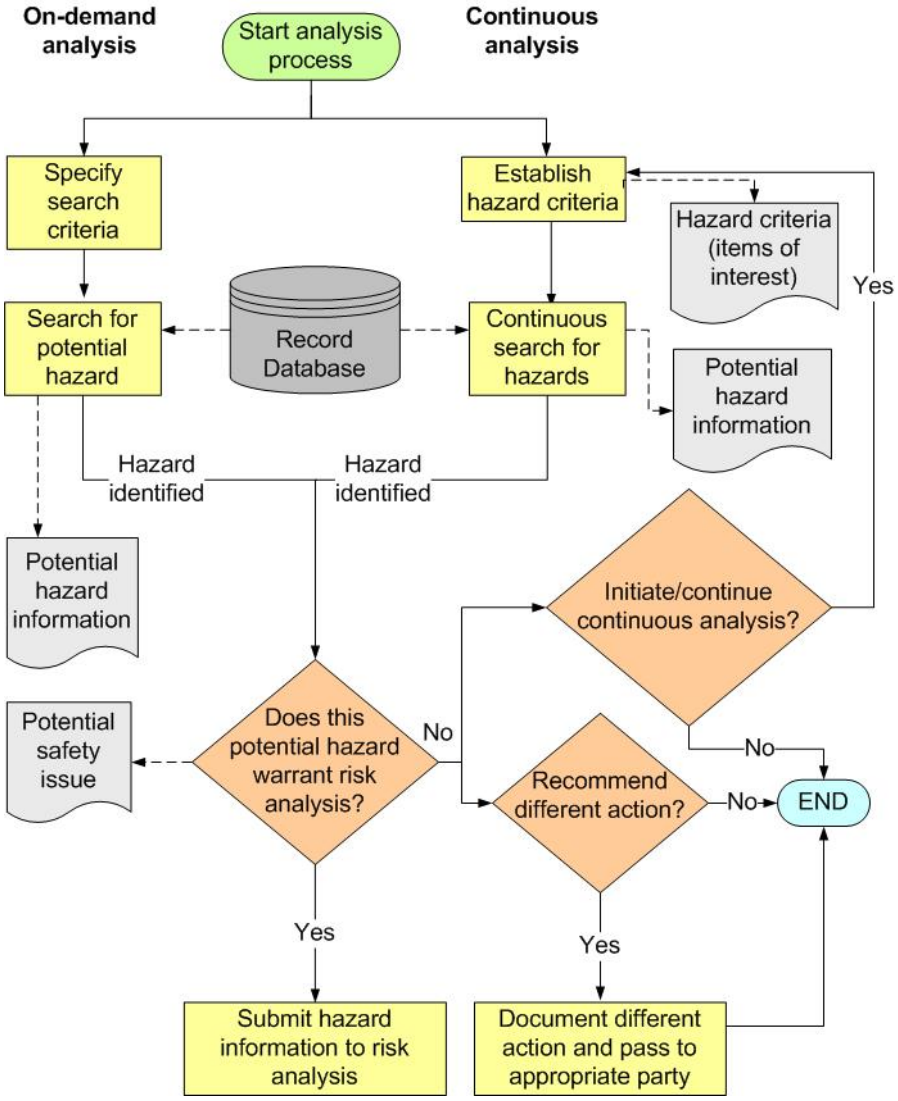
Hay diferentes elementos para utilizar en el proceso de identificación de peligros. Algunos de los más importantes son:

- Diseño del sistema: La identificación de los peligros comienza antes del inicio de las operaciones con una descripción detallada del sistema de la aviación particular y su entorno. El analista de seguridad operacional, a continuación, identifica los distintos peligros potenciales asociados con el sistema, así como los impactos en otros sistemas con los que tiene interfaz.
- Cambio del sistema: La identificación de los peligros comienza antes de la introducción de un cambio en el sistema (entorno operativo o funcional) e incluye una descripción detallada del cambio en particular para el sistema de aviación. El analista de seguridad operacional a

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

continuación identifica los distintos peligros potenciales asociados con el cambio propuesto, así como los impactos en otros sistemas con los que tiene interfaz.

- Monitorización continua y a demanda: La identificación de peligros se aplica a los sistemas existentes en funcionamiento. La Figura 3 muestra un ejemplo de un proceso que contiene tanto el análisis bajo demanda como la monitorización continua. Cabe señalar que la monitorización de los datos también ayuda a detectar: los peligros que son más frecuentes o más severos de lo esperado; y estrategias de mitigación adoptadas que son menos efectivas de lo esperado. Además, el análisis continuo se puede establecer con unos umbrales de notificación basados en un conjunto de elementos críticos de interés.



Métodos y herramientas en la identificación de peligros

Existen varios métodos y herramientas para la identificación de peligros. A continuación hay tres ejemplos[2].

1.-Lluvia de ideas

La lluvia de ideas (o *brainstorming* en inglés) es una discusión sin límites, pero moderada, por un grupo de expertos. Un moderador prepara unas pautas o asuntos antes de la sesión del grupo y fomenta durante las sesiones el pensamiento imaginativo y la discusión entre los miembros del grupo. El moderador inicia un hilo de discusión, y no hay reglas en cuanto a lo que está dentro o fuera del alcance durante el debate posterior. Todas las contribuciones se aceptan y registran y ninguna opinión se impugna o critica. Esto proporciona un entorno en el que los expertos se sienten cómodos en el pensamiento lateral.

Ventajas:

- Adecuado para identificar nuevos peligros en sistemas nuevos o no complejos.
- Involucra a todos los actores clave.
- Relativamente rápido y fácil de realizar.
- Se puede aplicar a una amplia gama de tipos de sistemas.

Desventajas:

- Relativamente no estructurado, por lo que puede no ser exhaustivo.
- Depende de la experiencia y el perfil de los participantes.
- Puede ser susceptible a la influencia de la dinámica de grupo o los objetivos de la alta dirección.
- Su éxito puede depender en gran medida de las habilidades del facilitador

2.- Estudio de peligros y operabilidad (HAZOP)

El HAZOP es un método sistemático y estructurado en el que se utilizan parámetros y desviaciones de palabras guía. La técnica se basa en una descripción muy detallada del sistema en estudio y por lo general consiste en descomponer el sistema en subsistemas bien definidos y en los flujos funcionales o procesos entre los subsistemas. Cada elemento del sistema se somete a continuación a la discusión por un grupo multidisciplinar de expertos frente a varias combinaciones de las palabras guía y de las desviaciones. La discusión del grupo es moderada por un presidente y los resultados de la misma registrados por un secretario, en los que se incluyen los peligros identificados cuando se discute una combinación particular de palabra guía y su desviación. Cuando una combinación particular de palabra guía y su desviación no produce ningún peligro, o no se cree creíble, esto también debería ser registrado para mostrarlo completo. Las palabras guía y las desviaciones deberían estar preparadas con anterioridad por el presidente HAZOP y pueden necesitar ser adaptadas al sistema u operación en estudio.

En el contexto de la aviación, pueden ser típicas palabras guía las siguientes:

[2] Del European Commercial Aviation Safety Team (ECAST), en particular del Grupo de Trabajo Safety Management System and Safety Culture Seguridad operacional la Guía sobre identificación de peligros.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

- Detección
- Coordinación
- Notificación
- Transmisión
- Autorización (tanto *authorization* como *clearance* en inglés)
- Selección
- Transcripción
- Giro
- Ascenso
- Descenso
- Velocidad
- Relectura (*read-back* en inglés)
- Monitorización
- Señalización
- Transferencia (*handover* en inglés)
- Supervisión

Pueden ser desviaciones típicas:

- Demasiado pronto / prematuro
- Demasiado tarde
- Mucho
- Demasiado poco
- Muy alto
- Muy bajo
- Desconocido
- Dos veces / repetido
- Fuera de secuencia
- Ambiguo
- Reversa/invertido

Ventajas del procedimiento HAZOP:

- Sistemático y riguroso.
- Implica la interacción de las opiniones de expertos multidisciplinarios.
- Se puede aplicar a una amplia gama de tipos de sistema.
- Crea un registro detallado y auditable del proceso de identificación de peligros.

Desventajas del procedimiento HAZOP:

- Exige una cantidad considerable de preparación.
- Es difícil de utilizar en un sistema no complejo.
- Puede depender en gran medida de las habilidades del presidente HAZOP.
- Puede llevar mucho tiempo y por lo tanto ser caro.
- Puede inhibir el pensamiento imaginativo y por lo tanto, descartar ciertos tipos de peligros.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

3.- Listas de chequeo

Las listas de chequeo son listas de peligros conocidos o de causas de peligros que se han derivado de la experiencia pasada. La experiencia pasada puede ser las evaluaciones de riesgos anteriores de sistemas u operaciones similares o los incidentes reales que han ocurrido en el pasado. Esta técnica consiste en el uso sistemático de una lista de chequeo apropiada y el examen de cada punto de la lista de chequeo para su posible aplicación a un sistema particular. La aplicación de las listas de chequeo siempre debería estar validada antes de su uso.

Ventajas:

- Pueden ser utilizadas por personas no expertas en el sistema.
- Capturan una amplia gama de conocimientos y experiencias previas.
- Se aseguran que los problemas más comunes y más evidentes no se pasan por alto.

Desventajas:

- Son de uso limitado cuando se trata de sistemas nuevos o sistemas no complejos.
- Pueden inhibir la imaginación en el proceso de identificación de peligros.
- Se pueden perder peligros que no han sido vistos anteriormente.

Esquemas o métodos para la identificación de peligros

EASA establece en su AMC1 ORO.GEN.200(a)(3) punto (1)(a) que se utilicen **esquemas reactivos y proactivos** para la identificación de peligros.

El doc. 9859 Safety Management Manual versión 3ª elaborado por OACI proporciona una definición de los diferentes métodos para la identificación de peligros e identifica las distintas fuentes de datos que podrían utilizarse en cada uno de estos métodos:

- **Método reactivo** consiste en analizar accidentes e incidentes que han ocurrido intentando entender los motivos. Fuentes de datos:
    - Sistema de notificación de sucesos obligatorio,
    - Informes de incidentes e
    - Informes de accidentes.
- **Método proactivo** consiste en analizar cómo se llevan a cabo las operaciones para identificar los potenciales peligros, analizar los riesgos asociados y mitigarlos antes de que se desencadene un accidente o incidente. Fuentes de datos:
    - Estudios,
    - Auditorías y
    - Sistema de notificación de peligros/sucesos voluntario
- **Método predictivo** consiste en identificar y mitigar los riesgos antes de que sean evidentes a través de, por ejemplo, extrapolación de datos o modelos estadísticos. Fuentes de datos:
    - Sistema de Análisis de Datos de Vuelo (FDM) y
    - Sistemas de observación directa.

Fuentes de datos externas para la identificación de peligros

El grupo EHEST en su **"Manual de gestión de la seguridad operacional"** propone una serie de fuentes de datos externas para la identificación de peligros como son:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

- Informes de accidentes e incidentes
- Publicaciones técnicas de los fabricantes (Safety Bulletins, por ejemplo)
- Boletines de Información de Seguridad operacional, alertas de seguridad operacional y otras publicaciones en el ámbito de seguridad operacional de EASA, la Comisión Europea, autoridades nacionales de aviación, OACI, Eurocontrol, la FAA y otras autoridades.
- Páginas web como Skybrary
- Publicaciones de seguridad operacional de asociaciones nacionales e internacionales y de iniciativas de seguridad operacional como EHEST, ECAST, la Flight Safety Foundation, etc…
- Publicaciones de seguridad operacional de la Industria, organizaciones de investigación y universidades.
- Revistas profesionales, conferencias, campañas de seguridad operacional,…
- Comparativas entre operadores, datos agregados a nivel sectorial o por el fabricante…

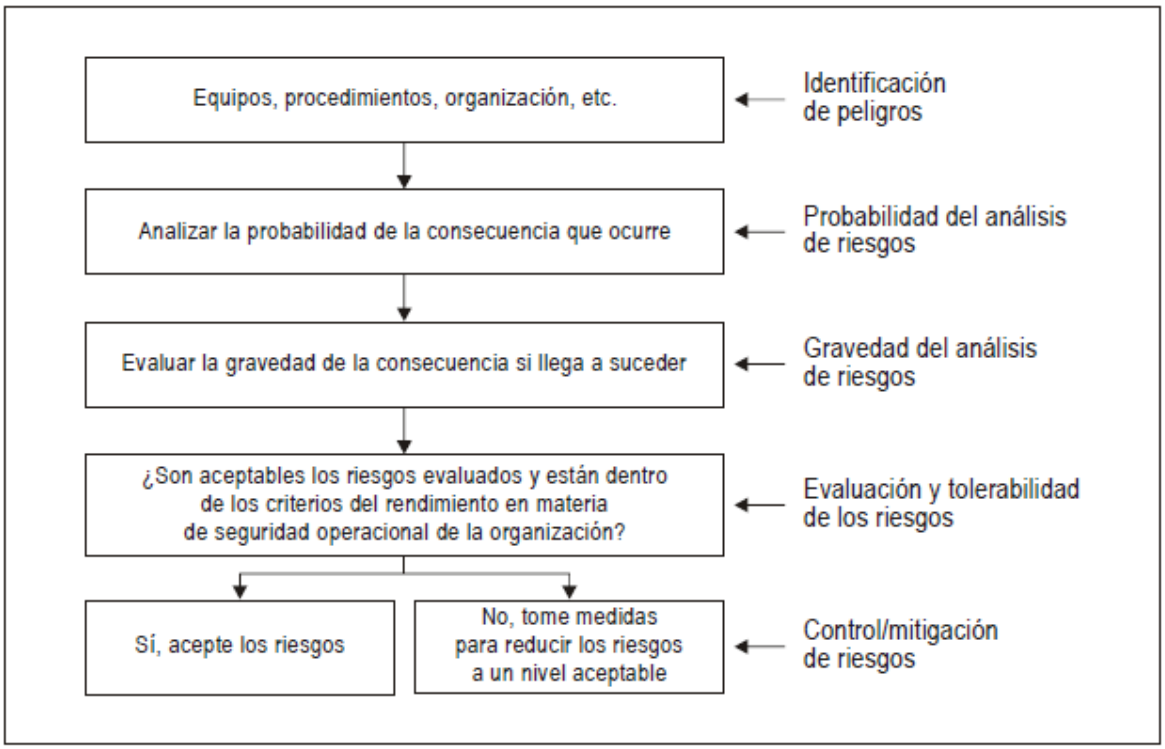
© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

6. EVALUACIÓN Y MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

El operador ha de establecer un proceso formal para gestionar los riesgos de seguridad operacional que garantice:

1. Análisis de las consecuencias de los peligros identificados en el apartado anterior en términos de probabilidad y severidad de ocurrencia
2. Evaluación de los riesgos analizados en términos de tolerabilidad y
3. Control, en términos de mitigación, de los riesgos a un nivel aceptable

La siguiente figura muestra el proceso para la gestión de riesgos propuesto por OACI en el doc. 9859 Safety Management Manual versión 3:



6.1 ANÁLISIS EN TÉRMINOS DE PROBABILIDAD Y SEVERIDAD DE OCURRENCIA

El siguiente texto se ha extraído del Capítulo 7 del documento "Risk Based Decision Making Principles" del SM ICG:

El siguiente paso en el proceso de la gestión de la seguridad operacional es evaluar o analizar el riesgo asociado a los posibles resultados de cada peligro en particular, en el que cada riesgo es el producto de la severidad y la probabilidad. Por lo tanto, la severidad y la probabilidad se deberían expresar en términos medibles, basados en los resultados potenciales de los peligros identificados, de manera que los peligros pueden clasificarse y compararse con las directrices de riesgo establecidos, lo que ayudará a determinar el alcance y el momento adecuado para la mitigación de los riesgos.

En la evaluación de los riesgos, se pueden utilizar métodos cuantitativos y cualitativos. Es preferible utilizar datos cuantitativos, ya que tiende a ser más objetivo. Sin embargo, cuando no están disponibles

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

algunos de los datos cuantitativos, es aceptable confiar en los datos cualitativos y en la opinión de los expertos. El juicio cualitativo varía de una persona a otra, por lo que si sólo una persona está llevando a cabo el análisis, el resultado debería ser considerado como una opinión. Con un equipo de expertos que participen en el análisis, se puede considerar el resultado basado en los datos cualitativos y la opinión de los expertos. Por lo tanto, la calidad del análisis se basa en el conocimiento previo de los expertos del equipo seleccionado.

Ventajas de los datos cuantitativos:

a) Los datos están expresados como un número o una cantidad.

b) Los datos tienden a ser más objetivos.

c) Los datos permiten un análisis y una justificación de las conclusiones más racional.

d) Los datos se pueden utilizar para la modelización.

Ventajas de los datos cualitativos:

a) Los datos están expresados como una medida de la calidad.

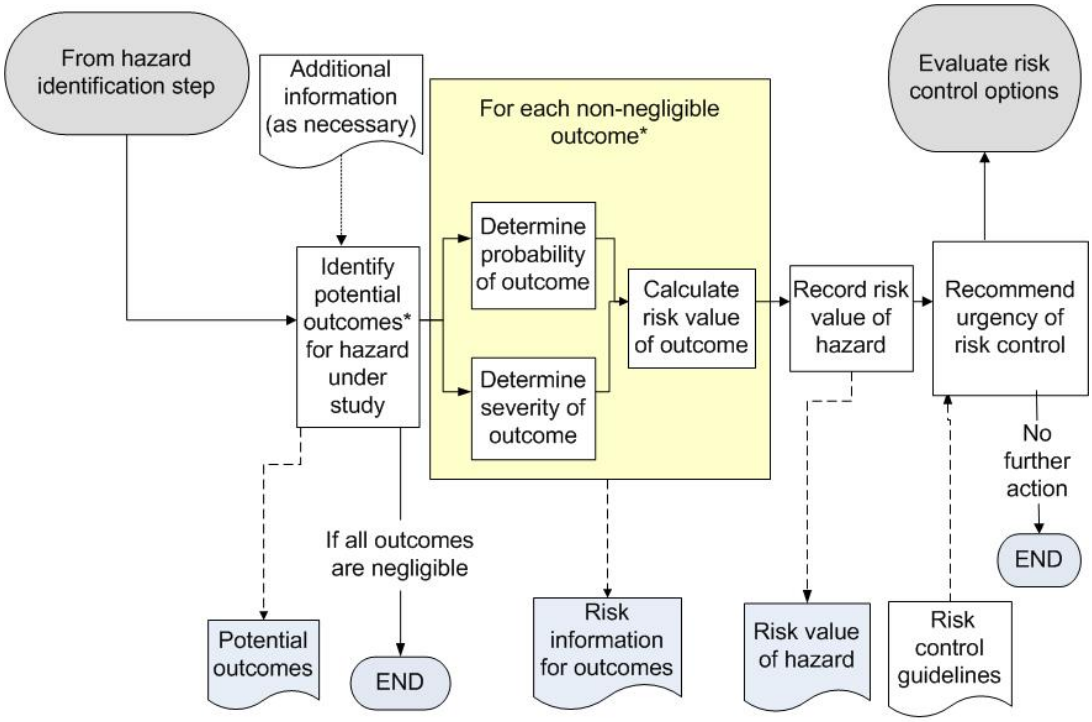
b) Los datos son subjetivos.

c) Los datos permiten la exploración de temas que no pueden a menudo ser expresados con números pero sí mediante el juicio experto,

Cabe señalar que si se requiere una modelización y los datos están disponibles, la evaluación del riesgo se debería basar en datos estadísticos u observados (por ejemplo, trazas radar, las tasas de fallo de hardware). Cuando no hay datos suficientes para realizar evaluaciones de riesgo puramente estadísticas, se pueden utilizar juicios expertos, pero deben ser expresados en términos cuantitativos. Por ejemplo, la tasa real de un determinado tipo de operación puede ser desconocida, pero puede estimarse mediante un juicio experto. En todos los casos, las medidas cuantitativas deberían tener en cuenta el hecho de que los datos históricos no pueden representar -o pueden dar lugar a una falsa configuración de - entornos operativos futuros. En tales casos, puede ser necesario algún ajuste en los datos de entrada.

La siguiente figura muestra un ejemplo de un proceso de análisis de riesgos utilizado para determinar el tipo y la prioridad de los controles de riesgo correctivos.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*



*A single hazard may have multiple undesired outcomes.

Cabe señalar que el riesgo puede ser visto y controlado frente a varios perfiles de riesgo, en el que uno puede ver el riesgo frente a un único vuelo de una aeronave, una flota de aviones, un segmento o segmentos de la industria, etc. El perfil de riesgo depende de los objetivos de la seguridad operacional global de un sector de la aviación en particular (autoridad o proveedor de servicios).

Además, un aspecto clave de cualquier análisis de riesgos es la documentación de los supuestos varios que conducen a una clasificación específica del riesgo. Estos pueden ser revisados en el futuro y actualizados cuando sean necesarios, especialmente si cambia el entorno de operación.

6.1.1 ANÁLISIS EN TÉRMINOS DE PROBABILIDAD Y SEVERIDAD DE OCURRENCIA. METODOLOGÍA OACI

Referencia: "Manual de gestión de la seguridad operacional" (SMM), doc. 9859 de OACI, 3ª edición

Definición de riesgo de seguridad operacional

OACI, en el Anexo 19 Gestión de la seguridad operacional, define el concepto de riesgo de seguridad operacional como *la probabilidad y la severidad previstas de las consecuencias o resultados de un peligro*.

En el Manual de gestión de la seguridad operacional, OACI establece una guía para determinar tanto la probabilidad como la severidad:

Probabilidad del riesgo de seguridad operacional

La probabilidad de riesgo de seguridad operacional se define como la probabilidad o frecuencia de que pueda suceder una consecuencia o un resultado de seguridad operacional.

Con las siguientes preguntas se puede ayudar a determinar dicha probabilidad:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

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

b) ¿Qué otros equipos o componentes del mismo tipo tienen defectos similares?

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

d) ¿Qué porcentaje del tiempo se usa el equipo sospechoso o el procedimiento cuestionable?

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

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

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

Se debe enfatizar que este es solo un ejemplo y que el nivel de detalle y complejidad de las tablas y matrices debe adaptarse para ser proporcional con las necesidades y complejidades particulares de las diferentes organizaciones.

A continuación se muestra otro ejemplo de OACI para determinar la probabilidad de un riesgo:

Nivel	*Descripción*	*Descripción de probabilidad*
A	Seguro/frecuente	Se espera que ocurra en la mayoría de las circunstancias
B	Probable/ocasional	Probablemente suceda en algún momento
C	Posible/remoto	Podría ocurrir en algún momento
Dr.	Poco probable/ improbable	Puede ocurrir en algún momento
E	Excepcional	Puede ocurrir solo en circunstancias excepcionales

Severidad del riesgo de seguridad operacional

La severidad del riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La evaluación de la severidad puede basarse en:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

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

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

La evaluación de la severidad debe considerar todas las posibles consecuencias relacionadas con una condición o un objeto inseguros, considerando la peor situación predecible.

La siguiente figura presenta una tabla de severidad de riesgo de seguridad operacional típico. Incluye cinco categorías para denotar el nivel de severidad, la descripción de cada categoría y la asignación de valor a cada categoría. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla solo es un ejemplo.

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

A continuación se muestran otros dos ejemplos de OACI de tablas con criterios para determinar la severidad de un suceso:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Nivel	*Descripción*	*Descripción de gravedad (personalización de acuerdo con la naturaleza de las operaciones del proveedor de productos o servicios)*
1	Insignificante	No tiene importancia para la seguridad operacional relacionada con la aeronave
2	Leve	Degrada o afecta los procedimientos o performance operacional de la aeronave
3	Moderado	Pérdida parcial de los sistemas de aeronave significativos/importantes o resultados en la aplicación anormal de procedimientos de operaciones de vuelo
4	Grave	Falla completa de los sistemas de aeronave significativos/importantes o resultados en la aplicación de emergencia de procedimientos de operaciones de vuelo
5	Catastrófico	Pérdida de la aeronave o vidas

La siguiente tabla dispone de unos criterios más sofisticados para la determinación de la severidad del suceso:

Nivel	*Descripción*	*Descripción de gravedad (personalización de acuerdo con la naturaleza de las operaciones del proveedor de productos o servicios)*					
		Seguridad operacional de la aeronave	*Lesión física*	*Daños a activos*	*Potencial pérdida de ganancias*	*Daños al ambiente*	*Daño a la reputación empresarial*
1	Insignificante	No tiene importancia para la seguridad operacional relacionada con la aeronave	Sin lesiones	Sin daños	Sin pérdida de ganancias	Sin efectos	Sin implicancias
2	Leve	Degrada o afecta los procedimientos o performance operacional de la aeronave	Lesión leve	Daño leve Menor que $__	Pérdida leve Menor que $__	Efecto leve	Implicancia localizada y limitada
3	Moderado	Pérdida parcial de los sistemas de aeronave significativos/importantes o resultados de la aplicación del procedimiento de las operaciones de vuelo	Lesión grave	Daño sustancial Menor que $__	Pérdida sustancial Menor que $__	Efecto contenido	Implicancia regional
4	Grave	Falla completa de los sistemas de aeronave significativos/importantes o resultados en la aplicación de emergencia de procedimientos de operaciones de vuelo	Un caso mortal	Daño importante Menor que $__	Pérdida importante Menor que $__	Efecto importante	Implicancia nacional
5	Catastrófico	Pérdida de aeronave/casco	Varios casos mortales	Daño catastrófico Más que $__	Pérdida masiva Más que $__	Efecto masivo	Implicancia internacional

6.2 EVALUACIÓN EN TÉRMINOS DE TOLERABILIDAD DEL RIESGO DE SEGURIDAD OPERACIONAL

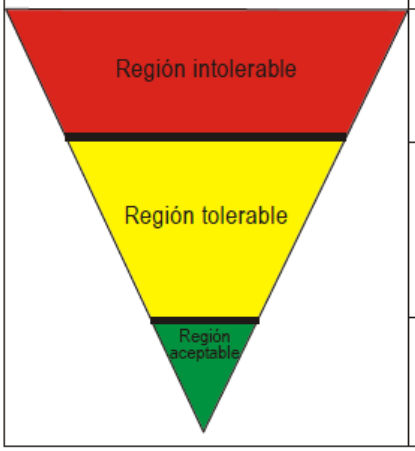
Referencia: "Manual de gestión de la seguridad operacional" (SMM), doc. 9859 de OACI, 3ª edición en español

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

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

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

El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a una matriz de tolerabilidad del riesgo de seguridad operacional que describe los criterios de tolerabilidad para una organización en particular.

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

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

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

La gestión de riesgo de seguridad operacional abarca la evaluación y mitigación de los riesgos de seguridad operacional. El objetivo de la gestión de riesgo de seguridad operacional es evaluar los riesgos asociados con los peligros identificados y desarrollar e implementar mitigaciones eficaces y adecuadas.

Los riesgos de seguridad operacional son evaluados en concepto como aceptables, tolerables o intolerables.

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

Los riesgos de seguridad operacional evaluados en la región tolerable son aceptables, siempre y cuando la organización implemente las estrategias de mitigación correspondientes. Un riesgo de seguridad operacional evaluado inicialmente como intolerable puede mitigarse y, posteriormente, trasladarse a una región tolerable, siempre y cuando dicho riesgo siga bajo el control de estrategias de mitigación adecuadas. En ambos casos, se debe realizar un análisis de coste-beneficio complementario, si se considera adecuado.

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

Otra opción que propone OACI para la matriz de evaluación del riesgo es la siguiente:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Probabilidad	*Gravedad*				
	1. Insignificante	*2. Leve*	*3. Moderado*	*4. Grave*	*5. Catastrófico*
A. Seguro/frecuente	Moderado (1A)	Moderado (2A)	Alto (3A)	Extremo (4A)	Extremo (5A)
B. Probable/ocasional	Bajo (1B)	Moderado (2B)	Moderado (3B)	Alto (4B)	Extremo (5B)
C. Posible/remoto	Bajo (1C)	Bajo (2C)	Moderado (3C)	Moderado (4C)	Alto (5C)
D. Poco probable/ improbable	Insignificante (1D)	Bajo (2D)	Bajo (3D)	Moderado (4D)	Moderado (5D)
E. Excepcional	Insignificante (1E)	Insignificante (2E)	Bajo (3E)	Bajo (4E)	Moderado (5E)

Índice de riesgo	*Tolerabilidad*	*Medida necesaria (personalización según sea necesario)*
5A, 5B, 4A	Riesgo extremo	Detenga la operación o el proceso de inmediato. Inaceptable según las circunstancias existentes. No permita ninguna operación hasta que se hayan implementado medidas de control adecuadas para reducir el riesgo a un nivel aceptable. Se requiere la aprobación del máximo nivel de la administración.
5C, 4B, 3A	Alto riesgo	Precaución. Asegúrese de que la evaluación de riesgos se ha completado satisfactoriamente y que los controles preventivos declarados están implementados. Aprobación de la evaluación de riesgos por parte de la administración superior antes del inicio de la operación o proceso.
1A, 2A, 2B, 3B, 3C, 4C, 4D, 5D, 5E	Riesgo moderado	Realice o revise la mitigación de riesgos, según sea necesario. Aprobación por departamentos de la evaluación de riesgos.
1B, 1C, 2C, 2D, 3D, 3E, 4E	Bajo riesgo	La mitigación o revisión de riesgos es opcional.
1D, 1E, 2E	Riesgo insignificante	Aceptable tal cual. No se necesita una mitigación de riesgos.

6.3 CONTROL, EN TÉRMINOS DE MITIGACIÓN, DE LOS RIESGOS A UN NIVEL ACEPTABLE

Referencia: Capítulo 8 Estrategias de Mitigación de Riesgos de la guía "Risk Based Decision Making Principles", del SM ICG:

El objetivo de la mitigación del riesgo es implementar planes adecuados para mitigar el riesgo asociado a cada resultado de los peligros detectados hasta que alcanzan un nivel aceptable de seguridad operacional. El analista de seguridad operacional desarrolla, documenta, y recomienda las estrategias de control o mitigación de riesgos. Un control de riesgo es todo aquello que mitiga el riesgo de los efectos/consecuencias de un peligro. Una estrategia de control de riesgos incluye las opciones y alternativas que reduzcan o eliminen el peligro. Algunos ejemplos son: la implementación de políticas o procedimientos adicionales, el desarrollo de sistemas y/o componentes redundantes, la revisión de las especificaciones de formación y de los resultados, y el uso de fuentes alternativas de producción.

Cuando se determina que el nivel de riesgo es inaceptable, el analista identifica y evalúa posibles estrategias de mitigación de riesgos que puedan reducir el riesgo a un nivel aceptable para la dirección de la organización, tal como se expresa en las políticas de la organización (autoridad o proveedor de servicios). A continuación, el analista evalúa cómo las estrategias de mitigación propuestas afectarían al riesgo global. Si es necesario, el analista repite el proceso hasta que una combinación de estrategias reduzca el riesgo a un nivel aceptable para la dirección de la organización. Si los resultados de una

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

evaluación del riesgo revelan un nivel inaceptable de riesgo, las operaciones o los procesos se deberían suspender de inmediato hasta que alguna acción de mitigación conduzca a un nivel aceptable del mismo.

Como siguiente paso, se debería realizar una evaluación de cada propuesta de control de riesgos. Los candidatos ideales de control de riesgos son aquellos de bajo coste, fáciles de realizar, de rápida implementación, completamente efectivos, y que no introduzcan riesgos secundarios (riesgos de consecuencias no intencionadas). Como la mayoría de las situaciones no se ajustan a estos ideales, los candidatos de controles de riesgos se deberían evaluar y seleccionar en base al equilibrio entre los atributos de eficacia, coste, plazos de ejecución, y la complejidad. Una vez que los controles de riesgo se han seleccionado y aplicado, entonces se deberían monitorizar y validar para asegurar que se han alcanzado los objetivos previstos.

El método seleccionado de mitigación de riesgo puede pertenecer a una o más de las siguientes categorías:

- **Estrategia de prevención de riesgos:** La estrategia de prevención de riesgos evita el suceso y/o consecuencia potencial mediante la selección de un procedimiento diferente, o la no participación en el desarrollo de la operación, procedimiento o sistema (hardware y software). Esta técnica debería llevarse a cabo cuando hay disponibles varias alternativas u opciones. La estrategia de prevención de riesgos se utiliza frecuentemente como base para una decisión "pasa" o "no-pasa" en el inicio de una operación o programa.
- **Estrategia de reducción de riesgos:** La estrategia de reducción de riesgos significa una reducción de la frecuencia de la operación o de la actividad, o una adopción de medidas específicas para reducir la severidad de las consecuencias de los peligros aceptados. Esta estrategia puede dar lugar a una acción de transferencia del riesgo si las acciones específicas para reducir el riesgo son controladas por un tercero.
- **Estrategia de transferencia del riesgo:** La estrategia de transferencia del riesgo cambia la titularidad del riesgo a un tercero. Las organizaciones transfieren el riesgo principalmente para asignar la propiedad a la organización u operación más capaz de gestionarlo. La parte receptora debería aceptar el riesgo, que debería estar documentado (por ejemplo, una Carta de Acuerdo, una Declaración del Acuerdo, un Memorando de Acuerdo). Un ejemplo de transferencia de riesgo es la transferencia de un sistema de aviación desde la organización de adquisición a la organización que se encarga del mantenimiento.
- **Estrategia de segregación a la exposición al riesgo:** En esta estrategia, se toman medidas para aislar los efectos de los riesgos o crear redundancia para protegerse de ellos. Un ejemplo de la segregación de la exposición es la de limitar la operación en un aeródromo circundado por una geografía compleja a las aeronaves con capacidades específicas de navegación.
- **Estrategia de adquisición del riesgo:** La estrategia de adquisición de riesgos es simplemente aceptar la posibilidad o probabilidad y la severidad de las consecuencias asociadas con la ocurrencia de un peligro. Normalmente, no es aceptable el uso de una estrategia de hipótesis para tratar un riesgo alto asociado a un peligro. El riesgo de seguridad operacional debería ser mitigado o reducido a niveles más bajos antes de que pueda ser aceptado. Al seleccionar este enfoque, deberían estar preparadas las contramedidas disponibles frente a los riesgos asumidos por adelantado.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

6.4 OTRAS METODOLOGÍAS PARA LA EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

El operador ha de identificar qué metodología utiliza para la evaluación y mitigación de los riesgos de seguridad operacional. Además de la metodología de OACI, a continuación se presentan diversas metodologías de evaluación de riesgos propuestas en diversos ámbitos europeos.

6.4.1 METODOLOGÍA DE EVALUACIÓN DE RIESGOS: ARMS

EASA, a través de su grupo ECAST, promociona la metodología ARMS. El grupo de trabajo ARMS (Soluciones de Gestión de Riesgos para las Aerolíneas) fue creado con el objetivo de elaborar un método de evaluación de riesgos operacionales útil y coherente para las compañías aéreas y otras organizaciones de aviación. La evaluación de riesgos es una de las partes más difíciles del proceso de gestión de riesgos.

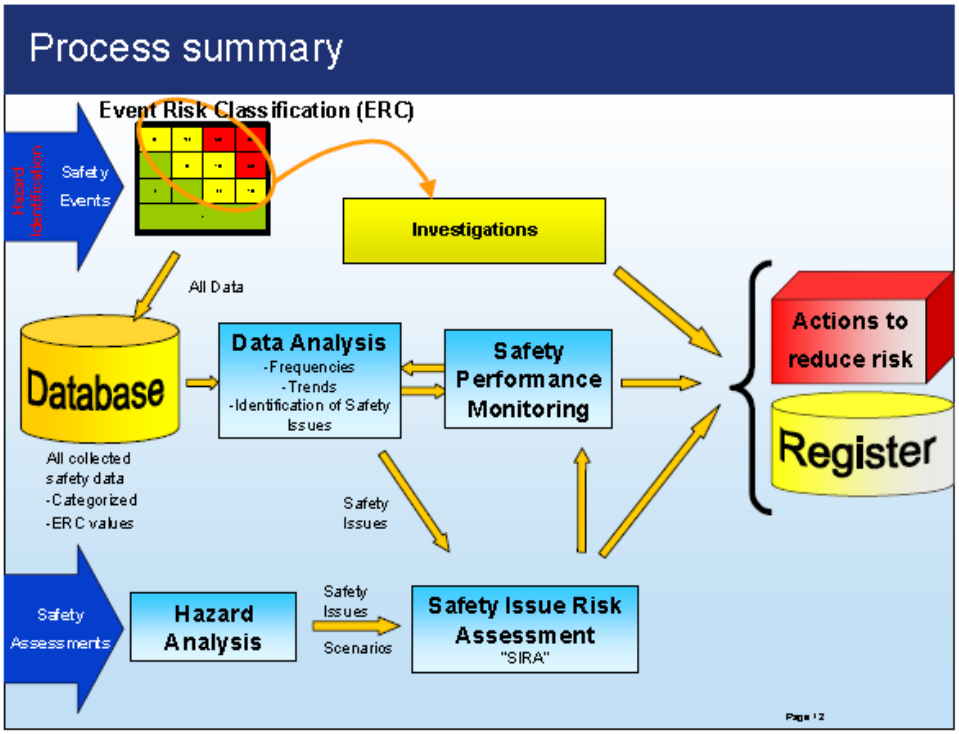
En la página web de EASA (http://easa.europa.eu/essi/ecast/main-page-2/sms/) se encuentran los siguientes documentos:

a) El documento ARMS - la descripción completa de la metodología con ejemplos

b) Guía de referencia rápida ARMS - resumen de una página para referencia diaria de la herramienta

c) Excel de Evaluación de Riesgos de Seguridad (SIRA) - la herramienta práctica SIRA

A continuación se muestra un esquema simplificado del proceso de evaluación del riesgo elaborado por el grupo ARMS:



Durante el proceso de **identificación de peligros** se trata de recopilar y analizar datos operativos de seguridad operacional, identificando de ese modo las **cuestiones de seguridad operacional**. Estos datos

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

de seguridad operacional suelen incluir las notificaciones de seguridad operacional, eventos de datos de vuelo y los resultados de los estudios de seguridad y de auditorías. La identificación de los peligros proporciona la entrada para el proceso de evaluación de riesgos.

Una persona con el conocimiento adecuado tiene que revisar estos datos con relativa rapidez a fin de que todas las cuestiones urgentes se puedan abordar de una manera oportuna. Este paso se aborda mediante el proceso de **Clasificación del Riesgo del Evento (ERC)**.

La posibilidad de tomar medidas basadas en eventos individuales constituye el primer paso en el proceso.

Todos los datos de seguridad operacional también se almacenan en una base de datos. La base de datos debería ser analizada de manera rutinaria con el fin de detectar posibles tendencias adversas y para realizar un seguimiento de la efectividad de las primeras acciones de mitigación de riesgos. Este análisis puede conducir a la identificación de un posible problema de seguridad que puede necesitar una evaluación formal de su riesgo asociado para determinar el nivel de riesgo y diseñar las medidas adecuadas de mitigación del riesgo.

Además, el análisis de la base de datos, iniciado como consecuencia de un evento o preocupación puede revelar riesgos que deben ser tratados inmediatamente antes de llevar a cabo un análisis más formal mediante un **SIRA (Safety Issue Risk Assessment),** explicado más adelante.

La "respuesta rápida" debería tener finalmente un SIRA formal llevado a cabo de manera que pueda ser adecuadamente medido y monitorizado en el Registro de Riesgos.

Las etapas del proceso

1. Fuentes de datos para la identificación de peligros

La metodología ARMS trata con varios tipos de datos para la identificación de peligros. La regla principal es que la ERC[3] se utiliza para eventos (incluso cuando no hay ninguna consecuencia real) y la SIRA[4] se utiliza para cuestiones de seguridad operacional (incluidos los peligros y las condiciones latentes).

2. Clasificación del Riesgo del Evento (ERC)

El objetivo principal de la Clasificación del Riesgo del Evento es la de actuar como un primer filtrado de todos los datos entrantes de seguridad operacional e identificar cuándo es necesaria una acción urgente. Este tipo de filtrado es necesario cualquiera que sea el método utilizado para la evaluación del riesgo. Por lo general, la clasificación de riesgo del evento debe tener lugar preferentemente entre uno o dos días después de tener conocimiento del evento y llevarse a cabo por una persona con experiencia operativa que haya sido entrenada en la evaluación de riesgos, en adelante denominado el analista de seguridad operacional.

El valor de ERC se basa en dos preguntas:

• Si el evento hubiera desembocado en un accidente, ¿cuál habría sido el resultado más creíble?

[3] Clasificación del riesgo de seguridad del evento –Event Risk Classification (ERC).

[4] Evaluación del riesgo de una cuestión de seguridad–Safety Issue Risk Assessment (SIRA).

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

• ¿Cuál fue la eficacia de las barreras que no fueron vulneradas entre este evento y el resultado de accidente más creíble?

The proposed practical ERC application is a 4x4 matrix, illustrated in figure 4 below.

Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

Effective	Limited	Minimal	Not effective			Typical accident scenarios
50	102	502	2500	Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
10	21	101	500	Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
2	4	20	100	Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
1				No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

El ERC tiene dos salidas. El primer resultado es una recomendación sobre qué se debe hacer sobre el evento.

→ Investigate immediately and take action.

→ Investigate or carry out further Risk Assessment

→ Use for continuous improvement (flows into the Database).

En el caso de un resultado "rojo", el evento puede ser considerado como un problema de seguridad operacional por propio derecho. En el caso de un resultado de color "amarillo", pueden ser investigados y/o su riesgo evaluado con más refinamiento. Esto se puede hacer usando la SIRA creando en primer lugar un problema de seguridad basado en el evento o algún aspecto del evento (por ejemplo, un peligro).

El Analista de Seguridad podrá, sobre la base de su propio juicio, decidir en algunas ocasiones sobre un riesgo más alto que la ERC podría indicar.

La segunda salida de la ERC es un número, llamado el índice de riesgo de ERC. Este índice proporciona un valor cuantitativo del riesgo relativo y es muy útil en la elaboración de las estadísticas.

En la matriz ERC propuesta, los índices de riesgo se mueven entre 1 y 2500 y cada cuadrado de la matriz tiene un valor único.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

3. Investigaciones

El propósito de la investigación interna es averiguar más sobre el evento y sus causas. Su alcance puede variar desde una llamada telefónica a la creación de un equipo de investigación multi-departamental que puede necesitar varios meses para presentar un informe final. Las investigaciones que involucran organismos externos no se consideran aquí.

La investigación puede incluir:

- Las llamadas telefónicas o reuniones para obtener información de las personas involucradas o especialistas
- Estudiar la meteorología imperante y otras condiciones
- El estudio de los registros técnicos
- Análisis de los datos de seguridad operacional y estudio de los datos históricos sobre eventos o condiciones similares
- Redacción de un informe con los resultados, que puede ser almacenado en el software de seguridad operacional relacionado con el evento.

4. Acciones para reducir los riesgos

La evaluación del riesgo como tal no reduce el riesgo. El SMS (Sistema de Gestión de la Seguridad) de la empresa deberá especificar los grupos funcionales que se requieren para identificar las acciones necesarias y dar seguimiento a su aplicación y eficacia. Por lo general, el Grupo de Acción de Seguridad Operacional (GAS) se centrará en ambas cuestiones. La organización también puede tener un Comité de Revisión de Seguridad Operacional (CRS) que se concentrará en el seguimiento del nivel general de riesgo y la realización de acciones clave y recomendaciones en el Registro de Riesgos.

El Registro del Riesgo es de gran ayuda en el seguimiento de las recomendaciones, tanto por su aplicación como por su eficacia.

5. Base de datos de seguridad operacional

Además de la ERC, todos los datos de seguridad deben ser incluidos en la base de datos de seguridad operacional. Es necesario contar con una base de datos "estructurada", que pueda ser utilizada para el análisis de datos y donde los eventos individuales se puedan encontrar fácilmente. La secuencia de las tareas, i) clasificación de Eventos de riesgo (ERC) y ii) entrada del evento en la base de datos de seguridad operacional puede variar, dependiendo del software del operador individual y de sus procedimientos.

Para crear una base de datos "estructurada", es necesario clasificar los datos en función de varios criterios. Los elementos típicos relacionados con cada caso son, por ejemplo:

- Fecha
- Tipo de avión
- Matrícula de la aeronave
- Punto de partida y de destino

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

- Fase de vuelo
- Lugar del evento
- Evento o escribe el descriptor
- Los sistemas de las aeronaves involucradas (lista de palabras clave)
- Cuestiones operacionales involucrados (lista de palabras clave)
- Valor del índice de la Clasificación de Riesgo del Evento

6. Análisis de Datos

El objetivo principal del análisis de datos es identificar los problemas de seguridad que afectan a la operación actual. El análisis de datos trata de examinar la base de datos de seguridad operacional para identificar las tendencias y grupos de eventos relacionados. Es un proceso de aprendizaje y descubrimiento de datos existentes.

Se generan cuadros, gráficos y filtros para clasificar los eventos por diferentes combinaciones, como por ejemplo:

- Periodo temporal
- Tipo de avión
- Aeropuerto / aproximación
- Los tipos de eventos
- Palabras clave
- Los sistemas de las aeronaves involucradas
- Cuestiones operacionales involucradas

A veces los resultados de inmediato pondrán de relieve temas que muy obviamente hay que abordar - incluso antes de emprender una evaluación de riesgos formal. Por ejemplo, si una aproximación a un aeropuerto tiene una tasa muy alta de aproximaciones no estabilizadas, el asunto, obviamente, debe ser abordado.

Los resultados pueden ser presentados como "número de eventos" o como "tasa de eventos", siendo este último a menudo más significativo. Por ejemplo, el número de aproximaciones no estabilizadas por aeropuerto de destino estará influenciado por el diferente número de vuelos realizados a estos aeropuertos. El aeropuerto base puede mostrar un número elevado de acontecimientos simplemente debido al alto número de vuelos. El cálculo de la tasa de aproximaciones no estabilizadas en función de todas las aproximaciones que volaron a ese destino proporcionará una idea más clara de la situación.

Es importante darse cuenta de que ni el "número de eventos", ni la "tasa de eventos" tienen en cuenta la severidad (real o potencial) de los eventos. Por lo tanto, mirar esas estadísticas puede ser engañoso. Los valores del índice de riesgo de ERC proporcionan una valiosa oportunidad de pasar de este enfoque "número/tasa" a un enfoque de "riesgo", dando una mejor base para la toma de decisiones. Los valores de ERC pueden ser utilizados para cualquier tipo de análisis estadístico.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

7. Monitorización del rendimiento en materia de seguridad operacional

Un requisito clave en el SMS es monitorizar el rendimiento en materia de seguridad operacional de la organización.

El objetivo es garantizar que el nivel de seguridad operacional objetivo (y al menos un nivel mínimo aceptable de rendimiento en materia de seguridad operacional) se consigue. En la práctica, los datos utilizados para la supervisión del rendimiento constituyen prácticamente la misma información que se utiliza para la identificación de peligros y evaluación de riesgos.

La monitorización del rendimiento puede basarse tanto en:

- Las medidas que procedan directamente de una fuente de identificación de peligro (por ejemplo, las notificaciones de seguridad o datos de vuelo).
- Medidas basadas en riesgos.

8. Evaluación de Riesgos de Cuestiones de Seguridad (SIRA)

Como resultado del análisis de los datos, la organización identificará gradualmente una serie de problemas de seguridad que afectan a su funcionamiento. Estos riesgos deben ser evaluados utilizando la metodología de Evaluación de Riesgos de Cuestiones de Seguridad (SIRA).

El primer paso es definir el alcance y la "cuestión de seguridad" correctamente. Aspectos típicos a definir son:

- Denominación de la cuestión de seguridad
- Descripción del peligro(s)
- Descripción del escenario(s) de accidente relacionado
- Tipos de aeronaves consideradas
- Lugares considerados
- Periodo de tiempo en estudio
- Los departamentos cuya participación en la evaluación es necesaria
- Otros

SIRA evalúa el riesgo mediante una fórmula donde el riesgo se analiza según cuatro aspectos:

- Frecuencia / probabilidad del evento denominado "Disparo"
- Efectividad de las barreras de prevención
- Efectividad de las barreras de recuperación
- La severidad del resultado de accidente (más probable)

9. Registro de Riesgos

El registro de riesgos contiene la información sobre los riesgos identificados que sean necesarios para su gestión.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Contenidos típicos son:

- Cuestiones de Seguridad
- Sus valores de riesgo
- Acciones concertadas
- Las personas responsables y fechas límite para las acciones
- El avance en las acciones y el impacto en los niveles de riesgo

El Registro es una buena herramienta para las personas en las operaciones de línea y de la Oficina de Seguridad que trabajen en la gestión de la seguridad operacional.

Algunas organizaciones pueden optar por rastrear los riesgos a un nivel más refinado e incluir en el Registro:

- Eventos de Disparo
- Eventos indeseados en la operación (UOE)
- Barreras y su efectividad se realiza el seguimiento
- Decisiones de seguridad (que tienen que ser registrados en algún lugar, de todos modos)

10. Evaluación de la seguridad operacional

Una evaluación de la seguridad es una evaluación de riesgos centrada en una parte específica de la operación. El objetivo es evaluar si aquella parte de la operación es suficientemente segura, es decir, si el nivel de riesgo es aceptable. Por lo general, la atención se centrará en una parte nueva o cambiante de la operación y el objetivo es garantizar que la operación planeada será segura. En este caso, la evaluación debe hacerse antes de que la decisión sobre la nueva operación se haya tomado, pero en cualquier caso antes de la nueva operación se inicie.

El origen de la evaluación también podría ser un cambio en el entorno operativo, en contraposición a una decisión interna de la empresa.

A veces las evaluaciones de la seguridad están hechas de “piezas ya existentes” de la operación. En este contexto, a menudo son llamados casos de seguridad y el objetivo es garantizar que el nivel de seguridad es (todavía) aceptable. En este caso, los datos de seguridad de la compañía deben estar disponibles para apoyar la evaluación.

Además del objetivo principal de evaluar el nivel de riesgo de la operación prevista en el enfoque, por lo general es deseable para evaluar:

- Si el nivel de riesgo es muy alto, ¿podría reducirse a un nivel aceptable?
- En caso afirmativo, ¿cómo?
- ¿Cómo de difícil y costoso sería?

Las respuestas a estas preguntas serán esenciales para la alta dirección cuando se está evaluando la viabilidad y la rentabilidad de una nueva operación.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Es importante darse cuenta de que las evaluaciones de seguridad no son más que un paso de un procedimiento en el proceso de Gestión de Cambios. Su utilidad deriva de las acciones consecuentes que se toman para reducir los riesgos identificados. Las acciones deben ser seguidas para asegurar que los riesgos se reducen a lo previsto.

11. Análisis de Peligros

Una vez que el área de enfoque de la evaluación de la seguridad se ha definido con precisión, será posible establecer una lista de los peligros relacionados. Esto puede hacerse de forma sistemática mediante el uso de un método reconocido, como AMFE (Análisis Modal de Fallos y Efectos), o bien, a través de una evaluación realizada por un grupo de personas con el conocimiento adecuado.

Una lista de los peligros detectados en sí mismo no siempre proporciona el material necesario para SIRA. Los peligros tienden a combinarse entre sí y con otros factores tales como las condiciones de visibilidad. Por lo tanto, el siguiente paso es la construcción de escenarios en los que los peligros identificados creen estados operacionales no deseados (UOS), que podrían dar lugar a un accidente.

12. Uso de SIRA para la Evaluación de la Seguridad Operacional

La etapa de análisis de peligros suele dar como resultado varios peligros potenciales y varios resultados posibles de accidentes, en torno a uno o más UOS. Por tanto, podría ser necesario limitar el estudio a los resultados más críticos.

El escenario(s) debe introducirse ahora en el marco SIRA. Esto significa identificar los UOS y el resultado más probable de accidente, el evento desencadenante y las barreras.

En el caso de varios escenarios, el que produce el mayor riesgo influiría en el nivel general de riesgo de la evaluación de la seguridad, pero todos los escenarios podrían considerarse en las acciones de reducción de riesgo resultantes.

6.4.2 METODOLOGÍA DE EVALUACIÓN DE RIESGOS: BOW-TIE

La metodología ARMS es considerada como la mejor práctica por ECAST. Sin embargo, ARMS no es la única metodología utilizable para la evaluación de riesgos.

Referencia: "Guidance on hazards identification" ECAST

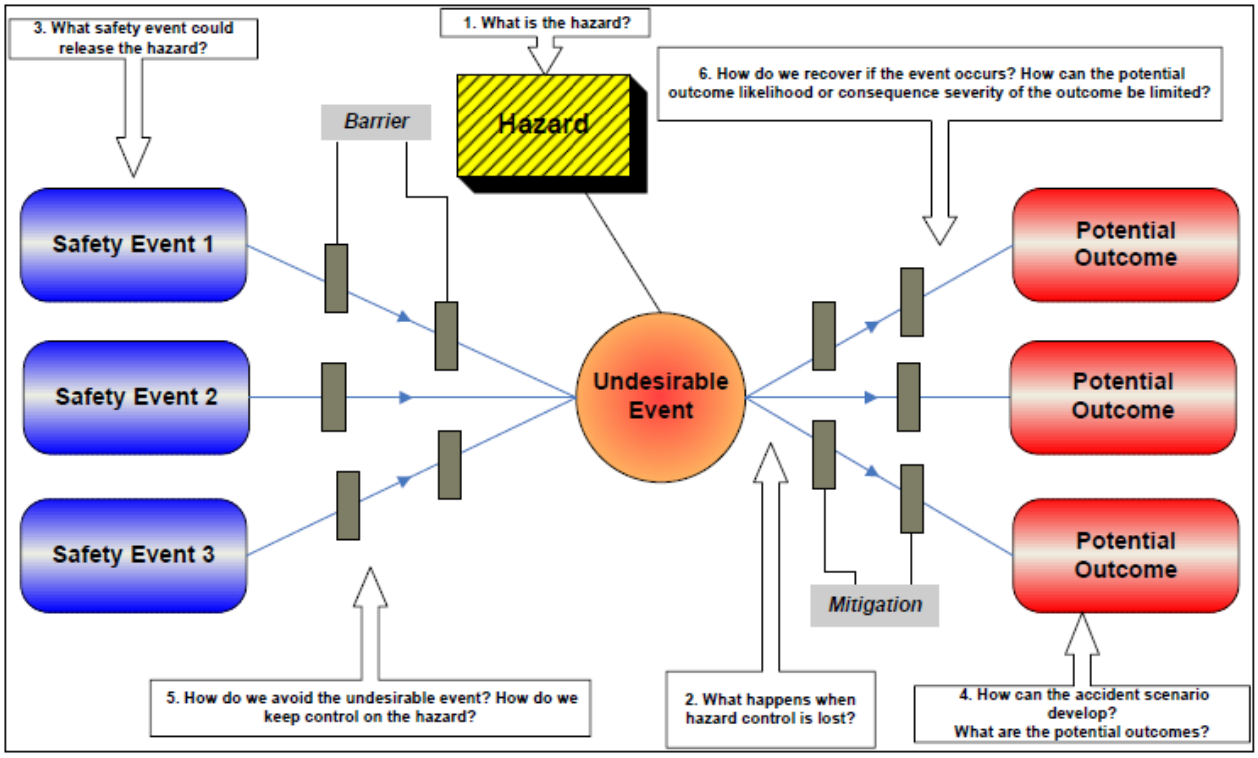
El método bow-tie muestra las relaciones entre los peligros, eventos principales, las consecuencias, los factores de escala y las barreras. La pajarita es una representación gráfica de cómo un peligro puede ser hipotéticamente liberado y dar lugar a una serie de consecuencias.

Para la construcción de un diagrama de pajarita es necesario realizar un conjunto estructurado de preguntas en una secuencia lógica:

1. ¿Cuál es el peligro?
2. ¿Qué ocurre cuando se pierde el control del peligro?
3. ¿Qué evento de seguridad podría liberar el peligro?
4. ¿Cómo podría desarrollarse un escenario (creíble) de accidente? ¿Cuáles serían los posibles resultados o consecuencias?

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

5. ¿Cómo se pueden evitar los eventos indeseados? ¿Cómo mantenemos control del peligro?
6. ¿Cómo se puede recuperar la situación si finalmente se produce el evento indeseado? ¿Cómo puede limitarse la probabilidad de que se produzca o la severidad de las consecuencias asociadas?



El análisis bow-tie tiene dos partes: prevención (identificar y controlar) y mitigación (evaluar y recuperar).

El método incluye los siguientes pasos:

– Identificación del peligro.

- Determinación del evento principal –*top event*– (definido como el punto en el que se pierde el control del peligro).
- Identificación de las amenazas o eventos iniciadores del peligro. Para cada amenaza es necesario identificar los controles preventivos y, cuando sea necesario, identificar controles de escala para evitar los factores de escala.
- Evaluación de las consecuencias. Para cada consecuencia es necesario establecer controles o barreras de recuperación y, si resultase necesario, se deben desarrollar factores de escala y controles de escala.

De acuerdo con *Edwards 99* los pasos del proceso son:

- Medidas proactivas:
  - Identificación de los peligros que pueden provocar un accidente.
  - Identificación de los contribuyentes del peligro.
  - Identificación de los eventos iniciadores o amenazas que podrían liberar los contribuyentes del peligro.
  - Evaluación de las barreras de control de riesgo existentes e identificación de controles adicionales que podrían ser necesarios para gestionar el riesgo adecuadamente.
- Medidas reactivas:
  - Evaluación de las medidas/barreras de recuperación apropiadas para devolver la situación a un estado lo más cercano posible a la normalidad.
  - Evaluación de las consecuencias que pueden originarse si los controles fallan y se libera el riesgo.
  - Identificación de las medidas de mitigación que se deben tomar para reducir al mínimo el efecto de las consecuencias sobre la compañía y las personas involucradas.

En la figura siguiente se puede ver una representación de los pasos anteriores:

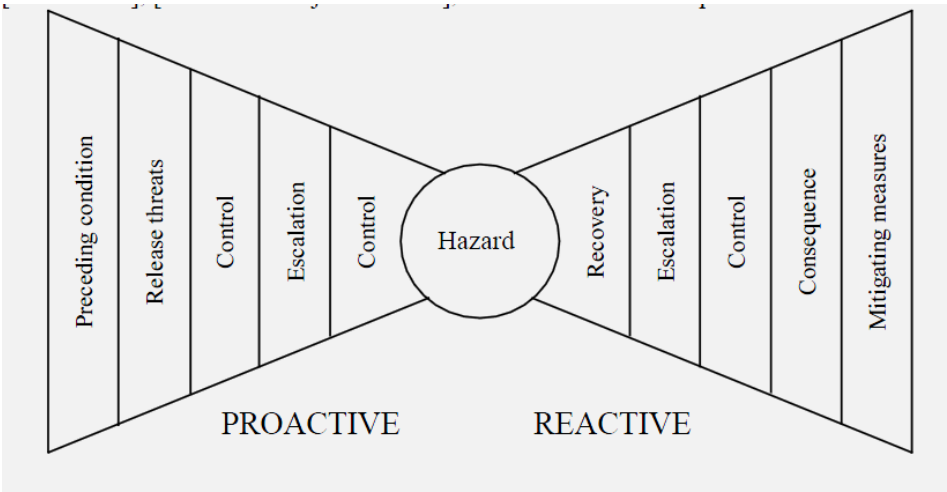


Imagen tomada de *Edwards99*

6.4.3 METODOLOGÍA DE EVALUACIÓN DE RIESGOS DEL GRUPO EHEST

Para analizar la probabilidad se realizan dos procesos en la metodología propuesta por el grupo EHEST de EASA:

- Las consecuencias de los peligros son analizadas para establecer las posibles causas, loa factores contribuyentes y las barreras existentes
- Las causas, los factores contribuyentes y las barreras son analizadas en detalle para determinar la probabilidad de un suceso.

En el análisis de las causas de la consecuencia se consideran factores humanos y de la organización como posibles efectos contribuyentes. Normalmente se consideran las causas directas ("actos inseguros"), las condiciones del lugar de trabajo y factores organizacionales ("desencadenantes de los errores o condiciones latentes").

Los efectos de las barreras y de los factores que reducen la probabilidad son tenidos en cuenta: requisitos de certificación, procedimientos de mantenimiento, procedimientos normales y especiales, equipo, formación, etc.

Para la realización de este tipo de análisis de las causas la compañía puede requerir a: árboles de fallos (fault tree analysis), FMECA (Failure Mode, Effects and Critical Analysis), diagramas de influencia, diagramas bow-tie, braimstorming…

Para analizar la severidad de todas las consecuencias de un peligro se tiene en cuenta el impacto en: pérdidas o daños a las personas, entorno, pérdidas o daños materiales, reputación.

6.4.4 OTRAS METODOLOGÍA DE EVALUACIÓN DE RIESGOS

Referencia: "FAA/Eurocontrol ATM Safety Techniques and Toolbox:

El documento de la FAA/Eurocontrol proporciona una lista de diversas metodologías que pueden ser usadas por el operador para la evaluación y mitigación de riesgos:

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

	Scoping	System Modeling	Hazard Identification	Risk Modeling	Risk Evaluation	Risk Reduction	Risk Monitoring	Feedback
Safety Management System	[Safety Plan]					Hazard tracking (HTRR)		Hazard Tracking (HTRR)
	[TLS]							
	TOPAZ							
General system safety techniques	FAST	System Modeling Techniques	HAZOP	Event Tree Analysis	Reliability Databases	HAZOP		
			FAST		FAST			
			FMECA	Fault Tree Analysis				
			External Events Analysis	Bow-Tie				
			Common Cause Analysis	Common Cause Analysis	Common Cause Analysis			
Operational Data Usage Specialised techniques			ASRS		ASRS		ASRS, ASAP	PLADS, GATE
			Air Safety Database		Bias & Uncertainty Assessment		Air Safety Database, FOQA, FDM, PDARS	Data Quality Filters, Data signatures, Morning Report
			Real-Time simulation					Data Signatures
		TOPAZ	TOPAZ	TOPAZ	TOPAZ	TOPAZ		
				Collision Risk Models	Collision Risk Models			
Human Factors		Hierarchical Task Analysis	Human Factors Case		Human Error Database	Human Factors Case		Future Flight Central
		SAFSIM			HEART		HERA	
		Reconfigurable flight simulator (RFS) SIMMOD-Pro	TRACER-Lite, Air-MIDAS + RFS		Air-MIDAS + RFS	TRACER-Lite		
		Human Performance Simulation	Human Performance Simulation	Human Performance Simulation	Human Performance Simulation	Human Performance Simulation		

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

7. OBSERVACIÓN Y MEDICIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL

Una vez iniciadas las operaciones por parte del operador aéreo, éste debe determinar las áreas de su sistema sobre las cuales deberá prestar particular atención en su monitorización de las operaciones, para verificar que las estrategias de mitigación funcionan de acuerdo con lo esperado. Tales áreas incluyen

- *Operaciones e instrucción*
- *Despacho*
- *Mantenimiento*

Referencia: "Manual de gestión de la seguridad operacional" (SMM), doc. 9859 de OACI, 3ª edición en español:

La observación y medición del rendimiento en material de seguridad operacional ha de satisfacer diversos objetivos. En primer lugar, las actividades de observación y medición de rendimiento se realizan para verificar las prestaciones de operador en relación con la política y objetivos de seguridad operacional del mismo. Es más, estas actividades han de garantizar que las estrategias de control o mitigación de los riesgos de seguridad operacional están siendo eficaces y eficientes.

La observación y medición del rendimiento se realiza a través de diversas actividades:

1.- Los *sistemas de notificación de incidentes obligatoria.*

2.- Los *sistemas de notificación voluntaria* permiten el envío de información relacionada con los peligros observados o errores accidentales sin un requisito legal o administrativo asociado para hacerlo. En estos sistemas, el operador puede ofrecer un incentivo para realizar un informe.

Los sistemas de notificación deben ser confidenciales, lo que requiere que cualquier información sobre la identidad del notificador sea protegida y eliminada o codificada antes de su distribución interna o difusión externa. Los informes desidentificados pueden respaldar futuros análisis de tendencias para rastrear la eficacia de la mitigación de riesgos y para identificar los peligros emergentes.

Para ser eficaces, las herramientas de notificación de seguridad operacional deben ser accesibles fácilmente para el personal operacional. El personal de operaciones debe aprender sobre los beneficios de los sistemas de notificación de la seguridad operacional y se les debe entregar retroalimentación acerca de las medidas correctivas tomadas en respuesta al informe. La alineación de los requisitos, las herramientas de análisis y los métodos del sistema de notificación pueden facilitar el intercambio de información de seguridad operacional, así como también, comparaciones de ciertos indicadores de seguridad operacional.

3.- *El estudio de seguridad operacional* es un análisis usado para obtener una comprensión de amplios temas de seguridad operacional o aquellos de una naturaleza global. Por ejemplo, la industria de las líneas aéreas puede producir recomendaciones de seguridad operacional e implementar medidas para reducir accidentes e incidentes durante las etapas de aproximación y aterrizaje. Los operadores

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

individuales pueden encontrar que estas recomendaciones globales mejoran el rendimiento en materia de seguridad operacional en el contexto de sus actividades de aviación.

4.- *Las revisiones de seguridad operacional* son un componente fundamental de la gestión de cambio. Estas se llevan a cabo durante la introducción de nuevas tecnologías, nuevos procedimientos o cambios sistémicos que afectan las operaciones de la aviación. Las revisiones de seguridad operacional tienen un objetivo claramente definido que se vincula con el cambio en consideración. Las revisiones de seguridad operacional garantizan que el rendimiento en materia de seguridad operacional se mantenga a niveles adecuados durante los períodos de cambio.

5.- *Las encuestas de seguridad operacional* examinan los procedimientos o procesos relacionados con una operación específica. Las encuestas de seguridad operacional implican el uso de listas de verificación, cuestionarios y entrevistas confidenciales e informales. Las encuestas de seguridad operacional proporcionan generalmente información cualitativa que puede requerir de validación para determinar la medida correctiva correspondiente. Sin embargo, las encuestas pueden ser una fuente de información de seguridad operacional importante.

6.- *Las auditorías* se centran en la integridad del SMS de la organización y en sus sistemas de respaldo. Las auditorías proporcionan una evaluación de los controles de riesgos de seguridad operacional y los procesos de aseguramiento de la calidad relacionados. Las auditorías pueden realizarse mediante entidades externas al operador o con un proceso de auditoría interna que cuente con las políticas y los procedimientos necesarios para garantizar su independencia y objetividad. Las auditorías tienen como fin proporcionar el aseguramiento de las funciones de la gestión de la seguridad operacional, lo que incluye al personal, el cumplimiento de reglamentos aprobados, niveles de competencia y capacitación.

7.- Las *investigaciones internas* se llevan a cabo para ciertos eventos de seguridad operacional que pueden notificarse, de acuerdo con los requisitos internos o reglamentarios. Los accidentes e incidentes graves que investiga el Estado también pueden proporcionar el estímulo para llevar a cabo investigaciones internas por parte del operador aéreo

Además de las fuentes indicadas por OACI, otras fuentes de datos a considerar serían:

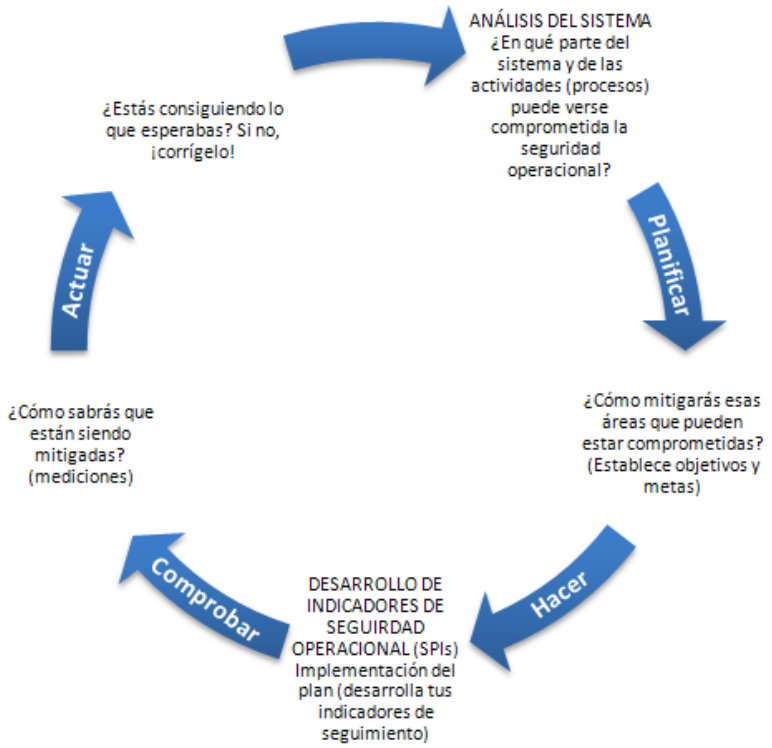
- El “technical book” de las aeronaves, los informes de despacho, los registros de mantenimiento y ls órdenes de compras de repuestos.
- Los registros de actividad de pilotos

El resultado final del control y la medición del rendimiento en materia de seguridad operacional es el desarrollo de indicadores de rendimiento en materia de seguridad operacional, basados en el análisis de los datos recopilados mediante las fuentes nombradas anteriormente. El proceso de control y medición implica el uso de indicadores de rendimiento en materia de seguridad operacional seleccionados y niveles de objetivos (metas) y alertas del rendimiento en materia de seguridad operacional correspondientes.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

7.1 CÓMO MEDIR: TIPOS DE INDICADORES DE RENDIMIENTO DE SEGURIDAD OPERACIONAL

Referencia: "Measuring Safety Performance. Guidelines for Service Provider" del SM ICG:



Una medición efectiva del rendimiento en materia de seguridad operacional no solo servirá para la identificación de oportunidades de mejora relacionadas con la seguridad operacional, sino también con la eficiencia y la capacidad.

La gestión de la seguridad operacional se basa en la capacidad de su organización para anticipar sistemáticamente, monitorizar y seguir desarrollando el rendimiento en materia de seguridad operacional de la organización para garantizar unos resultados seguros de sus actividades. La gestión eficaz de la seguridad operacional requiere un profundo conocimiento y una buena gestión de su sistema y procesos. Esto no se puede lograr sin alguna forma de medición. En lugar de seleccionar al azar los resultados que son fáciles de medir, habría que seleccionar los indicadores de rendimiento en materia de seguridad operacional teniendo en cuenta el tipo de información que se va a obtener de los mismos con el fin de asegurar que se pueda evaluar y mejorar adecuadamente la capacidad de la organización para gestionar la seguridad operacional. Esto implica que es necesario medir el rendimiento en todos los niveles de su organización mediante la adopción de un amplio conjunto de indicadores relacionados con aspectos clave de su sistema y operaciones, y permitir medir estos aspectos clave de diferentes maneras.

La OACI define **indicador de rendimiento en materia de seguridad operacional** como "*parámetro basado en datos que se utiliza para observar y evaluar el rendimiento en materia de seguridad operacional*" y **meta de rendimiento en materia de seguridad operacional** como "*el objetivo*

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

proyectado o que se desea conseguir, en cuanto a los indicadores de rendimiento en materia de seguridad operacional, en un período de tiempo determinado".

Los indicadores de rendimiento en materia de seguridad operacional (SPI) pueden ser "clasificados" de acuerdo con las características específicas; y comúnmente se utilizan diversas clasificaciones en diferentes áreas. Los tipos de indicadores que se describen en este documento se han definido después de una revisión las clasificaciones y definiciones habitualmente utilizadas para identificar puntos en común. Se proporciona una aclaración donde se estima relevante para cada uno. Usted puede adoptar cualquiera de los términos para sus indicadores de rendimiento en materia de seguridad operacional que mejor puedan ajustarse a su organización; la siguiente información se proporciona para complementar los conceptos necesarios para una medición efectiva del rendimiento en materia de seguridad operacional.

- Indicadores de resultados (o *lagging indicator* en terminología inglesa)

  "*Métrica que mide los eventos de seguridad operacional que ya han ocurrido, incluyendo los eventos de seguridad operacional no deseados y que se están tratando de evitar*" (SM ICG).

  Los indicadores de resultados (o *lagging indicator*) son medidas de los sucesos de seguridad operacional, en particular, los resultados negativos que la organización está tratando de evitar. Los indicadores de resultados se utilizan principalmente para las tendencias agregadas a largo plazo, ya sea a alto nivel o para tipos específicos de sucesos o ubicaciones. Dado que miden los resultados de seguridad operacional, pueden ser utilizados para evaluar la eficacia de las medidas, acciones o iniciativas, y son una manera de validar el rendimiento en materia de seguridad operacional del sistema. Además, se puede analizar la evolución de estos indicadores para determinar si existen condiciones latentes en los sistemas actuales que deberían ser abordadas.

  Hay dos tipos de indicadores de resultados que generalmente se definen como:

  1. Indicadores de resultados con severidad muy alta, como accidentes o incidentes graves.

     La baja frecuencia de resultados con severidad muy alta significa que la agregación (por ejemplo, en el ámbito del segmento de la industria o en el ámbito regional) puede producir análisis más significativos.

     Ejemplo: número de salidas de pista / 1000 aterrizajes.

  2. Indicadores de fallos en el sistema y de eventos de seguridad operacional de menor severidad que no se manifiestan en incidentes graves o en accidentes (incluidos los fallos del sistema y las desviaciones de procedimiento); sin embargo, el análisis de seguridad operacional indica que, potencialmente, pueden desencadenar un incidente grave o un accidente cuando se combinan con otros eventos o condiciones. Estos indicadores se denominan a veces como indicadores "precursores de eventos"[5].

[5] Este término se debe utilizar con precaución: antes de definir un evento o condición como un precursor de otro evento o condición más grave (p.ej. incidentes como precursores de accidentes), se debe asegurar que existe una correlación demostrable entre los dos. Tal correlación es la base de la validez del concepto de medición. Los factores que causan los

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Los indicadores de fallos en el sistema y de eventos de seguridad operacional de menor severidad se utilizan principalmente para monitorizar los problemas de seguridad operacional específicos y para medir la eficacia de los controles o barreras de seguridad operacional puestos en marcha para mitigar los riesgos asociados a dichos peligros.

Ejemplo: número de aproximaciones no estabilizadas / 1000 aterrizajes

- Indicadores predictivos (o *leading indicator* en terminología inglesa)

"Medidas que proporcionan información sobre la situación actual que puede afectar al rendimiento futuro" (SM ICG).

Los indicadores predictivos deberían medir tanto lo que tiene el potencial de convertirse o contribuir a un resultado negativo en el futuro (indicadores "negativos") como lo que contribuye a mejorar la seguridad operacional (indicadores "positivos"). Desde una perspectiva de gestión de seguridad operacional, es importante proporcionar suficiente atención en la monitorización de indicadores positivos para permitir el fortalecimiento de los factores positivos que conforman la capacidad de gestión de la seguridad operacional de su organización.

Los indicadores predictivos, que son particularmente relevantes desde una perspectiva de gestión, se pueden utilizar para influir en las prioridades de gestión de la seguridad operacional y en la definición de las acciones de mejora de la seguridad operacional. Puede usar este tipo de indicador para desarrollar de manera preventiva ("dirigir" o "*drive*" en terminología inglesa) las capacidades de gestión de seguridad operacional de su organización, y en particular durante la implementación inicial de SMS. Esto puede implicar el establecimiento de metas de rendimiento.

Ejemplo: porcentaje de cambios en los Procedimientos Operativos Estándar (SOPs que en inglés se corresponden con Standard Operating Procedures) que han sido objeto de identificación de peligros y gestión de riesgos de seguridad operacional

Los indicadores predictivos también se pueden usar para informar a la gestión acerca de la dinámica del sistema y cómo hacer frente a los cambios, incluyendo los cambios que se dan en su entorno operativo. El enfoque será: o bien en la anticipación de las debilidades y vulnerabilidades emergentes para determinar la necesidad de una acción, o bien en el seguimiento del grado en que se realizan ciertas actividades necesarias para la seguridad operacional. Los niveles de alerta se pueden definir para estos indicadores de "monitorización" (o *monitoring* en terminología inglesa).

Ejemplo: grado en que se lleva a cabo el trabajo de acuerdo con los SOPs

Idealmente, la medición del rendimiento en materia de seguridad operacional debería considerar una combinación de indicadores predictivos y de resultados. El objetivo principal debería ser el de medir y actuar sobre la presencia de los atributos sistémicos y operativos que permiten una gestión eficaz de la seguridad operacional dentro de su organización (indicadores predictivos) y, mientras tanto, utilizar los indicadores de resultados para asegurar que esta gestión de la seguridad operacional es eficaz. Los

---

incidentes definidos como "precursores" deben ser comunes entre estos incidentes y los accidentes que se supone que predicen.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

indicadores de resultados, particularmente los indicadores de fallos en los sistemas de menor nivel, son útiles para validar la eficacia de las medidas específicas de seguridad operacional y de las barreras de riesgo o para apoyar el análisis de la información derivada de los indicadores predictivos.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

8. PLAN DE ACCIÓN DE SEGURIDAD OPERACIONAL

El Plan de Acción de Seguridad Operacional del operador documentará las áreas de seguridad operacional que se han detectado como prioritarias o de mayor necesidad, durante la monitorización continua de las operaciones, junto con las acciones correctivas que se consideren apropiadas. Además, dicho Plan de Acción de Seguridad Operacional habrá de ser coherente con el Plan de Acción de Seguridad Operacional establecido por el Estado español.

Todas las actuaciones que se incluyan en el Plan de Acción de Seguridad Operacional irán acompañadas de los recursos humanos y económicos necesarios para conseguirlas así como de los plazos en los que han de ser alcanzadas. Se asignará un responsable para el logro de la actuación.

A modo de ejemplo, las actuaciones en el ámbito sistemático podrían ser:

- Actuaciones para el cumplimiento de la política y objetivos de seguridad operacional del operador.
- Actuaciones derivadas de los resultados de la gestión de riesgos y del aseguramiento de la seguridad operacional.
- Actuaciones derivadas del control de aspectos de seguridad operacional de los Proveedores Externos con los que interactúa el operador.
- Actuaciones derivadas de las necesidades de formación y comunicación en el ámbito de la seguridad operacional.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

9. GESTIÓN DEL CAMBIO

Referencia: "Manual de gestión de la seguridad operacional" (SMM), doc. 9859 de OACI, 3ª edición en español:

Los operadores experimentan cambios debidos a diversos factores:

a) la expansión o contracción;

b) cambios en los sistemas, equipos, procesos o procedimientos internos que respaldan la entrega del servicio;

c) cambios en el entorno de operación de la organización

Puede que se introduzcan peligros de forma accidental en el sistema de aviación cuando sucede un cambio. Los procesos base de la mitigación de riesgos de la seguridad operacional existentes también pueden verse afectados. Las prácticas de gestión de la seguridad operacional requieren que se identifiquen sistemáticamente los peligros a causa de los cambios y que se desarrollen, implementen y posteriormente evalúen las estrategias para gestionar los riesgos de seguridad operacional resultantes. Una gestión sólida de los riesgos de seguridad operacional asociados con el cambio es un requisito fundamental del Sistema de Gestión de la Seguridad Operacional.

La gestión de los riesgos de seguridad operacional resultantes de los cambios ha de considerar los siguientes tres puntos:

a) Criticidad de los sistemas y las actividades. Las evaluaciones de criticidad determinan los sistemas, los equipos o las actividades que son fundamentales para la operación segura de la aeronave. Aunque la criticidad se evalúa normalmente durante el proceso de diseño del sistema, también es relevante durante una situación de cambio. Los sistemas, los equipos y las actividades que tengan una criticidad de seguridad operacional más alta deben revisarse después del cambio para asegurarse de que se tomaron las medidas correctivas para controlar los riesgos de seguridad operacional potencialmente emergentes.

b) *Estabilidad de los sistemas y entornos operacionales.* Los cambios pueden ser planificados y estar bajo el control directo de la organización. Los cambios planificados pueden asociarse al crecimiento o contracción de la organización, así como también, a la introducción de nuevos equipos, productos o servicios. Los cambios no planificados, como aquellos que son de naturaleza operacional, política o económica, también pueden crear riesgos que requieren una respuesta de mitigación de la organización. Las instancias donde ocurren cambios sistémicos o del entorno frecuentes indican que los gerentes deben actualizar las evaluaciones de riesgo clave y la información asociada con más frecuencia que en situaciones más estables.

c) *Rendimiento pasado.* El rendimiento pasado de los sistemas fundamentales o críticos puede ser un indicador fiable de un rendimiento futuro. Los análisis de tendencias en el proceso de aseguramiento de la seguridad operacional deben usarse para evaluar el rendimiento en materia de seguridad operacional y para incluir tal información en la planificación de actividades futuras bajo situaciones de cambio. Es más, en aquellos lugares donde se han encontrado deficiencias y se han corregido, como resultado de auditorías, evaluaciones, análisis de datos, investigaciones o informes pasados, es esencial que dicha información se considere para garantizar la eficacia de las medidas correctivas.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Se han desarrollar los siguientes procedimientos:

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

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

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

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

ANEXO A. EJEMPLOS DE LA COMPONENTE GESTIÓN DE RIESGOS

1. CASO 1: OPERACIÓN EN UN AEROPUERTO EN OBRAS DE CONSTRUCCIÓN

Situación operativa

Un operador de transporte aéreo comercial recibe una notificación del gestor del aeropuerto, que es su base principal, sobre la instalación de un sistema de drenaje cerca de una de las cabeceras de la pista secundaria. El aeropuerto en cuestión tiene dos pistas paralelas, una principal y otra secundaria Los vehículos de construcción deberán cruzar la pista principal para llegar al sitio de construcción.

Debido a que durante el día se registra un elevado volumen de operaciones, el gestor aeroportuario ha decidido trabajar por la noche, cuando el volumen de tránsito es menor, para evitar grandes disrupciones de las operaciones diurnas. El análisis del plan de construcción propuesto por el gestor aeroportuario indica un peligro inmediato y obvio: el movimiento de vehículos de construcción hacia y desde el lugar de obra, que podría tener como consecuencia la posibilidad de incursiones en pista.

El operador decide llevar a cabo un análisis de gestión de riesgos de seguridad operacional, para evaluar las consecuencias para la seguridad operacional del plan de construcción nocturna del sistema de drenaje.

Descripción del sistema

La primera tarea en el análisis de gestión de riesgo de seguridad operacional es describir el sistema modificado en cuyo marco el aeropuerto continuará sus operaciones mientras se realizan las obras de construcción. Tal descripción debe abarcar:

a) el contexto físico de las pistas durante las obras nocturnas, que incluye un significativo volumen de tránsito de vehículos de construcción entre la rampa y el lugar de la obra;
b) la torre de control de tránsito aéreo y el hecho de que no existen radiocomunicaciones con los vehículos de construcción que no están equipados para ello; y
c) carteles, señales e iluminación para las calles de rodaje, pistas y zona de obras.

Identificación de peligros

Peligro genérico – Obras de construcción en el aeropuerto.

Componente(s) específico(s) del peligro genérico – Vehículos de construcción que cruzan la pista principal.

Consecuencia(s) de los componentes específicos del peligro genérico – El operador establece dos consecuencias posibles, de diferente severidad:

1) Los vehículos de construcción pueden desviarse de los procedimientos prescriptos y cruzar la pista principal sin escolta;

2) Puede haber conflicto entre aeronaves y vehículos que crucen la pista principal.

Evaluación de riesgos de seguridad operacional

La evaluación del operador lleva a la conclusión de que existe una probabilidad remota que un vehículo de construcción se desvíe de los procedimientos prescritos y cruce la pista principal sin escolta.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Hay operaciones aéreas nocturnas de volumen reducido en el aeropuerto, de modo que se evalúa que existe una probabilidad remota que una aeronave pueda entrar en conflicto con un vehículo que cruza.

Si bien la probabilidad de conflicto entre una aeronave y un vehículo de construcción es remota, el operador evalúa que, en caso de ocurrir dicho conflicto, la consecuencia podría ser de severidad catastrófica.

El operador evalúa las defensas (medidas de control/mitigación) propuestas por el gestor aeroportuario. Tales defensas abarcan un programa de instrucción de conductores, el uso de escoltas para vehículos de construcción, y la existencia de carteles, señales e iluminación. Aplicando su matriz de evaluación de los riesgos de seguridad operacional y de tolerabilidad de riesgos de seguridad operacional, evalúa el índice de riesgo de seguridad operacional como inaceptable en las circunstancias actuales.

Por lo tanto, las consecuencias del peligro generado por el movimiento de vehículos de construcción hacia el lugar de la obra son, en las condiciones propuestas, inaceptables y es necesario aplicar defensas (medidas de control/mitigación) adicionales.

Control/mitigación de los riesgos de seguridad operacional

El operador decide que es necesario proponer al gestor aeroportuario la utilización de un camino perimetral existente en el aeródromo, pero que debe ser reacondicionado, para que los vehículos de construcción accedan al sitio de la obra; y que todos los vehículos de construcción sean escoltados por el camino perimetral.

Con esta mitigación, el operador reevalúa como probabilidad extremadamente improbable que los vehículos de construcción atraviesen la pista principal sin escolta, o que las aeronaves puedan entrar en conflicto con un vehículo que cruza. No obstante, si ocurriera un conflicto entre aeronaves y vehículos de construcción, tal consecuencia sería de severidad catastrófica.

El uso del camino perimetral como mitigación conducirá a demoras en el tránsito de los vehículos de construcción debido a la distancia adicional que los vehículos deben recorrer. Aun cuando en la evaluación del operador el uso del camino perimetral no elimina enteramente la posibilidad de que ocurran las consecuencias del peligro (los vehículos de construcción todavía pueden atravesar la pista principal debido a varias circunstancias), no obstante reduce las consecuencias del peligro (vehículos de construcción que se desvían de procedimientos prescritos y atraviesan la pista principal sin escolta, y aeronaves en conflicto con un vehículo que cruza) a un nivel tan bajo como sea razonablemente práctico.

Registro de identificación de peligros y gestión de riesgos de seguridad operacional

Aplicando las matrices de evaluación de riesgos de seguridad operacional y de tolerabilidad de riesgos de seguridad operacional, el operador reevalúa el índice de riesgo de seguridad operacional como extremadamente improbable, y documenta este proceso de decisión para seguimiento futuro en el registro de identificación de peligros y gestión de riesgos de seguridad operacional, según se expone a continuación.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Registro de identificación de amenazas o peligros y gestión de riesgos de seguridad operacional

Tipo de operación o actividad	Peligro genérico	Componentes específicos del peligro	Consecuencias relacionadas con el peligro	Defensas actuales para controlar el riesgo de seguridad operacional e índice del riesgo	Acciones ulteriores para reducir el riesgo de seguridad operacional e índice del riesgo de seguridad resultante
Operaciones de vuelo	Construcción en el aeropuerto	Vehículos de construcción que cruzan la pista principal	a) Los vehículos de construcción pueden desviarse de los procedimientos prescritos y cruzar la pista principal sin escolta b) Las aeronaves pueden entrar en conflicto con los vehículos que cruzan	• Obras de construcción durante la noche • Programa de instrucción de conductores • Uso de escoltas para vehículos de construcción • Carteles, señales e iluminación ***Índice de riesgo de seguridad:*** *3A* ***Tolerabilidad del riesgo de seguridad:*** *Inaceptable en las condiciones actuales*	• Utilización de un camino perimetral ***Índice de riesgo de seguridad:*** *1A* ***Tolerabilidad del riesgo de seguridad:*** *extremadamente improbable*

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

2. CASO 2: INICIACIÓN DE OPERACIONES EN PISTAS DE PEDREGULLO

Informe sobre el análisis de la operación del BAe Jetstream 31 en pistas de pedregullo

Un operador pequeño va a iniciar operaciones en pistas de pedregullo con aeronaves BAe Jestream 31. Por ello, debe desarrollar e implementar las medidas necesarias para permitir las operaciones con tales aeronaves en tales pistas. Completadas las averiguaciones y acciones del caso, dando curso a la necesidad, se llega a una propuesta, que es aprobada. Se enmienda al Manual de Operaciones de la compañía para reflejar la propuesta, y se remite para su impresión, que llevará tres semanas. El cambio del Manual de Instrucción para acomodar la enmienda sobre operación en pistas de pedregullo es aprobada por la Autoridad de Aviación Civil, y hasta tanto los procedimientos de operación estándares (SOPs) sean incorporados a la enmienda del Manual de Operaciones, se publica un Memorando Provisional de Operaciones de inmediata aplicación firmado por el Post-holder o Responsable de Operaciones. Se completa el entrenamiento teórico terrestre, y se archiva el registro de la instrucción.

El siguiente personal integró el equipo de análisis:

- Gestor de seguridad operacional
- Supervisor de la flota BA31
- Comandante de BA31
- Supervisor de mantenimiento de la flota BA31
- Encargado de instrucción
- Representante de la Gerencia Comercial
- Primer Oficial de BA31
- Ex Comandante de BA31 (2000 hrs. de experiencia en pedregullo en BA31)

Resumen del análisis

1. -Planificación y operación

Se compiló un listado de las pistas de pedregullo utilizables, para su evaluación y aprobación de las operaciones en las mismas. Inicialmente la operación comenzará con pistas de pedregullo compactadas de 5000 pies de longitud. El tiempo de servicio de las tripulaciones se iniciará con una presentación de dos (2) horas de anticipación antes de la salida para prever la planificación adecuada de la operación y el briefing de la tripulación. Deberá ponerse una escoba en las aeronaves durante todo el año a fin de limpiar el área debajo de las hélices previo a la puesta en marcha.

Cualquier requerimiento de vuelo a una pista de pedregullo que no se encuentre en la lista de pistas aprobadas requerirá una evaluación del riesgo de seguridad operacional específico antes del vuelo. Esta coordinación demandará un tiempo adicional, pero se considera indispensable para asegurar el control adecuado de riesgos de seguridad operacional.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

2. Instrucción

La instrucción inicial en vuelo será realizada por dos comandantes supervisados por el comandante con gran experiencia en pistas de pedregullo. El gerente de seguridad operacional los acompañará si está disponible. No se programarán copilotos hasta que los dos comandantes hayan acumulado 10 despegues y aterrizajes cada uno en pistas de pedregullo. A menos que se combine la instrucción inicial en vuelo con los vuelos arrendados, esto significará aproximadamente 7 horas de vuelo. El responsable de la instrucción coordinará la instrucción con el departamento Comercial antes del comienzo de la operación en pista de pedregullo.

3. Mantenimiento

Aunque no existen requisitos normativos de mantenimiento para la autorización de la operación, se ha decidido lo siguiente:

- Remover la luz anti-colisión inferior
- Agregar una cubierta extra de tren de aterrizaje en el alojamiento para equipajes inferior
- Aplicar un aislante para la protección de los flaps
- Instalar hélices con palas Mk II (más robusta)
- Efectuar un servicio preventivo a los amortiguadores después de cada vuelo
- Completar una inspección preventiva de las botas deshieladoras de ala y hélice después de cada vuelo por posibles daños.

4. Documentación

Se documentan los cambios en el procedimiento de operación estándar (SOP) y el Memorando Provisional de Operaciones con los procedimientos y prácticas detalladas.

5. Mitigación del riesgo

Ver la tabla adjunta

6. Responsabilidades en el ámbito de la gestión de la seguridad operacional

Se mantendrá una reunión de información con el Director Responsable antes del comienzo de la operación en pedregullo.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

Registro de identificación del peligro y gestión del riesgo de seguridad operacional (simplificado)

Nº	**1.** Tipo de operación o actividad	**2.** Peligro genérico	**3.** Componentes específicos del peligro	**4.** Consecuencias relacionadas con el peligro	**5.** Acciones para reducir el riesgo de seguridad operacional e índice del riesgo de seguridad operacional resultante
	Operaciones de vuelo	Operación en pista de pedregullo	Largo de pista	Salida de pista	• Pista mínima 5000 pies • Calificación especial de aeródromo para las tripulaciones • Instrucción teórica y de vuelo • Enmienda al Manual de Operaciones • Establecimiento de una lista de pistas con pedregullo autorizadas para su operación • Revisión del tiempo de servicio de las tripulaciones por una presentación anticipada de dos (2) horas antes de la salida del vuelo • Toda nueva operación en pistas con pedregullo no listadas requerirá una evaluación de riesgo de seguridad operacional ***Índice de riesgo de seguridad:*** *2A* ***Tolerabilidad del riesgo de seguridad:*** *Aceptable en base a la mitigación*
2	Operaciones de vuelo	Operación de pista de pedregullo	Condición de la pista	• Daño a la luz anti-colisión inferior • Daño a cubiertas • Daño a los flaps • Daño a las palas de las hélices • Daño a los amortiguadores de tren de aterrizaje • Daño a las botas deshieladoras	• Remover luz anti-colisión inferior • Cubierta extra en el alojamiento inferior • Protector de flaps aplicado antes de cada operación • Instalar palas Mk. III • Servicio a los amortiguadores luego de cada operación • Inspección de botas luego de cada operación *Índice de riesgo de seguridad:* ***2A*** *Tolerabilidad del riesgo de seguridad:* ***Aceptable en base a la mitigación***

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

ANEXO B. EJEMPLOS DE INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL – MATERIAL OACI

En este Anexo se muestran ejemplos de indicadores de rendimiento en materia de seguridad operacional, tanto del Estado como del operador aéreo, junto con los criterios para el establecimiento de las alertas y metas asociadas a los mismos. Estos ejemplos se han extraído del documento 9859 versión 3 de OACI. Se hace hincapié con estos ejemplos en la necesidad de que los indicadores de rendimiento en materia de seguridad operacional del operador sean coherentes con los establecidos por el Estado en el marco del Programa Estatal de Seguridad operacional para la Aviación civil.

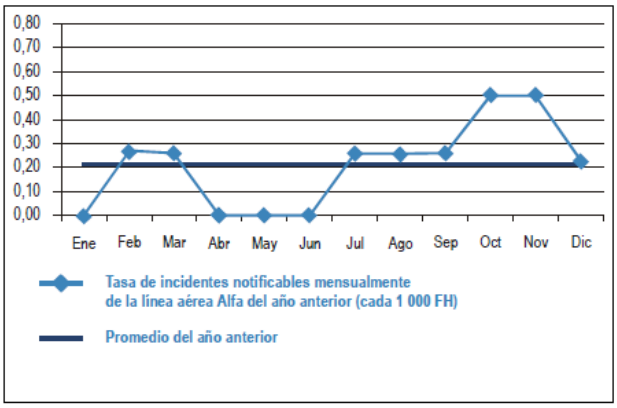
Indicadores de seguridad operacional del SSP (Estado colectivo)						*Indicadores de rendimiento en materia de seguridad operacional del SMS (proveedor de servicios individual)*					
Indicadores de alto impacto (basados en sucesos/resultados)			*Indicadores de bajo impacto (basados en eventos/actividad)*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

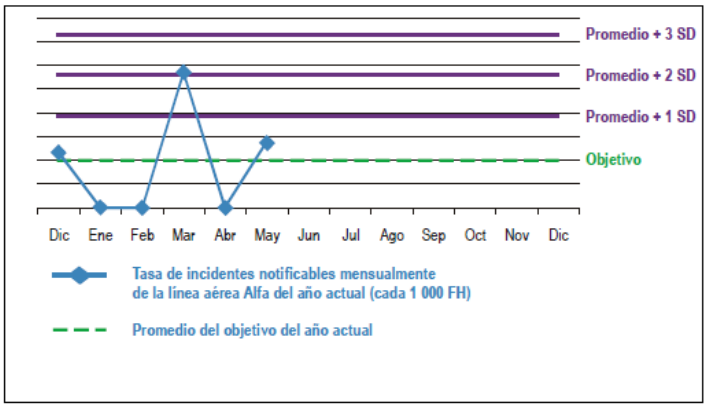
A continuación se muestra, a modo de ejemplo, la evolución de un indicador de rendimiento en materia de seguridad operacional. El indicador seleccionado es la tasa de incidentes de un operador aéreo. Se compara la evolución del año actual con respecto a la evolución del año anterior. Además, se ha definido el valor de alerta utilizando la desviación estándar según la fórmula:

$\sigma = \sqrt{\frac{\sum(x-\mu)^2}{N}}$, donde "X" es el valor de cada dato; "N" es el número de datos y "μ" es la media de todos los datos.

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

La meta se ha definido como una mejora porcentual del 5% de la media del año anterior.





Más ejemplos de indicadores de seguridad operacional propuestos por OACI:

Indicador de rendimiento en materia de seguridad operacional de alto impacto					
	Descripción del SPI	*Criterios del nivel de alerta del SPI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios del nivel de objetivos del SPI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Tasa de incidentes graves mensual de la flota A320 de la línea aérea Alfa (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No
2	Tasa de incidentes de IFSD de la flota A320 de la línea aérea Alfa (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	Sí	3% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
3	etc.				

Indicadores de seguridad operacional de bajo impacto					
	Descripción del SPI	*Criterios del nivel de alerta del SPI (para 2010)*	*Nivel de alerta violado (Sí/No)*	*Criterios del nivel de objetivos del SPI (para 2010)*	*Objetivo logrado (Sí/No)*
1	Tasa de incidentes mensual de la flota combinada del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	No
2	Tasa de % o hallazgos de LEI anual de la auditoría de QMS interna del explotador (hallazgos por auditoría)	Más del 25% del LEI promedio o cualquier hallazgo de Nivel 1 o más de 5 hallazgos de Nivel 2 por auditoría	Sí	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
3	Tasa del informe de peligros voluntario del explotador (por ejemplo, cada 1 000 FH)	TBD		TBD	
4	Tasa del informe de incidentes de DGR del explotador (por ejemplo, cada 1 000 FH)	Promedio + 1/2/3 SD (restablecimiento anual o cada 2 años)	No	5% de mejora de la tasa promedio de 2010 sobre la tasa promedio de 2009	Sí
5	etc.				

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

ANEXO C. EJEMPLOS DE INDICADORES DE RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL – MATERIAL SM ICG

A continuación se muestran los indicadores propuestos por el grupo SM ICG, a modo de ejemplo, en la guía "Medición del rendimiento en materia de seguridad operacional. Guía para proveedores de servicio":

INDICADORES DE CUESTIONES SISTÉMICAS

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
CONFORMIDAD	Monitorización de auditorías/cumplimiento internas: todos los incumplimientos	▪ Número total/tendencia en el ciclo de planificación de la auditoría, ▪ % de los incumplimientos analizados por su importancia para la seguridad operacional.
	Monitorización de auditorías/cumplimiento internas: incumplimientos importantes	▪ número de incumplimientos significativos en comparación con el número total de incumplimientos, ▪ número de incumplimientos repetidos dentro del ciclo de planificación de auditorías.
	Monitorización de auditorías / cumplimiento internas: la capacidad de respuesta a las solicitudes de acción correctiva	▪ Tiempo de espera promedio para completar las acciones correctivas por ciclo de planificación de supervisión – tendencia.
	Monitorización de auditorías/cumplimiento externas: todos los incumplimientos	▪ Número total/tendencia en el ciclo de planificación de la supervisión ▪ % de los incumplimientos analizados por su importancia para la seguridad operacional,
	Auditorías externas: incumplimientos importantes	▪ Número de incumplimientos significativos en comparación con el número total de incumplimientos
	Auditorías externas: la capacidad de respuesta a las solicitudes de acción correctiva	▪ Tiempo de espera promedio para completar las acciones correctivas por ciclo de planificación de supervisión - tendencia
	Consistencia de los resultados entre auditorías internas y externas / control del cumplimiento	▪ Número de incumplimientos significativos descubiertos solamente a través de las auditorías externas
EFECTIVIDAD DEL SMS	Gestión estratégica	▪ Grado en que se considera la seguridad operacional en los planes oficiales de la organización y los documentos de estrategia ▪ Frecuencia con la que los planes oficiales de la organización y los documentos de estrategia son revisados con respecto a la seguridad operacional
EFECTIVIDAD DEL SMS	Compromiso de la dirección	▪ Número de "walk-arounds" de la gestión por mes / trimestre / año ▪ Número de reuniones de gestión dedicadas a la seguridad operacional al mes / trimestre / año
	Tasa de rotación del personal clave de seguridad operacional	▪ Duración del mandato ▪ Número de casos en los que se han analizado las razones de la salida del personal clave
	Supervisión	▪ Número de casos en que los supervisores expresaron feedback positivo sobre el comportamiento consciente en materia de seguridad operacional de su personal al mes / trimestre / año

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
	Notificación	▪ Número de notificaciones recibidas al mes / trimestre / año y la tendencia ▪ % de las notificaciones a las que se proporcionó información al notificante dentro de los 10 días hábiles ▪ % de las notificaciones seguidas de una revisión independiente de la seguridad operacional
	Identificación de los peligros	▪ Número de escenarios de accidentes / incidentes graves analizados para apoyar la Gestión de Riesgos de Seguridad operacional (SRM) al mes / trimestre / año ▪ Número de nuevos peligros identificados a través del sistema de notificación interno al mes / trimestre / año y la tendencia ▪ Incumplimientos de las auditorías externas relacionados con peligros que no habían sido percibidos por el personal / gestión previamente ▪ Número de notificaciones de seguridad operacional recibidas del personal al mes / trimestre / año y la tendencia
	Controles de riesgo	▪ Número de nuevos controles de riesgo validados por mes / trimestre / año ▪ % del presupuesto total asignado a nuevos controles de riesgo
	Gestión y desarrollo de las competencias de recursos humanos	▪ % de la plantilla para la que se ha establecido un perfil de competencias ▪ % de personal que ha tenido formación en gestión de la seguridad ▪ Frecuencia de revisión de los perfiles de competencias ▪ Frecuencia de revisión del alcance, contenido y calidad de los programas de formación ▪ Número de cambios realizados en los programas de formación a raíz de la realimentación del personal al mes / trimestre / año ▪ Número de cambios realizados en los programas de formación a raíz del análisis de las notificaciones de seguridad operacional internas por mes / trimestre / año
	Gestión del cambio	▪ Número de cambios organizativos para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al mes / trimestre / año y la tendencia ▪ Número de cambios en los Procedimientos Operativos Estándar (SOPs) para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al mes / trimestre / año y la tendencia ▪ Número de cambios técnicos (por ejemplo , nuevos equipos, nuevas instalaciones , nuevo hardware) para los que se ha realizado una evaluación formal de los riesgos de seguridad operacional al mes / trimestre / año y la tendencia ▪ Número de controles de riesgo implementados por los cambios al mes / trimestre / año y la tendencia ▪ % de cambios (organizacionales/SOPs/técnicos, etc.) que han sido objeto de evaluación de riesgos

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

AREA	ENFOQUE DE LA MEDICIÓN	MÉTRICA
EFECTIVIDAD DEL SMS	Gestión de los contratistas	▪ % de los contratistas cuyo rendimiento en materia de seguridad operacional se ha evaluado ▪ Frecuencia con la que se determina el rendimiento en materia de seguridad operacional de los contratistas ▪ % de los contratistas integrados en el sistema de notificación de seguridad operacional de su empresa ▪ % de los contratistas para las cuales se ha impartido formación en seguridad operacional ▪ % de los contratistas que han implementado procedimientos de control de la formación ▪ % de los contratistas que tienen establecido un sistema de información (o feedback) sobre cuestiones de seguridad operacional con sus clientes ▪ Número de notificaciones de seguridad operacional recibidas de los contratistas por mes / trimestre / año y la tendencia ▪ Número de acciones de seguridad operacional iniciadas debidas a la evaluación del rendimiento en materia de seguridad operacional o de las notificaciones de seguridad operacional recibidas al mes / trimestre / año y la tendencia
	Planificación de la respuesta ante emergencias (ERP)	▪ Número de simulacros de emergencia por año ▪ Frecuencia de la revisión del ERP ▪ Número de cursos de formación en ERP por mes / trimestre / año ▪ % de personal formado en el ERP dentro de un cuarto / año ▪ Número de reuniones con los socios principales y contratistas para coordinar el ERP al mes / trimestre / año
	Promoción de la seguridad operacional	▪ Número de comunicaciones de seguridad operacional publicadas ▪ Número de cursos realizados ▪ Número de sesiones informativas (o briefings) de seguridad operacional realizadas. ▪ (por mes / trimestre / año)
	Cultura de la seguridad operacional	▪ Grado en que el personal considera la seguridad operacional como un valor que guía su trabajo diario (por ejemplo, en una escala de 1 = bajo a 5 = alto) ▪ Grado en que el personal considera que la seguridad operacional está muy valorada por sus gestores ▪ Grado en que se aplican los principios de actuación humana ▪ Grado en que el personal toma iniciativas para mejorar las prácticas organizativas o notificar un problema a la gestión ▪ Grado en el que el comportamiento consciente de la seguridad operacional es apoyado. ▪ Grado en que el personal y la gestión son conscientes de los riesgos de sus operaciones y lo que implican para ellos mismos y para los demás.

INDICADORES DE CUESTIONES OPERACIONALES

AREA	RESULTADOS DE ALTA SEVERIDAD A EVITAR	MÉTRICA
OPERADORES AÉREOS	Colisiones de tráfico	▪ Número de TCAS RA por cada 1.000 horas de vuelo (FH)
véase también	Salidas de pista	▪ Número de aproximaciones desestabilizadas por 1000 aterrizajes

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

AREA	RESULTADOS DE ALTA SEVERIDAD A EVITAR	MÉTRICA
Gestión del Tráfico Aéreo / Servicios de Navegación Aérea para indicadores adicionales	Colisiones en tierra	▪ Número de incursiones en pista por 1000 despegues
	Vuelo controlado contra el terreno	▪ Número de avisos GPWS y EGPWS por 100 despegues
	Accidente/incidente relacionado con una preparación pobre del vuelo	▪ Número de casos en los que la preparación del vuelo tuvo que hacerse en menos tiempo del normalmente asignado ▪ Número de eventos de cortos de combustible por cada 100 vuelos ▪ Número de errores de cálculo de combustible por cada 100 vuelos
OPERADORES AÉREOS	Accidentes/incidentes relacionados con la fatiga	▪ Número de extensiones de los períodos de servicio del vuelo al mes / trimestre / año y las tendencias
	Accidentes/incidentes relacionados con la asistencia en tierra	▪ Número de incidentes con la asistencia en tierra al mes / trimestre / año y las tendencias ▪ número de errores de masa y centrado de la asistencia en tierra al mes / trimestre / año y las tendencias ▪ Número de disfunciones de la asistencia en tierra al mes / trimestre / año y las tendencias
	Accidentes/incidentes relacionados con el mantenimiento	▪ Informes de Pilotos (PIREPS) por cada 100 despegues ▪ Diferidos por mes y aeronave ▪ In Flight Shut Down (IFSD) por 1000 FH ▪ In Flight Turn Backs (IFTB) y las desviaciones por cada 100 despegues ▪ Número de notificaciones acerca de dificultades en el servicio presentadas a la Autoridad de Aviación Civil Fiabilidad en el despacho: ▪ Número de retrasos superiores a 15 minutos, debido a problemas técnicos por cada 100 despegues ▪ número de cancelaciones por cada 100 vuelos programados debido a problemas técnicos ▪ Despegues abortados por cada 100 despegues debido a problemas técnicos
ORGANIZACIONES DE MANTENIMIENTO	Accidentes/ incidentes relacionados con la planificación/turnos del mantenimiento	▪ % de las órdenes de trabajo para las que se ha hecho una planificación detallada Fatiga de los ingenieros de mantenimiento / error de mantenimiento: ▪ % de las órdenes de trabajo con una diferencia > 10% entre el tiempo de espera propuesto y el tiempo de procesamiento real ▪ % de las órdenes de trabajo con una diferencia > 10% entre la carga de trabajo estimada y las necesidades reales
	Accidentes/ incidentes relacionados con el mantenimiento	Error de mantenimiento: ▪ % de las órdenes de trabajo que requieren re-trabajo ▪ Número de inspecciones duplicadas que identificó un error de mantenimiento
	Accidentes/ incidentes relacionados con datos de mantenimiento	▪ Número de notificaciones de seguridad operacional relacionadas con datos de mantenimiento ambiguos
	Accidentes/incidentes relacionados con mantenimiento	▪ Número de investigaciones realizadas debido a componentes fuera de servicio significativamente antes de que se alcanzase el límite de vida esperado

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

AREA	RESULTADOS DE ALTA SEVERIDAD A EVITAR	MÉTRICA
GESTIÓN DEL TRAFICO AÉREO / SERVICIOS DE NAVEGACIÓN AÉREA	Colisiones de tráfico	▪ Número de level bust/exposición ▪ Número de TCAS (RA) (con y sin pérdida de la separación) / exposición ▪ Número de infracciones de separación mínima / exposición ▪ Número de separaciones inadecuadas (en el espacio aéreo en el que la separación mínima no es aplicable) / Exposición ▪ Número de desviaciones de la aeronave de la autorización del control del tráfico aéreo (ATC) / exposición ▪ Número de vulneraciones del espacio aéreo/ exposiciones
	Colisiones de tráfico / Vuelo controlado contra el terreno	▪ Número de desvíos de aeronaves de los procedimientos de la gestión del tráfico aéreo (ATM) / exposición ▪ Número de inadecuada asistencia o falta de asistencia por parte de ATC a las aeronaves en peligro
	Vuelo controlado contra el terreno	▪ Número de cuasi CFIT IFSD / Exposición
	Salidas de pista	▪ Número de instrucciones ATC inapropiadas (sin instrucción, información incorrecta, acción de comunicación tardía, etc.)
	Incursiones en pista	▪ % de las incursiones en pista en las que no es necesario una maniobra evasiva ▪ % de las incursiones en pista en las que se haya requerido una maniobra evasiva
AEROPUERTOS	Fuego posterior a un accidente/incidente	▪ Relación de disminución del Servicio de Extinción de Incendios (según categoría OACI del aeropuerto) (# horas de disminución / # horas anuales de funcionamiento del aeropuerto) ▪ Número de fallos de la radio / el teléfono por cada 100 operaciones ▪ Número de fallos de los vehículos de bomberos por cada 100 operaciones
	Incursiones en pista	▪ Incursiones en pista por 1.000 operaciones Señalización: ▪ Número de fallos o defectos encontrados durante las inspecciones de rutina ▪ Número de defectos notificados ▪ Promedio de tiempo de reparación / reemplazo (por mes / trimestre / año y las tendencias) / año)
	Colisión con vehículo o equipamiento en tierra	▪ Violaciones notificadas de las normas de seguridad operacional en plataforma por cada 1000 operaciones
	Colisión con fauna en tierra	▪ Número de colisiones con fauna en tierra ▪ Número de inspecciones de los cepos y otros dispositivos de protección por mes / trimestre / año
	FOD (Foreign Object Damage)	▪ Número de FOD encontrados durante las inspecciones de rutina ▪ Número de FOD encontrados fuera de las inspecciones o tras una notificación
	Incursiones en pista	Luces de pista ▪ Número de fallos o defectos encontrados durante las inspecciones de rutina ▪ número de defectos notificados ▪ promedio de tiempo de reparación / reemplazo (por mes / trimestre / año y las tendencias)
	IFSD debidos a golpes de pájaros	▪ Número de IFSD por 10.000 FH después del golpe con el pájaro

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

AREA	RESULTADOS DE ALTA SEVERIDAD A EVITAR	MÉTRICA
ORGANIZACIONES DE INSTRUCCIÓN DE VUELO	Accidente / incidente relacionado con una escasa formación	▪ Número de alumnos por instructor ▪ Número de cambios de instructor por curso de formación ▪ Número de cambios importantes en el programa de formación ▪ (por mes / trimestre / año y las tendencias)
	Accidentes / incidentes relacionados con la mala formación / complacencia durante los exámenes	▪ Número de desviaciones significativas de las tasas medias de aprobados
ORGANIZACIONES DE DISEÑO	Accidentes/incidentes relacionados con el diseño	Durante la fase de diseño: ▪ Número de cambios de diseño solicitados por errores de diseño por programa y por período ▪ Número de demostraciones de cumplimiento rechazadas por programa y por período
	Accidentes/incidentes relacionados con la planificación del diseño	▪ % de informes técnicos con una diferencia> 10% entre el tiempo de entrega prevista y el tiempo real de procesamiento ▪ % de informes técnicos con una diferencia> 10% entre la carga de trabajo estimada y las necesidades reales
	Accidentes/incidentes relacionados con el diseño	PosCertificación: ▪ Número de notificaciones de dificultad de servicio/seguridad operacional debidas a errores de diseño por programa y por período ▪ Número de notificaciones de seguridad operacional relacionados con datos de diseño ambiguos ▪ Número de cambios de diseño clasificados incorrectamente (Menor / Mayor) por periodo
ORGANIZACIONES DE FABRICACIÓN	Accidentes/incidentes relacionados con la fabricación	▪ Número de sucesos de dificultad de servicio/seguridad operacional debido a errores de fabricación por programa y por período
	Accidentes/incidentes relacionados con el proceso de fabricación	▪ % de las órdenes de trabajo que requieren re-trabajo ▪ Número de investigaciones realizados debido a órdenes de trabajo que requieren re-trabajo ▪ % de las inspecciones duplicadas que identificaron un error de fabricación ▪ Número de casos en los que la entrega final se retrasó debido a importantes incumplimientos ▪ Número de investigaciones realizadas debido a una entrega tardía
	Accidentes/incidentes relacionados con los datos de fabricación	▪ Número de notificaciones de seguridad operacional relacionadas con datos de fabricación ambiguos
	Accidentes/incidentes relacionados con la planificación de fabricación	Fatiga en el personal de producción / error producción: ▪ % de las órdenes de trabajo con una diferencia de> 10% entre la carga de trabajo estimada y las necesidades reales ▪ % de órdenes de trabajo con una diferencia de> 10% entre el tiempo de entrega previsto y el tiempo de procesamiento real

INDICADORES PARA MONITORIZAR FACTORES EXTERNOS

AREA	ENFOQUE DE MONITORIZACIÓN	MÉTRICA
REGULACIONES	Regulaciones nuevas	Número de nuevos requisitos regulatorios que afectan a su organización en los próximos 12 meses

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*

	Enmiendas a las regulaciones	Número de requisitos normativos modificados que afectarán a su organización en los próximos 6 meses
	Evolución hacia normas basadas en el rendimiento	Número de normas basadas en objetivos para los que se han definido sus propios medios de cumplimiento
TECNOLOGÍA	Nuevas tecnologías relacionadas con su negocio principal - hardware	% de la inversión total que se invierte en nuevas tecnologías
	Nuevas tecnologías relacionadas con su negocio principal - Software	% de la inversión total que se invierte en nuevas tecnologías
	Nuevas tecnologías relacionadas con su negocio principal	Tasa de obsolescencia de las cualificaciones existentes
	Nuevas tecnologías instaladas en aeronaves	Número de modificaciones de aeronaves / Certificados Tipo Suplementario (STC) que requieren un cambio en la calificación de su empresa Número de nuevas modificaciones / STC que requieren nuevas cualificaciones
COMPETENCIA	Volumen de negocio	Evolución de la facturación
	Renovación de personal	Tiempo promedio para ocupar una vacante Número de personas que dejan de trabajar para irse a un competidor
	Oportunidades de mercado	Evolución en el número de solicitudes de cita de nuevos clientes Proporción de solicitudes de cita de los nuevos clientes que son seguidos por un pedido en firme
	Competidores	Evolución del número de sus competidores directos

© AESA *Cualquier copia impresa o en soporte electrónico, total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con su versión vigente en la Intranet*