Principios de la toma de decisiones basadas en el riesgo

30 Enero 2013

Este documento fue preparado por el grupo de trabajo de Estandarización del Safety Management International Collaboration Group (SM ICG) -. Grupo de Colaboración Internacional de Gestión de la Seguridad Operacional- El propósito del SM ICG es promover un entendimiento común de los principios y requisitos de los Sistemas de Gestión de Seguridad operacional (SMS)/Programas Estatales de Seguridad operacional (SSP), facilitando su aplicación a lo largo de la comunidad internacional de aviación.

Los miembros actuales del SM ICG son AESA (Agencia Estatal de Seguridad Aérea) de España, ANAC (National Civil Aviation Agency) de Brasil, la autoridad de aviación civil de los Países Bajos, la autoridad de aviación civil de Nueva Zelanda, la Civil Aviation Safety Authority (CASA) de Australia, la Direction Générale de l'Aviation Civile (DGAC) de Francia, la European Aviation Safety Agency (EASA), la Federal Office of Civil Aviation (FOCA) de Suiza, Japan Civil Aviation Bureau (JCAB), la United States Federal Aviation Administration (FAA) Aviation Safety Organization, la Transport Canada Civil Aviation (TCCA) y la autoridad de aviación civil del Reino Unido (CAA UK). Además la Organización de Aviación Civil Internacional (OACI) es un observador de este grupo.

Los miembros del SM ICG:

- Colaboran en materias de interés comunes del SMS/SSP
- Comparten lecciones aprendidas
- Fomentan el progreso de un SMS armonizado
- Comparten productos con la comunidad aeronáutica
- Colaboran con organismos internacionales como la OACI y las autoridades de aviación civil que hayan implementado o estén implementando el SMS

Para más información del SM ICG por favor contacte con:

Regine Hamelijnck, SM ICG Chair
EASA
+49 221 8999 1000
regine.hamelijnck@easa.europa.eu

Jacqueline Booth
TCCA
(613) 952-7974
jacqueline.booth@tc.gc.ca

Amer M. Younossi
FAA, Aviation Safety
(202) 267-5164
Amer.M.Younossi@faa.gov

Carlos Eduardo Pellegrino
ANAC
+55 213 5015 147
carlos.pellegrino@anac.gov.br

Peter Boyd
CASA
+61 2 6217 1534
peter.boyd@casa.gov.au

RESUMEN EJECUTIVO

Este documento presenta los principios necesarios para la toma eficaz de decisiones basadas en el riesgo. También identifica los atributos relevantes de los datos para permitir la utilización de los mismos en la toma de decisiones basadas en el riesgo, y presenta las consideraciones para la gestión de los datos.

La gestión de la seguridad operacional se está convirtiendo en el estándar para la seguridad operacional de la aviación en todo el mundo. La gestión de riesgos es uno de los componentes principales de la gestión de la seguridad operacional y los elementos clave para un proceso eficaz de gestión de riesgos son la identificación de peligros, la evaluación de los riesgos asociados con las consecuencias de estos peligros y la mitigación de los riesgos considerados inaceptables. Los proveedores de servicios y las autoridades reguladoras, ambos, tienen que desempeñar un papel en la gestión de los riesgos de la aviación. Ambos se necesitan para gestionar el riesgo, aunque la naturaleza y el alcance de los peligros y los procesos pueden ser diferentes. Por ejemplo, mientras que un proveedor de servicios puede identificar los peligros específicos de su organización particular, una autoridad puede estar identificando los peligros de tendencias emergentes en el sistema de aviación entero basándose en datos agregados de diferentes sectores.

Los procesos de gestión de la seguridad operacional que funcionan correctamente, ya sean establecidos bajo un Sistema de Gestión de Seguridad operacional (SMS) o por un Programa de Seguridad operacional del Estado (SSP), requieren datos para apoyar los análisis y evaluaciones, así como estrategias para garantizar que estos datos poseen ciertos atributos, como la validez, exhaustividad, actualidad, disponibilidad y exactitud de los mismos. Además, como la gestión de la seguridad operacional es un sistema basado en los datos, es dependiente de un proceso de gestión eficaz de los datos. La gestión de datos se define como el desarrollo y el mantenimiento continuo de los procesos y procedimientos para asegurar que una organización posee los datos que necesita y que los datos están organizados, son fiables y adecuados. El establecimiento de un plan de gestión de datos y de los requisitos de los atributos de los datos permitirán la identificación efectiva del peligro y la mitigación de riesgos.

La identificación de los peligros debería realizarse durante el diseño del sistema y en los procesos de cambio del sistema; y los peligros deberían seguir siendo identificados a través de la monitorización continua durante la operación del sistema. Durante la identificación del peligro, se deberían considerar todas las posibles fuentes de peligros. El riesgo asociado con los posibles resultados o consecuencias de cada peligro particular se debería evaluar o analizar, donde cada riesgo es el producto de la severidad y probabilidad. Como paso siguiente, los riesgos que se consideren inaceptables por la organización deberían ser mitigados.

Este documento proporciona una visión general de la toma de decisiones basada en el riesgo, los atributos de los datos, la gestión de datos, y los elementos de la gestión de riesgos de seguridad operacional. El último capítulo de este documento contiene ejemplos actuales de recopilación de datos, identificación de peligros y procesos de análisis de seguridad operacional de las autoridades miembros del Grupo de Colaboración Internacional de Gestión de la Seguridad Operacional(SM ICG).

INDICE

1. PROPÓSITO

El propósito de este documento es dar a conocer los principios necesarios para una toma de decisiones eficaz basada en el riesgo. Esto incluye los atributos de datos pertinentes necesarios para permitir la utilización de los mismos para tomar decisiones basadas en el riesgo y la gestión global de estos datos. Este documento está destinado a ser utilizado por las autoridades y proveedores de servicios que se encuentran en las etapas iniciales de los procesos de desarrollo/implementación de la gestión de la seguridad operacional. Este documento sólo introduce los principios básicos, por lo tanto, es recomendable el uso conjunto de otras fuentes.

2. INTRODUCCIÓN

La gestión de la seguridad operacional se está convirtiendo en el estándar para la seguridad operacional de la aviación en todo el mundo. Es una herramienta que ayuda a los gestores a tomar decisiones basadas en los riesgos que existen en su organización o en su entorno. La gestión de riesgos es uno de los principales componentes de la gestión de la seguridad operacional, ya que abarca la evaluación y mitigación de riesgos para la seguridad operacional, a los que están expuestas las organizaciones

Los proveedores de servicios y las autoridades reguladoras, ambos, tienen que desempeñar un papel en la gestión de los riesgos de la aviación; ambos necesitan gestionar el riesgo, aunque la naturaleza y el alcance de los peligros y los procesos pueden ser diferentes. Por ejemplo, mientras que un proveedor de servicios puede identificar los peligros específicos de su organización particular, una autoridad puede estar identificando los peligros de tendencias emergentes en el sistema de aviación entero basándose en datos agregados de diferentes sectores.
Los elementos clave de un proceso de gestión de riesgos son: la identificación de peligros, evaluación de los riesgos asociados con las consecuencias de estos peligros y la mitigación de los riesgos considerados inaceptables. Todos estos elementos requieren datos para apoyar la gestión eficaz del riesgo. Por lo tanto, la gestión adecuada de los datos en todo el ciclo de vida de la gestión de los riesgos es esencial para respaldar un proceso robusto de gestión de la seguridad operacional.

Este documento comienza con una discusión de los conceptos generales de utilización de datos. Luego se dan más detalles sobre los atributos de los datos, la gestión de datos, la identificación de peligros, los análisis de riesgos y los procesos de mitigación del riesgo. Por último, ofrece ejemplos actuales de recopilación de datos, identificación de peligros y métodos de análisis de riesgos de diversas autoridades.

El nivel de complejidad y sofisticación de los procesos de gestión de seguridad operacional y/o de las herramientas de gestión de la seguridad operacional de una organización variará en función del tamaño, la madurez y complejidad del sector de la aviación dentro de un determinado Estado u organización de la industria. Por lo tanto, los principios contenidos en el presente documento pretenden lograr una implementación de la gestión de la seguridad operacional escalada al tamaño, la madurez y la complejidad de un determinado sector de la aviación o proveedor de servicios. Por ejemplo, en los sectores relativamente pequeños y/o simples de la aviación, puede ser aceptable llevar a cabo la gestión de riesgos realizando manualmente la recogida de datos, el análisis y el almacenamiento, en lugar de utilizar herramientas complejas de Tecnologías de la Información (IT).

3. DESCRIPCIÓN DE LA TOMA DE DECISIONES BASADAS EN EL RIESGO

El objetivo principal de la gestión de riesgos consiste en aprovechar los datos relacionados con la seguridad operacional para identificar y controlar las posibles consecuencias de los peligros en el sistema de aviación antes de que se produzca un accidente o incidente grave. La gestión de riesgos es mucho más efectiva con una clasificación de los datos de seguridad operacional utilizando taxonomías comunes que permitan que los mismos sean vistos en más dimensiones para poder detectar peligros de manera más eficiente. El análisis de datos puede incluir las aportaciones de todos los datos relacionados con la seguridad operacional de la aviación procedente de uno o más sectores de la aviación, por lo que es importante la utilización de taxonomías comunes. Las salidas del proceso de análisis de los datos son las opciones de la gestión de riesgos. La Figura 1 muestra ejemplos de los tipos de entradas y salidas.

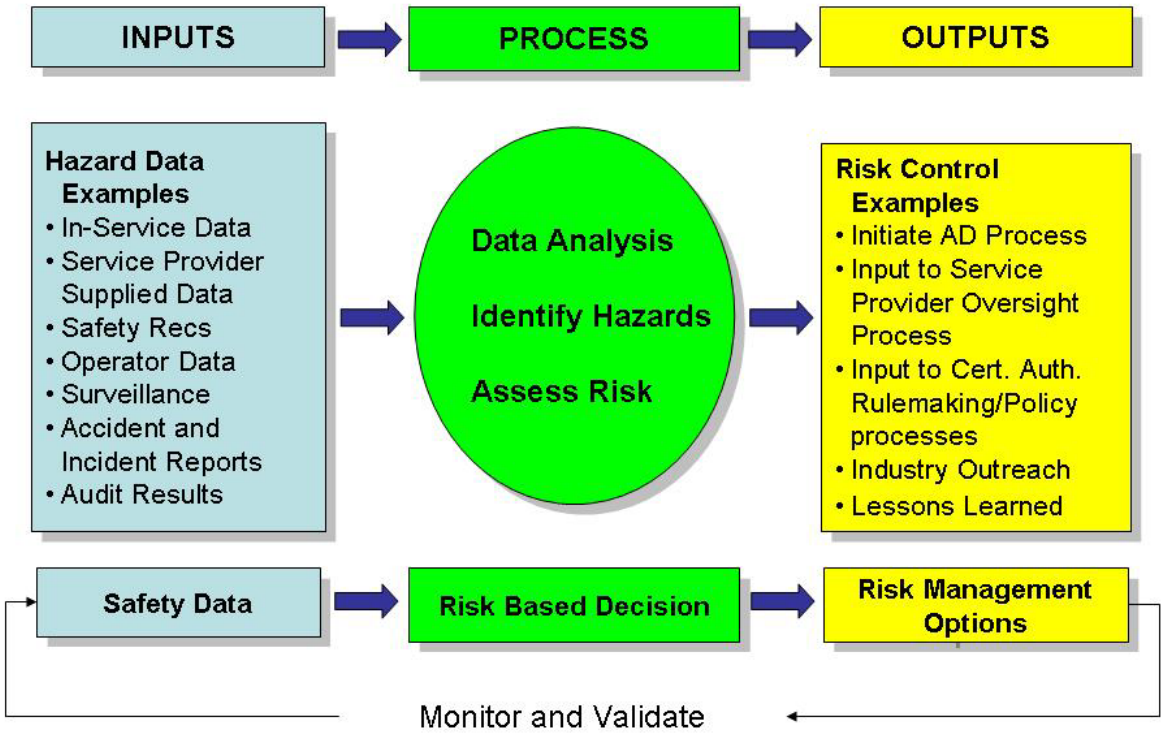


Figura 1: Entradas y Salidas del Proceso de Análisis de Datos

Como se mencionó anteriormente, las entradas pueden provenir de cualquier parte del sistema de la aviación, incluyendo el análisis de peligros de nuevos procesos o productos, la vigilancia de los sistemas de aviación actuales, eventos en el servicio, las investigaciones de accidentes/incidentes, sistemas de notificación voluntaria, etc. Cuando sea necesario, las salidas o controles de riesgo se aplican para eliminar el peligro o reducir el nivel de riesgo.

La identificación eficaz del peligro depende de la disponibilidad de los datos. Incluso si el análisis de peligros se lleva a cabo en procesos o en productos nuevos que aún no están en operación, se requieren datos que describen el proceso o producto. Además, los datos deberían ser gestionados y los atributos necesarios de los datos deberían ser tratados. Es más, puede ser apropiado combinar o

agregar datos de diferentes sectores de la aviación para asegurar una comprensión global de cada peligro identificado. Los apartados 4 y 5 de este documento proporcionan más información sobre los atributos de los datos y la gestión de datos.

Por otra parte, el proceso representado en la figura 1 debería utilizar metodologías reactivas, preventivas, y de predicción para identificar los peligros. El análisis de los peligros identificados como resultado de las investigaciones de incidentes o accidentes es un ejemplo de una metodología reactiva. Una metodología proactiva podría incluir la evaluación de riesgos después de las auditorías, las inspecciones o las notificaciones obligatorias, y una metodología predictiva podría implicar considerar los resultados del análisis de la vulnerabilidad del sistema en la operación día a día. Los apartados 6, 7 y 8 de este documento proporcionan más información acerca de la identificación de peligros, análisis y mitigación de riesgos.

4. ATRIBUTOS DE LOS DATOS

Los procesos de gestión de la seguridad operacional que funcionan correctamente, ya sean establecidos bajo un Sistema de Gestión de Seguridad operacional (SMS) o por un Programa de Seguridad operacional del Estado (SSP), requieren datos. En este capítulo se examinan brevemente los atributos de los datos que deberían ser considerados durante el diseño del sistema, la recopilación de datos, el análisis y los procesos de difusión.

Antes de hablar de los atributos de los datos, se debe considerar que los datos de seguridad operacional se pueden clasificar en varias categorías: datos de sucesos notificados obligatoriamente, datos de sucesos notificados voluntariamente, datos de observación y los datos de vigilancia. El reporte de los datos de sucesos notificados obligatoriamente es preceptivo por los reglamentos. Estos incluyen los datos obtenidos de la investigación de accidentes e incidentes graves, así como ciertos sucesos técnicos. Aunque no es requerido por las regulaciones, los datos se notifican voluntariamente para ayudar en la identificación de peligros e incluyen notificaciones sobre incidentes y errores. La observación puede ser utilizada para identificar los peligros mediante la observación de las desviaciones[1] de las operaciones normales. Esto incluye programas de monitorización de los datos de vuelo como FDM (Flight Data Monitoring) y FOQA (Flight Operational Quality Assurance). Los datos de vigilancia provienen de auditorías, encuestas o inspecciones que verifican la conformidad con requisitos específicos. Todas las categorías de datos son elementos importantes de un proceso de gestión de la seguridad operacional que funcione bien

Independientemente del tipo de datos, la calidad es uno de los elementos más importantes para garantizar que los datos puedan ser integrados y utilizados adecuadamente con el propósito de su análisis. Es importante que se apliquen principios y prácticas de calidad a los datos a lo largo de los procesos de captura y de integración de los mismos para el análisis. Algunos de los atributos de los datos más importantes son: la validez, exhaustividad, actualidad, disponibilidad y exactitud.

Validez de los datos

La validez de los datos no sólo es tan importante como cualquier otro atributo de los datos, sino que es el que más. Los resultados de un determinado análisis son sólo tan válidos como lo sean los datos de entrada que alimentan el análisis. Sin datos válidos, todos los resultados de los análisis, las tendencias identificadas, y las conclusiones pueden ser erróneos y potencialmente engañosos. La validez de los datos se refiere a la corrección y razonabilidad de los datos, así como a la garantía de

[1] Una desviación (u outlier) es una observación que se encuentra fuera del patrón general de una distribución. Puede ser la indicación de un área de preocupación o de un error de datos, pero en cualquier caso requiere un examen más detenido.

que en los datos recopilados están midiendo lo que se pretendía. Esto significa que los datos incluyen todos los dígitos necesarios y la ortografía correcta. Por ejemplo, las fechas tienen días, meses y años válidos y no puede haber 32 días o 13 meses.

Los errores de validez de los datos generalmente son causados por la introducción de datos incorrectos, cuando se introduce un gran volumen de datos en una base de datos o cuando diferentes bases de datos con estructuras de datos distintas se fusionan. Con el fin de reducir los errores de validez de los datos, se podrían adoptar técnicas sencillas de validación de los campos. Por ejemplo, si el campo de fecha en una base de datos utiliza el formato MM/DD/AAAA, se puede utilizar un programa con las siguientes dos reglas de validación de datos: "MM" no debe superar "12" y "DD" no debe superar "31". Este método se conoce frecuentemente como una verificación de la razonabilidad de los datos.

Exhaustividad de los datos

La exhaustividad es una medida de la cantidad de datos de los que se dispone en comparación con la cantidad de datos que se necesita para un análisis particular. Antes de desarrollar un nuevo proceso de análisis que apoye una toma de decisiones basada en el riesgo, se debería definir los datos mínimos necesarios. Debe tenerse en cuenta que cuanto mayor sea el volumen de datos que se necesitan, más recursos (por ejemplo, tiempo, mano de obra) se necesitarán para obtener los datos. Esto es algo que tiene que ser tomado en consideración seriamente durante el diseño de los sistemas de recopilación de datos. Los requisitos para la exhaustividad también deberían estar en consonancia con la información disponible. Por ejemplo, la cantidad de datos en un accidente es probable que sea mucho mayor que la de un incidente menor.

Actualidad de los datos

Aunque la actualidad está especificada por las expectativas del usuario, normalmente los mejores datos son los más recientes. Históricamente, las limitaciones de la tecnología y de los procesos tendían a excluir la posibilidad de entregar datos en tiempo real. Sin embargo, con el advenimiento de los ordenadores y la tecnología de red, siguen cayendo las barreras para la disponibilidad en tiempo real de los datos. Como resultado de ello, una organización en sus procesos de gestión de la seguridad operacional debería esforzarse por obtener acceso en tiempo real a los datos de seguridad operacional de la aviación, en la medida de lo posible. Por ejemplo, los sistemas actuales para la descarga inalámbrica de los datos FDM permiten a los operadores un acceso casi en tiempo real a los datos.

Disponibilidad de los datos

Los datos también deberían seguir estando disponibles cuando sean necesarios. En general, la disponibilidad de datos se logra por medio de redundancia que implica el lugar donde se almacenan los datos y la forma en que se pueden extraer. La disponibilidad de los datos se puede medir en términos de la frecuencia en la que los datos están disponibles (por ejemplo, 99,9% de disponibilidad) y la cantidad de datos que pueden fluir en un momento.

Exactitud de los datos

La exactitud de los datos es el grado en el que los datos reflejan correctamente el objeto del mundo real o el evento que se describe. Hay varias fuentes y causas de la inexactitud de los datos. La más común de ellas es la entrada inicial de datos, bien porque el usuario introduce un valor incorrecto o se cometen errores tipográficos. Esto se puede obviar asegurando que las personas que introducen los datos poseen las habilidades necesarias y la formación adecuada. La inexactitud de datos debida a la entrada de datos también puede evitarse teniendo componentes programáticos en la aplicación para detectar los errores tipográficos (por ejemplo, revisores de ortografía) u otros métodos para garantizar la exactitud de los datos, como el despliegue de listas de valores posibles.

En resumen, se debe tratar cada atributo de los datos. En algunos casos, tratar cada aspecto puede requerir un esfuerzo considerable. La confianza de una organización en los datos no es algo que se logra mediante un único atributo. Sin embargo, la confianza en los datos es un concepto estratificado – lográndose cada vez una capa. Cada vez que se añade otra capa, aumenta el factor de confianza en los datos. Además, todos estos atributos se deberían considerar desde el principio del diseño de un proceso o sistema, ya que una vez que el proceso o sistema se construye puede ser demasiado tarde para obtener los datos necesarios para que la dirección pueda tomar decisiones basadas en datos.

5. GESTIÓN DE LOS DATOS

La gestión de la seguridad operacional es un sistema basado en los datos, por lo que depende de un proceso eficaz de la gestión de los mismos. La gestión de datos es el desarrollo y mantenimiento continuo de los procesos y procedimientos para asegurar que una organización tiene los datos que necesita y que los datos están organizados, son fiables y adecuados. Al gestionar los datos, la organización debería definir qué información es necesaria y planificar cómo se utilizará dentro de sus procesos.

Para una gestión eficaz de los datos de seguridad operacional, una organización debería:
- Definir los datos necesarios para alcanzar los objetivos deseados;
- Diseñar las arquitecturas de datos y las estructuras de la base de datos, basándose en el uso previsto de los datos;
- Definir los estándares y formatos para los datos, incluyendo la frecuencia requerida para la recopilación de los datos;
- Desarrollar un proceso para asegurar que los datos recopilados se ajustan a los estándares y formatos definidos;
- Desarrollar herramientas de recopilación de datos, teniendo en cuenta la necesidad de los datos que deben recopilarse y su uso;
- Definir los datos que se agregan a partir de las diferentes fuentes;
- Integrar los datos de seguridad operacional con otros datos correlacionados que puedan ser relevantes;
- Asegurar un acceso adecuado a los datos para los usuarios;
- Considerar las cuestiones de protección de datos;
- Considerar la posibilidad de compartir datos con entidades dentro y fuera de la organización; y
- Gestionar los datos durante su ciclo completo de vida, incluyendo el control de configuración.

En este capítulo se presentan algunos de los principales aspectos de la gestión de datos que se deberían considerar para utilizar de forma eficaz los datos en la gestión de la seguridad operacional.

Planificación de la recopilación de los datos

Antes de la recopilación de los datos, una organización (autoridad o proveedor de servicios) debería identificar qué información le es necesaria. Por ejemplo, las autoridades o los proveedores de servicios por lo general poseen información detallada sobre los accidentes e incidentes graves. Sin embargo, es posible que no dispongan de datos sobre todos los sucesos de seguridad operacional en su sistema. En consecuencia, para obtener este conocimiento, la organización necesita desarrollar un plan para la recopilación de estos datos.

Después de identificar los datos que deben recopilarse, la organización debería determinar la fuente de información, así como los procesos de recopilación y almacenamiento. Por ejemplo, ¿el sistema estará abierto al público en general, a miembros de tripulaciones, a los proveedores de servicios, etc.? Para responder a esto, es necesario tener en cuenta los atributos de datos que se discuten en el capítulo 4 y determinar si la fuente será capaz de proporcionar ese nivel de detalle

Normalización de los datos

La normalización de los contenidos impacta directamente en la utilización de los datos. Por lo tanto, es necesario normalizar los datos con el fin de comparar, agregar, y combinar datos de diferentes fuentes. Para poder vincular los datos de diferentes fuentes, es necesario desarrollar y mantener estándares de taxonomías comunes o ser capaz de convertir o traducir entre diferentes taxonomías. Las taxonomías permiten que los datos sean identificados y almacenados utilizando la misma nomenclatura. Por ejemplo un tipo de aeronave puede ser registrado como "737-200" o "Boeing 737-200" o "732". Algunos ejemplos de estándares se describen a continuación:

- Modelo de aeronave: La organización puede construir una base de datos con todos los modelos certificados para operar.
- Aeropuerto: La organización puede utilizar para identificar los aeropuertos los códigos de la Organización de Aviación Civil Internacional (OACI) o de la Asociación Internacional del Transporte Aéreo (IATA).
- Tipo de suceso: La organización de investigación de accidentes puede usar taxonomías desarrolladas por OACI u otras organizaciones internacionales para clasificar los sucesos.

Debido a problemas legales así como a otros factores, a veces no es posible establecer taxonomías comunes entre diferentes bases de datos. En tal caso, se debería crear un mapeo de datos para permitir la normalización de los datos basándose en la tabla de equivalencia. Usando el ejemplo anterior de tipo de aeronave, un mapeo de los datos podría mostrar que un "737-200" en una base de datos es equivalente a un "732" en otra. En algunos casos, esto puede que no sea un proceso directo ya que durante la captura de datos el nivel de detalle puede ser diferente. Cuando el uso de una taxonomía común no es factible debido a la alta heterogeneidad de los datos, se deberían considerar otras formas de integración de datos.

Si se está creando una nueva normalización, la organización puede tener en cuenta las fuentes internas y externas para la elaboración de las normas necesarias.

Formato y estructura de los datos

Una vez que la organización ha decidido los procesos a utilizar para recopilar datos, el siguiente paso es definir la estructura de los datos que han de recopilarse. También será necesario tener en cuenta dónde se guardarán los datos. Si los datos se están combinando con bases de datos existentes, entonces tendrá que ser utilizada la misma estructura de los datos ya recopilados. Por ejemplo, si una base de datos existente contiene información detallada sobre las horas de vuelo, los miembros de la tripulación, aeronaves, aeropuertos y otros, para combinarla con una nueva base de datos se requerirá de campos de datos con el mismo formato que los de la base de datos existente, con el fin de integrar de manera efectiva esta información. El campo común entre los sistemas debería tener el mismo formato. Por ejemplo, un campo "fecha" sería el mismo en ambos sistemas (por ejemplo, "MM/DD/YYYY"). Otra posible estrategia para permitir la combinación de datos con diferentes estructuras o formatos es el uso de la transformación de datos. Esta estrategia se puede aplicar cuando los datos procedentes de diferentes fuentes sean equivalentes. Una vez que los datos se transforman, entonces los datos serán intercambiables y será posible el análisis que abarque diferentes bases de datos.

Herramientas de recopilación de datos

Una vez definidas las fuentes, contenidos, formatos y estándares, es necesario construir las herramientas adecuadas para recopilar los datos. En este punto, es muy importante tener en cuenta los siguientes atributos:

- **Facilidad de acceso**: El sistema de notificación debería estar disponible en un lugar fácil de encontrar y de acceder (por ejemplo, el enlace principal en la parte superior de la página principal del sitio web de la organización). El acceso debería bloquear a personas no autorizadas, pero debería ser de fácil acceso para los usuarios previstos. Por ejemplo, un miembro de la tripulación (usuario previsto) debería acceder a través de su número de licencia de piloto y una contraseña, que sería la misma contraseña utilizada para acceder a otros sistemas de la organización.

- **Facilidad de notificación**: Al rellenar la notificación, el usuario debería realizarlo con el mínimo esfuerzo posible para introducir la información. Por ejemplo, los campos de fecha y hora se deberían rellenar automáticamente haciendo clic en las opciones en un calendario.

- **Ausencia de información redundante**: Asegurarse de que la información que ya está disponible para la organización no se esté recopilando de nuevo. Por ejemplo, si la organización ya tiene una base de datos que contiene información sobre el personal de la tripulación, podría ser adecuado solicitar sólo los números de licencia de los pilotos.

- **Entrada controlada:** Se pueden diseñar restricciones de formato de manera que se obtenga la información en el formato deseado. Por ejemplo, si se introduce un tiempo como "0954", el sistema sería capaz de formatearlo de acuerdo con la estructura definida, que es el mismo que "9:54 am".

Estas son sólo algunas de las características que deben tenerse en cuenta al diseñar las herramientas de recopilación de datos. Además, tenga en cuenta que las herramientas de recopilación de datos pueden ser en papel o por ordenador, en función del tipo y la cantidad de datos que se recopilen.

Almacenamiento de los datos y mantenimiento de la base de datos

Una vez que los datos se han recopilado, entonces éstos deberían ser almacenados en lo que a veces se conoce comúnmente como una "biblioteca de seguridad operacional". Una de las características para el almacenamiento de datos es asegurar que existe una capacidad de almacenamiento suficiente para los datos recopilado. También puede ser necesario actualizar o disponer de ciertos datos después de un cierto período. Por otra parte, la base de datos que contenga estos datos se debería mantener para asegurar que datos válidos y fiables están disponibles cuando sean necesarios. El plan de almacenamiento también debería abordar la necesidad de sitios de almacenamiento redundantes para asegurar la disponibilidad de los datos.

Acceso y disponibilidad de los datos

Se deberían identificar las necesidades de datos de los usuarios de las bases de datos, así como las herramientas necesarias para acceder a los datos. Además, se debería evaluar y revisar periódicamente la necesidad de restricción al acceso. El plan de gestión de datos también debería tener en cuenta las responsabilidades de la gestión de datos en toda la organización, tales como el control del acceso a los datos almacenados, la determinación del ancho de banda suficiente para soportar el volumen de usuarios potenciales y la redundancia adecuada.

Guía de protección de datos

Los principios de protección de datos se aplican a todos los tipos de datos de seguridad operacional. Incluso los datos de un informe de un accidente, que están disponibles públicamente, tienen algunos datos protegidos, como los nombres de los miembros de la tripulación u otra información que les pueda identificar directamente. Para los datos voluntarios, la protección podría ser aún mayor ya que el objetivo no es sólo proteger la identificación directa de las personas que reportan, sino también fomentar el reporte. Sin embargo, la protección de los datos y los beneficios en la seguridad operacional están estrechamente relacionados con las leyes locales/nacionales y la cultura de

seguridad operacional del Estado/Proveedor de servicios, que pueden fomentar o inhibir la cultura de reporte.

Uno de los pilares de la gestión de la seguridad operacional es la comprensión de que la mayoría de los datos voluntarios que se notifican a una autoridad reguladora deberían ser confidenciales y la identidad de las personas que reporten permanezca anónima, según lo permitido por la ley. Si los acuerdos sobre notificación de datos voluntarios y no punitivos no están permitidos por la ley y reglamentados como parte del proceso de certificación/autorización, los Estados deberían considerar la propuesta de cambios en las leyes o reglamentos para permitir este concepto demostrado de intercambio de datos.

Otra cuestión importante a tener en cuenta es la política de uso de la información de seguridad operacional de la autoridad/proveedor de servicios. Una protección excesiva o desproporcionada de los datos de seguridad operacional puede afectar negativamente a la disponibilidad de los datos necesarios para llevar a cabo la gestión de la seguridad operacional y puede limitar la capacidad de la autoridad/proveedor de servicio para utilizar estos datos con eficacia. Por lo tanto, los esfuerzos para garantizar la protección de la información de seguridad operacional deberían lograr un delicado equilibrio de intereses entre la necesidad de proteger la información de seguridad operacional y la responsabilidad de administrar justicia. La política debería incluir orientación sobre la responsabilidad de la custodia de la información de seguridad operacional y las normas relativas a la divulgación de la información. La legislación relativa al acceso a la información por parte de entidades no aeronáuticas siempre debería tenerse en cuenta al determinar qué datos se recopilará, así como los procedimientos y condiciones bajo los cuales se difundirán los datos.

La protección de los datos y la confianza en que la protección es efectiva se puede lograr a través de diversos medios. Un posible método sería tener un tercero para recopilar los datos. Esto puede ser una parte independiente de la organización. Otro método que se ha utilizado con éxito es el establecimiento de una tercera parte neutral para recopilar, des-identificar, agregar y procesar los datos del proveedor de servicios antes de su puesta a disposición del grupo de la industria o de la autoridad reguladora. De esta manera, la tercera parte neutral proporciona una barrera protectora, asegurando así la confidencialidad de los datos. En algunos casos, este método puede tener la desventaja de que el tercero puede carecer de la experiencia necesaria para validar y analizar los datos con fines de seguridad operacional de la aviación.

En resumen, cualquier proceso de protección de datos debería basarse en acuerdos formales negociados que, como mínimo tengan en cuenta:

- **Anonimato:** Establecer que todos los datos identificables necesarios durante el proceso de análisis se eliminarán de forma permanente a la mayor brevedad posible, de conformidad con el acuerdo de protección de datos asociado.

- **Control y acceso a los datos:** Identificar los datos que requieren protección y asignar la responsabilidad general para la protección de los datos. Además, en el acceso y control de datos se proporcionan directrices y procedimientos para proteger los datos, para el acceso autorizado a los datos, el procesamiento de los mismos y los lugares de almacenamiento; para el acceso autorizado a los informes y otras salidas de datos, y se exige la destrucción de los datos después de que el período de retención ha expirado.

- **Servicios de análisis de datos:** Proporcionar facilidades de acceso seguro físicamente y controlado para todos los sistemas, oficinas, equipos, estaciones de trabajo, ordenadores y periféricos asociados con el programa de análisis de datos. Se deberían proporcionar sistemas

seguros físicamente para el almacenamiento de todos los materiales relacionados con el análisis de datos, incluyendo el papel, medios de comunicación y dispositivos de copias de seguridad operacional.

Intercambio de datos de seguridad operacional

Dado que el sistema de la aviación se compone de muchas partes interesadas que interactúan y afectan a todo el ciclo de vida de la aviación, el análisis de datos de seguridad operacional se debería realizar de una manera integrada. Las mejores prácticas de la gestión de la seguridad operacional fomentan que los proveedores de servicios compartan información agregada no identificable con la autoridad, por lo que las autoridades reguladoras pueden monitorizar las tendencias en el sistema de la aviación (por sector o en su conjunto) y orientar sus recursos para hacer frente a las áreas de mayor riesgo.

Antes de determinar qué datos pueden ser compartidos y los problemas de seguridad física relacionados, es importante tener en cuenta las taxonomías comunes. El intercambio de datos requiere que todas las fuentes de información proporcionen datos con campos y taxonomías similares o ser transformados para proporcionar estos elementos comunes. Este tema fue discutido anteriormente en la sección de *Normalización de los datos* de este capítulo.

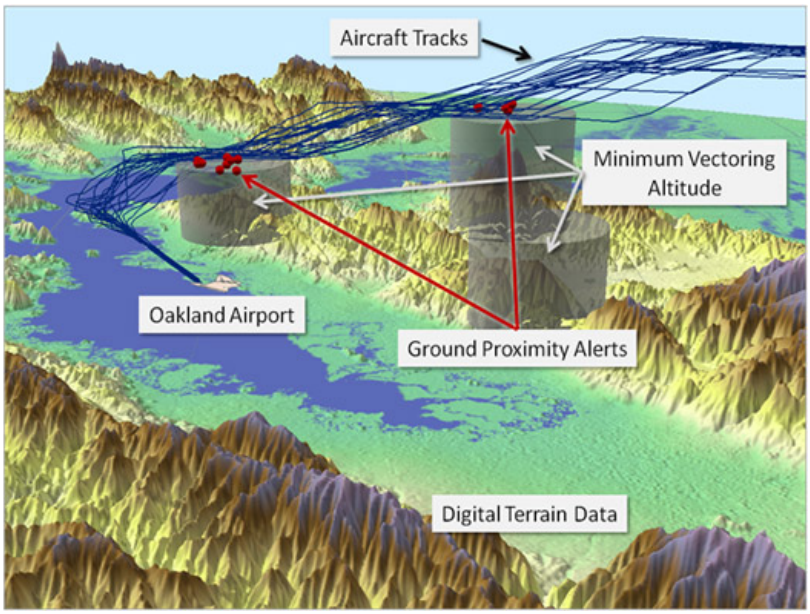
Fusión/Integración de los datos

Las herramientas disponibles hoy en día permiten la integración de datos y la síntesis con nuevas bases de datos con datos enriquecidos a partir de una recopilación de bases de datos existentes. La tecnología ha superado los obstáculos de la integración de las bases de datos con los sistemas, lo cual permite vincular diferentes bases de datos de aviación (por ejemplo, datos meteorológicos del aeropuerto, información de vuelo agregada des-identificada) sin revelar información protegida (por ejemplo, los números de vuelo, las compañías aéreas, la identidad del piloto).

Además, las autoridades reguladoras deberían promover el intercambio de datos, más allá de la capacidad de cualquier sector único de la aviación, mediante la agregación e integración de los datos. Se pueden hacer evidentes eventos atípicos, anomalías y excedencias en los gráficos generados por ordenador con la integración de los datos. Las trayectorias de vuelo reconstruidas a partir de los datos de la aeronave y los datos de la traza radar, por ejemplo, puede permitir que un analista observe que hay vuelos muy diferentes del resto. A continuación, los expertos en la materia deberían investigar las diferencias y comprender mejor las razones de que esto ocurra.

La Figura 2 ilustra el concepto de integración de datos. En este ejemplo, se puede observar la seguridad operacional de los vuelos en el entorno de un aeropuerto mediante la combinación o integración de los datos de muchas fuentes diferentes. Esta imagen es una integración de datos digitales del terreno alrededor de un aeropuerto y las trayectorias de vuelo de los aviones (línea azul) en aproximación y salida del aeropuerto.

Figura 2: Ejemplo de integración de datos



Otras consideraciones de los datos

Se deberían tener en cuenta algunas consideraciones adicionales sobre los datos de seguridad operacional para que un proceso de gestión de riesgos que se establece funcione bien: la seguridad física de los datos, la integridad de los datos y la decadencia de los datos. La seguridad física de los datos significa asegurar que los datos están seguros físicamente y protegidos de cualquier pérdida. Aunque se trata de un tema importante, va más allá del alcance de este documento.

Se debería de tener en cuenta cómo se manejan, procesan y comunican los datos de seguridad operacional dentro del sistema de la aviación, así como los medios que se deberían incorporar para mantener la integridad de los datos. La corrupción de los datos debida al error humano, al fallo de hardware, y a los errores de procesamiento del software puede comprometer la integridad de los datos y dar lugar a datos y resultados de los análisis no válidos. Idealmente, deberían realizarse comprobaciones de integridad de extremo a extremo -tales como una comprobación de redundancia cíclica (CRC), u otras técnicas equivalentes - para identificar la corrupción de los datos que pueda aparecer a lo largo de los procesos de manipulación/procesamiento de los datos.

Por otra parte, el deterioro de los datos puede dar lugar a datos inexactos. Muchos valores de los datos que son precisos pueden llegar a ser inexactos a lo largo del tiempo (es decir, el deterioro de los datos). Por ejemplo, la matrícula de la aeronave y el tipo de certificado del operador, y el número de aeronaves operadas por una compañía pueden cambiar con el tiempo. Si no se actualizan, los datos deteriorados pasan a ser inexactos. Por último, en algunos casos, satisfacer plenamente un requisito puede perjudicar significativamente a otro. Por ejemplo, la protección de los datos reduce la fiabilidad de los mismos, y cuando se lleva al extremo, puede hacer que sea casi imposible comprobar la calidad de los datos.

En resumen, los capítulos 4 y 5 de este documento discuten la importancia de los atributos de los datos y de la gestión de los mismos. Los siguientes capítulos analizan el uso de estos datos para identificar los peligros y en el proceso de gestión de riesgos.

6. IDENTIFICACIÓN DE PELIGROS

El grupo de Colaboración Internacional en la Gestión de la Seguridad Operacional (SM ICG) define un peligro como *una condición que puede causar o contribuir a un incidente o accidente de la aeronave*. Durante la fase de identificación del peligro, el analista[2] de seguridad operacional de la autoridad o del proveedor de servicio 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);
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) Procedimientos de Mantenimiento;
g) Interfaces externas (por ejemplo, servicios de outsourcing);
h) Procedimientos de la organización; y
i) Cambios en la organización.

Desencadenantes de la identificación de peligros

[2] Un analista de seguridad operacional, en el contexto de este documento, 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.

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 (operativo o de organización) e incluye una descripción detallada del cambio en particular para el sistema de aviación. El analista de seguridad operacional a 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.

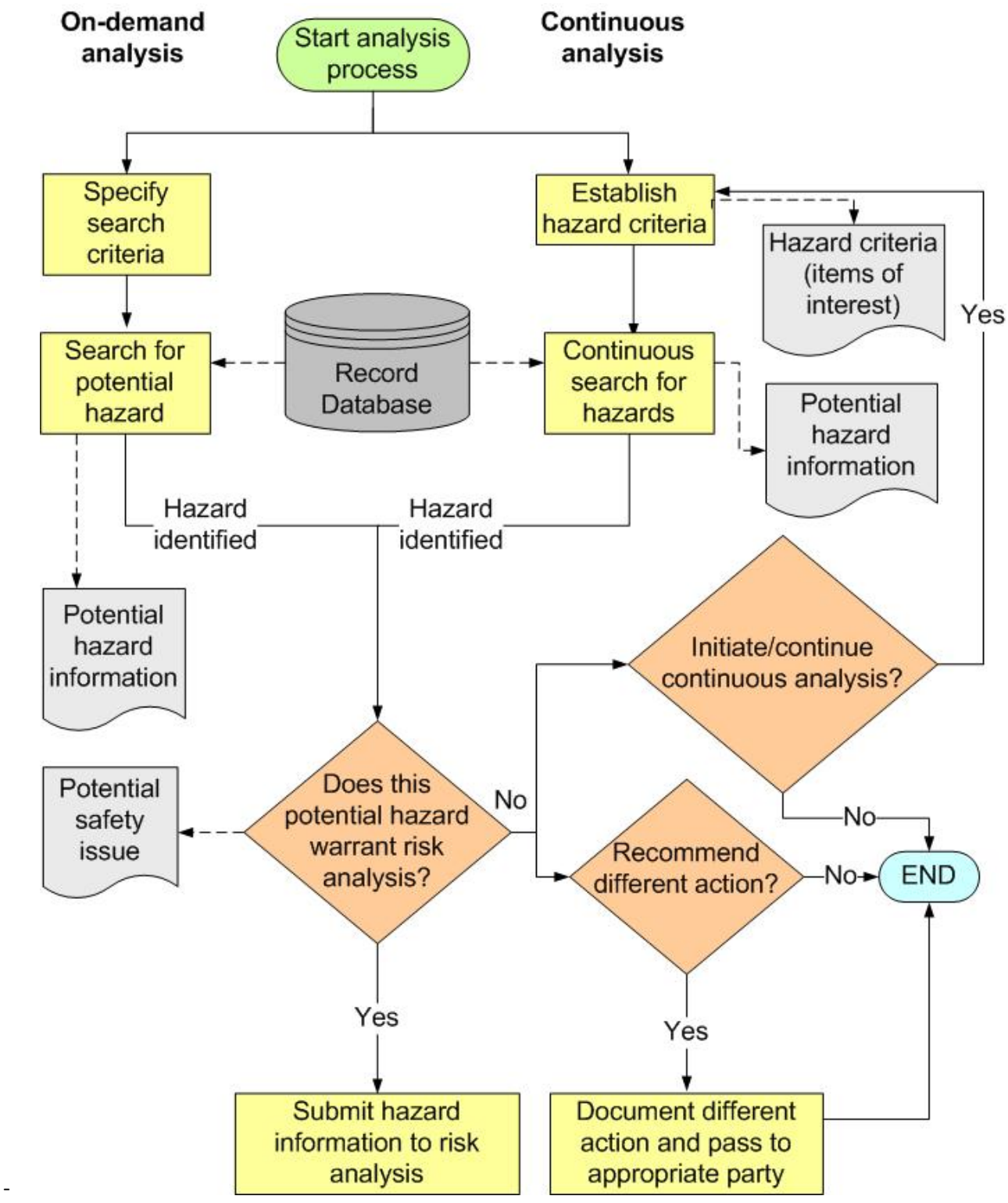


Figura 3: Identificación de peligros en un análisis continuo y bajo demanda

Métodos y herramientas en la identificación de peligros

Existen varios métodos y herramientas para la identificación de peligros. A continuación hay tres ejemplos[3].

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

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:

- Detección
- Coordinación
- Notificación
- Transmisión
- Autorización (tanto authorization como clearance en inglés)
- Selección

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

- 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.

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.

7. ANÁLISIS DE RIESGOS

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 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 figura 4 muestra un ejemplo de un proceso de análisis de riesgos utilizado para determinar el tipo y la prioridad de los controles de riesgo correctivos.

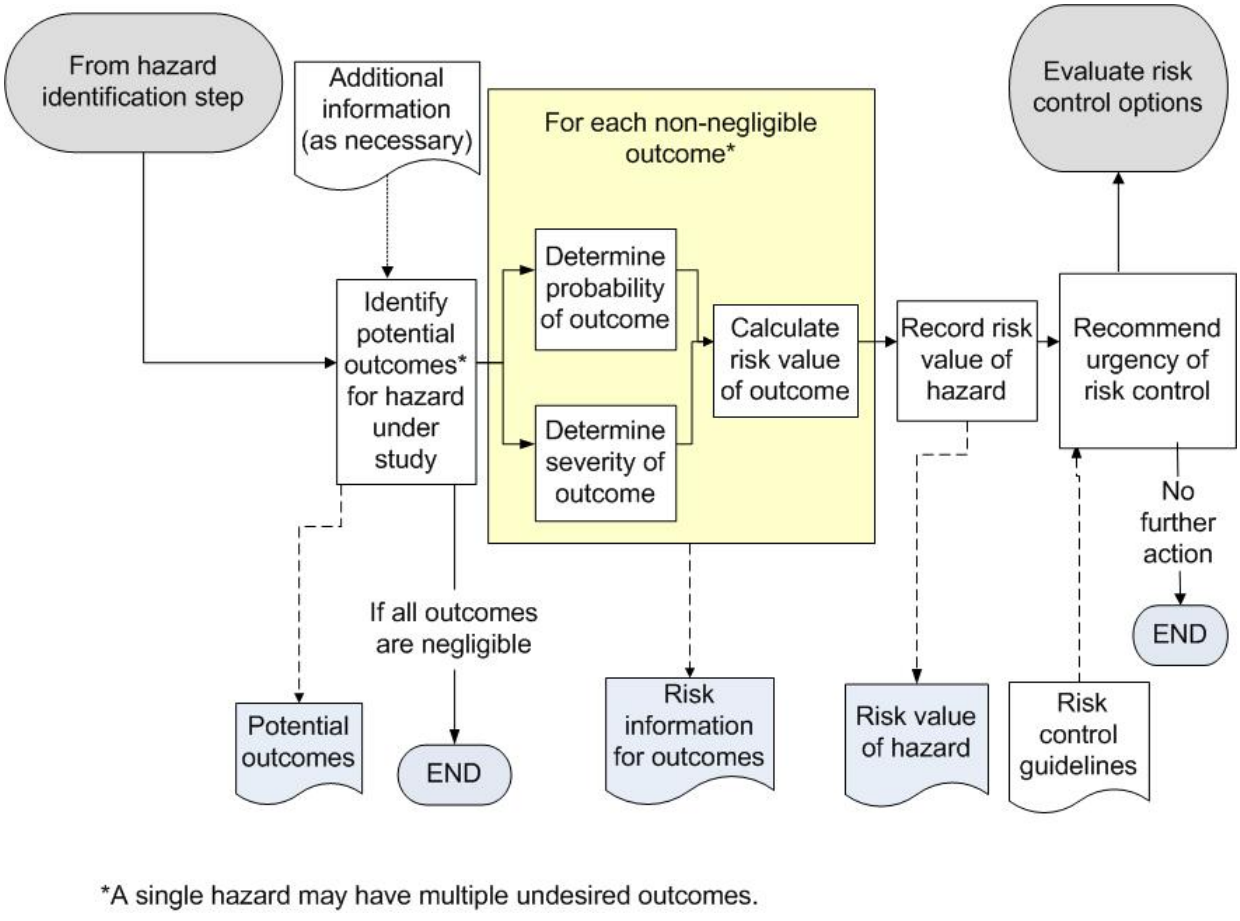


Figura 4: Ejemplo de proceso de análisis de riesgos

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.

8. ESTRATEGIAS DE MITIGACIÓN DE RIESGOS

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 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.

En resumen, la guía ha descrito y proporcionado en los capítulos 6, 7 y 8 los métodos generales que pueden ser utilizados para identificar los peligros, evaluar el riesgo asociado a los resultados de los peligros, y mitigar el riesgo a unos niveles aceptables. El siguiente capítulo ofrece ejemplos de identificación de los peligros y los métodos de análisis utilizados por algunas autoridades.

9. EJEMPLOS DE MÉTODOS ACTUALES DE GESTIÓN DE RIESGOS USADOS POR AUTORIDADES

El SM ICG realizó una encuesta entre las autoridades participantes para establecer una línea de referencia actual de las prácticas existentes para la recopilación de datos, la identificación de los peligros, y los procesos de análisis. El propósito de establecer la línea de referencia es proporcionar ejemplos de los métodos e instrumentos existentes, junto con las direcciones URL de referencia para obtener información adicional, los Estados que están desarrollando sus procesos de gestión de la seguridad operacional. Las autoridades han proporcionado tanto procesos maduros como aquellos casi desplegados. Algunos ejemplos, resultado de la encuesta, se encuentran en la tabla inferior. Siguiendo la tabla, el primer ejemplo de la tabla -el sistema Decolagem Certa (DCERTA)- está más dirigido al caso de un proceso de gestión de riesgo existente.

Tabla 1: Ejemplos de métodos de gestión de riesgos de Autoridades

Autoridad Regulatoria	Nombre del Proceso/Sistema	Descripción y Propósito del Proceso/ Sistema	Referencias para información adicional
Agencia Nacional de Aviación Civil (ANAC) de Brasil	Decolagem Certa (DCERTA) Sistema	Brasil ha desarrollado un sistema automatizado, conocido como el Sistema Decolagem Certa (DCERTA), que verifica el cumplimiento normativo de los vuelos de aviación general con respecto a la tripulación técnica (licencia, habilitación y certificado médico), aeronaves y aeródromos operados, basándose en la información contenida en los planes de vuelo presentados por los pilotos en los aeropuertos AIS. Este sistema proporciona los datos para los análisis de seguridad operacional, que a su vez han sido utilizados para generar indicadores de tendencia que permiten el establecimiento de un programa de auditoría basado en el riesgo.	http://www2.anac.gov.br/decolagemcerta/
Agencia Europea de Seguridad operacional Aérea (EASA)	Centro Europeo de Coordinación de Sistemas de Reporte de Incidentes y Accidentes	La misión del Centro Europeo de Coordinación de Sistemas de Reporte de Incidentes y Accidentes (ECCAIRS) es ayudar a las autoridades nacionales y europeas de transporte y a los organismos de investigación de accidentes en la recopilación, intercambio y	http://eccairsportal.jrc.ec.europa.eu/index.php?id=1

	(ECCAIRS)	análisis de la información de seguridad operacional con el fin de mejorar la seguridad operacional en el transporte público.	
Federal Office of Civil Aviation (FOCA) de Suiza	SRM (Safety Risk Management)	La FOCA ha puesto en marcha una agencia interna de SMS compatible con el marco de la OACI (Doc. 9859). La identificación de los peligros se realiza en base a datos desencadenantes/disparadores procedentes de la notificación de sucesos, los resultados de la vigilancia, las investigaciones de Air Accidents Investigation Branch (AAIB) y otras fuentes. El análisis es normalmente cualitativo (estudios de identificación de peligros (HAZID), HAZOP). El análisis de riesgo subsiguiente es cualitativo o cuantitativo o ambos. Los resultados se capturan en un catálogo de peligros/cartera de riesgos. Las aportaciones de los SMS de terceras partes también se integran.	http://www.bazl.admin.ch/
United States Federal Aviation Administration (FAA)/ Aircraft Certification Service (AIR)	Monitor Safety/ Analyze Data (MSAD)	Monitor Safety/ Analyze Data (MSAD) es una metodología basada en datos que permite identificar, evaluar y mitigar los peligros durante el servicio de los productos aeronáuticos, que utiliza criterios de peligros definidos por productos para mostrar los peligros potenciales a partir de datos de seguridad operacional de la aviación. MSAD utiliza una taxonomía estándar para la organización de los datos de seguridad operacional de la operación continua (COS) con el fin de promover la rápida identificación de tendencias emergentes de seguridad operacional a través del análisis de las variables dependientes. Los problemas de seguridad operacional se analizan para determinar el riesgo el cual se utiliza para establecer el alcance y el momento de la acción correctiva. El MSAD utiliza un enfoque de análisis causal. Este enfoque puede identificar los factores subyacentes que contribuyen, como las imperfecciones del proceso, que a su vez se comunican a la adecuada organización supervisora Aviation Safety Organization (AVS) del proceso de negocio.	http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/215154
Transport Canada Civil Aviation (TCCA)	TP 13905 "Risk Management, Type 2A (Short Process)"	El documento TP 13905 "Risk Management, Type 2A (Short Process)" define el proceso a seguir con detalle. Advisory Circular (AC) 107-001 "Guidance on SMS Development" proporciona también detalles de la gestión de los riesgos.	http://www.tc.gc.ca/eng/civilaviation/publications/tp13905-menu-1906.htm
Nueva Zelanda CAA	Valoraciones del perfil de riesgo	Los operadores son calificados en una escala de 1 a 5, en cada área evaluada, en la que 1 es una calificación ejemplar. Es una calificación cualitativa y se refiere únicamente a la interacción que está teniendo el miembro del	http://www.caa.govt.nz/Surveillance_System/The_Risk_Profile_Ratings.htm

		personal de la CAA con el cliente en ese momento, o a los cambios en la organización registrados en la base de datos CAA. Las puntuaciones de 2 a 5 se utilizan para registrar los niveles más altos de riesgo. Los elementos de riesgo son ponderados de acuerdo con la evaluación de la CAA de su posible efecto sobre el riesgo global de un operador. Cuando se combinan las calificaciones en cada una de las áreas evaluadas, se puede deducir un perfil de riesgo comparativo, en el que la calificación del perfil de riesgo (expresado como un porcentaje del posible) de un operador individual se muestra en un diagrama, en comparación con las calificaciones del resto de operadores en el mismo documento. Las calificaciones son confidenciales entre cada operador y la CAA.	
Bureau de la Aviación Civil Japonesa (JCAB)	Aeronautical Safety Information Management and Sharing System (ASIMS)	Los operadores están obligados a notificar los accidentes, incidentes y sucesos que puedan afectar la operación segura al sistema ASIMS. JCAB analiza las causas y evalúa los riesgos de seguridad operacional de los hechos notificados. Los resultados se utilizan para llevar a cabo una supervisión eficaz y la adopción de las medidas de seguridad operacional necesarias.	

Ejemplo de utilización de datos de la Autoridad de Aviación Civil

Caso: ANAC – Autoridad de la Aviación Civil Brasileña – Sistema *Decolagem Certa* (DCERTA).

La Agencia Nacional de Aviación Civil (ANAC) de Brasil, a través del análisis de accidentes e incidentes de la aviación general, observó que un gran número de las operaciones que acabaron en accidentes presentaban algún tipo de incumplimiento de la normativa. El gran número de operadores de aviación general y las limitaciones de ANAC en cuanto a recursos financieros y humanos implicaban dificultades para controlar estas situaciones a través de las actividades de inspección. En un intento de resolver este problema, ANAC decidió la implantación de un enfoque sistemático para identificar los focos de riesgo y optimizar las inspecciones a través de un método basado en los datos.

ANAC ha desarrollado un sistema llamado Sistema Decolagem Certa (DCERTA), traducido como "Sistema de despegue seguro." El sistema recopila datos sobre los planes de vuelo en el momento en que se hacen e interactúa con las bases de datos de la agencia, en busca de los incumplimientos acerca de las licencias de pilotos, habilitaciones y certificados médicos, el certificado de aeronavegabilidad, y los procedimientos operativos de cada vuelo. Estos datos recopilados a través del sistema DCERTA son principalmente datos del cumplimiento de la regulación, pero también están relacionados con la seguridad operacional, una vez que las normas se ponen en marcha para asegurar servicios de aviación seguros operacionalmente para la sociedad.

Los datos se utilizan para identificar los incumplimientos más frecuentes, las regiones donde son más frecuentes, e incluso el proveedor de servicios que presenta mayores tasas de incumplimientos. Las medidas de mitigación se toman con dos enfoques diferentes:

1. El primero, el incumplimiento, cuando se confirma como una violación, se trata de acuerdo con la normativa. Esta es la gestión de riesgos reactiva, que castiga las violaciones con el fin de inhibir al proveedor de servicios de mantener una operación fuera de la ley y, por lo tanto, insegura operacionalmente.

2. El segundo enfoque es la gestión preventiva de los riesgos. Al analizar estadísticamente los datos, es posible identificar a los operadores con más "no conformidades", y el sector que requiere más atención (por ejemplo, un operador que cuenta con un control deficiente de licencias de personal). Esto permite a ANAC planificar las inspecciones centrándose en los operadores identificados como de alto riesgo y corregir sus operaciones antes de que ocurra cualquier evento mayor.

Dentro de la gestión preventiva del riesgo, también es posible supervisar de forma remota a los operadores de aeronaves y definir los indicadores y las metas futuras que se deben alcanzar. Por ejemplo, ANAC supervisa varios sectores de la aviación (aviación comercial, instrucción, aviación general, etc.) a través de tres indicadores principales - uno para el total de incumplimientos, otro para los incumplimientos relacionados con el personal, y otro para las no conformidades relacionadas con las aeronaves-. La relación entre los incumplimientos y las operaciones inseguras operacionalmente se puede observar en las figuras 4 y 5.

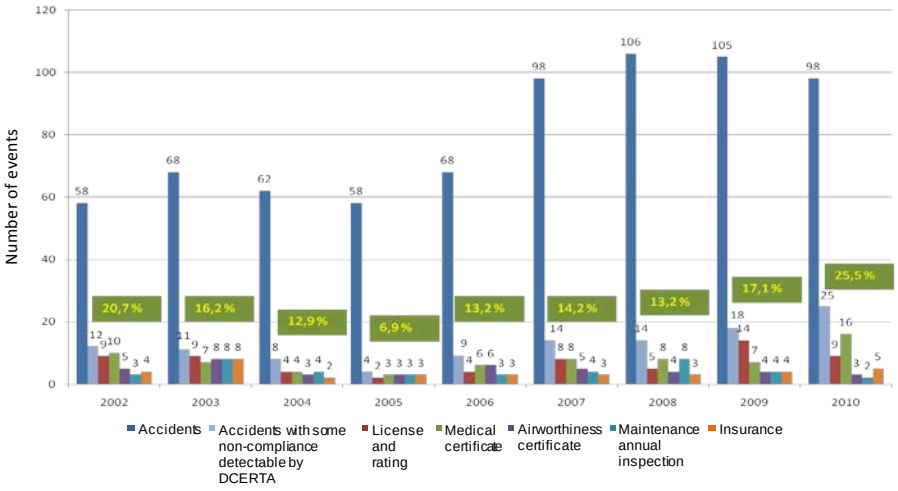


Figura 5: Incumplimientos y eventos relacionados

En la Figura 5, la columna azul representa el número de accidentes en la Aviación Civil Brasileña (aviación general incluida) y el resto de columnas representan los incumplimientos detectados por el Sistema DCERTA.

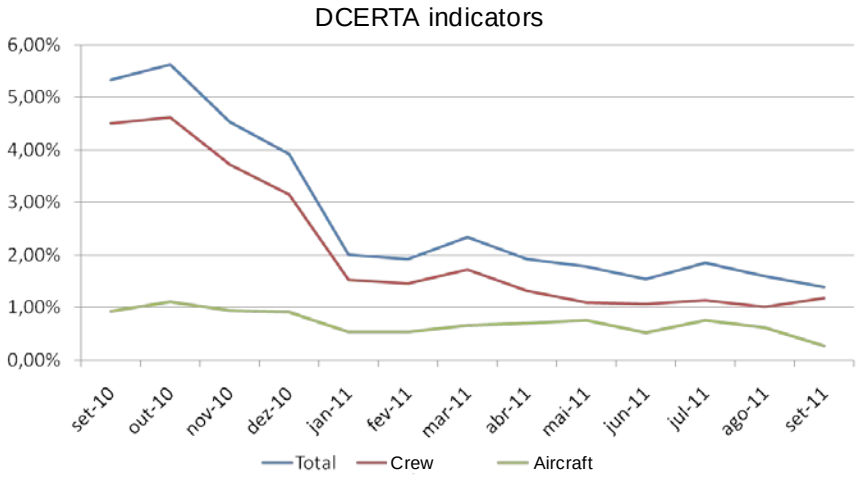


Figura 5: Indicadores DCERTA

En la figura 6, la línea azul representa el porcentaje de vuelos que presentaron algún incumplimiento en el Sistema DCERTA. La línea roja representa los incumplimientos relacionados con la situación de la tripulación y la verde con las situaciones de los aviones. Como muestra el gráfico, el número total de vuelos que presentaron algún incumplimiento en septiembre de 2011 corresponde a menos del 1,5% del número total de vuelos. Por otra parte, de la figura 5 se observa que el número total de vuelos que presentaron algunos incumplimientos entre las operaciones que dieron lugar a accidentes representan el 25,5% del total durante el 2010.

Este análisis muestra claramente la relación entre el incumplimiento y el nivel de riesgo implicado en la operación, lo que hace que el sistema DCERTA sea una herramienta muy útil para la gestión de los riesgos de seguridad operacional de la Agencia Brasileña de Aviación Civil.