NORMA TÉCNICA COMPLEMENTARIA

NTC : 004–2013
FECHA : 04/06/2013
REVISIÓN : ORIGINAL
EMITIDA POR: DGAC/SOP

TEMA: REQUISITOS PARA EFECTUAR EVALUACIONES DE SEGURIDAD OPERACIONAL PARA PROVEEDORES DE SERVICIOS DE TRÁNSITO AÉREO Y EXPLOTADORES DE AERÓDROMOS.

1. ANTECEDENTES:

1.1. En la RAP 311 Servicios de Tránsito Aéreo, en el párrafo 2.28.3 se requiere que todo cambio significativo relacionado con la seguridad operacional que se haga al sistema ATC debe entrar en vigor únicamente después que una evaluación de la seguridad operacional haya demostrado que se mantendrá un nivel aceptable de seguridad operacional.

1.2. En la RAP 314 Aeródromos, Volumen I — Diseño y operaciones de aeródromos, y la RAP 139 Certificación de Aeródromos figuran requisitos similares respecto a todo cambio en el entorno de operaciones de un aeródromo. El alcance de una evaluación de la seguridad operacional debe ser lo suficientemente amplio como para abarcar todos los aspectos del sistema que puedan resultar afectados por el cambio, directa o indirectamente, y debería incluir los elementos humanos, de equipo y de procedimientos.

1.3. Una evaluación de seguridad operacional deberá proporcionar toda la documentación y las referencias necesarias para demostrar, tanto a los proveedores ATS y de aeródromos así como a la DGAC, que un nuevo sistema o un cambio en un sistema existente, tiene un nivel aceptable de riesgo y que cumplirá con los objetivos de seguridad operacional.

1.4. En tal sentido, se hace necesario establecer los requerimientos técnicos necesarios para efectuar una evaluación de seguridad operacional con el fin de conseguir un nivel aceptable de seguridad operacional.

1.5. La OACI publicó el Documento de Información (N º 9) en la 11^{ava} Conferencia Mundial de Navegación que contiene un proyecto de "Manual de Gestión de Seguridad de Servicios de Tránsito Aéreo". Este fue actualizado posteriormente y publicado como primera edición del Doc. 9859 “Manual de Gestión de la Seguridad Operacional”. Dentro de este manual se definía un proceso de evaluación de la seguridad operacional de siete pasos. La presente Norma Técnica Complementaria se basa en ese proceso.

2. OBJETIVO:

La presente Norma Técnica Complementaria (NTC) establece un proceso, aceptable para la DGAC, para que un proveedor de servicios de tránsito aéreo y/o explotador de aeródromo efectúe una evaluación de seguridad operacional. Este proceso también es válido para efectuar un análisis de riesgo dentro de un estudio aeronáutico.

3. APLICABILIDAD

3.1 Esta norma técnica complementaria es aplicable a todos los proveedores de servicio de tránsito aéreo y explotadores de aeródromos sujetos a las RAP´s 139, 311 y 314.

3.2 Sin embargo el proceso aquí presentado es lo suficientemente flexible para que pueda ser adaptado[1] por otros proveedores de servicios aeronauticos, tales como los explotadores de aeronaves, escuelas de aviación u organizaciones de mantenimiento aprobadas, que deseen efectuar evaluaciones de seguridad operacional dentro del marco de un Sistema de gestión de seguridad Operacional (SMS).

4. DEFINICIONES Y ABREVIATURAS:

Accidente. Todo suceso, relacionado con la utilización de una aeronave, que ocurre dentro del período comprendido entre el momento en que una persona entra a bordo de la aeronave, con intención de realizar un vuelo, y el momento en que todas las personas han desembarcado, durante el cual:

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

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

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

b) la aeronave sufre daños o roturas estructurales que:

- afectan adversamente su resistencia estructural, su performance o sus características de vuelo, y
- normalmente exigen una reparación importante o el recambio del componente afectado, *excepto* por falla o daños del motor, cuando el daño se limita al motor, su capó o sus accesorios; o por daños limitados en las hélices, extremos de ala, antenas, neumáticos, frenos o carenas, pequeñas abolladuras o perforaciones en el revestimiento de la aeronave; o

c) la aeronave desaparece o es totalmente inaccesible.

AIS (Aeronautical Information Service) *Servicio de Información Aeronáutica*: Servicio establecido dentro de un área de cobertura definida responsable de la provisión de información aeronáutica y datos necesarios para la seguridad, regularidad y eficiencia de la navegación aérea.

ALARP. (As Low As Reasonably Practical) *Tan bajo como sea razonablemente practicable*: Un riesgo es lo suficientemente bajo como para no intentar que sea más bajo, o el costo de la evaluación de la mejora obtenida en un intento de reducción de riesgos, en realidad sería más costoso que cualquier costo probable que provenga del propio riesgo.

ATC (Air Traffic Control) *Control de Tránsito Aéreo***:** Servicio suministrado con el fin de prevenir colisiones entre aeronaves; o entre aeronaves y obstáculos (en el área de maniobras); con el fin de acelerar y mantener ordenadamente el movimiento del tránsito aéreo.

[1] *Las adaptaciones se refieren a las tablas de los párrafos 9.3, 9.4 y 9.5 de los pasos 3, 4 y 5 respectivamente.*

Barreras de seguridad: Término utilizado para indicar sistemas, subsistemas o métodos utilizados para reducir la probabilidad de un riesgo de generar un incidente o accidente, y /o reducir su gravedad.
Criterios de evaluación de seguridad operacional: El conjunto de criterios cuantitativos o cualitativos para ser utilizados en una evaluación de seguridad operacional para determinar la aceptabilidad del nivel evaluado de seguridad.
Evaluación de riesgo: Un proceso en donde se evalúa los peligros identificados en términos de probabilidad y severidad de las consecuencias.
Evaluación de Seguridad Operacional. Evaluación que consiste en una proceso estructurado de identificación de peligros y una evaluación de riesgos operativos de una manera sistemática y coherente.
FMECA (Failure Modes Effects and Criticality Analysis) *Análisis de modo, efectos y criticidad de la falla***:** Una metodología sistemática de identificación y evaluación de peligros que identifica en forma secuencial el impacto de fallas de componentes críticos en la función de un sistema en una serie de escenarios.
HAZOP (Hazard and Operability study) *Análisis de Peligros y Operabilidad***:** Un proceso sistemático de identificación de peligros que utiliza un grupo de expertos para llevar a cabo un análisis estructurado de un sistema, utilizando una serie de palabras claves para explorar los posibles peligros en las operaciones.
Incidente: Todo suceso relacionado con la utilización de una aeronave, que no llegue a ser un accidente, que afecte o pueda afectar la seguridad de las operaciones.
Incidente Grave: Un incidente en el que intervienen circunstancias que indican que hubo una alta probabilidad de que ocurriera un accidente, que está relacionado con la utilización de una aeronave y que, en el caso de una aeronave tripulada, ocurre entre el momento en que una persona entra a bordo de la aeronave, con la intención de realizar un vuelo, y el momento en que todas las personas han desembarcado, o en el caso de una aeronave no tripulada, que ocurre entre el momento en que la aeronave está lista para desplazarse con el propósito de realizar un vuelo y el momento en que se detiene, al finalizar el vuelo, y se apaga su sistema de propulsión principal. Ejemplos típicos incluyen:

- Una cuasi colisión que requiera una maniobra evasiva, o cuando una maniobra evasiva habría sido adecuado para evitar una colisión o una condición insegura.
- Vuelo controlado contra el terreno (CFIT) evitado con escaso margen.
- Un despegue interrumpido en una pista cerrada u ocupada, o un despegue de una pista de aterrizaje con separación marginal de los obstáculos.
- Un aterrizaje o intento de aterrizaje en una pista cerrada u ocupada.
- Una incapacidad grave de lograr el rendimiento previsto durante el despegue o ascenso inicial.
- Todos las notificaciones de incendios y humo en la cabina o en los compartimientos de carga, o en los motores, a pesar de que estos incendios se apaguen con agentes de extinción.
- Cualquier suceso que obligue al uso de oxigeno de emergencia por la tripulación de vuelo.
- Un fallo estructural de las aeronaves o la desintegración del motor que no se clasifica como un accidente.
- Mal funcionamiento de uno o más sistemas de la aeronave que afecten gravemente el funcionamiento de la aeronave.
- Cualquier caso de incapacidad de la tripulación en vuelo.
- Cualquier estado de combustible que requerirá la declaración de emergencia por el piloto.

- Incidentes en el despegue o aterrizaje, tales como aterrizajes cortos, demasiado largos o rodar al lado de las pistas.
- Fallas de los sistemas, fenómenos meteorológicos, operaciones fuera de los parámetros de vuelo aprobado u otros acontecimientos que pudieran haber ocasionado dificultades en el control de la aeronave.
- Fallo de más de un sistema de un sistema redundante obligatorio para la guía de vuelo y de navegación.

Índice de riesgo: Indicación relativa al nivel de riesgo. Es el producto de la probabilidad de que una sucesión de eventos ocurra y produzca una consecuencia específica, la severidad de la consecuencia específica para el que toma la decisión. Índice de riesgo (I_R)= Probabilidad (P) x Severidad (S).

Nivel inicial aceptable de desempeño de seguridad operacional: Será el nivel alcanzado por los proveedores de servicios aeronáuticos que cumplan las normas aeronáuticas nacionales e implanten satisfactoriamente un sistema de gestión de seguridad operacional.

Objetivo de Seguridad Operacional: La definición de un peligro, junto con su meta como tasa máxima de ocurrencia. Una meta o propósito que, cuando se logra, demuestra que un nivel tolerable de seguridad está siendo o será alcanzado por el peligro identificado.

Proyecto: Término utilizado para describir cualquier equipo, procedimiento (por ejemplo procedimientos utilizados por los operadores de aeródromo o proveedor de servicios ATS, o alternativamente, un procedimiento de mantenimiento para un equipo relacionado) y a las personas involucradas de la organización. En la presente norma es sinónimo de sistema.

Peligro: Cualquier condición, suceso o circunstancia el cual pueda inducir a un accidente.

Riesgo: Una combinación de la probabilidad y la severidad de la consecuencia de un peligro que podría resultar en un accidente; por ejemplo cuando mayor es el riesgo, es más probable del accidente se produzca y/o será más severa la consecuencia.

Requisitos de seguridad operacional: Criterios especificados de un sistema que son necesarios con el fin de reducir el riesgo de un accidente o incidente a un nivel aceptable. También se define como el requisito que ayuda a lograr un objetivo de seguridad operacional.

Requisitos reglamentarios aplicables de seguridad operacional: Los requisitos para la prestación de los servicios de tránsito aéreo, o para la operación de un aeródromo respecto de las facilidades aplicables a una situación concreta que se examina en relación con, entre otros:

a) la competencia técnica y operativa y la idoneidad para prestar el servicio o la instalación;
b) los sistemas y procesos para la gestión de la seguridad;
c) los sistemas técnicos, sus componentes y procedimientos asociados.

Sistema: Término utilizado para describir la colección de equipos, procedimientos y/o el personal necesarios para llevar a cabo una función. En la presente norma es sinónimo de proyecto.

TLS (Target Level of Safety) *Nivel aceptable de seguridad*: Un objetivo de seguridad operacional definido como una tasa tolerable de accidentes en términos de probabilidad de un accidente dada cierta cantidad de actividad.

5. FECHA EFECTIVA

Esta NTC entra en vigencia a partir del día siguiente de la fecha de su publicación en el Diario Oficial El Peruano.

6. BASE LEGAL

- Ley de Aeronáutica Civil del Perú, Le y N.º 27261,
- Reglamento de la Ley de Aeronáutica Civil Aprobado con DS. N°050-2001-MTC
- RAP 139 “Certificación de Aeródromos”
- RAP 311 “Servicios de Tránsito Aéreo”
- RAP 314 “ Aeródromos”
- NTC-001-2011 Requerimientos para implantar y mantener el Sistema de Gestión de Seguridad Operacional (SMS) en los servicios de tránsito aéreo”.
- NTC-003-2011 Requerimientos para implantar y mantener un Sistema de Gestión de la Seguridad Operacional (SMS) en un aeródromo”.

7. DOCUMENTOS RELACIONADOS

- OACI Anexo 11 “Servicios de Tránsito Aéreo”
- OACI Anexo 14 “Aeródromos”
- OACI Doc. 9859 AN/474 “Manual de la Gestión de la Seguridad Operacional” 1^{era} y 2da edición.
- OACI Doc. 9774 AN/969 “Manual de Certificación de Aeródromos”
- Circular de Asesoramiento 311-2.28.03 Implantación de la Fase 2 “Gestión de Riesgos” de la Seguridad Operacional en un Proveedor de Servicios de Tránsito Aéreo
- Circular de Asesoramiento 139-200-02 Implantación de la Fase 2 “Gestión de Riesgos” de la Seguridad Operacional en un Explotador de Aeródromo

8. REGULACION:

8.1. INTRODUCCIÓN

8.1.1. La gestión de la seguridad operacional proporciona los medios por los que las organizaciones pueden controlar los procesos que podrían conducir a sucesos peligrosos, a fin de asegurarse de que el riesgo de lesiones o daños se limita a un nivel aceptable. Gran parte de esta actividad se concentra en peligros que se identifican por medio de procesos y actividades como: investigación de eventos relacionados con la seguridad operacional, sistemas de notificación de incidentes y programas de vigilancia de la seguridad operacional. Las evaluaciones de la seguridad operacional proporcionan otro mecanismo preventivo para identificar posibles peligros y encontrar las maneras de controlar los riesgos relacionados con ellos.

8.2.1. Antes de poner en práctica cambios importantes que puedan afectar a la seguridad de las operaciones debería realizarse una evaluación de la seguridad operacional a fin de demostrar que el cambio logrará un nivel aceptable de desempeño de seguridad operacional. Por ejemplo, cuando se prevén cambios importantes relativos a los procedimientos operacionales, a la adquisición o configuración de equipo, a las relaciones de trabajo en la organización, etc. puede justificarse una evaluación de la seguridad operacional.

8.3.1. Durante la vigencia de un sistema (desde el diseño hasta la retirada del servicio) puede haber varias interacciones de la evaluación y mitigación de riesgos y las actualizaciones de evaluaciones de seguridad. Una evaluación de seguridad operacional es, por tanto, un "documento vivo" y debe ser desarrollada junto con el ciclo de vida del sistema. El trabajo en el caso de

seguridad por lo tanto, debe comenzar cuando un proyecto está en su fase de concepto inicial y el contenido debe ser añadido a medida que el proyecto avanza a lo largo de su ciclo de vida a través de su retiro del servicio. Pueden ser aplicables a ciertos tipos de sistemas o equipos las normas internacionales adoptadas a nivel nacional.

8.4.1. Si el resultado de una evaluación es que el sistema objeto de examen no satisface los criterios de seguridad operacional, será necesario encontrar los medios de modificar el sistema para reducir los riesgos. Este proceso se llama mitigación de riesgos. La elaboración de medidas de mitigación es parte integral del proceso de evaluación. Las medidas de mitigación propuestas deberían someterse a prueba para ver si son adecuadas, reevaluando cuál sería el riesgo una vez implantadas dichas medidas.

8.5.1. El proceso de evaluación de la seguridad operacional está dirigido a responder las tres preguntas fundamentales que siguen:

a) ¿Qué podría andar mal?
b) ¿Cuáles serían las consecuencias?
c) ¿Cuán a menudo podría ocurrir?

8.6.1. La evaluación de seguridad operacional es un proceso estructurado y sistemático para la identificación de peligros y la evaluación del riesgo asociado a cada peligro, o grupo de peligros. La aceptabilidad de los riesgos se determina comparando el nivel evaluado de riesgo contra los criterios de evaluación de la seguridad operacional establecidos previamente u Objetivos de Seguridad Operacional. Este proceso consta de siete pasos para efectuar la identificación de peligros, evaluación de las consecuencias de estos peligros, establecer el nivel de riesgo de cada peligro, diseñar medidas para eliminar o mitigar los riesgos y establecer si el sistema está o no dentro de los parámetros aceptables de seguridad operacional.

8.7.1. En la RAP 311 Servicios de Tránsito Aéreo párrafo 2.28.3 a), requiere que cualquier cambio significativo del sistema ATS relacionado con la seguridad operacional, incluida la implantación de una mínima reducida de separación o de un nuevo procedimiento, solamente entrará en vigor después de que una evaluación de la seguridad operacional haya demostrado que se satisfará un nivel aceptable de seguridad y se haya consultado con los usuarios. Por lo tanto, cualquier sistema nuevo o cambio a un sistema existente debe ser evaluado a través de un proceso estructurado de evaluación y mitigación del riesgo

8.8.1. En la RAP 314 Aeródromos, se establece requisitos similares para los aeródromos certificados.

8.2. NECESIDAD DE EVALUACIONES DE SEGURIDAD OPERACIONAL

8.2.1. Aunque no es posible producir una lista exhaustiva detallando cada circunstancia que requiere de una evaluación de riesgos, la siguiente lista es un ejemplo de cuando es necesario efectuar una evaluación de seguridad operacional:

a) Aplicación de nuevas, o cambios en, comunicaciones, navegación, vigilancia u otros sistemas y/o equipos importantes para la seguridad, incluidos los que proporcionan nuevas funcionalidades y / o capacidades.
b) Cambios físicos en el diseño de las pistas y calles de rodaje o en un aeródromo.
c) Cambios físicos en plataformas y rutas de rodaje.
d) Introducción de un nuevo tipo o clase de aeronave en un aeródromo.

e) Desarrollo o modificación de los procedimientos de aeródromo, incluyendo nuevos procedimientos para operar en las instalaciones del aeródromo, cambios en los procedimientos de rescate y combate contra incendios, etc.
f) Cambios / implantación de entrenamiento o re-entrenamiento de personal técnico / operativo.
g) Cambios a la separación mínima a aplicarse dentro de un espacio aéreo o en un aeródromo.
h) Nuevos procedimientos operativos, incluyendo los procedimientos de salida y de llegada, a ser aplicados en determinado espacio aéreo o aeródromo.
i) Reorganización de la estructura de rutas ATS.
j) Re sectorización del espacio aéreo.
k) La introducción de un sistema de gestión de la seguridad nueva (SMS) para una organización, donde el SMS requiere la evaluación de riesgos de los sistemas que lo cubre.

9. PROCESO DE EVALUACIÓN DE LA SEGURIDAD OPERACIONAL

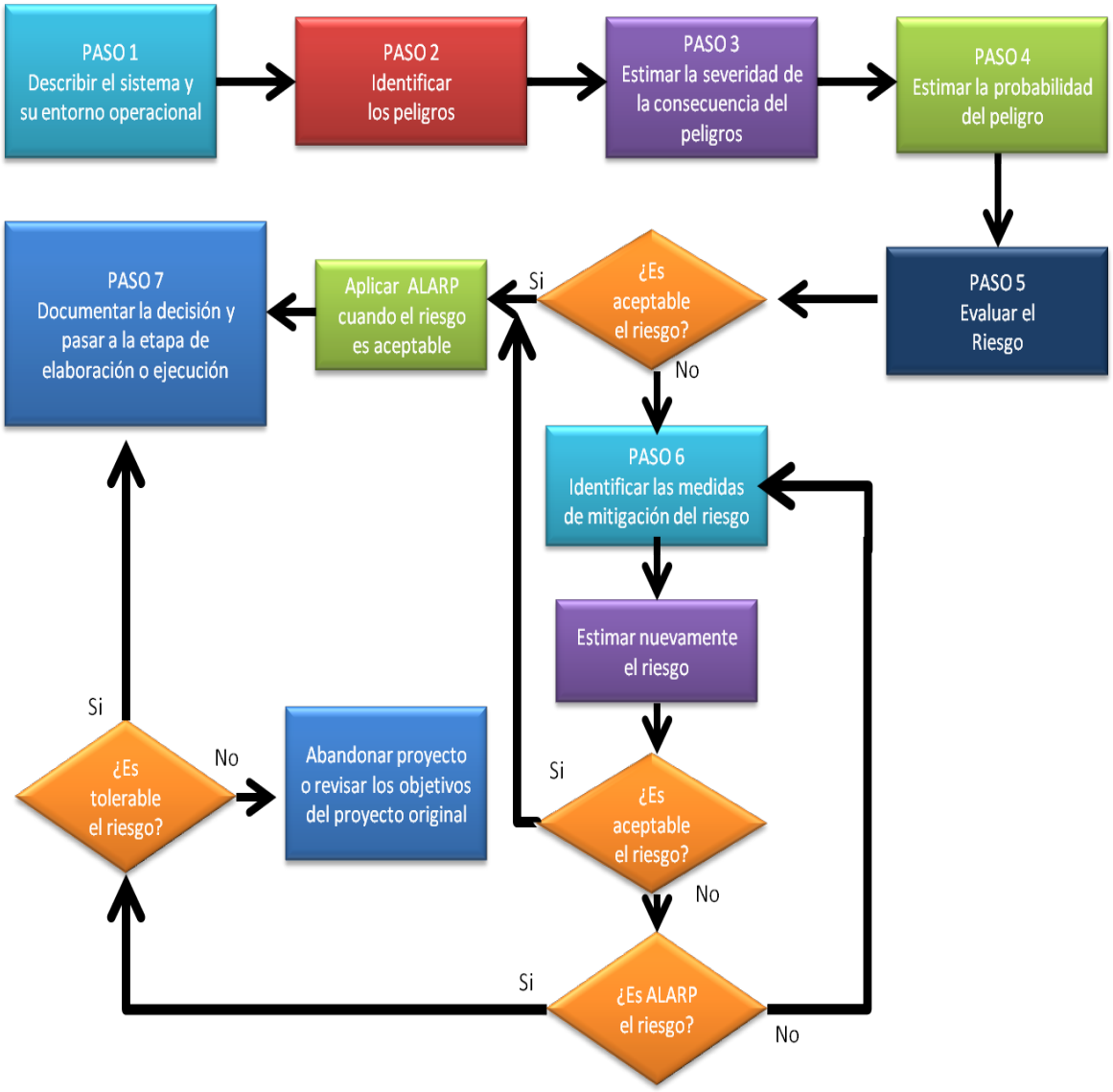
a) Las evaluaciones de la seguridad operacional son una aplicación particular del proceso de gestión de riesgos, fundadas en los procesos sistemáticos. El proceso de evaluación de la seguridad operacional puede dividirse en siete pasos que se describen en la Tabla 1-1.

Tabla 1-1. Siete pasos para la evaluación de la seguridad operacional

Paso	Actividad
1er	Elaboración de una descripción completa del sistema que se debe evaluar y del entorno en que el sistema debe funcionar
2do	Identificar peligros
3er	Estimar la severidad de las consecuencias de que un peligro se materialice
4to	Estimación de la probabilidad de que un peligro se materialice
5to	Evaluación de riesgo
6to	Mitigación de riesgo
7mo	Elaboración de los documentos de evaluación de la seguridad operacional

b) En la Figura 1-1 se presenta un diagrama que ilustra el proceso de evaluación de la seguridad operacional y muestra la posible necesidad de realizar varios ciclos del proceso hasta encontrar un método satisfactorio de mitigación de riesgos. Seguidamente se examinarán con más detalles cada uno de los siete pasos de una evaluación de la seguridad operacional.

Figura 1.1: PROCESO DE EVALUACION DE LA SEGURIDAD OPERACIONAL



9.1. PASO 1: ELABORACIÓN DE UNA DESCRIPCIÓN COMPLETA DEL SISTEMA QUE SE DEBE EVALUAR Y DEL ENTORNO EN QUE EL SISTEMA DEBERÁ FUNCIONAR

9.1.1. Las actividades claves del primer paso a describir son:
a) sistema/ cambio
b) propósito del sistema
c) cómo el sistema será utilizado (concepto de operación)
d) funciones del sistema (requisitos operacionales)
e) límites del sistema
f)medio ambiente incluido las interfaces con sistemas más grandes.

9.1.2. Si todos los riesgos potenciales deben ser identificados, las personas involucradas en la evaluación de la seguridad deben tener una buena comprensión del nuevo sistema propuesto, o cambio en el sistema existente, y cómo va a interactuar con los otros componentes del aeródromo, o sistema ATS. Por esta razón, el primer paso en el proceso de evaluación de seguridad consiste en preparar una descripción del sistema propuesto o cambio, así como el entorno en el que va a operar.

9.1.3. El proceso de identificación de los peligros sólo pueden identificar los peligros que vienen en el ámbito de la descripción del sistema. Los límites del sistema, tal como se define para los fines de la evaluación del riesgo, deben ser por lo tanto lo suficientemente amplio para abarcar todos los posibles impactos que el sistema podría tener. En particular, es importante que la descripción incluya las interfaces con cualquier sistema más grande de los cuales el proyecto puede ser una parte.

9.1.4. Una descripción detallada del sistema debe incluir:
a) la finalidad del sistema;
b) cómo se utiliza el sistema (esto puede ser descrito como un concepto de operación);
c) una descripción de las funciones del sistema (esto puede lograrse, en parte, mediante la descripción de los requisitos operativos del sistema);
d) los límites del sistema y las interfaces externas;
e) otros sistemas que pueden ser influidos por, o influir en éste, y
f)una descripción del entorno en el que el sistema funcionará.
NOTA: Para facilitar la lectura, se deben evita las largas descripciones técnicas de cómo funcionan los equipos individuales. En su lugar, se pueden hacer referencia a los documentos técnicos.

9.1.5. El impacto en la seguridad de una pérdida potencial, degradación, o falla del sistema será determinada, en parte, por las características del entorno operativo en el cual el sistema está integrado. La descripción del medio ambiente por lo tanto, debe incluir todos los factores que podrían tener un efecto significativo en la seguridad. Estos factores varían de un caso a otro. Se podrían incluir, por ejemplo:
a) características del tráfico;
b) infraestructura del aeródromo;
c) dependencia de los sistemas basados en el espacio por ejemplo, las comunicaciones y navegación por satélite;
d) peligro aviario;
e) área de movimiento;
f) horas de operación (día / noche);

g) clima, por ejemplo, prevalencia de vientos cruzados o cizalladura, o la duración de las operaciones en baja visibilidad;
h) la frecuencia de las desviaciones debidas a condiciones meteorológicas adversas.

9.1.6. La descripción del sistema debe incluir todas las hipótesis acerca de las interfaces u otros sistemas con los que este sistema interactúa. Se deben incluir la justificación de los supuestos siempre que sea posible.

9.1.7. La descripción del sistema debe abordar también procedimientos de contingencia pre-existentes y otras operaciones no estándar, por ejemplo, durante:
a) falla en el equipamiento ATS;
b) reducción del Servicio de Salvamento y Extinción de Incendios (SEI);
c) reducción de las distancias declaradas.

9.1.8. Para muchos proyectos será adecuado para la descripción del sistema abordar la estrategia para la transición del antiguo al nuevo sistema. Por ejemplo, ¿El sistema existente debe ser dado de baja y reemplazado inmediatamente por el nuevo sistema, o deben operar los dos sistemas en paralelo por un período de tiempo?

9.1.9. Puede haber varias actualizaciones a la descripción del sistema en todo el ciclo de vida de los proyectos. Es importante mantener actualizada la descripción del diseño del sistema de cuando se tomaron y se aplicaron las decisiones. Sin ello, existe el riesgo de que las sesiones de identificación de peligros, que pueden tener lugar en varias etapas en la vida de un proyecto, no considere el diseño del sistema más reciente.

9.1.10. La descripción del sistema a menudo se presentan mejor utilizando una combinación de texto y diagramas. El uso de diagramas puede ser un medio eficaz para transmitir información, por ejemplo:
a) el uso de diagramas de flujo para mostrar un proceso del sistema o de la secuencia de actividades requerido por un procedimiento;
b) la utilización de dibujos para mostrar la disposición general del aeródromo incluyendo las calles de rodaje, pista de aterrizaje, puntos de cruce, la ubicación SEI, tiendas de combustible, ubicación del equipo ATS, etc.;
c) el uso de dibujos o diagramas que muestran los arreglos del espacio aéreo, incluyendo los sectores, las rutas normalizadas de salida y llegadas, rutas de aproximaciones frustradas, área de guía vectorial radar, etc.;
d) el uso de diagramas de bloques para mostrar las interacciones entre los componentes del sistema y los flujos de información y datos.

9.2. PASO 2: IDENTIFICACIÓN DE PELIGROS

9.2.1. Las actividades claves del Paso 2 son:
a) crear un registro de peligros.
b) identificar los peligros
c) identificar las consecuencias de cada peligro; y luego
d) actualizar el registro de peligros

9.2.2. Registro de peligros

Un registro de peligros es un método formal utilizado para documentar los peligros identificados para un sistema. El registro de peligros consiste en una serie de formularios en que los detalles de cada situación de peligro pueden ser registrados. Cuando la información esté disponible. Los detalles de los riesgos asociados a cada peligro, junto con cualquier medida de mitigación

se deberán indicar también en los formatos. En el **Apéndice A** se muestra un ejemplo de estructura de un formato de registro de peligros.

9.2.3. Cuando realizar la identificación de peligros

La etapa de identificación del peligro se debe ser iniciar en la etapa más temprana posible del ciclo de vida del proyecto. Para proyectos de gran envergadura, puede haber identificación de los peligros en varios sesiones de las diferentes etapas del desarrollo del proyecto. El nivel de detalle requerido dependerá de la complejidad del sistema bajo examen y la etapa del ciclo de vida del sistema en el que la evaluación se lleva a cabo. En general, se espera que haya menos análisis requerido para una evaluación llevada a cabo durante la primera etapa de definición de los requisitos operacionales que para una etapa de diseño posterior.

9.2.4. Fuentes de Peligros

9.2.4.1. La etapa de identificación del peligro deben considerar todas las posibles fuentes de fallas de sistema. Dependiendo de la naturaleza y el tamaño del sistema en consideración estos podrían incluir:

a) equipo (hardware y software);
b) entorno operativo (incluyendo las condiciones físicas, espacio aéreo y diseño de aerovías y obstáculos);
c) operadores humanos (pilotos, controladores de tránsito aéreo, técnicos de mantenimiento);
d) interfaz hombre-máquina (HMI);
e) procedimientos operacionales;
f)procedimientos de mantenimiento;
g) servicios externos por ejemplo, electricidad, líneas telefónicas;
h) servicios contratados.

9.2.4.2. Se deben de considerar todas las configuraciones posibles del sistema. Por ejemplo, si la dotación de personal y de sectorización del espacio aéreo es diferente en la noche que durante el día, se deben examinar los peligros de ambas configuraciones. Se deben considerar las operaciones con equipo fuera de servicio para el mantenimiento regular.

9.2.4.3. También deben ser considerados las configuraciones no estándar de operación del aeródromo, si es apropiado, por ejemplo, durante operaciones de baja visibilidad o mientras hay "trabajo en progreso".

9.2.5. Métodos de identificación de peligros

9.2.5.1. Los métodos de identificación de peligro se dividen en los 3 criterios genéricos siguientes:

a) **Histórico:** Uso y análisis de los registros de peligros existentes y los informes de accidentes/incidentes (Esto puede ser necesaria como parte de un SMS). También los peligros identificados a partir de otros procesos de evaluación del riesgo en otros sistemas que pueden ser similares a este sistema (por ejemplo, ¿Tiene un sistema similar en servicio una historia significativa en un modo comparable de operación?);
b) **Lluvia de ideas** (Brainstorming): Sesiones organizadas y planificadas con vistas a alentar a un equipo de los participantes con experiencia y pericia en diversas áreas para explorar los peligros potenciales del sistema de una manera creativa. El **Apéndice B** proporciona orientación sobre el proceso de identificación de peligros utilizando lluvia de ideas;
c) **Comprobación sistemática:** Sesiones que implican una revisión secuencial a fondo de un sistema, a menudo usando diagramas

de sistemas y descripciones que piden palabras clave para ayudar a enfocar los tipos de fallas que se deben evaluar. Los procesos sistemáticos de identificación de peligros son:

- Modos de fallo, efectos y análisis de la criticidad (Failure Modes Effects and Criticality Analysis FMECA) (Ver **Apéndice C**)
- Análisis de Peligros y operatividad (Hazard and Operability Analysis HAZOP). (Ver **Apéndice D**)

NOTA: *Para obtener la máxima eficacia de los enfoques históricos y de lluvia de ideas, estos deben ser utilizado en conjunción con los procesos sistemáticos. La salida del método histórico puede alimentar a los métodos de lluvia de ideas y de comprobación sistemática para desencadenar una mejor exploración de los peligros identificados en el nuevo contexto.*

9.2.5.2. Algunos de los peligros más complicados se identificaron utilizando los procedimientos anteriores, especialmente aquellos que involucran secuencias de eventos. Estos se pueden beneficiar de un examen más detenido con árboles de eventos (**Apéndice E**), que pueden usarse para explorar la gama de consecuencias y barreras disponibles para un peligro en particular.

9.2.5.3. Para una eficaz identificación de peligros, es importante que el personal apropiado y los expertos del sistema se involucren en los procesos de identificación de peligros. Las personas típicas que pueden participar son los siguientes:

a) controladores de tránsito aéreo;
b) pilotos;
c) ingenieros de mantenimiento y diseño;
d) personal especialista en aeródromos como el personal SEI, personal de seguridad y personal de estaciones de servicio.

NOTA: Por razones de eficiencia, el personal involucrado en los procesos de identificación de peligros se puede incluir en las mismas sesiones de la evaluación de la severidad y la probabilidad (pasos 3 y 4) tras el proceso de identificación de los peligros.

9.2.6. Registro Especial de Peligros

9.2.6.1. Un sistema efectivo de gestión de la seguridad operacional (SMS) debe garantizar que se anima todo el personal a buscar y reportar los problemas de seguridad y los peligros potenciales como parte normal del día a día del trabajo. Los peligros relevantes identificados de esta manera deben ser capturados en el Registro de peligros.

9.2.6.2. Para una captura efectiva de peligros, los métodos para informar de los peligros deberían ser procedimientos claramente definidos, por ejemplo, procedimientos establecidos de como registrar un peligro y que peligros deben ser reportados.

NOTA: *Se debe desarrollar una cultura de reporte dentro de la organización para alentar la identificación de peligros*.

9.2.7. Consecuencias del peligro

9.2.7.1. Las consecuencias del peligro se determina mediante el análisis de lo que podría suceder si el peligro se manifiesta en un accidente o incidente. Algunas consecuencias pueden ser obvias, con la existencia de sólo un resultado posible como resultado de un determinado peligro. Sin embargo otros peligros pueden resultar en una serie de consecuencias de diversas severidades. Utilizando el análisis de árbol de eventos (**ver Apéndice E**) puede ayudar a

determinar el rango de las consecuencias. Se deben de considerar la extensión de los efectos sobre los siguientes:

a) la tripulación de vuelo (carga de trabajo, la capacidad para realizar funciones);
b) los controladores de tránsito aéreo (carga de trabajo, la capacidad para realizar funciones);
c) las capacidades funcionales de la aeronave;
d) las capacidades funcionales de los sistemas ATS de tierra;
e) la capacidad de proporcionar los servicios de seguridad de gestión del tránsito (por ejemplo, la magnitud de la pérdida o corrupción de los servicios de gestión del tránsito aéreo o funciones).
f) el personal operativo del aeródromo (carga de trabajo, la capacidad para realizar funciones);
g) los procedimientos operacionales del aeródromo (que podría ser deficientes).

9.2.7.2. Una vez que todos los peligros han sido identificados deberán estar inscritos en el registro de peligros junto con sus posibles consecuencias.

9.2.8. Registro de resultados de la identificación de peligros

9.2.8.1. A todos los peligros identificados se le debe asignar un número de peligro, y registrar en el registro de peligros. (**Ver apéndice A**)

9.2.8.2. El registro de peligros debe contener una descripción de cada uno de los peligros, sus consecuencias, la probabilidad y severidad evaluada (pasos 3 y 4), así como las medidas de mitigación necesarias (paso 6).

9.2.8.3. 9.2.8.3 Las entradas adicionales de registro de peligros tendrán que hacerse donde hay más de una preocupación de consecuencia creíble.

NOTA: *No siempre la consecuencia más grave es el riesgo más alto. Esto es debido a que la consecuencia más grave puede ser muy poco probable que ocurra, mientras que una menos severa, pero con consecuencias indeseables pueden ser más probables que ocurra. Cabe recordar que el "riesgo" es una combinación de severidad y probabilidad.*

9.2.8.4. El registro de peligros se deberá actualizar con los nuevos peligros identificados y las propuestas para la mitigación se introducirán a través del ciclo de vida del proyecto.

9.2.8.5. Los peligros registrados en el registro de peligros se debe utilizar para alimentar los pasos posteriores de evaluación de riesgo de este procedimiento.

9.3. PASO 3: ESTIMACIÓN DE LA SEVERIDAD DE LAS CONSECUENCIAS DE QUE UN PELIGRO SE MATERIALICE

9.3.1. Las actividades claves del Paso 3 son:

a) evaluar la severidad de cada consecuencia; y
b) registrar el resultado en el registro de peligros.

9.3.2. Antes de iniciar este paso, deberían consignarse en el registro de peligros las consecuencias de cada peligro identificado en el paso 2. El paso 3 supone la evaluación de la severidad de cada una de estas consecuencias.

9.3.3. El grupo que identificó los peligros sería el más apropiado para evaluar la severidad de las consecuencias.

9.3.4. Si bien la evaluación de la gravedad de las consecuencias siempre significará cierto grado de juicio subjetivo, las discusiones en grupo

estructuradas, guiadas por una clasificación de riesgos normalizada y con participantes que tienen amplia experiencia en sus respectivas especialidades, deberían asegurar que el resultado será un juicio con conocimiento de causa.

9.3.5. La Tabla 1, contiene la clasificación de severidad que se podría utilizar en el caso. La clasificación de la severidad de todas las consecuencias verosímiles de un peligro se determinan en la tabla. Si se utiliza un esquema alternativo, debe de definirse claramente.

9.3.6. Una vez que se ha terminado la evaluación de la severidad de todos los peligros identificados, los resultados deberían consignarse en el registro de peligros, incluyendo la justificación de la clasificación dada a la severidad.

TABLA 1. Ejemplo de clasificación de Severidad

Severidad (S) Secuencia de eventos que ha pasado. ¿Cuán serio es el impacto de las consecuencias?	
5 Catastrófico	• Accidente • También incluye la pérdida o daños considerables a las principales instalaciones del aeródromo. • Lesiones graves o la muerte de personal múltiple / los miembros del público en el aeródromo.
4 Mayor	• Incidente grave- Cuasi Colisión • Para el aeródromo, un evento donde estuvo cerca un accidente. • No hay barreras de seguridad restantes. • El resultado no está bajo control y muy probablemente puede conducir a un accidente. • Daño a las principales instalaciones del aeródromo. • Lesiones graves para el personal / miembros del público en el aeródromo.
3 Moderado	• Un incidente relacionado con la operación de una aeronave, en la que la seguridad de las aeronaves ha sido puesta en peligro, que podría haber llevado a una cuasi colisión entre aeronaves, con el suelo o con obstáculos. • Una gran reducción en los márgenes de seguridad. • El resultado es controlable por el uso de procedimientos de emergencia o no estándares y/o equipos de emergencia. • Muy pocas barreras de seguridad. • Lesiones leves a los ocupantes de la aeronave o el personal / miembros del público en el aeródromo. • Pueden ocurrir daños menores a las aeronaves o las instalaciones principales del aeródromo.
2 Menor	• Incidentes significativos que indican que un accidente, un incidente grave o importante podría haber ocurrido, si el riesgo no se habría gestionado dentro de los márgenes de seguridad, o si otra aeronave había estado en la vecindad. • Una reducción significativa de los márgenes de seguridad, pero permanecen varias barreras de seguridad para prevenir un accidente. • Disminución de la capacidad de la tripulación de vuelo o de control del tráfico aéreo para hacer frente al aumento de la carga de trabajo como consecuencia de condiciones que impiden su eficiencia. • Sólo en raras ocasiones puede convertirse en la ocurrencia de un accidente. • Molestias a los ocupantes de la aeronave o el personal o miembros del público en el aeródromo.
1 Despreciable	• Sin efecto inmediato en la seguridad operacional • Sin impacto directo en la seguridad o bajo impacto • Las barrera de seguridad entran en juego para evitar que el evento se convierta en incidente importante

9.4. PASO 4: ESTIMACIÓN DE LA PROBABILIDAD DE QUE UN PELIGRO SE MATERIALICE

9.4.1. Las actividades claves del paso 4 son:

a) Estimar la probabilidad de las consecuencias de la ocurrencia del peligro, y

b) registrar los detalles en el registro de peligros.

9.4.2. En la estimación de la probabilidad de que ocurra un suceso peligroso se emplea un enfoque similar al adoptado en los pasos 2 y 3; es decir, mediante discusiones estructuradas empleando una clasificación normalizada como guía. En Tabla 2 se presenta un ejemplo de tabla de probabilidad.

9.4.3. La Tabla 2 especifica la probabilidad como categorías cualitativas, pero también incluye valores numéricos para las probabilidades relacionadas con cada categoría. En algunos casos, puede haber datos disponibles que permitirán hacer estimaciones numéricas directas de la probabilidad de fallas. Por ejemplo, a menudo hay muchos datos disponibles sobre índices de fallas de componentes para varios años con respecto a los elementos de soporte físico de un sistema.

9.4.4. La estimación de la probabilidad de que ocurran sucesos peligrosos relacionados con errores humanos generalmente supondrá un grado de evaluación subjetiva y debería tenerse presente que aun cuando se evalúe el soporte físico, existe siempre la posibilidad de fallas debidas a errores humanos como, por ejemplo, procedimientos de mantenimiento incorrectos. Sin embargo, al igual que en el caso de la estimación de la severidad, las discusiones en grupo estructuradas, con participantes que tienen amplia experiencia en sus respectivas especialidades, y la adopción de una clasificación de riesgos normalizada deberían asegurar que el resultado será un juicio con conocimiento de causa.

9.4.5. Una vez que se ha completado la evaluación de probabilidad para todos los peligros identificados, los resultados deberían consignarse en el registro de peligros, incluyendo la justificación de la clasificación escogida.

Tabla 2: Ejemplo de tabla de probabilidad

Probabilidad (P)	¿Cuál es la probabilidad de que esa sucesión de eventos pase, incluyendo la consecuencia?		
Probabilidad	Definición Cualitativa	Definición Cuantitativa	Cuantitativa anual/diaria equivalente (aproximado)
5 Frecuente	Ha ocurrido frecuentemente. (Ocurre una vez por intervalo de exposición y es muy probable que vuelva a ocurrir dentro de ese intervalo)	$1 – 10^{-3}$ por hora	Desde una vez por hora hasta una en 40 días
4 Razonablemente probable	Ha ocurrido infrecuentemente. (Ocurre menos de una vez por intervalo de exposición y es probable que vuelva a ocurrir dentro de ese intervalo)	$10^{-3} – 10^{-5}$ por hora	Desde una vez cada 40 días hasta una cada 10 años
3 Remoto	Improbable que ocurra durante el total de la vida operacional del sistema	$10^{-5} – 10^{-7}$ por hora	Desde una vez cada 10 años hasta una vez cada 1,000 años
2 Extremadamente Remoto	Evento estudiado. (Se ha planteado y puede ser posible, pero no se conoce que haya ocurrido)	$10^{-7} – 10^{-9}$ por hora	Desde una vez cada 1,000 años hasta una en 100,000 años
1 Extremadamente Improbable	Prácticamente nunca ocurre	Menor a 10^{-9} por hora	Nunca

9.5. PASO 5: EVALUACIÓN DEL RIESGO

9.5.1. Las actividades claves del paso 5 son:
a) Decidir si el riesgo es aceptable o no; y
b) Registrar los detalles en el registro de peligros

9.5.2. Puesto que la aceptabilidad de un riesgo depende tanto de su probabilidad, severidad de sus consecuencias y exposición, se deben establecer los criterios para juzgar la aceptabilidad del riesgo. La aceptabilidad generalmente se basa en la comparación con una matriz de severidad /probabilidad, a veces llamada matriz de tolerabilidad. Por lo tanto, es necesario generar una matriz de tolerabilidad con el fin de definir y evaluar el nivel de riesgo.

9.5.3. Un ejemplo de matriz de tolerabilidad al riesgo se muestra en la Tabla 3[2]

9.5.4. Los proveedores de servicios de tránsito aéreo y operadores de aeródromo pueden diseñar su propia Matriz de tolerabilidad de riesgo, sin embargo, se debe de proporcionar a la DGAC la justificación de las cifras utilizadas en la matriz.

Tabla 3. Ejemplo de Matriz de tolerabilidad de riesgo

			SEVERIDAD (S)				
			A Catastrófico	B Mayor	C Moderado	D Menor	E Despreciable
PROBABILIDAD (P)	**5** **Frecuente**	$1 - 10^{-3}$ por hora	I_R=5A Inaceptable	I_R=5B Inaceptable	I_R=5C Inaceptable	I_R=5D Revisar	I_R=5E Revisar
	4 **Razonablemente probable**	$10^{-3} – 10^{-5}$ por hora	I_R=4A Inaceptable	I_R=4B Inaceptable	I_R=4C Revisar	I_R=4D Revisar	I_R=4E Revisar
	3 **Remoto**	$10^{-5} – 10^{-7}$ por hora	I_R=3A Inaceptable	I_R=3B Revisar	I_R=3C Revisar	I_R=3D Revisar	I_R=3E Aceptable
	2 **Extremadamente Remoto**	$10^{-7} – 10^{-9}$ por hora	I_R=2A Revisar	I_R=2B Revisar	I_R=2C Revisar	I_R=2D Aceptable	I_R=2E Aceptable
	1 **Extremadamente Improbable**	$< 10^{-9}$ por hora	I_R=1A Aceptable	I_R=1B Aceptable	I_R=1C Aceptable	I_R=1D Aceptable	I_R=1E Aceptable

$$I_R = P \times S$$

Nota. El I_R resultante es la multiplicación del valor asignado de probabilidad por el valor asignado de la severidad

9.5.5. Cada consecuencia, deberá cotejarse con la tabla de tolerabilidad poniendo la consecuencia en el casillero correcto que se alinea con la probabilidad y severidad. La consecuencia caerá en una de las tres regiones:

a) **Aceptable (1A, 1B, 1C, 1D, 1E, 2D, 2E)**: La consecuencia es tan poco probable o no lo suficientemente severa como para causar preocupación. El riesgo es tolerable, y se cumple con el objetivo de seguridad. Sin embargo, se debe considerar la posibilidad de reducir aún más el riesgo al nivel más bajo como sea razonablemente posible (ALARP - véase más

[2] El TLS (Target Level Safety) para la región CAR-SAM es de 2.5 x 10^{-9} accidentes por hora de vuelo. La Tabla 3 se ajusta con este parámetro

adelante) con el fin de minimizar aún más el riesgo de un accidente o incidente.

b) **Revisar (2A, 2B, 2C, 3B, 3C, 3D, 4C, 4D, 4E, 5D, 5E)**: La consecuencia y / o la probabilidad es de preocupación, se debe buscar medidas para mitigar el riesgo ALARP. Cuando el riesgo sigue estando en la región "revisión" después que se ha llevado a cabo la reducción del índice de riesgo ALARP, entonces el riesgo puede ser aceptado a condición de que el riesgo se entienda y se cuente con el aval de la persona responsable en última instancia por la seguridad dentro de la organización.

c) **Inaceptable (5A, 5B, 5C, 4A, 4B, 3A):** La probabilidad y / o severidad de la consecuencia es intolerable. Puede ser necesarias mitigaciones mayores o rediseño del sistema para reducir la probabilidad o la severidad de las consecuencias asociadas con el riesgo.

9.5.6. Varios peligros diferentes, pueden dar lugar a la misma consecuencia (de accidentes / incidentes). Cuando este sea el caso, no es suficiente evaluar la tolerabilidad de cada situación de peligro de forma independiente ya que esto puede ser engañoso. Por ejemplo, puede haber cincuenta peligros que llevan a la misma consecuencia no deseada, donde cada situación de peligro tiene una probabilidad muy baja de ocurrir, por ejemplo "extremadamente remota" en la Tabla 3.

9.5.7. La suma de las probabilidades no son tan sencillas cuando se han utilizado las estimaciones de probabilidad cualitativas porque no hay números para sumar. Cuando este sea el caso, se pueden hacer los siguientes sencillos supuestos:

a) Se requieren más de 50 consecuencias de peligros "extremadamente improbable" para mover la probabilidad de consecuencia general hacia la categoría "extremadamente remota".

b) Se requieren más de 50 consecuencias de peligro “muy remotas” para mover la probabilidad de consecuencia general hacia la categoría de “remoto”.

c) Se requieren más de 50 las consecuencias de peligros “remotas” para mover la probabilidad de consecuencia general hacia la categoría de "Razonablemente probable".

d) Se requieren más de 50 consecuencias de peligros “razonablemente probables” para mover la probabilidad de consecuencia general hacia la categoría “frecuente”.

9.5.8. Al considerar la tolerabilidad de cada peligro individual y su consecuencia, se puede encontrar que cada una cae en la región "aceptable" de la matriz de tolerabilidad. Sin embargo, cuando todos los cincuenta peligros se consideran en conjunto, habrá un aumento en la probabilidad de que ocurra y como consecuencia, se puede mover la consecuencia de la región "aceptable" a la región "revisión" o "inaceptable" de la Tabla. Por consiguiente, es importante identificar los peligros que contribuyen a la misma consecuencia y evaluar junta todas las probabilidades para conseguir una probabilidad total de que la consecuencia ocurra. Es esta probabilidad global que se utiliza para evaluar la consecuencia para identificar en donde la consecuencia se establece en la Tabla 3 anterior.

9.5.9. Cuando varios peligros contribuyen a la misma consecuencia y es necesaria la reducción del riesgo debido a que la consecuencia se establece en la matriz de la tolerabilidad, se puede utilizar la matriz para priorizar los peligros más importantes para intentar mitigarlos primero. Esto se consigue mediante la colocación de todas las probabilidades individuales de las consecuencias

de peligro en la matriz para ver que se encuentran dentro o cerca de las regiones intolerables. Estos peligros son el mayor riesgo y deben ser mitigados primero cuando sea práctico. Esto puede permitir el riesgo general se establezca en una categoría aceptable con mayor rapidez a través de hacer frente a los peligros más importantes primero en lugar de tratar con un número de peligros menos significativos de menor impacto.

9.5.10. ALARP significa que un riesgo es lo suficientemente bajo como para no intentar que sea más bajo, o que el costo de la evaluación de la mejora obtenida en un intento de reducción de riesgos, en realidad sería más costoso que cualquier costo probable que provenga del propio riesgo. Esto no significa automáticamente que el riesgo es aceptable tal como está; se deberá efectuar una evaluación del riesgo y justificarla.

9.5.11. Una vez que la evaluación de la aceptabilidad del riesgo se ha terminado para todas las consecuencias de los peligros identificados, los resultados deben ser registrados en el registro de peligros. Es particularmente importante que todos los casos en que el riesgo se estableció en la región "revisión" de la tabla, pero que ha sido aceptado como ALARP y tolerable, estén bien documentados y que se indica claramente la justificación de la decisión.

9.6. PASO 6: MITIGACIÓN DEL RIESGO

9.6.1. Las actividades claves del Paso 6 son:
a) mitigar aquellos riesgos identificados como inaceptables;
b) aplicar los principios generales ALARP; y
c) generar **Requisitos de Seguridad Operacional**

9.6.2. Como se señaló en el paso 5, si el riesgo no satisface los criterios de aceptabilidad predeterminados, siempre se debería intentar reducirlo a un nivel aceptable o, si esto no es posible, al nivel más bajo practicable ALARP empleando los procedimientos de mitigación apropiados.

9.6.3. Se recomienda aplicar el principio ALARP a todos los riesgos identificados, aun cuando los riesgos caigan en la región "aceptable" de la matriz de tolerabilidad. Esto es con el fin de apoyar el objetivo de mejora continúa de la seguridad operacional siempre que sea posible

9.6.4. La identificación de medidas apropiadas de mitigación de riesgos exige una buena comprensión del peligro y de los factores que contribuyen a que ocurra un evento de este tipo, puesto que todo mecanismo que sea eficaz para reducir el riesgo tendrá que modificar uno o más de estos factores.

9.6.5. Las medidas de mitigación de riesgos pueden producir efecto reduciendo la probabilidad de que el suceso ocurra o la severidad de las consecuencias, o ambas cosas. Lograr reducir el riesgo al nivel deseado se puede exigir la aplicación de más de una medida de mitigación.

9.6.6. Entre las medidas posibles para mitigar los riesgos cabe mencionar:
a) revisión del diseño del sistema;
b) modificación de los procedimientos operacionales;
c) cambios en la dotación de la organización;
d) capacitación del personal para hacer frente al peligro;
e) desarrollo de planes de contingencia/emergencias; y
f)por último, parar la operación.

9.6.7. Cuanto más pronto se identifiquen los peligros en el ciclo de vida del sistema, tanto más fácil será cambiar el diseño del sistema, si es necesario. A medida que el sistema se acerca a su implantación, cambiar el diseño se hace más difícil y costoso. Esto podría reducir las opciones de mitigación

posibles para aquellos peligros que no se identifican hasta las últimas etapas del proyecto.

9.6.8. La eficacia de toda medida de mitigación de riesgos que se proponga debe evaluarse, primero examinando muy de cerca si la aplicación de las medidas de mitigación puede introducir nuevos peligros, y después repitiendo los pasos 3, 4 y 5 para evaluar la aceptabilidad del riesgo con la aplicación de las medidas de mitigación propuestas. Si la medida de mitigación propuesta puede afectar otras partes del sistema, o tal vez, incluso la idoneidad del sistema para lograr con su función - puede ser necesario repetir los pasos 2 o incluso el paso 1. Lamentablemente, no es posible dar una orientación más específica sobre cuándo podría ser necesario volver a evaluar el sistema en su conjunto, porque este juicio sólo se puede hacer por los que entienden completamente el sistema.

9.6.9. Las medidas de mitigación que son necesarias para que el sistema cumpla con los criterios de seguridad se les conoce como **Requisitos de seguridad operacional** y deben estar claramente documentados. La puesta en servicio del sistema operativo no puede continuar hasta que todos estos Requisitos de seguridad operacional se cumplan. En el Paso 7 de este proceso, aborda los argumentos y las evidencia necesarias para demostrar que cada Requisito de seguridad operacional se ha cumplido.

9.7. PASO 7: ELABORACION DE LOS DOCUMENTOS DE EVALUACIÓN DE LA SEGURIDAD OPERACIONAL

9.7.1. Las principales actividades en el Paso 7 son:

a) la identificación de todos los objetivos de seguridad aplicables y los requisitos de seguridad operacional; y
b) la documentación de los resultados de una manera lógica y completa.

9.7.2. El propósito de los documentos de evaluación de la seguridad operacional es tener un registro permanente de los resultados finales de la evaluación de la seguridad operacional y los argumentos y pruebas que demuestran que los riesgos relacionados con la implantación del sistema o el cambio propuesto se han eliminado o han sido controlados adecuadamente y reducidos a un nivel tolerable.

NOTA: *Esta presentación de los argumentos y pruebas para demostrar la seguridad operacional se menciona en muchos textos sobre gestión de la seguridad operacional como un caso de seguridad operacional. También se emplea a veces la expresión argumentación de seguridad operacional con un significado similar.*

Si bien los documentos de la evaluación de la seguridad operacional se mencionan aquí en el último paso, durante los pasos anteriores ya se habrá producido una cantidad considerable de documentos.

9.7.3. Además de describir los resultados de la evaluación de la seguridad operacional, la documentación debería contener un resumen de los métodos empleados, los peligros identificados y las medidas de mitigación que son necesarias para satisfacer los criterios de evaluación de la seguridad operacional. El registro de peligros debería incluirse siempre. La documentación debería prepararse con detalles suficientes de modo que quien quiera que la lea pueda ver no sólo qué decisiones se tomaron, sino también cuál fue la justificación para clasificar los riesgos como aceptables o tolerables. También debería incluir los nombres de los miembros del personal que participaron en el proceso de evaluación. La persona

responsable de que se realice la evaluación de seguridad operacional y que firma la aceptación final de dicha evaluación será diferente según sean la magnitud y complejidad del proyecto y la política de la organización. En algunos casos será el director del proyecto. Cuando no se haya nombrado un director del proyecto, podrá ser el supervisor responsable del sistema de que se trata. En algunas organizaciones, la aceptación puede requerir la aprobación de un nivel superior de administración en los casos en que el riesgo residual no se puede reducir a un nivel aceptable, pero se debe aceptar como tolerable y ALARP. También es necesario de acuerdo con la normativa nacional, la consulta a los usuarios sobre la materia de la evaluación de seguridad operacional, por lo que esta consulta debe hacerse por escrito, para obtener una opinión sobre la evaluación de seguridad operacional.

La firma de los documentos de evaluación de la seguridad operacional por el jefe responsable, para indicar la aceptación, es el acto final del proceso de evaluación.

9.7.4. Estructura de Evaluación de seguridad operacional

9.7.4.1. La tabla 4 muestra la estructura de la Evaluación de seguridad operacional. Tenga en cuenta que también, dependiendo de la etapa del ciclo de vida que el proyecto tiene, no todas las secciones de la tabla pueden ser aplicables, salvo la consulta a los usuarios que es obligatoria.

Tabla 4. Estructura de una Evaluación de Seguridad Operacional

Parte o sección	Descripción
Pagina de titulo	Incluye: el nombre de la organización a la que el Caso de seguridad operacional es relevante, el sistema que se evalúa, estadio del proyecto; problema que se evalúa; fecha de emisión, autor (es).
Pagina de Control de la documentación	Una tabla que muestra el historial de las versiones del documento, incluida una breve descripción de lo que ha cambiado entre las versiones
Resumen Ejecutivo	Una breve descripción del caso de seguridad que incluye: una breve introducción al sistema, de donde han venido los requisitos de seguridad, si se han cumplido, las principales actividades pendientes, los riesgos residuales y las conclusiones extraídas.
Abreviaturas y Acrónimos	Incluya una lista que explica las siglas y abreviaturas utilizadas en el caso de la seguridad operacional.
Índice de paginas	Contienen capítulos o secciones, tablas, diagramas, figuras, apéndices y numeración de las páginas.
Alcance	Incluye: El papel global del sistema, porque es necesario, como se relaciona con otros sistemas y los límites de lo que cubre el caso de seguridad operacional.
Descripción funcional	Incluya una descripción de las funciones del sistema, incluir las necesidades de funcionamiento, el uso de diagramas y figuras, muestran como este sistema encaja con otros sistemas, incluyendo las interfaces.
Descripción del Sistema	Describe los componentes del sistema, interfaces entre ellas, diagramas de uso y figuras; describir las diferentes configuraciones permisibles del sistema. Registre aquí el

Parte o sección	Descripción
	número de versión, desarrolle el problema del sistema o procedimiento para que el caso de seguridad sea aplicable.
Operación del sistema	Describa cómo el sistema opera o funciona; incluir el concepto de operación; describir el flujo de información o datos, entradas y salidas (por ejemplo, aspectos de la interfaz hombre-máquina [HMI]), que procesos se llevan a cabo o qué decisiones se toman.
Diseño de Sistemas	Describir cómo el sistema fue diseñado, quien lo diseñó, las normas de diseño utilizadas. *Nota: En esta sección se puede ampliar para que actúe como soporte (respaldo) de las pruebas Cuando los requisitos de seguridad exigen pruebas de prácticas de un buen diseño.*
Dependencias del diseño	Incluya todos los sistemas o insumos de los que este sistema depende para una operación segura. Sea breve cuando éstas ya han sido descritas en las secciones anteriores del documento.
Supuestos	Incluya todos los supuestos acerca de las interfaces u otros sistemas con los que interactúa este sistema y cualquier otra hipótesis; incluir la justificación de los supuestos que sea posible. *Nota: Estas hipótesis es probable que han sido hechas durante la identificación de peligros y los procesos de evaluación de riesgos*.
Objetivos de seguridad	Cuando se han establecido los objetivos de seguridad para los peligros individuales, estos deberán alcanzarse. Cuando se ha utilizado la probabilidad tolerable para un conjunto de peligros que comparten la misma severidad de consecuencia (como en el caso de utilizar una matriz de riesgo para establecer objetivos de seguridad), entonces se debe de indicar la probabilidad tolerable para cada nivel de severidad, junto con una lista de peligros asociado con cada nivel de gravedad.
Derivación de requisitos de Seguridad	Indique cómo se produjeron los requisitos de seguridad, en referencia a los peligros relacionados, por ejemplo, la documentación los informes de lluvia de ideas, HAZOP o FMECA.
Requisitos de seguridad operacional	Indique los requisitos de seguridad derivados del sistema, es decir, los requisitos de seguridad obtenidos por este procedimiento. Cuando sea disponible/aplicable, incluir el nivel de confianza requerido para cada requisito de seguridad es decir, alta, media o baja (véase el Apéndice G).
Objetivos de seguridad y requisitos normativos	Referencia a textos normativos que contiene los objetivos de seguridad y requisitos aplicables a este sistema, sólo que replantear si compacto (Vea el apartado 7.5 - Requisitos de Seguridad más adelante).
Limitaciones y deficiencias	Identificar las deficiencias encontradas en el sistema. Identificar los objetivos de seguridad o requisitos que sólo se

Parte o sección	Descripción
	han demostrado, lo que no se ha podido probar o no se tiene evidencias suficientes para proporcionar el nivel requerido de confianza (con excepción de los requisitos previstos que necesitan posterior). Identificar cualquier evidencia contraria al sistema es decir, cualquier evidencia que demuestra que el requisito no se cumple. Reitere todas las hipótesis para que el sistema no se valide, o que no existe suficiente evidencia o justificación.
Monitoreo Continuo	Identificar los objetivos de seguridad y los requerimientos que requieren de monitoreo permanente con el fin de acumular pruebas de que las exigencias siguen siendo satisfechas.
Consulta a los usuarios	En el Párrafo 2.28.3 Evaluación de seguridad operacional establece que se requiere que exista una consulta previa a los usuarios cuando se efectué cualquier cambio significativo a la seguridad operacional, incluyendo cambios en las mínimas reducida de separación o de un nuevo procedimiento. Esta consulta debe estar documentada.
Conclusión	Sacar una conclusión de la Evaluación de seguridad Operacional. Indique si su organización cree que el sistema es seguro para su puesta en servicio o si es necesario un trabajo adicional, o bien indicar si cree que el trabajo previsto dará lugar a que el sistema sea seguro. Indicar la existencia de limitaciones y carencias con las que su organización está dispuesta a vivir y con cualquiera otra que son inaceptables, incluyendo las acciones para corregir la situación.
Referencias	Cuando sea aplicable, se incluyen las siguientes referencias: a) normas; b) identificación del peligro y la documentación de evaluación de riesgos; c) las fuentes de evidencia.
Apéndices	Se deben utilizar los apéndices para almacenar texto, diagramas, tablas, etc. que si figura en el cuerpo principal del Caso de seguridad operacional, puede distraer de la corriente principal del documento. Por lo general, los anexos deberán contener: a) Extractos de manuales por ejemplo, donde forman parte de la descripción del sistema; b) resumen de evidencias (se debe hacer referencia a los documentos de mayor tamaño en lugar de reproducir los mismos); c) Matriz de cumplimiento normativo;

9.7.5. Requisitos de seguridad Operacional (incluidos los objetivos de seguridad operacional)

9.7.5.1. El propósito de la Evaluación de Seguridad Operacional es demostrar que se han abordado todos los requisitos de seguridad del sistema en cuestión y que el sistema es bastante seguro. Por tanto, es necesario

establecer claramente desde el principio los requisitos de seguridad operacional que se abordan en el caso de seguridad Operacional.

9.7.5.2. Los requisitos de seguridad operacional a ser declarados proceden de varias fuentes:

a) Los generados por el proceso de evaluación de riesgos (pasos del 1 al 6 de este procedimiento). Éstos se llaman “requisitos derivados de seguridad operacional”;

b) Los aplicables a partir del material reglamentario y/o estándares, llamados “Objetivos de seguridad y requisitos normativos”, por ejemplo:

- Anexos de la OACI por ejemplo, Anexo 10 Requisitos técnicos para las comunicaciones, la navegación y vigilancias (incluyendo radar y ADS-B);
- RAP 65 Licencias de Personal Aeronáutico excepto Miembros de la Tripulación, Capitulo B Licencias de Controlador de Tránsito Aéreo, Requisitos de conocimientos para obtener licencia.
- RAP 139 Certificación de aeródromos; Apéndice C. Requisitos relativos a la autorización de funcionamiento de aeródromos.
- RAP 311 Servicio de Tránsito Aéreo, Capítulo 7 Requisitos de los ATS respecto a información.

9.7.5.3. La Identificación de los Requisitos de Seguridad operacional dentro de los muchos e interoperables requisitos contenidos en las normas internacionales, como los identificados en 9.7.5.2 b) anterior, no siempre es sencillo. Una de las maneras más simples de identificar si algún requisito especial es un requisito de seguridad operacional es plantear la pregunta, "si este requisito no se cumple o se cumple parcialmente, va a aumentar el riesgo para la seguridad del sistema en cuestión? Si hace aumentar la probabilidad de un incidente, o la severidad de un incidente a un nivel intolerable, entonces debe considerarse los requisitos de seguridad operacional que deben ser abordados en la evaluación de seguridad Operacional.

9.7.5.4. Los requisitos que se encuentran en las normas internacionales que no son requisitos explícitos de seguridad a menudo se refiere a la interoperabilidad y aún tendrá que ser satisfechas cuando la norma ha sido aprobada por la DGAC. Por lo tanto debe considerarse la posibilidad de demostrar el cumplimiento con todos los requisitos dentro de los estándares y la documentación de los resultados en la evaluación de seguridad operacional.

APÉNDICE A

REGISTRO DE PELIGROS

1.0 Introducción

1.1. El Registros de los peligros es una forma estructurada para registrar los peligros potenciales identificados en relación con una proyecto o sistema y para registrar las acciones que se planean o han llevado a cabo para enfrentar a los peligros registrados.

1.2. 1.2 El registro de peligros se debe utilizar desde el comienzo de un proyecto y se mantendrá actualizado como un documento vivo en todo el ciclo de vida del proyecto.

1.3. En el inicio del registro de peligros, la información registrada para cada peligro puede ser limitada. Se pueden agregar más detalles de acuerdo a como se desarrolla el proyecto y se llevan a cabo otros procesos de evaluación y mitigación de riesgos.

1.4. En los hitos de un proyecto, por ejemplo, justo antes de poner en servicio un nuevo sistema en operación, se puede revisar el registro de peligros para ver el estado de los peligros asociados, es decir, para asegurar que se han abordado (mitigado) o aceptado todos los peligros y llegar a ser un riesgo tolerable.

1.5. El registro de peligros puede ser utilizado para registrar el resultado de la identificación de peligros por ejemplo, los procesos de lluvia de ideas, FMECA, HAZOP, etc.

2.0 Desarrollo de un Registro de Peligros

1.1. El registro de peligros normalmente se presenta como una serie de formatos, donde cada uno, debidamente llenado, representa un peligro o una de varias consecuencias de un peligro. La figura 1 muestra una composición típica de un registro de peligros. El llenado de los casilleros del formato se explica a continuación:

a) **Organización o área:** Consignar la organización o el área de la organización al que el peligro identificado es aplicable.

b) **ID del registro de peligro:** Usar este casillero con un único número que registre el peligro.

c) **ID del peligro:** Copiar en este casillero cualquier número de identificación de peligro asignado durante el proceso de identificación de peligros.

d) **Identificado por**: Nombrar la persona o grupo que identificó el peligro.

e) **Fecha de creación**: Ingresar la fecha en que por primera vez este formato de registro de peligros fue usado.

f) **Acción de la última actualización**: Consignar los últimos casilleros de este formato que fueron actualizados.

g) **Fecha de la última actualización**: Ingresar la fecha de la última vez que este formato fue actualizado.

h) **Descripción del peligro**: Describir el peligro. Esto puede tomar la forma de cómo el peligro fue registrado durante el proceso de identificación de peligros.

i) **Categoría del peligro**: Usar este casillero para ingresar las categorías en la clasificación de los peligros, ejemplo: técnico, operacional, entrenamiento, procedimiento, etc.

j) **Consecuencia del peligro**: Ingresar la consecuencia que el peligro podría producir.

k) ***NOTA****: un solo peligro puede generar más de una consecuencia. Usar varias hojas cuando otras consecuencias importantes se requieren registrar.*

l) **Barreras existentes**: Incluir todas las defensas (Reglamentarias, Tecnológicas o Instrucción) existentes para el peligro estudiado.

m) **Probabilidad de peligro**: Ingresar la probabilidad de la consecuencia del peligro. Ingresar la descripción cualitativa o cuantitativa de la probabilidad.

n) **Severidad**: Ingresar la severidad.

o) **Índice de riesgo**: ingresar el nivel de riesgo o índice de riesgo de la tabla de tolerabilidad.

p) **Probabilidad de peligro acumulado**: Donde se haya identificado que más de un peligro genera la misma consecuencia, ingresar la suma de las probabilidades de los peligros identificados y que contribuyen a la misma consecuencia con el propósito de identificar la probabilidad general (total) de que ocurra la consecuencia.

q) **Mitigación/acción propuesta**: Ingresar la acción o mitigación que se ha ideado para hacer frente a este peligro.

r) **Probabilidad de peligro resultante**: Ingresar la nueva probabilidad calculada de la consecuencia del peligro luego de aplicar las medidas mitigadoras. Ingresar la descripción cualitativa o cuantitativa de la probabilidad

s) **Severidad resultante**: Ingresar la nueva severidad calculada luego de aplicar las medidas mitigadoras.

t) **Índice de riesgo resultante**: ingresar el nivel de riesgo o índice de riesgo de la tabla de tolerabilidad.

u) **Propuesto por**: Nombre de la persona o equipo que propuso la acción o mitigación.

v) **Responsable**: Nombre de la persona, equipo u organización que llevará a cabo la acción o mitigación.

w) **Fecha prevista**: Ingresar la fecha en que la propuesta de acción o mitigación será implantada.

x) **Mitigación/acción tomada**: Consignar las medidas realmente realizadas (estas pueden ser como se propusieron anteriormente).

y) **Fecha de la acción**: Ingresar la fecha en que las medidas fueron tomadas.

z) **Situación de la acción**: Consignar si la acción está en curso, parcialmente completada o completa.

aa) **Situación de este registro de peligro**: Anotar si este registro de peligro está esperando alguna entrada más, está a la espera de cierre, etc.

bb) **Fecha de cierre**: Ingresar la fecha cuando se haya acordado que ninguna otra acción se adoptará con respecto a este registro de peligro.

cc) **¿Continuación de la hoja?**: Ingresar “Si” cuando haya más información relevante a este registro de peligro contenido en una hoja adicional de papel.

Figura 1. Formato de registro de peligros.

Organización o área:		**ID del registro de peligro:**
ID del peligro:	**Identificado por**:	**Fecha de creación**:
Acción de la última actualización:		**Fecha de la última actualización**:
Descripción del peligro:		
Categoría del peligro:		
Consecuencia del peligro:		
Barreras existentes:		
Probabilidad de peligro:	**Severidad del peligro**:	**Índice de Riesgo:**
Probabilidad de peligro acumulado(Cualitativo o Cuantitativo):		
Mitigación/acción propuesta:		
Probabilidad de peligro resultante:	**Severidad del peligro resultante**:	**Índice de Riesgo resultante:**
Propuesto por:	**Responsable**:	**Fecha prevista**:
Mitigación/acción tomada:		
Fecha de la acción:	**Situación de la acción**:	
Situación de este registro de peligro:		**Fecha de cierre**:
¿Continuación de la hoja?:(S/N)		

Intencionalmente dejada en blanco

APENDICE B

IDENTIFICACION DE PELIGROS UTILIZANDO "LLUVIA DE IDEAS"

1.0 INTRODUCCIÓN

1.1. Esta guía de lluvia de ideas (brainstorm) se ha derivado de la orientación de la metodología de evaluación de seguridad operacional de Eurocontrol sobre identificación de peligros.

1.2. La identificación de peligros mediante lluvia de ideas es complementario a los métodos sistemáticos de identificación de peligros, por ejemplo HAZOP, FMECA, etc. El método de lluvia de ideas puede revelar peligros no señalados en el enfoque sistemático.

1.3. Lo ideal sería que la identificación del peligro con lluvia de ideas se lleve a cabo antes que el enfoque sistemático. Esto se debe a que los participantes de ambos métodos serían más abiertos y menos centrados en temas de diseño durante la lluvia de ideas, si no han sido informados de los detalles del proyecto como lo exige el enfoque sistemático.

1.4. La Tabla A proporciona una visión general de todo el proceso de lluvia de ideas, desde la planificación inicial y preparación hasta la evaluación de los resultados. El resto de este Apéndice describe cada punto planteado en la tabla.

2.0 PLANIFICACIÓN INICIAL

2.1. La identificación de peligros mediante tormenta de ideas puede llevarse a cabo en diferentes fases del ciclo de vida del proyecto. A principios de un proyecto, se puede llevar a cabo la lluvia de ideas una vez que el concepto de la operación o la descripción del sistema propuesto han sido redactados. Esto es necesario para que el grupo de lluvia de ideas pueda tener una visión general del proyecto y material para el trabajo. De acuerdo a como se desarrolla el proyecto y se disponga de más detalles, este ejercicio se puede repetir.

2.2. Puede ser necesario convocar a algunos expertos cuya participación en las sesiones de lluvia de ideas es valiosa, con la debida anticipación para no entrar en conflicto con sus otras responsabilidades. Pudiendo incluir:

a) Controladores de tránsito aéreo;
b) Pilotos;
c) personal del servicio de salvamento y extinción de incendios;
d) Personal de operaciones de aeródromo;
e) Personal de seguridad de aviación.
f) Personal de recarga de combustible, etc.

Tabla A Proceso completo de lluvia de ideas

Plan	• Alinear las actividades de evaluación de riesgos (incluida la identificación de peligros) con los planes de trabajo. • Involucrar al Operador del aeródromo, proveedor de servicios de tránsito aéreo y aerolíneas para la participación de controladores, pilotos, etc. en las primeras etapas del proyecto debido a su limitada disponibilidad.
Preparación	• Organizar a los participantes, los cuales pueden ser: o Especialistas operacionales tales como: pilotos, controladores de tránsito aéreo, etc. (sería ideal que NO hayan participado antes en una identificación sistemática de peligros). o Moderador. o Secretario. o Expertos operacionales o en el sistema (Gerentes del ATC, ingenieros, Gerentes de aeródromo, etc.). o Analistas de seguridad operacional • Preparación de cómo realizar la lluvia de ideas. • Preparación en los peligros y categorías usando: o Alcance preliminar de lluvia de ideas; o Literatura, registro de peligros y bases de datos de incidentes y accidentes. • Preparar presentaciones de : o Que es un peligro, cómo hacer la lluvia de ideas y sus reglas; o Antecedentes generales del sistema y la operación. • Hacer un cronograma la sesión de lluvia de ideas. • Arreglo de los detalles de la reunión: o Sala de reunión libre de distracciones; o Papelógrafo y pizarra; o Computadora portátil y proyector multimedia; o Cofee break.
Lluvia de ideas	• Iniciar la sesión con la presentaciones preparadas • Lluvia de ideas: o Tener cuidado que se respeten las reglas básicas: ▪ Tantos peligros como sea posible; ▪ Sin críticas, sin retirar a nadie, sin análisis; o Tomar notas breves sobre los peligros en el papelógrafo; o Dirigir la reunión a través de los peligros y las categorías del peligro preparados; o Hacer breaks cortos para evitar que se reduzca significativamente la productividad. • Cerrar la sesión.
Evaluar	• Distribuir las actas de la reunión con los registros de peligros solicitando las correcciones que sean necesarias. • Evaluar la eficacia de la tormenta de ideas: o ¿Se cubrieron todas las categorías de los peligros? ; o ¿Hay alguna categoría de peligro que se sospecha que falta? • Decidir cuándo es necesario otra lluvia de ideas

3.0 LLUVIA DE IDEAS PRELIMINAR (ALCANCE)

3.1. El objetivo de la actividad preliminar de la lluvia de ideas es establecer un conjunto de categorías del peligro y problemas que posteriormente se pueden utilizar para guiar todas las actividades de la lluvia de ideas. Normalmente, el moderador del grupo de lluvia de ideas es el que puede llevar a cabo el anteproyecto de la lluvia de ideas o con la ayuda de otros, por ejemplo de un Analista de Seguridad Operacional. Esta actividad debe realizarse antes que se realice la lluvia de ideas completa.

3.2. La entrada para la lluvia de ideas preliminar puede ser los datos históricos de los peligros en sistemas similares por ejemplo bases de datos de incidentes / accidentes, información sobre los sistemas o registros de peligros.

3.3. El entregable de la lluvia de ideas preliminar debe ser una lista de categorías de peligros y otras problemas, tales como:

a) Aspectos operacionales;
b) Aspectos técnicos;
c) Posibles conflictos: despegues, calles de rodaje
d) Fases de vuelo

3.4. Dado que la actividad preliminar de la lluvia de ideas es un ejercicio de una o dos personas, y el propósito es que no se produzca algo en detalle, el desarrollo de este ejercicio se puede dejar a discreción de los involucrados. La guía que sigue a continuación de lluvia de ideas completo, no necesariamente es aplicable a la lluvia de ideas preliminar.

4.0 PREPARACIÓN PARA LA LLUVIA DE IDEAS COMPLETA

4.1. Participantes

4.1.1. El número de participantes a una sesión de lluvia de ideas debe limitarse a un máximo de 6 personas. Un número mayor hace que la reunión se vuelve improductiva y se deberían tomar medidas especiales para recuperar algo de la eficiencia:

a) Dividir todo el grupo en grupos de trabajo más pequeños;
b) Los participantes deben tomar notas individuales, seguido de una discusión de grupo de las notas de cada persona.

4.2. Participantes con roles administrativos

4.1.2. Todos los participantes deberán tomar parte en las actividades de generación de ideas en la tormenta de ideas, sin embargo algunos de los participantes también tienen una función administrativa:

a) **Moderador***:* Controla el flujo y el tiempo en la reunión, establece las normas de conducta y presenta el material y las categorías del peligro a considerar. El principal objetivo del moderador es garantizar que la actividad de lluvia de ideas es productiva;
b) **Analista de seguridad operacional:** Debe estar familiarizado con los peligros, sus causas y efectos, y ayudar al grupo con la terminología de seguridad operacional y la estructuración del registro de peligros;
c) **Secretario***:* Alguien deberá tomar nota del detalle de los peligros; esto podría estar en una computadora portátil conectado a un proyector para que los participantes puedan corregir cualquier malentendido (no obstante la corrección de notas debe tener una prioridad menor que la generación de ideas);
d) **Experto operacional/sistema***:* Este debe ser alguien familiarizado con el sistema o funcionamiento de la organización de manera que

puedan responder a cualquier pregunta aclarando a los participantes sobre cualquier duda sobre el sistema. Típicamente es el gerente del proyecto, jefes de tránsito aéreo o Ingenieros de sistemas. Ellos pueden presentar un breve descripción del proyecto al inicio de la sesión.

NOTA: *el moderador puede ser también el analista de seguridad operacional. El secretario puede ser el analista de seguridad operacional (cuando éste no es también el moderador) lo que permite que la definición de peligros de seguridad operacional sea utilizando la terminología correcta.*

4.3. Participantes creativos

4.3.1. Los participantes antes mencionados tienen una función administrativa en el proceso de lluvia de ideas. Sin embargo, la función principal de los demás participantes es la de identificar creativamente los peligros en el sistema o proyecto. La clave está en la designación del personal operativo:

a) **Controlador de Tránsito Aéreo**: en la medida de lo posible que no hayan participado anteriormente en una tormenta de ideas, pero que esté familiarizado con el tipo de funciones del ATC, tales como: control de aproximación, control de área, etc.

b) **Piloto***:* en la medida de lo posible que no hayan participado anteriormente en una tormenta de ideas, pero que esté familiarizado con los tipos de aeronaves y operaciones que se realizaran en el proyecto;

c) **P*ersonal de Aeródromo*:** en la medida de lo posible que no hayan participado anteriormente en una tormenta de ideas.

5.0 PREPARACIÓN PARA UNA SESIÓN DE LLUVIA DE IDEAS

5.1. Sesión logística

5.1.1. Las sesiones de lluvia de ideas pueden ser tediosas para los participantes, por lo tanto debe tenerse en cuenta lo siguiente al organizar la logística de una sesión:

a) El salón de reuniones debe estar protegido de distracciones, tales como llamadas telefónicas.

b) La preparación de un cronograma de las reuniones que divida el tiempo asignado en descansos flexibles con refrescos, por ejemplo: cada media hora dar diez minutos de descanso.

NOTA: *Los participantes normalmente son más proactivos en sesiones por la mañana que por la tarde*.

c) La fácil disponibilidad de refrescos.

5.2. Presentación de lluvia de ideas

5.2.1. Algunos participantes a una sesión de lluvia de ideas pueden no estar familiarizados con el proceso o lo que se espera de ellos. Por lo tanto, es importante explicar esto, la mejor manera sería en forma de una breve presentación que cubra:

a) La definición de peligro;

b) Cómo será administrada la lluvia de ideas, por ejemplo las reglas:

- No se permiten contradicciones o retiro del personal;

- Cómo los participantes deben informar al grupo de sus ideas del peligro, por ejemplo: abierta y libre para toda discusión; generando notas pegado un “post-its” en la pizarra; solicitar la atención del moderador esperando con las manos en alto.

NOTA: *Se les debe proporcionar a los participantes lapiceros y block de notas para escribir los peligros tal como se les ocurre en caso que el peligro tenga que ser discutido posteriormente o para su registro.*

5.2.2. El moderador normalmente explicaría las reglas en una presentación que no exceda de diez minutos.

5.3. Presentación del sistema o proyecto

5.3.1. Los participantes en una lluvia de ideas necesitan información para realizar el trabajo, por lo tanto se debe presentar una visión general del sistema:

a) La presentación no debe de ser de más de media hora.
b) No debe ser muy detallado pero debería cubrir:
   - o El objetivo del sistema;
   - o Concepto de la operación, por ejemplo: Configuración del espacio aéreo e interfaces, diseño del aeródromo, características del tránsito, horas de operación.
   - o Funciones (rol) de las personas (controladores, pilotos, personal de aeródromos, etc.);
   - o Políticas y procedimientos;
   - o Sistemas técnicos.
c) Pueden ser utilizados fotos o diagramas.

NOTA*: Las fotos y diagramas por ejemplo, el diseño del aeropuerto y la estructura de aerovías y cartas de procedimientos deben convertirse en carteles y debe estar pegados alrededor de la habitación donde la actividad de lluvia de ideas se llevará a cabo para promover su examen constante y una fácil referencia.*

5.3.2. Los expertos de la operación/sistema (Gerentes) son los que llevarían a cabo esta presentación.

6.0 CONDUCCIÓN DE LA REUNIÓN DE LLUVIA DE IDEAS

6.1. Después que se ha realizado la presentación introductoria de la lluvia de ideas y del sistema o proyecto (ver anterior), el moderador tomaría el control procediendo a dirigir al grupo para revisar las categorías del peligro y los problemas previamente identificados en la etapa preliminar de la lluvia de ideas.

6.2. Todos los participantes explorarían cada una de las categorías del peligro y problemas planteados teniendo la libertad de aumentar cualquier tema de seguridad operacional que se les ocurra. Debe tomarse nota rápidamente de los peligros planteados en un papelógrafo para ser discutido y ampliado aún más (aunque no se requiere de un análisis en detalle en esta etapa).

6.3. El analista de seguridad operacional ayudaría a formular los peligros identificados con la redacción apropiada y el secretario se aseguraría de que estos estén correctamente registrados.

6.4. Si se utiliza una computadora portátil y un proyector, el secretario puede asegurar que se ha registrado la correcta comprensión del peligro planteado por el participante.

6.5. Esto continuará, de acuerdo con el cronograma previsto, hasta que todas las categorías del peligro y los temas identificados se hayan agotado a partir de la lluvia de ideas preliminar. Sin embargo, si durante la actividad de lluvia de ideas, han sido identificados otros problemas y categorías del peligro además de los determinados durante los trabajos preliminares, estos deben ser explorados hasta que se agote el tema.

7.0 DESPUÉS DE LA SESIÓN DE LLUVIA DE IDEAS

7.1. Las actas o notas de la sesión de lluvia de ideas, que debe ser dividido en las categorías del peligro discutidos en la reunión, deben ser proporcionadas a los participantes dentro de unos días para que verifiquen los errores.

7.2. Los resultados del proceso de identificación del peligro deben ser revisados y evaluarse que tan exitoso ha sido el proceso. Si, por ejemplo, parece que una categoría del peligro en particular no ha alcanzado el número esperado de peligros, entonces debe considerarse la posibilidad de organizar más sesiones de lluvia de ideas (en el ciclo de vida del proyecto, podría haber muchas iteraciones planeadas de identificación de peligros, proveyendo la oportunidad de enfocarse en un problema en particular en un estado posterior).

7.3. Los peligros identificados en la sesión de lluvia de ideas deben ser ingresados en el registro de peligros, que es donde serán mantenidos (ver Apéndice A).

***NOTA**: El grupo de lluvia de ideas puede ser el mismo equipo que realizará la evaluación de riesgos, por lo que el grupo puede asignar la información de severidad y probabilidad inicial a las consecuencias del peligro inmediatamente después del proceso lluvia de ideas para ayudar a la posterior evaluación.*

Intencionalmente dejada en blanco

APENDICE C
Análisis de modos, efectos y criticidad de la falla (FMECA)

1.0 Introducción

1.1. El Análisis de modo, efectos y criticidad de la falla (FMECA) es un método popular usado para identificar peligros para una evaluación de riesgos. Se trata de un método de análisis sistemático para identificar los peligros a un nivel de descripción funcional que se pueden desarrollar aún más en detalle a medida que el sistema esté disponible.

1.2. Aunque el proceso FMECA en sí es simple, puede que parezca complicado y que consuma mucho tiempo la cantidad de datos a evaluar y registrar. Por lo que es esencial un enfoque metódico y disciplinado para la realización de trabajos FMECA para obtener un beneficio completo del análisis FMECA a entregar.

1.3. La orientación genérica en el FMECA y FMEA (Análisis de modo y efectos de la Falla) se puede encontrar en:

a) Norma Técnica Internacional IEC 60812 - Técnicas de Análisis de Confiabilidad del Sistema - Procedimiento para el Análisis de modo, efecto y criticidad de Falla.

b) MIL-STD 1629A - procedimiento de ejecución de los modos de fallo y análisis de efectos de la criticidad (aunque retirado de la publicación del proceso FMECA en esta norma es comúnmente utilizado).

1.4. Este documento proporciona una orientación más específica sobre la realización de análisis de FMECA para identificar y clasificar los riesgos cuando se consideran las operaciones en los servicios de tránsito aéreo y aeródromos.

2.0 El proceso de FMECA

2.1. La Figura 1 muestra un diagrama de flujo del proceso FMECA.

2.2. El proceso de FMECA puede llevarse a cabo en varios puntos del ciclo de vida de un proyecto, por lo general:

a) En el concepto inicial de las operaciones o diseño del proyecto o en la fase de ideas, donde se han definido las funciones del sistema, pero no necesariamente los equipos, las personas o los procedimientos. La ejecución de un FMECA en esta primera etapa se identificará las funciones más críticas o componentes de un sistema que puede influir en decisiones posteriores de diseño.

b) En el diseño inicial del sistema o la definición inicial del proyecto, en donde las funciones están asociadas con los tipos de equipos y se encuentra disponible más información sobre las personas y los procedimientos involucrados. La ejecución de un FMECA en esta etapa puede ayudar en la selección final de los equipos.

c) En la etapa final de equipos actuales, procedimientos y las personas que se utilizarán. La ejecución de un FMECA en esta etapa se identificará las fallas y sus consecuencias en los equipos/procedimientos específicos que pueden no haber sido evidente en las etapas anteriores con información menos

detalladas y confirmar o actualizar los resultados, estimaciones y suposiciones de las anteriores evaluaciones FMECA.

2.3. Realizar una FMECA en el primer punto práctico de un proyecto puede reducir la cantidad de trabajo que se requiere más adelante. Se pueden encontrar que algunas funciones de nivel superior no representan riesgos significativos si fallan, y por lo tanto puede no ser necesaria mayores análisis detallados tipo FMECA sobre sistemas de apoyo de menor a esta función. Cualquier decisión de limitar el análisis posterior sobre la base de ello deberá justificarse y registrarse.

2.4. Una persona o un grupo de personas podrá hacerse cargo del FMECA. Dependiendo del nivel en el que se desarrolla el FMECA realizar y su alcance, el individuo o el equipo debe:

a) Tener un buen conocimiento del concepto de operación o de las intenciones del proyecto.
b) Tener un buen conocimiento del entorno en el que funcionará el sistema.
c) Tener experiencia de procedimientos operativos, cuando éstos están siendo analizados.
d) Tener un buen conocimiento de las funciones de los equipos y modos de falla.

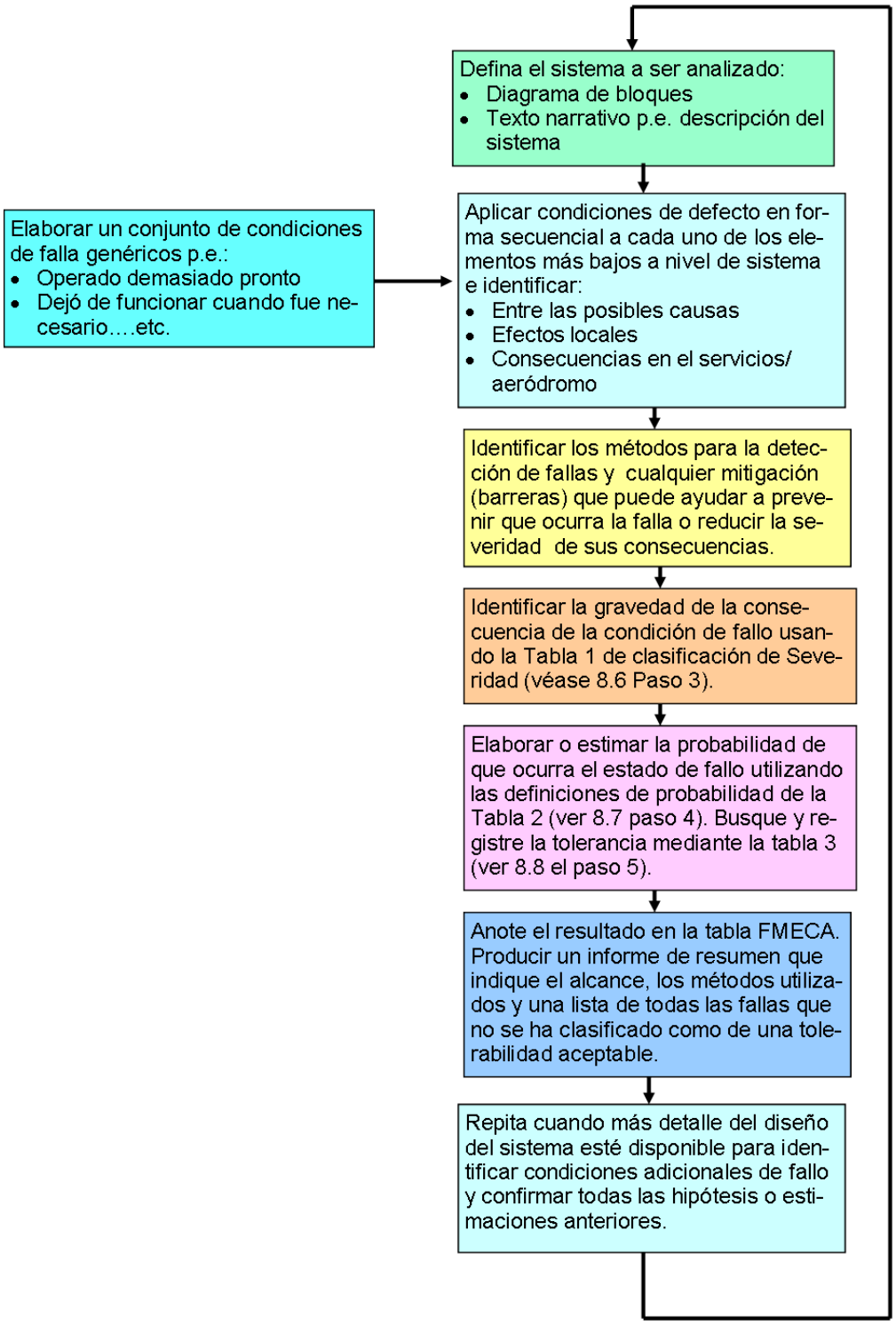
3.0 Definición del sistema a ser Analizado

3.1. El alcance de un análisis FMECA se puede ejecutar en cualquier nivel, desde sistemas integrados completos hasta equipos individuales. Por lo general se pueden aplicar las siguientes aplicaciones de FMECA:

a) Ejecución de un FMECA funcionales de nivel superior de operaciones de tránsito aéreo o de aeródromo. Esto ayudará a definir las interacciones de alto nivel y las funciones críticas y ayuda a definir las estructuras necesarias que requieren un análisis FMECA de menor nivel.
b) Ejecución de un FMECA nivel medio en un conjunto de sub-sistemas de apoyo por ejemplo, la función global un sistema de vigilancia combina sensores de radar, transmisión de datos y sistemas de representación visual o de una operación de reabastecimiento de vuelo en aeródromo, involucrando a personas, equipos y procedimientos, etc.
c) Ejecución de un FMECA detallada sobre un equipo o procedimiento. Este puede ser el caso en el que están siendo instalados nuevos equipos o sustituyendo un sistema existente, o cuando un procedimiento ha sido modificado o sustituido por uno nuevo.

3.2. En cualquier nivel que el análisis FMECA se está realizando, es esencial que sea claramente definido el sistema a ser analizado. Normalmente, esto implica el desarrollo de diagramas de bloques y el texto de apoyo narrativo.

Figura 1 : PROCESO FMECA



4.0 Diagramas de Bloques

4.1. El propósito de un diagrama de bloques es proporcionar una representación gráfica de los componentes del sistema, lo que hacen y cómo se relacionan el uno al otro. Dependiendo del nivel de la FMECA, los bloques y enlaces entre los bloques puede contener información diferente.

4.2. Los bloques pueden contener: Títulos de funciones, elementos del sistema (equipos, personas y procedimientos), sub-sistemas (por ejemplo, parte de un equipo o de un procedimiento) a nivel de componentes. Estos deben ser etiquetados dentro de los bloques. Se recomienda numerar los bloques para facilitar la referencia en los debates y en las referencias de texto de la descripción narrativa.

4.3. Los vínculos entre los bloques son generalmente direccionadas a las entradas y salidas, es decir (o más generalmente la influencia en el bloque y las influencias que el bloque tiene a otros bloques). Las líneas entre los bloques deberán estar etiquetados con la influencia que tiene.

NOTA: *Si se utiliza un proceso para analizar FMECA Procedimientos, a continuación, el diagrama de bloques puede tomar la forma de una serie de pasos que se muestran como una secuencia de operaciones*.

5.0 Textos Narrativos

5.1. El propósito del texto narrativo es proporcionar una descripción del sistema. Se relaciona típicamente con el diagrama de bloques, ampliando las funciones y las influencias en caso necesario. Se puede declarar aquí cualquier hipótesis sobre el sistema. En el diagrama de bloques se muestra el texto relacionado a los elementos del sistema y se puede relacionar a través de referencias en la numeración de los bloques.

6.0 Definición de los modos de fallo

6.1. En lugar de pensar aleatoriamente en las condiciones de fallo para cada elemento del sistema, se recomienda identificar un conjunto de condiciones de fallo que pueden ser aplicados secuencialmente a cada elemento del sistema. Los modos de fallos de alto nivel son comunes en muchos sistemas y por lo general incluyen:

a) Operar antes de tiempo o de forma inesperada.
b) Falla en detener la operación en el momento correcto.
c) Falla en operar cuando es necesario.
d) Opera, pero con errores.
e) Fallas durante la operación.

6.2. Dependiendo del nivel del análisis FMECA y los elementos del sistema que se están considerando, puede ser definido un conjunto de modos de fallo más específicos. Para equipos ATS éstos pueden incluir:

a) Falla en transmitir.
b) Atascado en transmitir.
c) Transmitir intermitente.
d) Pérdida de datos.
e) Perdida de datos parciales.
f) Corrupción de datos total.
g) Corrupción de datos parcial.

6.3. Para las funciones del aeródromo estos pueden incluir:

a) Derrame de combustible.
b) Daños en la superficie del Área de Maniobras.

6.4. Para procedimientos estos pueden incluir:
a) Falla en ejecutar un paso.
b) Salto de un paso.
c) Ejecutar proceso en orden incorrecto.
d) Ejecutar parcialmente un paso.

7.0 Realización del Análisis

7.1. Con el diagrama de bloques del sistema, el texto narrativo asociado y la lista de posibles modos de fallo, ahora es posible iniciar el análisis. Los resultados del análisis deben ser registrados y la Figura 2 da un ejemplo de construcción de una tabla adecuada para este propósito.

7.2. El proceso de análisis puede ser largo, con muchos modos de fallo que se analizan, otros que son muy poco probables que se produzca o que tengan consecuencias insignificantes. Sin embargo, es importante ejecutar sistemáticamente todo el proceso para registrar los fallos que se consideran. Se pueden requerir muchas hojas para registrar los resultados. La industria ha producido Software FMECA para PC para ayudar a registrar y presentar los resultados.

7.3. El proceso de análisis consiste en abordar cada elemento que se muestra en el diagrama de bloques, a su vez, la aplicación de los modos de fallo de las entradas y salidas o la misma función y el registro subsiguiente en la tabla:
a) El elemento del sistema que está siendo considerado, incluyendo su número de identidad (numeradas en el diagrama de bloques).
b) El modo de falla que se aplica.
c) Las posibles causas de falla, en los análisis de más alto nivel esto puede limitarse a las causas de fallas genéricas, en lugar de una lista larga de causas específicas. En los análisis de nivel inferior, se pueden enumerar las causas específicas.
d) El efecto del fallo local, esto puede limitarse al efecto en la salida para el elemento siguiente del sistema, que describe las características del efecto.
e) El efecto final del fallo, esto es el efecto global sobre el servicio de tránsito aéreo o la operación del aeródromo. Aquí podría ser expeditivo indicar el nivel de severidad de acuerdo a la Tabla 1 (ver 8.6 - Paso 3).
f) Los métodos de detección de fallas, registrar todos los mecanismos para la identificación de la condición de falla, por ejemplo Sistemas de control y monitoreo, detección de errores en pantalla ATCO.
g) Las barreras y mitigaciones - registrar todos los mecanismos existentes para reducir la probabilidad de que la falla se produzca o reducir su severidad (consecuencias). Esto es sólo para los mecanismos existentes, y no para la definición de nuevas barreras o mitigaciones - esto viene más adelante en el paso 6 del proceso. Véase también el Apéndice X de árbol de eventos para ver si el análisis de árbol de eventos le ayudará a identificar cualquier otra barrera.
h) La probabilidad que se produzca la falla, los datos pueden obtenerse de los proveedores de equipos o el historial de servicio de campo de un equipo similar. Las estimaciones de personal con experiencia operacional y de los ingenieros pueden ser la mejor alternativa.
i) La tolerabilidad del fallo - Utilice la Tabla 3 (véase 8.8 - Paso 5) para identificar y registrar los criterios de tolerabilidad de la severidad y la

probabilidad de las cifras registradas, por ejemplo Aceptable, Revisión o Inaceptable.

j) Cualquier otro comentario – registrar aquí cualquier cosa de importancia que no se registran en las otras secciones de la tabla por ejemplo los supuestos adicionales o la explicación efectuada de las decisiones difíciles.

8.0 Modo de Fallos comunes

8.1. Los efectos ambientales y algunas fallas en el sistema puede tener un impacto en más de un sistema. Se debe considerar a éstos, por ejemplo:

a) El incumplimiento del suministro eléctrico exterior.
b) Mal tiempo.
c) La falta de aire acondicionado.
d) Incendios.

9.0 El informe FMECA

9.1. Debido al gran volumen de material de análisis que puedan producirse como resultado del proceso FMECA, es importante resumir el proceso y los resultados en un informe FMECA. La finalidad del proceso de FMECA descrito anteriormente es el de identificar y clasificar los peligros a fin de que se puede considerar aún más en los pasos posteriores del proceso Paso 7.

9.2. Es posible que se hayan realizado varios procesos FMECA para analizar un sistema complicado o grande. El informe FMECA es el lugar para reunir a los resultados de estos análisis.

9.3. El informe debe contener:

a) El alcance del informe, es decir lo que los sistemas han sido analizados.
b) Resumen de cómo se realizó el análisis: ¿quién, cuándo y cómo se realizó el análisis.
c) Un resumen de todas las condiciones de fallo que no sean las que se encuentran son intrascendentes.

10.0 Actualización del registro de Peligros

10.1. Los peligros identificados por el análisis FMECA debe ser inscrito en el registro de peligros (**ver Apéndice A**).

Elemento del sistema	I/D N.	Modo de Fallo	Causa	Efecto Local	Efecto final	Severidad	Método de detección	Barreras/ mitigación	Probabilidad	Comentarios

Figura 2. Ejemplo de Tabla de Estructura FMECA

Intencionalmente dejada en blanco

APENDICE D
Apéndice C Análisis de Peligros y Operatividad (HAZOP)

1.0 Introducción

1.1. El Análisis de peligros y Operatividad (HAZOP) es un proceso sistemático de identificación de peligros que utiliza un grupo de expertos para llevar a cabo un análisis estructurado de un sistema, utilizando una serie de palabras de guía para explorar los posibles peligros.
1.2. El enfoque sistemático HAZOP para analizar peligros es complementario a los enfoques no sistemáticos, tales como el método de lluvia de ideas.
1.3. La Tabla 1 proporciona una visión general del proceso HAZOP completo, desde la planificación inicial y la preparación a través de la evaluación de los resultados. El resto de este apéndice expande en cada punto hecho en la tabla.

2.0 Planificación Inicial

2.1. El análisis HAZOP puede llevarse a cabo en varias etapas del ciclo de vida de un proyecto. A principios de un proyecto, el estudio HAZOP puede llevarse a cabo una vez que se ha redactado el concepto de la operación. De acuerdo con el desarrollo del proyecto y se disponga de más detalles, el estudio HAZOP debe repetirse por lo general en la fase de diseño detallado, y una vez que el sistema ha sido implementado. Por lo tanto la realización de estudios HAZOP debe ser programado desde el principio en proyectos y planes de seguridad operacional.
2.2. El personal de operaciones, por ejemplo, los controladores de tránsito aéreo (ATCO), ingenieros de sistemas, pilotos y personal del aeródromo son normalmente los principales participantes en un grupo HAZOP. Sin embargo los compromisos operacionales pueden limitar su disponibilidad. Por lo tanto es necesaria una alta planificación y notificación de la actividad HAZOP para permitir que el proveedor de servicio de tránsito aéreo (ATSP), las compañías aéreas y el Administrador de Aeródromo puedan planificar la liberación de este personal.

Tabla 1. Proceso HAZOP completo

Planee	• Alinear el plan de evaluación de riesgos (incluyendo identificación del peligro) al plan del proyecto • Involucrar proveedor de servicios ATC, la compañía aérea y al Administrador del aeropuerto para la participación del personal operativo desde el principio del proyecto debido a su limitada disponibilidad.

Prepare	• Organice a los participantes
	  • El líder del estudio - que planifica y controla las reuniones
	  • Un registrador (Tomador de notas) que asiste al líder del estudio con la administración
	  • Expertos de sistema o el diseñadores tiene que ser capaz de

	explicar la intención del diseño de los componentes del sistema • Los usuarios del sistema por ejemplo, ATCOs, ingenieros, pilotos y personal de los aeródromos. • Otros expertos, en particular con conocimientos acerca de los peligros con sistemas similares • Preparar el HAZOP • Prepare las representaciones del sistema: Componentes, entidades y atributos • Elaborar listas de Palabras Guía • Hacer presentaciones de • El proceso de HAZOP y reglas de conducta • Introducción al sistema general • Haga un horario para la sesión de HAZOP • Organizar las cuestiones prácticas: • Sala de libre de distracciones • Papelógrafo • PC portátil y el proyector • La disponibilidad de refrescos
HAZOP	• Inicie con la presentación preparada • HAZOP • Conduzca el análisis del sistema en forma secuencial • Tome cortas notas de los peligros en el papelógrafo • Acuerde las causas y consecuencias creíbles de situaciones peligrosas y regístrelas • Aplicar pausas breves antes que la productividad se reduzca significativamente • Cierre de la sesión
Evalúe	• Distribuya los registros de HAZOP con el registro de peligros, solicitando correcciones • Evalúe la eficacia de la HAZOP: • ¿Alguna pregunta sin respuesta? • Decida si otra sesión HAZOP es necesario y cuando.

3.0 Preparación para el análisis HAZOP

3.1. Los participantes

3.1.1. El número de participantes en un estudio HAZOP debe limitarse a entre 5 y 7 personas.

3.1.1. Los siguientes participantes deben participar en una sesión de estudio HAZOP:

a) **El director:** controla el flujo y la fecha de la reunión, establece las normas de conducta de la reunión. El líder debe conducir a la reunión a través del análisis, postulando posibles desviaciones de la intención del diseño mediante la aplicación de las palabras guía HAZOP de forma secuencial en el diseño del sistema. El líder del estudio debe ser:

- Independiente del proyecto, pero conocedor de las representaciones de diseño (diagramas de bloque, etc.) y conocimientos en el campo técnico / operativo del sistema.
- Lo ideal es que esté familiarizado, o capacitado en la conducción de un estudio HAZOP.
- Un presidente competente, manteniendo un armonioso control sobre los procedimientos.

b) **Registrador (Tomador de notas)**: Alguien debe anotar el detalle de los peligros, que puede ser en una Laptop conectada a un proyector de manera que los participantes puedan corregir cualquier malentendido.

c) **Experto en el funcionamiento / Sistema:** Este debe ser alguien directamente involucrado con el proyecto previsto. Tendrá que explicar el papel del diseño de cada parte del sistema bajo consideración. Normalmente, puede ser el Gerente de Proyecto, un controlador de tránsito experimentado o un Ingeniero de Sistemas. También pueden presentar un resumen del proyecto al comienzo de la sesión.

d) **Los usuarios del sistema:** Por lo general estos serán Personal de operaciones, tales como:

- Controlador de Tráfico Aéreo: Esta persona debe estar familiarizado con el proyecto si es posible o debe estar familiarizado con el tipo de funciones ATC prevista que realiza por ejemplo, Aproximación, área, etc.
- Piloto: Esta persona debe estar familiarizada con el proyecto previsto si es posible o debe estar familiarizada con los tipos de aeronaves que pueden estar implicados en el proyecto previsto.
- Ingeniero: si es posible que esta persona debe estar familiarizado con la prevista proyecto o tienen experiencia en funcionamiento o mantenimiento de sistemas similares.

e) **Personal de Aeródromo:** dependiendo de la naturaleza del sistema, éstas podrían ser SSEI, personal de seguridad, abastecimiento de combustible, etc. personal donde, posiblemente, estas personas deben estar familiarizados con el proyecto previsto y el tipo de funciones que realizado.

f) **Otros Expertos:** Otros expertos operacionales o de Sistema familiarizados con el sistema que pueden añadir valor al proceso de HAZOP, por ejemplo un experto en el análisis de seguridad puede estar presente para ayudar al grupo con la terminología de la Seguridad Operacional y la estructuración del registro de peligros (esta función se puede combinar con la función de registrador para facilitar la reunión).

4.0 Planificación de una sesión de HAZOP

4.1. Logística de sesión

4.1.1. Las sesiones HAZOP pueden ser agotadoras para los participantes, por lo tanto, debería tomarse en cuenta lo siguiente al organizar la logística de una sesión:

a) Una sala de reuniones protegida de las distracciones por ejemplo, no se toman llamadas.
b) La elaboración de un calendario de reuniones que divide el tiempo asignado en porciones manejables con descansos frecuentes, por ejemplo, varias sesiones de media hora dividida por descansos de 10 minutos.

NOTA: *Los participantes suelen ser más pro-activa en las sesiones de la mañana a la tarde períodos de sesiones;*

c) Fácil disponibilidad de refrescos.

4.2. Presentación introductoria HAZOP

4.2.1. Algunos de los participantes a una sesión de HAZOP pueden no estar familiarizados con el proceso o lo que se espera de ellos. Por consiguiente, es importante explicar esto, idealmente en forma de una breve presentación que cubra:

a) La definición de un peligro.
b) Como será administrado el método HAZOP es decir, las reglas.

4.2.1. El líder del estudio, normalmente llevará a cabo la presentación anterior, de una duración de 10 minutos.

4.3. Presentación del proyecto o sistema

4.3.1. Si bien muchos de los participantes HAZOP pueden que estén familiarizados con el proyecto, algunos pueden no estarlo, por lo tanto debe ser presentada una visión general del proyecto:

a) la presentación no debe durar más de media hora.
b) No debe ser muy detallada, pero por lo general abarcan:
- El objetivo del proyecto.
- Concepto Operacional por ejemplo, configuración del espacio aéreo e interfaces; Diseño del aeródromo, características del tráfico; calendarios.
- Roles Humanos (por ejemplo, punto de vista del ATC, piloto, etc.).
- Procedimientos.
- Sistemas Técnicos.

c) Debe estar sesgados hacia imágenes y diagramas.

NOTA: *Las fotografías y diagramas p.e diseño del aeropuerto, estructura de las aerovías y gráficos, pueden estar en carteles y estar colocados alrededor de la habitación donde se lleva a cabo la actividad HAZOP para facilitar la referencia.*

4.3.1. El Experto / Operación del sistema que normalmente llevaría a cabo la presentación anterior.

5.0 Distribución del proceso de HAZOP

5.1. Representación documentados del sistema

5.1.1. Uno de los requisitos clave de la sesión HAZOP es una clara y completa representación del sistema que se analiza. Esto es necesario con el fin de permitir que el líder del estudio seleccione de forma secuencial los componentes o las interconexiones a ser analizadas.

5.1.2. La representación del sistema normalmente toman la forma de un diagrama de bloques que muestra los componentes del sistema y sus interconexiones. Estos pueden ser a nivel físico o nivel lógico.

5.1.3. Se puede requerir de más de un diagrama para representar todo el sistema.

5.1.4. La representación del sistema debe mostrar el sistema como un conjunto de:

a) **Componentes:** estructuras discretas, por ejemplo dentro del sistema total un transceptor de radio tal como se utiliza para comunicarse con las aeronaves, o entre el personal de tierra.

b) I**nterconexiones entre componentes**: por ejemplo, vincular una salida de transceptor de radio con un receptor a bordo de una aeronave o de otros receptores en el aeródromo.

c) **Entidades**: Estos se relacionan directamente con un componente o una interconexión entre componentes. Toman la forma de los sustantivos que describen los sub componentes del componente principal y/o describir el contenido de las interconexiones por ejemplo, una entidad del transceptor de radio sería el micrófono. Entidades típicas de las interconexiones son 'datos' y 'datos de control'.

d) **Atributos**: Estas son palabras que describen las propiedades de una entidad. Ellos normalmente implican propiedades mecánicas o eléctricas que pueden tener valores asociados con ellos por ejemplo: voltaje, nivel, velocidad de bits y el rendimiento. Los atributos de una entidad son los elementos contra los cuales las palabras guía HAZOP se aplican, por ejemplo, para el micrófono de radio transceptor, los atributos incluyen la transformación (de audio a electricidad) y alcance dinámico.

NOTA: Lo anterior suena más complicado de lo que es en la práctica. En términos generales, el sistema se descompone en un componente, y luego en sub-componentes a nivel de interconexiones y después son designados con atributos físicos o eléctricos relacionados con el funcionamiento del componente, subcomponentes o de interconexión.

5.1.5. Es importante tener cuidado al poner la representación del sistema en conjunto, ya que forma el punto de partida del estudio HAZOP.

5.2. Las palabras guía

5.2.1. Un conjunto de palabras guía genéricos que representen desviaciones de los parámetros del proceso deseados, un ejemplo se muestran en la Tabla 2.

5.2.2. Se pueden generar más palabras guía de manera más explícita en relación con el sistema bajo consideración.

Tabla 2. Palabras Guía Genéricas HAZOP

Palabras Guía Genéricas	
NO	No se logra ninguna parte de la intención del diseño, por ejemplo, No hay energía eléctrica. O no se logra el aspecto operacional.
MAS	Se produce un incremento cuantitativo de la intención del diseño, por

	ejemplo Demasiado energía eléctrica.
MENOS	Se produce una disminución cuantitativa de la intención del diseño, por ejemplo, muy poca energía eléctrica.
TAMBIEN	Se alcanza la intención del diseño, pero junto con otras cosas, ruido en la energía eléctrico.
PARTE DE	Se produce una parte de la intención del diseño, por ejemplo, energía eléctrica intermitente
INVERSO	Se produce lo opuesto de la intención del diseño, por ejemplo, sin energía eléctrica pero corto circuito a tierra o corriente inversa
OTROS	Se produce la actividad pero no en el modo deseado, por ejemplo, se espera energía DC y se obtiene en su lugar energía eléctrica AC
TEMPRANO	Algo que pasa antes del tiempo esperado
TARDE	Algo que pasa después del tiempo esperado
ANTES	Algo que pasa antes de los esperado, relacionado con una secuencia u orden
DESPUES	Algo que pasa después de los esperado, relacionado con una secuencia u orden

5.3. Organización de la reunión HAZOP

5.3.1. El líder del estudio, hará uso de la representación del sistema para presentar en forma secuencial todos los atributos asociados a los componentes, subcomponentes y las interconexiones (entidades).

5.3.2. Inicialmente, el líder del estudio identificará un componente del sistema o la interconexión de la Representación de diseño. El experto operacional / Sistema continuación, se explicará la función prevista del cambio propuesto.

5.3.3. El líder del estudio, entonces ejecutará secuencialmente a través de las entidades y los atributos asociados con el componente o la interconexión de la aplicación de cada una de las palabras guía de los atributos (ver Tabla 2), a su vez.

5.3.4. El grupo analizará si la desviación de la función prevista tal como se entiende de la palabra guía es creíble o no. Si no es creíble, la decisión debe registrarse para la integridad y para la facilidad de referencia en el futuro. Si creíble, se debe registrar:

a) Datos relativos al peligro identificado incluidos los mecanismos de detección.
b) Recomendaciones para mitigar el riesgo o sus efectos.
c) Recomendaciones para el estudio adicional donde existe incertidumbre acerca de cualquier aspecto del peligro, la causa o las consecuencias.
d) Las preguntas a ser respondidas debido a las incertidumbres.
e) Cruzar referencia a cualquier otro estudio y documentos pertinentes.

5.3.5. La Figura 1 muestra un método recomendado para registrar los resultados del estudio HAZOP.

NOTA: La presencia de mecanismos de protección o vigilancia no debe detener la exploración del peligro. Su eficacia en la reducción de la probabilidad o mitigar las consecuencias de los peligros pueden ser evaluados y los resultados registrados en la documentación de HAZOP.

5.3.6. La líder del estudio, concluye el análisis de atributos elegidos de las palabras guía con un resumen de las conclusiones, las cuales deberán estar documentadas por el Registrador.

5.3.7. Si se utiliza un ordenador portátil y el proyector, el registrador podrá asegurar que se han registrado la correcta comprensión de los peligros, las causas y las consecuencias analizadas por los participantes.

5.3.8. Este proceso continúa, de acuerdo con el calendario previsto, hasta que se han agotado todos los componentes del sistema, entidades, atributos y palabras guía.

6.0 Después de la sesión HAZOP

6.1. El acta de la sesión HAZOP debe ser proporcionada días después a los participantes para la comprobación de errores.

6.2. Se deben de revisar los resultados del proceso de identificación de peligros y emitir un juicio de cuan exitoso fue el proceso. Si, por ejemplo, se plantearon preguntas sin respuesta en la sesión de HAZOP, entonces es necesario encontrar las respuestas a estas preguntas y prestar atención si se necesita más de una sesión HAZOP para hacer frente a cualquier nueva información.

6.3. Los peligros identificados a partir de la sesión HAZOP, junto con otros peligros identificados por otros métodos, alimentan a los pasos siguientes del proceso de análisis de riesgos para establecer la gravedad y la probabilidad de sus consecuencias.

6.4. Los peligros identificados con el proceso de HAZOP se deben registrar en el Registro de peligros, donde este se mantiene (ver Apéndice A).

NOTA: *El grupo HAZOP puede consistir en el mismo equipo que efectúa la evaluación del riesgo, por lo que el grupo puede asignar la severidad inicial y la información probabilidad de que las consecuencias de riesgo inmediatamente después del proceso HAZOP para ayudar a la evaluación posterior.*

Titulo del Sistema bajo análisis *Descripción del Sistema*

Figuras/Diagramas usados:

Fecha:

Lider del Estudio

Registrador

Miembros del equipo:

Ítem HAZOP	Entidad (Sub Componente/ Interconexión)	Atributo	Palabra Guía	Causa	Consecuencia	Indicación o protección	Preguntas/ Recomendaciones	Comentarios

Figura 1 Ejemplo de Hoja de registro HAZOP

APÉNDICE E

UTILIZACIÓN DE ÁRBOL DE EVENTOS

1.0 Introducción

1.1. El Análisis de árbol de eventos se utiliza para analizar las secuencias de acontecimientos que conducen a los incidentes o accidentes. No se debe utilizar para la identificación de peligros. Se utiliza para apoyar la identificación de peligros y evaluación de riesgos, proporcionando una mayor comprensión de los fenómenos peligrosos mediante el examen de las circunstancias coincidentes que deben estar en su lugar, y las barreras que deben ser violadas, a fin de que un peligro pueda manifestarse en un accidente o incidente .Los árboles de eventos por lo tanto se pueden utilizar en los análisis de peligros para identificar una probabilidad más realista que ocurra un accidente o incidente.

1.2. Los árboles de eventos se puede utilizar para determinar la probabilidad y la severidad de una serie de consecuencias dadas las diferentes secuencias de eventos. Esto se ilustra mejor mediante un ejemplo.

2.0 Ejemplo de uso de un árbol de eventos

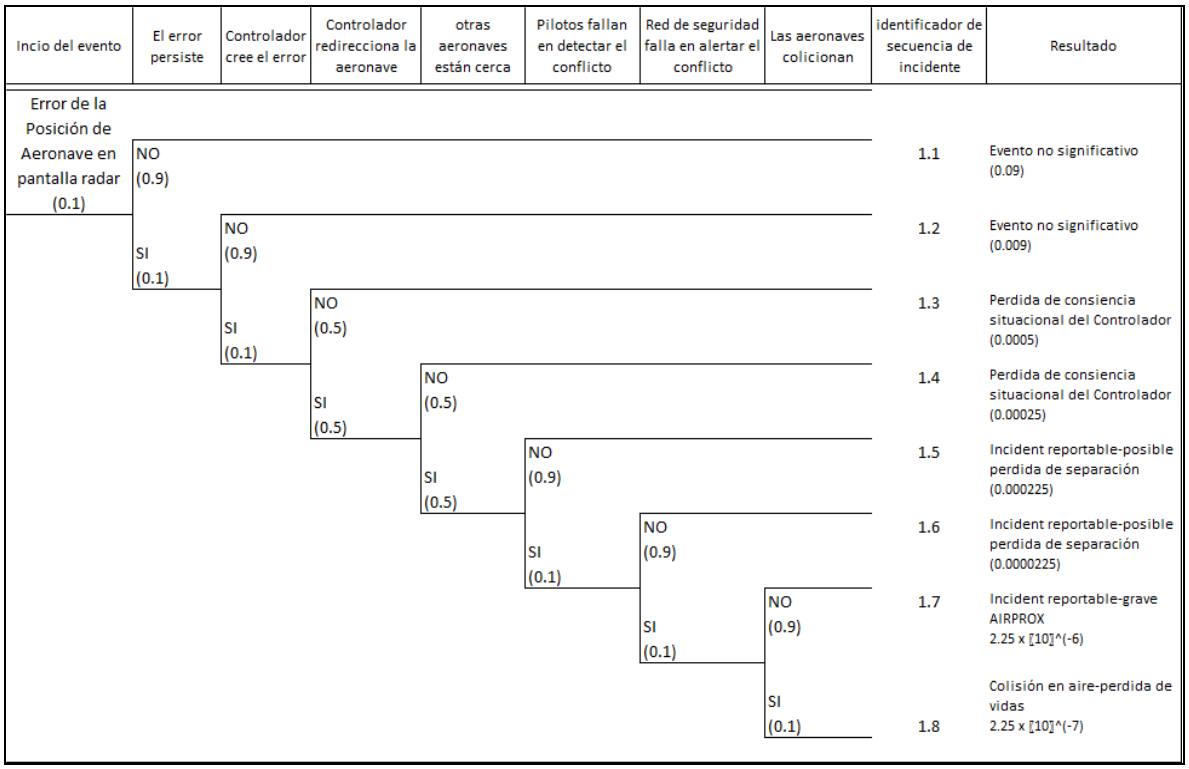
2.1. Considerar el trazado erróneo de una posición de aeronave en una pantalla de radar. Esto puede haber sido identificado como un peligro durante una sesión de identificación de riesgos sistemático, sin embargo, no está claro cuál es la consecuencia del error de la posición sin tener en cuenta otros factores relacionados, por ejemplo:

a) ¿Es el error persistente, o simplemente es una falla?
b) ¿El controlador de tránsito aéreo cree en el error, es decir, la posición presentada de la aeronave parece un error creíble?
c) ¿El controlador tomará medidas para reorientar a las demás aeronaves basados en datos de posición erróneos?
d) ¿Habrá otro avión cercano, con el potencial de causar un conflicto? es decir, si se ha trazado erróneamente la posición de la aeronave ¿es la única aeronave en la zona, y por lo tanto, no habrá conflicto con otras aeronaves?;
e) ¿Los pilotos se dieron cuenta del posible conflicto y pueden resolverlo?
f) ¿Las alertas de seguridad por ejemplo, Alerta de conflicto a corto plazo (CAW) y las alertas del Sistema de Alerta Anticolisión (TCAS) pueden evitar el conflicto potencial y que este se resuelva?
g) ¿los aviones llegan a tocar a medida que pasan unos a otros?

2.2. La anterior secuencia de eventos puede ser representado esquemáticamente como un árbol de eventos, como se muestra en la Figura 1, donde la trama errónea en el radar es el "suceso iniciador" es decir, el primer evento de disparo de la secuencia. Los enlaces posteriores en el árbol menudo se llaman "líneas de aseguramiento 'y consisten en los sistemas de protección, las acciones humanas u otros eventos fortuitos que tienen alguna relación con el suceso iniciador.

2.3. Cada rama del árbol puede tener una probabilidad asociada con ella (se muestra en los soportes de la Figura 1). Se puede calcular el producto de los caminos a través de los árboles para cada consecuencia. Se puede observar a partir de la secuencia anterior que, incluso cuando el trazado erróneo de una aeronave en una pantalla de radar es un suceso común, es decir 1 en 10, las otras coincidencias que tienen que producirse y las barreras que ayudan a prevenir la ocurrencia de incidentes críticos (por ejemplo, el controlador, el piloto y las redes de seguridad) mantienen a la probabilidad de la colisión de los aviones baja. Sin embargo, también se puede ver que la secuencia anterior puede producir una gama de incidentes de diferente severidades y probabilidades por ejemplo la pérdida de la conciencia situacional del controlador y por lo tanto la pérdida de la separación son tanto más probable que la colisión de aeronaves, sino también de menor gravedad.

Figura 1. Árbol de Eventos para una presentación errónea.



3.0 Identificación de barreras y mitigaciones mediante árboles de sucesos

3.1. Modelar los peligros utilizando los árboles de sucesos puede ayudar a identificar todas las barreras y las coincidencias que tienen que ocurrir para que un incidente se produzca. Esto ayuda a producir probabilidades más realistas y la reducción de las ocurrencias de incidentes. Esto puede ayudar a reducir la cantidad de argumentos y pruebas de trabajo requeridos en las últimas etapas de la evaluación del riesgo y el proceso de mitigación.

3.2. El proceso de árbol de eventos puede ayudar en el diseño del sistema, identificar dónde es mejor colocar las barreras o mitigaciones que ayudan a prevenir incidentes que se produzcan.

NOTA: *Estas barreras y mitigaciones serán convertidas en requisitos de seguridad, es decir, sin ellas en el lugar, el riesgo de un incidente aumenta.*

3.3. Los árboles de eventos se pueden utilizar después que se ha producido un incidente para ayudar a determinar las causas, la probabilidad de que el evento vuelva a ocurrir y en donde poner la mejor barrera para evitar que el evento vuelva a ocurrir.

4.0 Procedimiento para el análisis de árbol de eventos

4.1. El procedimiento para realizar el análisis de árbol de eventos consta de los siguientes seis pasos:

a) Identificar o definir el sistema o procedimiento de su interés.
b) Identificar los sucesos iniciadores de interés
c) Determinar las líneas de aseguramiento, otros eventos relacionados o coincidentes u otros factores que influyen.
d) Definir los escenarios de incidentes y accidentes - los árboles de sucesos.
e) Analizar los resultados de la secuencia de incidentes.
f) Resumir y presentar los resultados.

4.2. Cada paso se explica con más detalle a continuación.

4.3. Paso 1 - Identificar o definir el sistema o procedimiento de Interés

4.1.1. Cuando se utiliza el análisis de árbol de eventos para apoyar el análisis sistemático de otro proceso de peligro (por ejemplo, HAZOP y FMECA), entonces es probable que los procesos sistemáticos ya se han definido en el sistema o procedimiento para ser analizados. Cuando sea este el caso, el análisis de árbol de sucesos se puede volver a utilizar esta información.

4.1.2. Cuando no se haya llevado a cabo un análisis sistemático anterior, entonces será necesario definir el sistema o procedimiento sobre los cuales se efectuará el análisis de árbol de eventos. Deben ser considerados lo siguiente:

a) Las funciones destinadas a ser analizadas.
b) Los equipos y las personas involucradas.
c) Los límites del sistema.
d) Las interfaces entre los diferentes sub-sistemas y las interacciones entre las personas.
e) Las diferentes condiciones iniciales del sistema o procedimientos, por ejemplo, ¿Esta el equipo en funcionamiento o en modo de espera?

4.1.3. La descripción del sistema, que cubra todo lo anterior, se puede presentar en forma de texto narrativo con diagramas de apoyo (por ejemplo, diagramas de bloques del sistema).

4.4. Paso 2 - Identificar los sucesos iniciadores de interés

4.4.1. El análisis de árbol de eventos se puede realizar en un sub-conjunto de peligros que han sido seleccionados de un conjunto más amplio de peligros. El conjunto más amplio de peligros debería haber sido

desarrollado a partir de un proceso sistemático de identificación de peligros, tales como HAZOP o FMECA u otra amplia técnica de identificación de peligros. El conjunto mayor de peligros tiene que ser revisados para identificar los peligros de una naturaleza más compleja o interactivo que garantiza su posterior análisis mediante árboles de sucesos. Esta revisión debería ser llevada a cabo por expertos en el sistema y pueden formar parte del proceso sistemático de identificación de peligros.

4.4.2. Cuando se realiza el análisis de árbol de eventos, puede ser más expeditivo eliminar algunas categorías de eventos que podrían tener un impacto en todos los árboles de sucesos, por ejemplo, hechos de sabotaje y todos los desastres naturales a gran escala. Otros puntos comunes de modo de fallo, tales como fuentes de alimentación también pueden ser excluidos de los árboles de sucesos que se utilizan para explorar áreas con detalles particulares de problemas. La falla de las fuentes de alimentación puede ser modelada en un nivel más genérico. Se deben establecer las limitaciones.

4.4.3. Con frecuencia, los tipos de riesgos identificados pueden agruparse en conjuntos de eventos similares y tratado de forma genérica, lo que puede ayudar a limitar el número de árboles de eventos necesarios.

4.5. Paso 3 - Identificar las líneas de aseguramiento, otros eventos relacionados o coincidentes u otros factores que influyen

4.5.1. Este paso consiste en identificar un conjunto de factores que formaran más adelante las ramas del árbol de eventos.

4.5.2. Hay varios factores que determinan si un suceso iniciador dará lugar a un incidente. Estos factores deben ser identificados y pueden incluir:

a) Las barreras, las salvaguardias y las mitigaciones. Estos son los equipos y procedimientos diseñados a propósito para evitar que el evento inicial se manifieste en un incidente grave. En el ejemplo de la Figura 1 se trataría de las redes de seguridad que alertan al controlador de tránsito aéreo o pilotos en el conflicto potencial.

b) Sistemas administrativos o de personal, tales como los bomberos o la respuesta de emergencia. Estos pueden limitar la gravedad de un incidente.

c) Detección e intervención humana. Aquí es donde los seres humanos en la cadena de acontecimientos detectan el peligro y toman las medidas que lo mitigan. En el ejemplo de la Figura 1, tanto el controlador de tránsito aéreo desestima el error de posición por increíble y los pilotos ven el conflicto potencial, son ejemplos de detección humana.

d) Eventos coincidentes. Estos son eventos que deben ocurrir al mismo tiempo, o en secuencia con el suceso iniciador para que la cadena del incidente se propague. Se trata de eventos fortuitos. En el ejemplo de la Figura 1 “otras aeronaves están muy cerca" y “las aeronaves colisionan" se puede considerar eventos casuales o al azar.

e) Otros factores que influyen. Estos son otros fenómenos que puedan afectar a la probabilidad o la severidad de un incidente. Estos incluyen el clima y la hora del día. El ejemplo de la Figura 1 no incluye el clima, pero se puede observar que en condiciones atmosféricas de baja visibilidad se puede afectar la capacidad de los pilotos para detectar la situación de conflicto.

4.5.3. Al final de este paso se deben definir el conjunto de factores a partir del cual se puede construir el árbol de eventos.

4.6. Paso 4 - Definir el incidente y los escenarios de accidentes - los árboles de eventos

4.6.1. Este paso define la estructura del árbol de eventos, comenzando con el evento inicial y la selección de factores relacionados con el conjunto desarrollado en el paso anterior y ponerlos en el orden en que son más probables de ocurrir.

4.6.2. Hay una progresión lógica de una secuencia de incidentes que se mueve hacia adelante desde el momento en que el evento inicial se produce. Como la secuencia de incidentes progresa y se vuelve más severa o menos probable, los diferentes sistemas responden de distintas maneras. La comprensión de la progresión y el tiempo del sistema, físico y la respuesta humana es esencial en el desarrollo de la lógica del árbol de eventos.

4.6.3. Se debe tener cuidado cuando se construye el árbol de considerar lo siguiente:

a) Las dependencias del sistema - La mayoría de los sistemas interactúan de alguna manera con otras máquinas y procesos. Estas interacciones pueden influir o degradar el nivel de protección ofrecido por el equipo de reserva y sistemas de reserva. Por ejemplo, la falla del sistema de aire acondicionado en una torre de control no sólo puede causar que algunos equipos electrónicos se recalienten y fallen, sino que también colocan a los controladores aéreos, que tratan de lidiar con el equipo, bajo coacción física que puede obstaculizar su desempeño.

b) Respuestas condicionales - La probabilidad de éxito para una línea de seguridad (es decir una mitigación o barrera) puede estar condicionada por el éxito o el fracaso de las líneas de la seguridad que lo preceden. Por ejemplo, la capacidad de los pilotos para ser capaz de detectar visualmente un conflicto potencial puede estar condicionada a las condiciones meteorológicas prevalecientes o a la hora del día. No es raro que por lo tanto, la misma línea de factor de seguridad cuente con diferentes probabilidades asociadas a ella en diferentes árboles de eventos o partes de un mismo árbol, en función de los eventos anteriores o que factores son.

c) La correcta asignación de las probabilidades – Cuando se posible, los resultados de las probabilidades de la rama del árbol de eventos deben consignarse en el árbol de eventos. Sin embargo, la obtención de datos confiables de probabilidad de la eficacia de las barreras puede ser difícil, por ejemplo, la probabilidad de que

un humano actué de una manera particular, es difícil de predecir. Lo siguiente puede ayudar a proporcionar estimaciones de probabilidades más certeras:

- Modelado particular del dispositivo de protección, o procedimiento o persona por ejemplo, mediante el uso de análisis de la fiabilidad humana (una técnica para predecir el rendimiento humano - no se incluyen en este documento).
- Uso de las pruebas de campo del desempeño de otro sistema similar para estimar el rendimiento del sistema.
- El juicio de los expertos en los sistemas afectados.

4.7. Paso 5 - La construcción de la lógica del árbol de eventos

4.7.1. Construcción del árbol de eventos se compone de los siguientes pasos:

a) Liste el suceso iniciador en el lado izquierdo del árbol.
b) Haga una lista de las líneas de seguridad, las barreras y otros factores que influyen en las condiciones o en la parte superior del árbol en orden secuencial.
c) Determinar el éxito y ramas de error en cada punto de ramificación (el punto debajo de una línea de seguridad, etc.) y añadir las probabilidades si se conocen. Considere lo siguiente:
   - Algunos puntos de ramificación puede tener más de dos resultados.
   - Algunos puntos de ramificación puede tener sólo un resultado en donde la probabilidad condicional es 1 ó 0, es decir, como resultado de un evento anterior, el resultado de este evento es 100% seguro.
d) Mantener ramas de probabilidad positiva o alta de los pares de ramas o grupos en la parte superior de cada punto de ramificación para ayudar más adelante a la clasificación de los temas prioritarios, es decir, si los más altos resultados de probabilidad se mantienen siempre en la parte superior, entonces el resultado más alto será el más probable.
e) Continuar el desarrollo de las ramas y los puntos de ramificación a la derecha hasta que la secuencia de factores se haya agotado.

4.7.2. La figura 1 es un ejemplo de lo que puede parecer un árbol de eventos.

4.8. Paso 6 - Analizar los resultados de secuencia de incidentes

4.8.1. El resultado final para cada combinación de las ramas se encuentra al lado derecho del árbol de eventos. También puede ser beneficioso etiquetar cada una de las combinaciones de rama con un número identificador de secuencia o una letra para ayudar a cualquier referencia posterior de las secuencias específicas en el árbol de eventos.

4.8.2. La consecuencia final de cada secuencia de eventos puede ser obvia y puede ser fácilmente añadida al árbol de eventos en la última columna. Sin embargo, puede que algunas secuencias de eventos no sean inmediatamente claras cuáles pueden ser las consecuencias. Cuando éste sea el caso, entonces se debe seguir trabajando el modelado de la secuencia de eventos o puede ser necesario el juicio de expertos para determinar las consecuencias antes de ingresarlos al árbol de eventos.

4.8.3. Cuando se han utilizado probabilidades en las ramas de los árboles de eventos, entonces la probabilidad para cada secuencia de acontecimientos que conducen a un resultado puede calcularse multiplicando juntando todas las probabilidades en una secuencia.

4.8.4. Una evaluación cualitativa de la probabilidad de un resultado puede basarse en el recuento del número de ramas (barreras, medidas de mitigación y coincidencias) entre el evento inicial y el resultado, es decir, contando el número de eventos que tienen que unirse con el fin de provocar el resultado. Un número bajo significa un resultado probable, mientras que un número elevado equivale a un resultado poco probable. Sera necesaria una estimación para evaluar qué tan probable o improbable es el resultado, teniendo conocimiento de la eficacia de los sistemas de protección y de los procedimientos que forman las ramas de los árboles de eventos.

4.9. Paso 7 - Resumir los resultados

4.9.1. Dónde se han producido grandes conjuntos de árboles de eventos se requerirá presentar la información de los árboles de una manera práctica. Esto puede lograrse a través de la tabulación de lo siguiente:

a) El inicio del evento.
b) Número de secuencia de eventos (para la trazabilidad de nuevo al árbol de eventos).
c) La probabilidad o posibilidad.
d) El resultado o consecuencia.

4.9.2. La Tabla 1 muestra la tabla de resumen para el árbol caso de la Figura 1.

Inicio de suceso: Error de posición de la aeronave en la pantalla del radar		
Numero de secuencia de incidente	**Probabilidad**	**Consecuencia**
1.1	0.09	Evento no significativo
1.2	0.009	Evento no significativo
1.3	0.0005	Pérdida de conciencia situacional de controlador
1.4	0.00025	Pérdida de conciencia situacional de controlador
1.5	0.000225	Notificación de incidente- posible pérdida de separación
1.6	0.0000225	Notificación de incidente- posible pérdida de separación
1.7	2.25×10^{-6}	Notificación de incidente- AIRPROX severo
1.8	2.5×10^{-7}	Colisión de Aeronaves –Pérdida de vidas