Agencia Estatal
de Seguridad Aérea

Sistemas de Gestión de la Seguridad Operacional (SMS)

GOBIERNO DE ESPAÑA
MINISTERIO DE FOMENTO
AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

DOCUMENTACIÓN PÚBLICA

A-DEA-GSMS-01

© AESA
AGENCIA ESTATAL DE SEGURIDAD AÉREA
Este documento se acoge al amparo del Derecho de la Propiedad Intelectual. Quedan reservados todos los derechos inherentes a que ampara la Ley, así como los de traducción, reimpresión, transmisión radiofónica, de televisión, Internet (página web), de reproducción en forma fotomecánica o en cualquier otra forma y de almacenamiento en instalaciones de procesamiento de datos, aun cuando no se utilice más que parcialmente.

Cualquier copia impresa o en soporte informático, total o parcial de este documento se considera como copia no controlada y siempre debe ser contrastada con su versión vigente en la web.

Índice

1. PRÓLOGO DEL DIRECTOR 3

2. AGRADECIMIENTOS 17

3. INTRODUCCIÓN 18

4. CAPÍTULO 1: SISTEMA DE GESTIÓN DE SEGURIDAD OPERACIONAL (SMS): LOS FUNDAMENTOS 22

4.1 SEGURIDAD OPERACIONAL, PROVISIÓN DE SERVICIOS Y RECURSOS 22
4.2 DOS PREGUNTAS CLAVES 24
4.3 DOS PROCESOS FUNDAMENTALES 29

5. CAPÍTULO 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL 33

5.1 INTRODUCCIÓN 33
5.2 LA VULNERABILIDAD DE LA SEGURIDAD OPERACIONAL DE LOS SISTEMAS 33
5.3 LA DESCRIPCIÓN DE LAS VULNERABILIDADES DE SEGURIDAD OPERACIONAL DEL SISTEMA 36
5.4 LA IDENTIFICACIÓN DE LOS PELIGROS 38
5.5 MEDICIÓN Y CONTROL 44
5.6 APÉNDICE 1 AL CAPÍTULO 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL – OPERADOR DE GRAN TAMAÑO O COMPLEJIDAD 54
5.7 APÉNDICE 2 AL CAPÍTULO 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL – OPERADOR PEQUEÑO 58

6. CAPÍTULO 3: ASEGURAMIENTO DE SEGURIDAD OPERACIONAL 61

6.1 INTRODUCCIÓN 61
6.2 INICIO DE LAS OPERACIONES 64
6.3 OBSERVACIÓN Y MEDICIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL 64
6.4 CAMBIOS EN EL CONTEXTO OPERATIVO Y/O LAS OPERACIONES 69
6.5 ACCIÓN CORRECTIVA 71
6.6 SRM Y SA – UN EJEMPLO CONJUNTO 72
6.7 PLANIFICACIÓN – SRM 72
6.8 OPERACIÓN – SA 74
6.9 APÉNDICE 1 AL CAPÍTULO 3: OBSERVACIÓN Y MEDICIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DE SMS 75

7. CAPÍTULO 4: POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL 79

7.1 INTRODUCCIÓN 79
7.2 POLÍTICA DE SEGURIDAD OPERACIONAL 80
7.3 OBJETIVOS DE SEGURIDAD OPERACIONAL 82
7.4 RENDICIÓN DE CUENTAS SOBRE LA seguridad operacional 83
7.5 DOCUMENTACIÓN SMS 88
7.6 LA IMPLEMENTACIÓN DE SMS EN LA PRÁCTICA – OCHO ACTIVIDADES CLAVE 90
7.7 GRUPO DE PLANIFICACIÓN SMS 90
7.8 DESCRIPCIÓN DEL SISTEMA 90
7.9 ANÁLISIS DE CARENCIAS 91
7.10 IDENTIFICACIÓN DEL GERENTE RESPONSABLE Y RENDICIÓN DE CUENTAS SOBRE LA SEGURIDAD OPERACIONAL 92
7.11 POLÍTICA DE SEGURIDAD OPERACIONAL 93
7.12 PROGRAMA INTERNO DE INSTRUCCIÓN EN SMS 93
7.13 COMUNICACIÓN SOBRE LA INICIACIÓN DEL PROYECTO DE IMPLANTACIÓN DE SMS 93
7.14 EVALUACIÓN Y PROPUESTA DE PUESTA EN MARCHA DE LAS FUENTES DE ADQUISICIÓN DE DATOS SOBRE DEFICIENCIAS DE SEGURIDAD OPERACIONAL Y PELIGROS 93
7.15 PLAN DE IMPLEMENTACIÓN 94
7.16 APÉNDICE 1 AL CAPÍTULO 4: ESTRUCTURA SMS DE LA OACI 94

8. CAPÍTULO 5: PROMOCIÓN DE LA SEGURIDAD OPERACIONAL.....98
8.1 INTRODUCCIÓN.....98
8.2 ACTIVIDADES DE PROMOCIÓN DE SEGURIDAD OPERACIONAL.....98
8.3 COMUNICACIÓN.....99
8.4 FORMACIÓN.....100
8.5 INSTRUCCIÓN.....101
8.6 PERSONAL TÉCNICO U OPERATIVO.....102
8.7 POST-HOLDERS (O PERSONAL RESPONSABLE) Y OTROS CARGOS.....102
8.8 BRIEFING ESPECIAL PARA EL GERENTE RESPONSABLE.....102

9. BIBLIOGRAFÍA.....103
9.1 ICAO.....103
9.2 EASA.....103
9.3 CASA.....103
9.4 EUROCONTROL.....103
9.5 IATA.....103
9.6 IBAC.....103
9.7 IBA.....104
9.8 TRANSPORT CANADA.....104
9.9 UK CAA.....104
9.10 SM ICG.....104

1. PRÓLOGO DEL DIRECTOR

1. Los sistemas de gestión de seguridad en aviación, tanto en la industria como en el Estado, ya son una realidad en nuestros días. El camino recorrido hasta este punto es realmente fascinante, viéndolo desde la perspectiva que nos da, como en casi todo, el transcurrir de los años y de las décadas.

2. Durante los años 50 del siglo pasado, se produjeron grandes avances tecnológicos en aviación, y parecía que la tecnología resolvería todos nuestros problemas (aún hoy en día, algunos fabricantes de aeronaves, parecen seguir vendiendo esta quimera). Posteriormente, en los años 70-80 recuperamos al casi olvidado (y a veces denostado) elemento humano; ampliándose el campo de la ergonomía, e integrándose el elemento humano como uno más a tener en cuenta durante el diseño y operación del sistema. En los años 90 surge el concepto de accidente organizacional (modelo epidemiológico) y el ya famoso modelo de queso suizo de James Reason (*James Reason. El error humano. Modus laborandi*), y comenzamos a comprender el fallo catastrófico de un sistema como un fallo organizacional en su conjunto, en el que se ponen de manifiesto las fallas latentes o durmientes de las barreras de seguridad intrincadas en su diseño. En la última década han surgido modelos más complejos de accidentes, dinámicos, sistémicos, que tienen en cuenta las distintas interrelaciones de los elementos del sistema, factores culturales, y factores sociales. Han surgido los conceptos de accidente de resonancia funcional y el de resiliencia organizacional (*Erik Hollnagel. Barreras y prevención de accidentes. Modus laborandi*), reconociendo que la terca realidad siempre acaba resultando más compleja de lo que en principio alcanzaban nuestros modelos previos.

3. Ni que decir tiene que todos estos avances se han ido siempre superponiendo y se han ido sumando; es decir, no se han abandonado ninguno de estos enfoques, sino que se han ido complementando como si de las piezas de un complejo puzle se tratara. Así, por tanto, la tecnología hoy en día sigue resultando clave y continúa siendo una de las tres más importantes barreras de seguridad, junto con la reguladora o procedimental, o la formativa. Baste citar como ejemplo el ya famoso "San TCAS (o amigo TCAS)" o el EGPWS que tantos accidentes evitan todos los días, y han evitado.

4. Los sistemas de gestión de seguridad surgen de la necesidad de gestionar el riesgo de seguridad cuando los sistemas se encuentran en operación, lejos ya de su fase de diseño. El concepto en sí no es complicado de entender, y hoy en día puede parecer hasta trivial; pero en su día supuso introducir una nueva perspectiva en la gestión del riesgo y un gran avance en seguridad en la industria del transporte (y en otras industrias). Lo que sí puede resultar bastante complejo, como en breve comentaremos, es su implantación, su aplicación práctica y su desempeño diario.

5. El primer gran avance es reconocer que la seguridad operacional, al igual que las finanzas, la calidad, los riesgos laborales o los medioambientales, se puede gestionar. El asunto puede parecer banal, pero es crítico. Supone, en primer lugar, entender que la seguridad 100% es inalcanzable. El ser humano por desgracia es imperfecto, y diseña, por tanto, sistemas imperfectos. Claro que explicar esto, a veces, no es políticamente correcto. Lo políticamente correcto es decir que mi compañía o mi organización es tan segura que está libre se sufrir accidentes. Pero esto no es real; hasta la empresa más comprometida con la seguridad no está libre de pecado, y puede sufrir, muy a su pesar, un accidente o un incidente grave. En sistemas complejos de alto riesgo, como defiende Perrow (*Charles Perrow. Accidentes normales. Modus Laborandi*), el accidente no debe verse como un hecho extraordinario sino como algo "normal" atribuible a la complejidad misma del sistema.

6. Y esto es así, además, por una razón muy sencilla; porque el sistema se diseñó para que fallara con una determinada probabilidad de fallo catastrófico. Esto parece una perogrullada, pero muchas veces se nos olvida. En el caso del diseño de aeronaves se utiliza la cifra de un fallo catastrófico cada 10^9 horas de vuelo, y la tasa de accidentes en el transporte aéreo comercial en Europa se situó en 2016 en tres accidentes por cada millón de vuelos, según informe de la Agencia Europea de Seguridad Aérea (EASA) sobre la evolución en los 32 países miembros de la organización. Además, este nivel de seguridad no se consigue por casualidad, sino con plena consciencia. Reconociendo, que una vez alcanzado cierto nivel de seguridad, no resulta rentable seguir invirtiendo recursos en hacer el sistema más seguro. Hay ciertos riesgos residuales evaluados de los que no se protege al sistema porque la probabilidad de enfrentarse a ellos se considera extremadamente improbable o el tiempo de exposición a los mismos es residual. Es el concepto ALARP (tan bajo como resulte razonablemente posible) recogido en la regulación anglosajona. Es decir, claro que podemos hacer el sistema más seguro (nunca 100% seguro como hemos argumentado) pero, ¿a qué coste?

7. Este concepto de seguridad, que resulta clave en lo que se refiere a los sistemas de gestión de seguridad, lo introdujo la OACI, Comandante Mauriño a la cabeza, en su Doc. 9859 –Manual de Gestión de la Seguridad Operacional: "*Seguridad operacional: Estado en que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel aceptable, o por debajo del mismo, por medio de un proceso continuo de identificación de peligros y gestión de riesgos*", de acuerdo con la definición recogidas en sus primeras ediciones.

8. La primera parte de la definición recoge el concepto que acabamos de explicar; …se reduce y se mantiene en un nivel aceptable (el de diseño) o por debajo del mismo. La segunda parte de la definición recoge la forma en la que se consigue este objetivo; …por medio de un proceso continuo de identificación de peligros y gestión de riesgos.

9. Pero, ¿por qué tenemos que hacer algo para mantener el nivel de seguridad de diseño? La respuesta es que tenemos que hacer ese algo porque todos los sistemas, durante su operación van poco a poco sufriendo una deriva, y se acaban desviando paulatina e inexorablemente del modo de operación para el que cual se habían diseñado. Además, pueden surgir cuestiones que no se tuvieron en cuenta durante la etapa de diseño, bien por error, bien por resultar impredecibles. Es aquí donde entran a jugar su papel los sistemas de gestión de seguridad. Nos devuelven al sistema, durante su operación, al punto de diseño del que no debían haber salido (o lo mejoran), evitando así adentrar el sistema en una zona de riesgo inaceptable.

10. Para conseguir esto, los sistemas de gestión de seguridad, de forma continua, captan datos de seguridad, identifican peligros reales o potenciales, analizan los datos, evalúan los riesgos, y en el caso de encontrarse en una región de riesgo inaceptable, implantan medidas de mitigación y control de riesgo, y evalúan, recopilando más datos, si las mismas están resultando efectivas.

11. En definitiva, los sistemas de gestión de seguridad permiten adoptar decisiones de manera informada y destinar los recursos disponibles en aquellas áreas donde realmente son más necesarios. Su gran potencial reside en que las decisiones se apoyan en datos, y no en meras opiniones o suposiciones.

12. Los sistemas de gestión de seguridad en la industria aeronáutica se han integrado en dos niveles: por un lado, con alcance nacional (o plurinacional) en el Estado; y por otro, en la industria aeronáutica, a nivel organizacional, en el proveedor de un producto o servicio. Veamos brevemente en qué consisten.

13. Lo primero que habría que mencionar del Programa Estatal de Seguridad Operacional (PESO), es que no se debería llamar "programa", porque en realidad, como hemos explicado, es un sistema de gestión para la gestión de la seguridad operacional por parte del Estado. Conceptualmente los procesos que ha de implantar el estado para gestionar la seguridad, no difieren de aquéllos que debe implantar la industria a través de sus SMS; lo que sí resultarán muy distintas son las actividades asociadas a estos procesos.

14. La implantación y desarrollo de un Programa Estatal de Seguridad Operacional conlleva tener que coordinar diversas organizaciones y agencias gubernamentales con incidencia sobre la seguridad aérea de la aviación civil. Es decir, no es ni mucho menos una cuestión que afecte únicamente a la autoridad aeronáutica (AESA), sino que se integra e implanta por medio de las distintas

organizaciones que componen la administración aeronáutica o que interfieren con ella.

15. En cuanto a los SMS, de acuerdo a la doctrina que emana de OACI, se exigen a un amplio espectro de la industria aeronáutica: gestor aeroportuario, proveedor se servicios de navegación aérea, aerolíneas, centros de mantenimiento, centros de formación, etc. El SSP del Estado y los SMS de la industria están interconectados y se complementan; uno actuando a nivel macro, y otro a nivel micro.

16. Por otro lado, conviene subrayar que los sistemas de interés en aviación son sistemas socio-técnicos –sistemas compuestos de organizaciones humanas y de tecnología, y que por tanto, los comportamientos de interés comprenderán el desempeño de estos dos principales componentes: elemento humano y tecnología.

17. Con esta perspectiva in mente, se puede afirmar que los SMS son realmente algo más que un sistema. Necesitan de la debida cultura organizacional, de una apropiada cultura de seguridad, para poder ser realmente efectivos; entendiendo por cultura organizacional el conjunto de percepciones, sentimientos, actitudes, hábitos, creencias, valores, tradiciones y formas de interacción aceptadas y compartidas dentro y entre los grupos existentes en las organizaciones. Esta "cultura de seguridad" permitirá, por ejemplo, que exista un proceso sólido de reporte de eventos o deficiencias de seguridad y de peligros. Podemos decir, por tanto, que en el centro mismo de los SMS se encuentra el elemento humano; las personas. Comprender adecuadamente el comportamiento humano y los factores organizacionales resultará clave para el éxito de un SMS. Los factores humanos deben ser, sin duda, parte integrante de los SMS.

18. Uno de los primeros problemas a los que se enfrenta un estado o un proveedor a la hora de implantar estos sistemas es conseguir identificar o establecer las fuentes de datos de seguridad de las que se alimentará el sistema. Un principio básico en gestión dice que no se puede gestionar lo que no se puede medir. Los datos de seguridad componen la base de la pirámide de la que se derivan los procesos de identificación de peligros y gestión de riesgos, y en último caso, de medición del rendimiento del sistema de gestión de seguridad. Sin esos datos, sin esa información, no es posible construir nada de forma efectiva.

19. Además, no vale cualquier dato. Es decir, los datos no deben dirigir los procesos sino en general, deben ser los procesos los que dirijan e identifiquen los datos que resultarán necesarios; dicho de otro modo, debemos saber lo que vamos buscando. Puede existir cierta tentación de pretender utilizar únicamente aquellas fuentes de datos que se encuentran más a mano y estructuradas, y que por tanto, son fácilmente explotables. Caer en dicha tentación nos puede llevar a manejar un volumen elevado de datos de los que no vamos a poder extraer grandes enseñanzas.

20. No obstante, también nos podemos encontrar con determinados tipos de análisis en los que sean los propios datos quienes guíen nuestras decisiones. Nos referimos a técnicas de minería de datos y *clustering* en las que se trata de identificar precursores ocultos de eventos de mayor severidad. Caerían dentro de esta última clasificación las técnicas de *knowledge discovery* y *machine learning* empleadas en programas *Big-data*. En este tipo de escenarios, se juega con los datos para intentar encontrar algún tipo de interconexión y diferenciación entre ellos, a priori, no estipulada. Se puede dar incluso el caso en el que, sin poder llegar a identificar y entender la causa que interconecta los distintos tipos de datos, debemos actuar de manera preventiva. Es decir, que sin buscar determinados datos de modo intencionado, el análisis de los mismos ponga en evidencia un problema que a priori no se había identificado. Pensemos por ejemplo en los primeros accidentes e incidentes producidos en aviación por el fenómeno de fatiga de los materiales.

21. En cuanto al origen de los datos, el foco de nuestra identificación de peligros no se encontrará en la investigación de accidentes. Considerando que, por cada accidente, se pueden producir en torno a 50 incidentes graves, unos 500 incidentes de menor consideración, y del orden de miles de fallas latentes en nuestro sistema, está claro que nuestras mayores fuentes datos provendrán de procesos que nos permitan captar desviaciones de seguridad de poca gravedad o de poca consideración. La gestión de la seguridad es un esfuerzo desperdiciado si la identificación de los peligros se limita solamente a aquellos raros eventos donde hay lesiones serias o daños materiales significativos.

22. Otro aspecto importante al que se debe prestar la debida atención es a la calidad y validación de los datos que van a soportar nuestro análisis. Siguiendo una máxima sencilla de recordar, si metemos en nuestro sistema de análisis basura, sacaremos basura (*rubbish in, rubbish out*). Por tanto, resultará necesario realizar primero un depurado apropiado de los datos recopilados, eliminar duplicaciones, valores atípicos (*outliers*), y validar, mediante juicio experto, si aquello que se recopiló goza o no de significado. Sólo entonces nos encontraremos en disposición de realizar un análisis robusto y pormenorizado.

23. Por último, se debe subrayar la importancia de la taxonomía o método de clasificación utilizado para agrupar los datos. Sin una taxonomía apropiada seremos incapaces de llegar a identificar determinados tipos de eventos que pudieran ser de nuestro interés; es decir, seremos incapaces de explotar los datos apropiadamente. Esta taxonomía también resultará clave a la hora de intercambiar o de comparar datos con otras autoridades o proveedores. Si los métodos de clasificación utilizados son distintos, puede llegar a resultar inviable comparar o intercambiar datos. Como se dice comúnmente, tendremos que comparar peras con peras y manzanas con manzanas. Esta comparación resulta clave para implantar herramientas estratégicas que soporten la toma de decisiones. Con este fin la OACI desarrolló la taxonomía ADREP -*Accident Data Reporting System*, que es utilizada por un elevado número de estados y

organizaciones, y por la herramienta ECCAIRS, desarrollada por el *Joint Research Centre* de la Comisión Europea.

24. En cuanto a las taxonomías, mucho se ha escrito al respecto, y recientemente se van introduciendo tendencias que tratan de capturar no sólo datos sobre aquellas cuestiones que fueron mal y fallaron (taxonomía convencional o negativa), sino también datos que nos permitan identificar las barreras de seguridad que funcionaron y que eventualmente impidieron que el evento de seguridad desembocase en un evento de mayor consideración (taxonomía positiva).

25. En cuanto a la protección de la información y del notificante, está claro que una de las cuestiones prácticas que más preocupa a los estados a la hora de implantar estos sistemas –SSP y SMS, es establecer un clima de confianza apropiado entre los miembros que conforman la comunidad aeronáutica que permita capturar información de seguridad valiosa y de alta calidad. Para ello, el estado debe establecer regulaciones e implementar procedimientos que protejan tanto a la información facilitada como al propio notificante.

26. La información se debe proteger en al menos dos vertientes; por un lado, para que no acceda a la misma mas quien esté autorizado a ello; y por otro, para que el uso que se vaya a realizar sea el mismo para el cual se recopiló. Es decir, si recopilamos la información con el único objeto de mejorar los niveles de seguridad, debemos evitar que esta misma información, con las debidas excepciones, se utilice para fines distintos, como por ejemplo establecer sanciones o iniciar procedimientos disciplinarios (aunque desde un punto de vista purista, en parte, en su aspecto coercitivo, las sanciones o los procedimientos disciplinarios también producen un efecto directo y positivo sobre la seguridad; lanzan el mensaje de que determinado tipo de conductas son inaceptables).

27. Al notificante se le debe de facilitar protección tanto respecto a posibles represalias de su empleador como respecto a procedimientos adoptados por la administración. Lo primero supone considerar nulas aquellas actuaciones adversas (incluido el despido) en contra de un trabajador que pudieran haber sido adoptadas por un empleador por el simple hecho de notificar un evento que afecta a la seguridad. Lo segundo, exige establecer claramente una política sancionadora que prime recopilar información esencial de seguridad por parte del regulador o del proveedor en lugar de sancionar administrativamente o disciplinariamente a unos pocos.

28. En el caso de la investigación de accidentes, que también forma parte íntegra del SSP, deberemos considerar la protección de la información con el fin de evitar indeseables interferencias con el proceso de administración de justicia y así conseguir que en futuras investigaciones de seguridad el investigador cuente con información clave facilitada por el personal operativo involucrado en el accidente. De otro modo, el personal operativo se inhibirá de facilitar información que en último caso se pudiera emplear para auto-incriminarle. Es en este caso en particular de la investigación de accidentes, a diferencia de otros sistemas de

captación de información de seguridad del SSP, donde suele haber un juez detrás de la información y datos gestionados, dado que los hechos manejados han derivado en víctimas o daños materiales de consideración, y por tanto, los familiares de las víctimas o los sufridores del daño causado buscan legítimamente una restitución de su pérdida, una compensación, o un resarcimiento por los daños y perjuicios que se les ha ocasionado.

29. Además, como ya se ha mencionado, en el caso de la protección de la información el estado debe establecer las excepciones que correspondan que rompan con los principios generales de protección establecidos. A parte de la conducta dolosa o intencionada, o de la negligencia grave, se deben considerar los principios constitucionales del estado, como por ejemplo, el deber de colaboración con los jueces y tribunales de justicia; pero buscando, lo cual no resulta siempre fácil, un fino equilibrio que permita mantener la información a disposición del investigador de seguridad a la vez que no se impida un actuación efectiva por parte de la administración de justicia. La forma de alcanzar este fino equilibrio suele llegar muchas veces en forma de acuerdo: sobre el acceso al lugar del accidente, intercambio de datos factuales, preservación y custodia de evidencias, pruebas y ensayos (destructivos y no destructivos), etc.

30. Además, tampoco se debe olvidar uno nunca del objeto fundamental por el cual se recopila la información de seguridad; el de prevenir que se reproduzcan accidentes e incidentes graves. Y este fin último nos llevará indudablemente a tener que llegar en algún punto a tener que divulgar las enseñanzas aprendidas, a tener que prevenir, y a tener que intercambiar datos de seguridad con otras autoridades u organizaciones, siempre que persigan los mismos fines. Nuevamente, se tratará de alcanzar un equilibrio entre proteger y divulgar adecuadamente. Esto resultaría innecesario recordarlo si no existieran regulaciones, bastante cercanas, que han querido proteger de tal modo los datos recopilados, que han evitado una explotación eficiente y un análisis apropiado de los mismos, hasta el punto de resultar su análisis prácticamente inviable.

31. Y también conviene recordar esto mismo a la hora de etiquetar lo que se considera una acción apropiada o inapropiada, en respuesta al acceso a determinada información de seguridad. Por poner un ejemplo ajeno a la aviación, imaginemos una persona que acude al hospital y le informa al médico que sufre una determinada enfermedad infecciosa grave y fácilmente transmisible a otras personas. Sí, el enfermo le ha podido facilitar al médico en la más absoluta de las intimidades y con absoluta confidencialidad esta información; pero el médico actuaría con total irresponsabilidad si no actuara en consecuencia poniendo en cuarentena a dicho paciente. Esto, a mi entender y creo que del de todos, sería una actuación "apropiada" ante una información facilitada confidencial y protegida. Lo mismo sucede en el campo de la aviación; en ocasiones el regulador también deberá actuar ante determinada información recibida y analizada, con el fin de evitar un mal mayor, o de lo contrario caería en una irresponsabilidad que le sería achacable.

32. Por último, no podría cerrar este apartado de la protección de la información y de sus fuentes, sin antes mencionar el término "cultura justa" –*just culture*, acuñado en Europa y Norteamérica. Como se ha mencionado, los sistemas de gestión de seguridad son algo más que un sistema, y requieren de una cultura organizacional apropiada como conveniente caldo de cultivo para que los SMS florezcan. Según Eurocontrol y la reciente regulación europea en materia de navegación aérea y notificación de sucesos, el término cultura justa se definiría como: "*Una cultura en la que el personal operativo de primera línea u otras personas no son castigados por sus acciones, omisiones o decisiones adoptadas en consonancia con su experiencia y formación, pero en la que la negligencia grave, las violaciones intencionadas y los actos destructivos no son tolerados*." Es decir, una cultura justa no equivale a una cultura no-punitiva. Una cosa es que se premie y se aliente notificar deficiencias de seguridad sin miedo a recibir por ello represalias, y otra es que esto suponga una carta blanca para que cualquier actuación pueda quedar impune por el simple hecho de haber sido notificada. Evidentemente, la clave estará en saber transmitir e identificar qué resulta una conducta aceptable y qué resulta inaceptable; en otras palabras, en saber definir y transmitir la línea roja que no se debe cruzar, y que en caso de cruzarse y notificarse, la información comunicada no se encuentre protegida. La solución más bien vendrá de la mano de tratar de identificar quién o quienes deben ser los responsables de tomar una decisión al respecto y con qué metodología, en lugar de tratar de definir y tipificar un conjunto de escenarios o situaciones clasificándolos entre aceptables e inaceptables; cuestión esta última deseable, pero inabordable dado el número infinito e impredecible de posibles situaciones que se pueden presentar en todos los ámbitos de la aviación civil.

33. Mención aparte tienen los esfuerzos realizados durante los últimos años por parte de la comunidad aeronáutica para evitar lo que se ha venido en denominar la criminalización del error humano (bienintencionado y conmensurable a la formación y experiencia del individuo). Tales esfuerzos han consistido principalmente en intentar modificar la legislación aplicable y difundir o comunicar a los jueces y fiscales, y a la sociedad en general, las implicaciones que tiene sobre la seguridad el incriminar a profesionales de la aviación por causa de los accidentes.

34. En lo que se refiere a la evaluación del riesgo, primero hay que aclarar su definición. Se entiende por riesgo la probabilidad y severidad predictivas de las consecuencias o resultados de un peligro. La noción de riesgo supone por tanto ambas cuestiones: incertidumbre y algún tipo de pérdida o daño que puede llegar a producirse. De acuerdo con esta definición, un peligro sería todo aquello que pudiéramos identificar como la fuente de un riesgo real o potencial; por ejemplo, viento lateral racheado en pista. El peligro existe como tal fuente, y el riesgo supone evaluar la probabilidad de que este peligro se convierta en un daño real o pérdida. Para lidiar con el riesgo empleamos medidas de control y mitigación del mismo, pero reconociendo siempre que aun pudiéndolo reducir, nunca lo podremos igualar a cero (a no ser que se cese la operación); toda actividad humana conlleva asumir un determinado riesgo ineludible.

35. En definitiva, en el proceso de evaluación de riesgos tratamos de dar contestación a las siguientes preguntas: ¿Qué puede suceder? ¿Cómo de probable? Y si finalmente ocurre, ¿qué consecuencias?

36. Otra cuestión interesante de resaltar, es que el riesgo depende del observador, y de lo que éste conoce o desconoce. Sin querer entrar en disquisiciones filosóficas, lo importante de esta apreciación es reconocer que nuestro proceso de evaluación de riesgo dependerá mucho de la información de la que dispongamos, y de ahí se infiere la importancia de la cantidad y calidad de los datos recopilados por nuestros sistemas de captación de datos de seguridad a los que anteriormente nos hemos referido.

37. De acuerdo con la anterior definición de riesgo, deberíamos preocuparnos de tratar de identificar peligros (fuentes de riesgo) en nuestros sistemas de recopilación de datos de seguridad para después en nuestro análisis, evaluar la probabilidad de que se produzca un determinado escenario y las consecuencias, en términos de daños (severidad) de dicho escenario. Las medidas de mitigación irían por tanto dirigidas, a reducir la probabilidad o severidad de estos riesgos asociados, caso de encontrarse en una región inaceptable de acuerdo con el diseño de nuestro sistema.

38. Con esta perspectiva in mente, interesaría captar en nuestros procesos de recopilación de datos de seguridad no sólo información reactiva (un incidente o fallo de componente o subsistema ya producidos) sino también información preventiva acerca de peligros que de momento no han supuesto que se produzcan ningún evento de seguridad reseñable. Además, este tipo de información no va aparejada de ninguna carga de culpabilidad, porque el evento en sí, todavía no se ha producido, y por tanto, es más sencillo que nos la notifiquen sin ningún temor a ningún tipo de represalia. Desafortunadamente, la mayoría de los sistemas de captación de datos en la actualidad, recopilan principalmente información de tipo reactiva.

39. Los procesos utilizados en aviación para evaluar el riesgo suelen consistir en matrices de riesgo en términos de probabilidad y severidad, con distintas regiones dibujadas distinguiendo en la matriz lo que corresponde a una región inaceptable o aceptable, y su frontera o región intermedia. Esta representación del riesgo permite distinguir gráficamente entre escenarios de baja probabilidad y alta severidad, de los de alta probabilidad y baja severidad, por poner un ejemplo. Además, sirven como una buena herramienta de comunicación dado que resulta muy intuitiva.

40. En relación a esta misma cuestión se han desarrollado diversas metodologías, sencillas de implementar, tales como RAT (*Eurocontrol Risk Analysis Tool*), o la desarrollada por ARMS (*Aviation Risk Management Solutions*), que tiene en cuenta la eficacia de las barreras que siguen existiendo entre evento de seguridad y el accidente más creíble.

41. No obstante, varias críticas se pueden realizar de estos sistemas de clasificación de riesgo. La primera es que, en términos de probabilidad, lo que se suele utilizar realmente es una tasa de fallo o de evento, en lugar de entender la probabilidad como una medida de nuestro grado de creencia de que se produzca un escenario futuro (como resultado de un peligro determinado). Además, se simplifica lo que en realidad son distribuciones de probabilidad y de severidad por sus esperanzas matemáticas o medias, que suponen nuestro "disparo" en una matriz bidimensional, cuando en realidad lo que tendríamos es una familia de curvas que relacionaría las distintas severidades con su frecuencia de ocurrencia, y una determinada creencia o probabilidad asociada a cada curva, normalmente expresada mediante un porcentaje de confiabilidad o intervalo de confianza. Obviamente, con la simplificación que supone el disparo en la matriz perdemos mucha información al respecto y mucho más si como a veces se hace, se compara un único escalar multiplicando probabilidad por severidad.

42. Por otro lado, en relación a la evaluación del riesgo el Doc. 9859 de la OACI recoge, que para realizar la evaluación del riesgo debemos de tener en cuenta el caso más desfavorable creíble. Y aquí volvemos a tener los mismos problemas citados anteriormente. Es decir, tratar se simplificar curvas de riesgo por un único escalar, y saber qué se debe entender por "caso más desfavorable creíble". Además, uno podría preguntarse por qué debo de controlar los riesgos asociados al caso más desfavorable creíble, y si en tal caso estaría sobre-protegiendo mi sistema con medidas que resultarían poco eficientes.

43. Todo lo anterior nos hace concluir, que en materia de evaluación de riesgo todavía contamos con un gran margen para investigar y refinar nuestros procedimientos para el cálculo cuantitativo del riesgo. Esto no significa que lo hasta ahora realizado no sirva, o que tengamos que paralizar nuestros cálculos hasta dar con una metodología más refinada. Lo que sí indica es que debemos ser conscientes de las simplificaciones que estamos realizando hoy en día, y manejar el concepto de riesgo con rigor científico.

44. En cuanto a las Medidas de mitigación y control del riesgo, interesa resaltar al menos dos aspectos. El primero está ligado a la noción de aceptabilidad o inaceptabilidad del riesgo. El segundo, al papel que juega este tipo de medidas en el estado (SSP) versus el papel de este mismo tipo de medidas en la industria (SMS).

45. En cuanto al primer aspecto, se ha de tener en cuenta que la aceptabilidad o inaceptabilidad del riesgo, en términos absolutos, carece de sentido. Ello se debe a dos cuestiones principalmente. La primera es puramente práctica, dado que, como acabamos de ver, la noción de riesgo como una medida lineal y escalar fácilmente comparable, resulta bastante desacertada. La segunda, se refiere a que la cuestión de aceptabilidad de riesgo debe venir acompañada de un determinado problema de decisión. Es decir, el riesgo resultará ser aceptable o inaceptable, dependiendo de lo que me cueste reducirlo (y sí, se puede expresar

en términos económicos) y de los beneficios (o disminución de beneficios) que me puede suponer tal reducción. O dicho de otro modo, uno acepta un riesgo determinado dependiendo del beneficio que vaya a poder obtener al exponerse a dicho riesgo. Y el riesgo resultará aceptable o inaceptable, dependiendo de si se puede o no obtener ese mismo beneficio exponiéndome a un riesgo menor.

46. Por complicarlo todo un poco más (lamentablemente la realidad es así de compleja), el problema de decisión asociado al riesgo puede ser multi-objetivo, y tener que considerar otros tipos de riesgo (por ejemplo, el financiero, el medioambiental o el de *security*) aparte del riesgo de seguridad operacional. Si es una decisión que adopta una única persona podemos hablar de distintas curvas de aversión o afición al riesgo. Y hasta podríamos estar hablando de decisiones colaborativas, en las que se tienen que tener presentes los distintos intereses (utilidades) o actitudes frente al riesgo de aquellos que adoptan las decisiones.

47. En la práctica, el ser consciente de que el proceso de evaluación del riesgo debe venir ligado a un problema de decisión, ha supuesto que algunas empresas estén enfrentándose a las medidas de mitigación y control del riesgo no aisladamente, sino ligadas a una evaluación coste-beneficio para la empresa. Y este enfoque está resultando verdaderamente efectivo.

48. El otro aspecto a destacar en lo que se refiere a las medidas de mitigación y control del riesgo es que, mientras que el estado con su SSP debe intentar atajar con este tipo de medidas las causas comunes de un determinado tipo de ocurrencia, la industria con su SMS debe por el contrario tratar de atajar las causas particulares o específicas de dicha ocurrencia, que normalmente estarán ligadas a las particularidades de la organización y al contexto en que desarrolla su actividad.

49. El estado no debe promulgar normativa pensando en las causas particulares de una organización en concreto, en cuyo caso estaría exigiendo adoptar medidas ineficientes a casi toda su industria. Esto nos lleva a comprender que la regulación no puede tener en cuenta todas las particularidades en las que se desenvuelve la industria. Donde no llega la regulación, contamos con el SMS; éste sistema es el que debe abordar las cuestiones particulares de una ocurrencia. Así por ejemplo, en el nivel Estado tendríamos la exigencia de llevar embarcado un equipo de anticolisión a bordo –ACAS/TCAS (para evitar colisiones en el aire) o sistemas de alarma de aproximación al terreno EGPWS (para evitar colisiones con el terreno – del tipo CFIT), y en el nivel proveedor, tendríamos por ejemplo la obligación de contar con los sistemas de auto-reversa o de auto-freno operativos para realizar operaciones con destino a un aeropuerto que carece de área de seguridad de extremo de pista (RESA).

50. Esta concepción de los distintos papeles que deben jugar uno y otro sistema (SSP vs. SMS), nos lleva a comprender que uno sin el otro no tienen mucho sentido. Ambos se encuentran interconectados y uno viene a suplir las áreas en las que el otro no alcanza. También nos advierte de la responsabilidad compartida que

en materia de gestión de seguridad tienen estado e industria. Este mismo concepto ha llevado en los últimos años a pasar de una regulación prescriptiva a una regulación basada en el desempeño, en la que se tiene en cuenta el espacio libre de actuación que se debe permitir a la industria, con el objeto de que gestione la seguridad con la complejidad y detalle que conlleva su contexto de operación. Y todo ello sin abandonar, sino complementar, el enfoque tradicional de verificación del cumplimiento de unos determinados requisitos normativos, pero adaptado al tamaño, naturaleza y perfil de riesgo del proveedor, y su capacidad para gestionar la seguridad de forma efectiva.

51. Este devenir de la regulación está suponiendo un auténtico reto a las autoridades de aviación civil para adaptar la cualificación de su personal de forma que sea capaz de evaluar y certificar sistemas (software) en lugar de productos (hardware). Y además, evaluar sistemas adaptados a su contexto en particular; todo un desafío.

52. Nos estamos adentrando en un contexto en el que cumplir con la norma (requisitos prescriptivos) ya no significa necesariamente ser seguro, y en el que hay que saber mirar más allá de la norma y considerar el rendimiento de mis sistemas de gestión de seguridad.

53. El paso de un sistema prescriptivo a un sistema basado en el desempeño conlleva necesariamente tener a disposición un modo de medir el rendimiento de mi sistema de gestión de seguridad (tanto SMS como SSP) a lo largo del tiempo y de las medidas de mitigación del riesgo implantadas. Ya hemos comentado que los reguladores deben adaptar su sistema de supervisión y vigilancia de la seguridad operacional a un sistema basado en el perfil de riesgo del proveedor y convenientemente soportado por datos (convenientemente informado).

54. Para ello se utilizan los denominados indicadores del rendimiento de la seguridad – o SPIs. En consecuencia, la implantación de los sistemas de gestión de seguridad nos lleva en la práctica a tener que definir unos indicadores que nos permitan tomar el pulso al rendimiento de nuestros sistemas; el estado a nivel macro, y la industria a nivel micro. Indudablemente, uno y otro nivel de rendimiento, nivel estado y nivel industria, hasta cierto punto, deben estar relacionados, dado que, como ya hemos apuntado, el SSP y el SMS se encuentran interconectados.

55. En relación a los indicadores se han establecido varias aproximaciones y clasificaciones. No es mi intención hacer una descripción académica de todas las aproximaciones y clasificaciones propuestas. Desde un punto de vista pragmático, se utilice la clasificación o tipología que se considere oportuna, la definición y establecimiento de estos indicadores debe estar dirigida a los procesos internos de mi sistema de gestión de seguridad (gestión de riesgo y aseguramiento de la seguridad), y deben por tanto ser útiles para medir el rendimiento de estos procesos y no sólo los resultados.

56. Resulta no obstante interesante mencionar los que recientemente se han venido a denominar indicadores precursores, siendo éstos métricas que miden los fallos del sistema y los eventos menos severos (y más probables) que no se manifiestan en graves incidentes o accidentes, pero que, cuando se combinan con otros eventos, el análisis pormenorizado de los datos muestra que tienen el potencial de dar lugar a un incidente grave o accidente; es decir, existe una correlación estadística entre este tipo de indicadores y los incidentes graves o accidentes. Algunos esfuerzos con relativo éxito se han venido realizando en los últimos años para tratar de identificar este tipo de indicadores, que en caso de poderse precisar, vienen a suponer el cumplimiento del sueño de cualquier analista de riesgo; contar con una bola de cristal con la cual ser capaz de vaticinar y anticiparse con ciertas garantías al futuro accidente.

57. Un enfoque práctico a la hora de establecer los indicadores de rendimiento de la seguridad sería por ejemplo tratar de identificar una decena de indicadores por ámbito de actividad del proveedor, a la que habría que adicionar, en el caso de que cada proveedor, los que se considerasen oportunos dependiendo de las especificidades de su contexto de operación y del grado de madurez de su sistema de gestión de seguridad. La decena de indicadores (por ámbito) le permitirían al estado medir el rendimiento de su SSP, mientras que esta misma decena más los adicionados, le permitirían al proveedor medir el rendimiento de su SMS. Este enfoque debería irse adaptando paulatinamente, a medida que la madurez de los sistemas de gestión de seguridad de estado e industria se fueran depurando con el tiempo; aventurando, en consecuencia, un mayor grado de afinamiento.

58. Como conclusión a esta primera sección, se puede afirmar que los sistemas de gestión de seguridad supondrán, sin duda, un importante avance en la mejora de los niveles de seguridad del transporte aéreo. No obstante, la implantación de estos sistemas, tanto en la industria como en el Estado, todavía se encuentra en una fase muy incipiente, y por tanto, es pronto todavía para recoger la fruta madura de la mejora que supondrán estos sistemas. Su implantación práctica supone reconocer al elemento humano en el centro de estos sistemas, y prestar atención a aspectos tales como la cultura de seguridad de las organizaciones y a los factores humanos.

59. Los procesos que suponen el nudo gordiano de estos sistemas, se alimentan de información y datos de seguridad, y resulta indispensable velar por la captación y recopilación de este tipo de datos; lo que en la práctica conlleva establecer disposiciones normativas y procedimientos con el objeto de proteger tanto la información recopilada (o por recopilar) como al notificante.

60. El análisis de los datos y la evaluación del riesgo adolecen muchas veces del correspondiente rigor científico, y todavía hay terreno para avanzar en el desarrollo de metodologías prácticas de utilizar, tanto para el proveedor como para el estado. La medición del desempeño de estos sistemas mediante de la definición de unos indicadores de rendimiento, también se encuentra en una fase

de madurez muy embrionaria, y nos queda por tanto un largo camino por explorar.

61. No obstante, a pesar de sus complicaciones prácticas e imperfecciones, la implantación de estos sistemas ya está dando parte de los resultados esperados. La autoridad, aplicando un enfoque holístico y sistémico (basado en la definición de perfiles de riesgo) a la supervisión de la seguridad operacional y empleando las disposiciones normativas como una herramienta de control y mitigación de riesgo a gran escala. La industria por su lado, refinando sus herramientas y heurísticas utilizadas en los procesos de análisis de datos y evaluación de riesgo, y atajando cada vez más aguas arriba las deficiencias de seguridad precursoras o desencadenantes de eventos de seguridad más severos. Ambos sistemas, SSP (estado) y SMS (industria), se buscan y se complementan, en un reparto proporcional de responsabilidades.

62. El futuro inmediato está repleto de retos. Debemos apoyar y dirigir la implantación de estos sistemas en la industria y debemos reconocer que esta implantación será lenta y paulatina dado que afecta a conductas, hábitos, y culturas organizacionales. Las autoridades debemos preparar a nuestro personal y capacitarle para ser capaz de evaluar y certificar estos sistemas, y desarrollar una supervisión basada en el rendimiento de los SMS. Debemos mejorar los sistemas de intercambios de datos de seguridad con la industria y de información de seguridad con otras autoridades. Debemos mejorar nuestras metodologías de evaluación de riesgo y nuestros procesos de medición del rendimiento de estos sistemas. Debemos, en definitiva, pasar de un enfoque reactivo sobre la seguridad, a un enfoque preventivo y predictivo. Debemos hacer todo esto y más, pero también saber mirar hacia atrás y reconocer el camino que llevamos recorrido; caminamos por la buena senda y resultará muy interesante y altamente gratificante alcanzar nuestro punto de destino.

Pablo Hernández-Coronado Quintero
Director de Evaluación de la Seguridad y Auditoría Técnica Interna
Agencia Estatal de Seguridad Aérea (AESA)
phernandez@seguridadaerea.es

2. AGRADECIMIENTOS

1. Esta guía no hubiera sido posible sin la inestimable ayuda y aportación del Comandante Daniel Mauriño, quien lleva años colaborando con AESA y con quien seguimos manteniendo una estrecha colaboración de la que estamos profundamente orgullosos y de la que nos vanagloriamos; muchas gracias Daniel por tu valiosísima contribución, no sólo a esta guía, si no a la mejora de la seguridad de la aviación civil en España y en todas las regiones del Planeta.

3. INTRODUCCIÓN

1. La responsabilidad de la implementación de un sistema de gestión de la seguridad operacional (SMS, *Safety Management System*) por parte de un proveedor se servicio surge de la normativa emanada por la Organización de Aviación Civil Internacional (OACI), cuya aplicabilidad se remonta en principio a noviembre de 2006 y más recientemente a noviembre de 2010. Es asimismo una responsabilidad que surge de normativa similar establecida por EASA (*European Aviation Safety Agency*).

2. La fuente conceptual de SMS se encuentra en una disciplina de las ciencias de la ingeniería conocida por su término inglés *system safety*, o *seguridad de sistema*, cuyos orígenes pueden rastrearse a los finales de la Segunda Guerra Mundial, con las primeras experiencias en cohetería, y más formalmente al inicio de la exploración espacial hacia los finales de la década del 50. *System safety* es una disciplina integrada por conocimientos y actividades de ingeniería (*engineering*) y gestión (*management*), aplicados en forma combinada. El objetivo de *system safety* es contribuir a la seguridad operacional del sistema, cualquiera sea el sistema en cuestión, una vez que éste se vuelve operativo, introduciendo seguridad operacional *a priori*, es decir, "diseñando" seguridad operacional en el sistema durante su concepción y desarrollo.

3. Para lograr tal objetivo, *system safety* le presta seria atención a factores que son típicos del diseño de un sistema, que a veces entran en competencia – cuando no en conflicto – entre sí. Estos factores incluyen costes de desarrollo, cronogramas, fiabilidad del diseño propuesto, etc. No obstante toda la importancia que le asigna a la fase de diseño, *system safety* desdobla su quehacer, y concentra similar nivel de atención a la operación proyectada del sistema. Esto se debe a que es durante la operación donde las herramientas (tomando el término en el más amplio sentido) que necesitan tanto el sistema como los operadores del mismo interactúan en formas que pudieron no haber sido anticipadas por los diseñadores, con el consiguiente impacto en la seguridad de las operaciones.

4. La diferencia básica entre *system safety* de los años 50 y la actual gestión de la seguridad operacional a través de SMS es que, debido a sus orígenes como herramienta de apoyo a la exploración espacial, que estaba basada en tecnología en el mejor de los casos híbrida, las actividades orientadas a la ingeniería eran casi excluyentes en *system safety*; es decir, *system safety* se concentraba principalmente en las potenciales consecuencias para la seguridad operacional de los aspectos y componentes tecnológicos del sistema en consideración, a veces a expensas del componente de gestión, e invariablemente a costa del componente humano (recuérdese que la primera versión de la cápsula *Mercury* no tenía ventanillas para el ocupante). En cambio, la gestión de la seguridad operacional a través de SMS amplía la perspectiva (y por consiguiente el dogma) para incluir la consideración de Factores Humanos y el desempeño humano (*human performance*) como factores fundamentales para la gestión de la seguridad operacional del sistema durante su diseño y posterior operación.

5. Hay coincidencia en la literatura sobre *system safety* en cuanto a los dos procesos básicos y genéricos sobre los cuales se fundamenta un sistema de gestión que apoya la provisión de servicios: tales procesos son la *gestión de riesgos* y la *garantía de entrega*. En el caso del SMS, que es un sistema de gestión de la seguridad operacional en apoyo a la provisión de servicios de aviación comercial, la adaptación de estos dos procesos básicos y genéricos a la gestión específica de la seguridad operacional lleva a sus designaciones como *gestión de riesgo de seguridad operacional* y *aseguramiento de la seguridad operacional* respectivamente.

6. En la literatura sobre *system safety* hay también coincidencia en cuanto a que el desarrollo y la operación permanente de los dos procesos básicos de un sistema de gestión que apoya la provisión de servicios no puede tener lugar en el vacío institucional. A no ser que se hayan establecido arreglos institucionales que sirvan como cimiento y faciliten la implementación y el mantenimiento efectivo – en el caso de SMS – de la gestión de riesgo de la seguridad operacional y del aseguramiento de la seguridad operacional, el mantenimiento de estos dos procesos básicos y, más importante aún, de sus actividades subyacentes, es una verdadera misión imposible. Distintas fuentes de lectura sobre *system safety* sugieren variantes en cuanto a la designación de estos arreglos institucionales. No obstante, una generalización de las variantes de designación adaptadas para el caso de SMS sugiere dos rótulos generales para los arreglos institucionales que funcionan como cimiento de SMS: *política y objetivos de seguridad operacional*, y *promoción de la seguridad operacional*.

7. Los alineamientos generales de las normativas sobre SMS emitidas respectivamente por OACI y la Comisión Europea (EASA) son – como no podría ser de otra manera – similares en cuanto a los dos procesos básicos y los arreglos institucionales necesarios en apoyo de los mismos. No obstante, hay algunas diferencias en el énfasis asignado a ciertas actividades específicas relacionadas con la operación de SMS entre la normativa de OACI y la de EASA. Por ello, la adherencia al dogma básico propuesto por la literatura sobre *system safety*, adaptado de acuerdo a lo propuesto por los párrafos anteriores a los imperativos de SMS, hace que el material contenido en esta Guía satisfaga las necesidades de implementación de SMS por los operadores españoles bajo ambas normativas.

8. Tal necesidad es esencial, porque es imprescindible recordar que la normativa EASA, aun cuando su importancia e influencia en el contexto mundial es de vasto alcance, es regional en cuanto a su competencia legal. La normativa OACI, en cambio, es de competencia legal internacional. Debido a ello, para operaciones fuera del ámbito de competencia legal de EASA, de suscitarse diferencias entre la normativa OACI y EASA, la normativa OACI prevalecerá, en función del instrumento legal internacional conocido como Convenio de Aviación Civil Internacional (o Convenio de Chicago), del cual todos los países bajo EASA, incluyendo España, son signatarios.

9. Siguiendo con el hilo de la discusión sobre los aspectos normativos y de competencias, es importante clarificar cuál es el valor real de la notificación de

diferencias por un Estado signatario del Convenio de Chicago a la OACI, en caso de asimetrías entre las normas internacionales y la transposición de tales normas a la normativa nacional o regional para su cumplimiento por las organizaciones aeronáuticas nacionales o regionales.

10. Las normas de OACI son de cumplimiento obligatorio para operaciones internacionales. Su no cumplimiento significaría que las aeronaves de un operador estarían operando sin un certificado de operación válido – aun cuando lo tuviese – fuera del ámbito de competencia de la autoridad certificadora. Aun cuando un Estado hubiese notificado una diferencia a la OACI sobre cualquier aspecto de la normativa SMS, o cualquier otra normativa, tal notificación es a *efectos informativos solamente* y no exime del cumplimiento de la norma por el operador que brinda servicios internacionales, ni resguarda de las potenciales consecuencias legales en cuanto al incumplimiento. Es fácil advertir la seriedad de la situación, y de ahí la decisión de basar el material en esta Guía en alineamientos de validez universal, en vez de únicamente en alineamientos particulares adoptados por una autoridad u otra. Un operador que implemente su SMS siguiendo los alineamientos ofrecidos por esta Guía cumplirá con la normativa OACI así como con la normativa Europea.

11. La Guía de Implementación SMS de la Agencia Estatal de Seguridad Aérea (AESA) para operadores se divide en cinco capítulos, que reflejan la fundamentación dogmática, los procesos básicos y los arreglos institucionales necesarios para apoyar la implementación y mantenimiento efectivo de SMS por un operador. El capítulo de apertura presenta la fundamentación sobre la cual se construye SMS. Los dos capítulos subsiguientes abarcan los dos procesos básicos de SMS (gestión de riesgos de seguridad operacional y aseguramiento de la seguridad operacional respectivamente) y sus actividades subyacentes. Los dos capítulos finales abarcan los arreglos institucionales necesarios para apoyar la implementación y mantenimiento efectivo de un SMS (política y objetivos de seguridad operacional, y promoción de la seguridad operacional respectivamente) y sus actividades subyacentes.

12. El material contenido en la Guía incluye ejemplos prácticos de aplicación a los efectos de facilitar no solamente la comprensión sino también apoyar la implementación de las actividades. Los procesos y arreglos institucionales, y sus actividades, presentan un verdadero plan de vuelo para la puesta en marcha de SMS, o para la reacomodación de procesos, arreglos institucionales y actividades ya existentes dentro de un operador para satisfacer los requerimientos combinados de implementación de SMS. La Guía incluye un apéndice que contiene bibliografía así como portales informáticos referidos a SMS.

13. No es inoportuno recordar el objetivo que inspiró la redacción de esta Guía. El objetivo de la Guía es presentar y clarificar los fundamentos conceptuales de los procesos que han de establecerse por un operador para implementar su SMS, de sus elementos constitutivos, y sus actividades subyacentes, sin especificar más que en términos globales *cómo* han de establecerse elementos y actividades. Dicho de otra manera, la Guía no es prescriptiva. Por ejemplo, la Guía desarrolla

conceptualmente las actividades subyacentes a "procesos de identificación de peligros" y proporciona ejemplos, pero no prescribe un método como el más adecuado para identificar los peligros. La razón es triple. Por un lado, la disponibilidad del *Manual OACI de gestión de la seguridad operacional* (Doc. 9859), que es altamente prescriptivo, suple esta necesidad. Segundo, los métodos que son útiles para un operador pueden no serlo para otros. Tercero y quizás lo más importante, AESA considera que hay abundante conocimiento, experiencia y relativo estado de madurez entre los operadores españoles como para no necesitar un *"abc"* de la implementación de SMS. La perspectiva de AESA es que la necesidad actual es la clarificación de aspectos y unificación de criterios, cuya más completa apreciación es decisiva en el éxito de la implementación de SMS por un operador. A esto último apunta fundamentalmente esta Guía.

14. Para concluir esta introducción, es necesario reconocer que el cuadro relativo a SMS en la escena internacional es uno de sumo dinamismo. Se trata de una situación en constante evolución, en la medida en que la industria mundial adquiere realimentación producto de las experiencias diarias de los operadores en actividades de desarrollo, implementación y operación de SMS. Por ello, esta Guía es un documento vivo, que será modificado según lo impongan las circunstancias de manera tal que su contenido mantenga constante validez y vigencia. Las consultas y comentarios sobre la Guía y sus contenidos deben ser dirigidos a la dirección de correo electrónico peso.aesa@seguridadaerea.es.

4. CAPÍTULO 1: SISTEMA DE GESTIÓN DE SEGURIDAD OPERACIONAL (SMS): LOS FUNDAMENTOS

4.1 SEGURIDAD OPERACIONAL, PROVISIÓN DE SERVICIOS Y RECURSOS

1. A lo largo de su historia, la tradición aeronáutica ha desarrollado un amplio espectro de nociones sobre la seguridad operacional, que van desde lo filosófico en un extremo al estereotipo en el extremo opuesto. Este amplio espectro puede sintetizarse en el axioma más atesorado – o por lo menos más proclamado – por la comunidad de aviación sin excepción: en aviación, la seguridad operacional es la primera prioridad (*safety first; safety is the first priority*).

2. El axioma es social, ética y moralmente impecable, debido a su reconocimiento inherente del valor supremo de la vida humana. A pesar de ello, la visión que el axioma transmite se hace difícil de sustentar en forma práctica durante las operaciones diarias de la industria aeronáutica, sin que esto signifique caer en un juicio inmoral. Las razones del tan difícil sustento del axioma en la aplicación diaria se hacen evidentes cuando se las considera bajo la perspectiva de *system safety* a que se ha hecho alusión en la Introducción a esta Guía. Como prólogo a tal consideración, una premisa es rigor medular: *las cuestiones de seguridad operacional de la aviación no son ni inherentes ni son condición natural de las operaciones de vuelo. Tales cuestiones son el resultado colateral, por parte de las organizaciones de la industria, de las actividades necesarias para la provisión de servicios a efectos de lograr un producto.*

3. La literatura de *system safety* postula categóricamente que todo sistema se concibe y pone en marcha con un objetivo de producción, vale decir, para generar un producto (*output*) mediante la entrega de servicios. El sistema en cuestión puede abarcar desde una biblioteca pública (cuyo producto es el enriquecimiento intelectual de la población, por medio del préstamo gratuito de libros para su fácil acceso por la mayor cantidad de lectores) a una línea aérea (cuyo producto es la generación de dividendos para sus accionistas y/o dueños, por medio del transporte aéreo de personas y/o mercancías).

4. A los efectos de la consideración de la ubicación jerárquica de la seguridad operacional entre las prioridades de las organizaciones de aviación, es necesario considerar la *provisión de servicios*. La misma tiene lugar dentro de contextos operativos específicos que incluyen componentes naturales, tales como la meteorología, eventos geofísicos, tales como erupciones volcánicas, orografía, etc. Los contextos operativos incluyen también componentes técnicos, tales como equipamientos, combustibles, materiales, etc. Los componentes técnicos son las herramientas necesarias para la provisión de servicios. Tanto componentes naturales como componentes técnicos pueden, según determinadas combinaciones de circunstancias específicas, según ciertas *interacciones*, convertirse en escollos de un tipo u otro para la provisión de servicios (y por lo tanto para el logro del producto): la meteorología se puede tornar adversa, ciertos eventos geofísicos pueden imponer demoras y/o cancelaciones, el equipamiento puede fallar, el combustible que hace funcionar al equipamiento puede incendiarse o explotar, etc.

5. El párrafo anterior permite una doble conclusión. Primero, es evidente que, dada la naturaleza dinámica y cada vez más compleja de los contextos operativos en los cuales la provisión de servicios aeronáuticos tiene lugar, es cada vez más difícil anticipar – y muchísimo más difícil eliminar – *todas* las consecuencias no deseadas de *todas* las posibles *interacciones* entre *todos* los componentes naturales y técnicos del contexto operativo. Segundo, los componentes en cuestión no solamente son inherentes al contexto operativo (la meteorología, los eventos geofísicos) sino, como herramientas del sistema, también *necesarios* para la entrega de servicios (el equipamiento, el combustible).

6. Para lograr la entrega de servicios, el sistema (por ejemplo, la línea aérea) debe controlar, al máximo grado posible, tanto componentes naturales como técnicos y sus interacciones. Para ello, debe poner en marcha mitigaciones contra las posibles consecuencias de las interacciones entre los componentes que pueden generar situaciones adversas a la provisión de servicios. Para ello, debe adjudicar recursos como sustento para la puesta en marcha y el mantenimiento de las actividades de mitigación.

7. Las situaciones adversas generadas por las consecuencias de las interacciones entre los componentes naturales y técnicos del contexto operativo son un peligro para la capacidad de un sistema de alcanzar su producto mediante la entrega de servicios. La adjudicación de recursos para la mitigación de las consecuencias de las interacciones entre componentes del sistema es sin duda una de las decisiones más delicadas que enfrentan quienes administran el sistema. Se trata de una decisión que involucra, en numerosas circunstancias, un difícil compromiso entre factores de variada naturaleza que pesan en las decisiones. Muy frecuentemente, las decisiones no son las óptimas desde el punto de vista axiomático de la seguridad operacional (absoluta prioridad de recursos a las actividades de seguridad operacional), sino las más razonables o tolerables bajo las circunstancias existentes al momento de tomar las decisiones en cuestión.

8. El compromiso en la decisión en cuanto a la adjudicación de recursos es inevitable porque no existe sistema cuyos administradores tengan acceso a recursos ilimitados para adjudicar a todas las actividades que apoyan la provisión de servicios: aún en los sistemas financieramente más sólidos, limitaciones presupuestarias de diverso tipo son realidades del diario decurso institucional. Más de una vez los administradores de un sistema deben, utilizando un dicho popular, desvestir a un santo para vestir a otro.

9. La complejidad de las situaciones bajo consideración, la confluencia de factores de muy distinta naturaleza, y la siempre presente limitación en la disponibilidad de recursos para asignar a actividades de mitigación de las consecuencias de las interacciones entre componentes del sistema son todos factores de significación. Por lo tanto, la única posibilidad que el compromiso en la toma de decisiones para la adjudicación de recursos se aproxime de manera realista a una adjudicación

equilibrada entre las distintas áreas de necesidad se basa en la disponibilidad de datos – de amplio espectro y naturaleza diversa – para apoyar tales decisiones.

10. Este es el dominio de competencia de SMS, y su real contribución al logro de los objetivos globales de un operador: la generación de los datos necesarios para apoyar la toma de decisiones estratégicas sobre la base de datos para la adjudicación de recursos institucionales, para mitigar las consecuencias de las interacciones entre componentes del sistema con potencial de generar situaciones que amenazan la capacidad del operador de alcanzar su producto mediante la entrega de servicios.

4.2 DOS PREGUNTAS CLAVES

11. Hay dos preguntas que se formulan frecuentemente sobre SMS. Una pregunta es: *"¿cuál es la diferencia entre SMS y un programa de prevención de accidentes?".* La compañera inseparable de la anterior es: *"¿qué tiene SMS de nuevo o diferente con respecto a lo que anteriormente se hacía en cuanto a seguridad operacional?".* Una clara respuesta a estas dos preguntas claves es esencial para basar el desarrollo, implementación y mantenimiento de SMS por un operador sobre cimientos sólidos.

12. Para responder a estos interrogantes, hay dos nociones cuya comprensión es fundamental. La primera es la caracterización de una empresa de aviación comercial como un *sistema de sistemas*. La otra es la diferencia entre *sistemas de gestión* y *programas de ejecución*.

13. Una empresa de aviación comercial es un sistema que como mínimo abarca siete sistemas de gestión tributarios:

    a) Sistema de gestión de la seguridad operacional;

    b) Sistema de gestión del medioambiental;

    c) Sistema de gestión de seguridad física *(security);*

    d) Sistema de gestión financiero;

    e) Sistema de gestión legal;

    f) Sistema de gestión de recursos humanos; y

    g) Sistema de gestión de la calidad.

14. Un *sistema de gestión* es un recurso institucional de apoyo a la toma de decisiones estratégicas por parte de los más altos niveles gerenciales de la empresa. El rasgo característico de un sistema tal es que el apoyo a la toma de decisiones está *basado en datos generados por el sistema de gestión.* Vale decir, las prioridades en la

adjudicación de recursos para contrarrestar deficiencias que tienen el potencial de amenazar la capacidad institucional de una efectiva provisión de servicios se deciden sobre la base de datos.

15. La naturaleza de los datos en cuestión dependerá del ámbito del sistema que se considere. Así, un sistema de gestión financiero es un sistema de colección y análisis de datos mayoritariamente (pero no exclusivamente) financieros, a los efectos de apoyar la toma de decisiones sobre aspectos financieros por parte de la conducción superior de la empresa; un sistema de gestión de la calidad es un sistema de colección y análisis de datos mayoritariamente (pero no exclusivamente) de calidad, a los efectos de apoyar la toma de decisiones sobre aspectos de la calidad de los servicios por parte de la conducción superior de la empresa, y así sucesivamente. Por lo tanto, un *sistema de gestión de la seguridad operacional* es un sistema de colección y análisis de datos mayoritariamente (pero no exclusivamente) de seguridad operacional, a los efectos de apoyar la toma de decisiones sobre aspectos de la misma por parte de la conducción superior de la empresa.

16. En virtud de lo expuesto en los dos párrafos anteriores, se concluye que SMS es el sistema tributario de gestión de la seguridad operacional con que cuenta el operador para adoptar decisiones estratégicas relativas a adjudicación de recursos para actividades que tienen que ver con la seguridad operacional, decisiones que se basan en datos.

17. Una vez que los datos han sido analizados y se ha extraído información e inteligencia de los mismos, la conducción superior del operador está en condiciones de adoptar decisiones de naturaleza estratégica en cuanto a prioridades de actividades y adjudicación de recursos para las mismas sobre la base de datos. Tales decisiones se materializan, se *ejecutan*, por medio de actividades llevadas a cabo bajo el rótulo de *programas de ejecución*.

18. En aviación, y más específicamente en lo que a seguridad operacional se refiere, los programas de ejecución se conocen como *programas de seguridad operacional*[1]. Típicos ejemplos de programas de seguridad (es decir, programas que ejecutan decisiones formuladas por los niveles gerenciales del operador) incluyen:

    a) Programa de instrucción en gestión de los recursos de la tripulación (*Crew Resource Management, CRM);*

    b) Programa de instrucción en gestión de amenazas y errores *(Threat and Error Management, TEM);*

    c) Programa de instrucción sobre mercancías peligrosas;

[1] En Europa, al programa de seguridad operacional ligado al EASP se le conoce como el "European Plan for Aviation Safety" (EPAS) y en España el plan ligado al SSP (PESO) se conoce como el "Plan de Acción de Seguridad Operacional" para el Estado (PASO).

d) Programa de competencias lingüísticas;

e) Programa de prevención de vuelo controlado contra el terreno *(Controlled Flight Into Terrain, CFIT);*

f) *Programa de pre*vención de accidentes durante aproximación y aterrizaje *(Approach and Landing Accident Reduction, ALAR);*

g) etc.

19. La exposición en los párrafos anteriores proporciona la respuesta a la primera de las dos preguntas claves presentadas en el primer párrafo de esta sección (*"¿cuál es la diferencia entre SMS y un programa de prevención de accidentes?").* SMS es el sistema de gestión que le permite al operador adjudicar recursos para un abanico de actividades relacionadas con la gestión de la seguridad operacional, mientras que un programa de prevención de accidentes es un conjunto de actividades específicas para prevenir pérdidas humanas o materiales, que están agrupadas bajo un programa de seguridad operacional específico. En síntesis, SMS es un sistema de gestión, un programa de prevención de accidentes es un programa de ejecución.

20. Al presente, la implementación por un operador de programas de seguridad operacional específicos no es necesariamente una respuesta a decisiones estratégicas sobre la base de datos, sino más bien es una respuesta a imposiciones normativas. En una gran mayoría de los casos, el origen de tales normativas no es siquiera de naturaleza nacional, sino más bien internacional, y es respuesta a deficiencias de seguridad operacional de naturaleza global. Estas deficiencias pueden ser prioritarias en determinados ámbitos nacionales o regionales específicos, pero pueden no serlo en otros, por lo menos al nivel en que lo son en los ámbitos que propulsaron la formulación de normativa internacional. No obstante, dado que se trata de normativa internacional, la transposición de la norma internacional a la normativa nacional es inevitable.

21. Bajo este estado de situación, un significativo número de operadores no cuenta con un mecanismo formal que permita evaluar, sobre la base de datos, la importancia específica a su contexto operativo de una deficiencia particular, su impacto en la seguridad operacional durante la provisión de sus servicios, y por ende, el valor agregado que podría aportar al operador la eventual normativa sobre el tema en cuestión. Ausente tal mecanismo, el operador no tiene otra alternativa que adjudicar recursos para implementar un programa de seguridad operacional que quizás no proporciona una respuesta a problemas de seguridad operacional de primacía para sus operaciones específicas, pero que debe implementar para alinearse con la normativa en vigor.

22. Lo expuesto en el párrafo anterior tiene una doble consecuencia. En primer lugar, el concentrarse en la implementación de programas de seguridad operacional para satisfacer imposiciones normativas que no son necesariamente una respuesta a

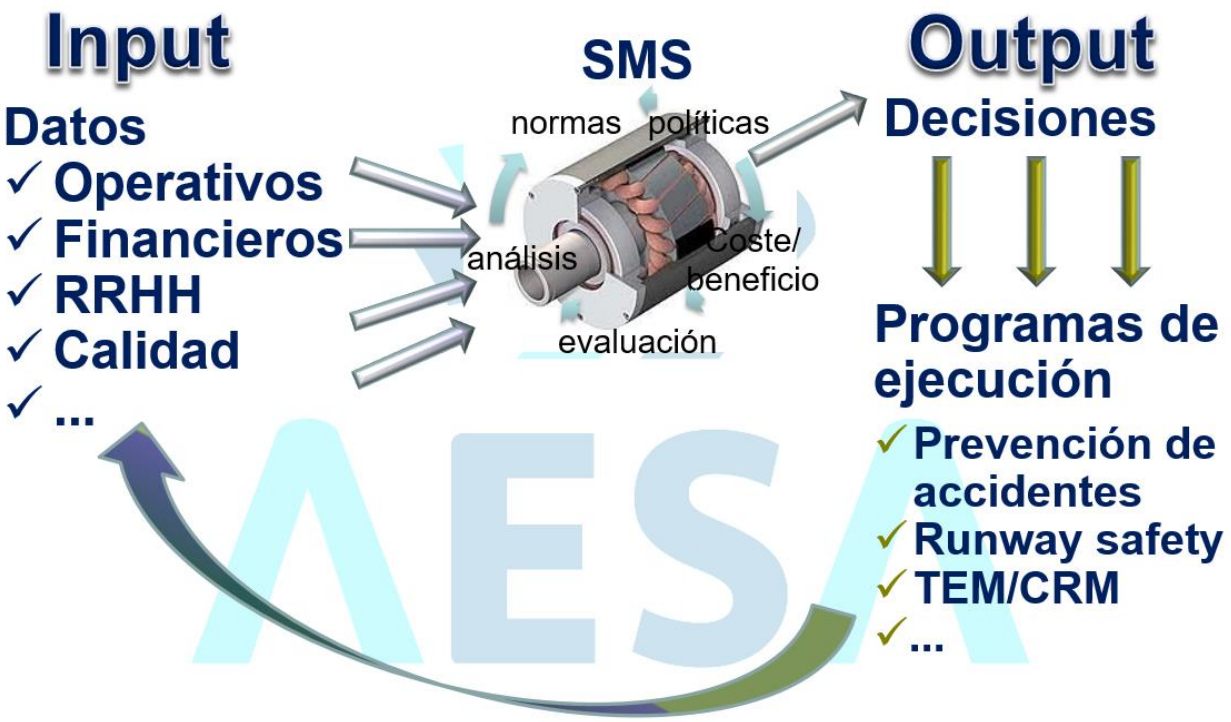
deficiencias de seguridad operacional que afectan específicamente al operador puede obstaculizar la identificación de deficiencias que *sí* afectan directamente al operador, generando una situación de precariedad en la gestión de la seguridad operacional. Segundo, puede forzar la adjudicación de recursos a actividades de relativa importancia para la seguridad operacional, distrayéndolos de otras actividades de real importancia, potencializando aún más la aparición de grietas en la gestión de la seguridad operacional.

23. Es ante esta situación que SMS genera un valor añadido. El operador, por medio del SMS, adquiere datos sobre deficiencias de seguridad específicas de su contexto operativo. Algunas deficiencias serán un espejo de deficiencias de naturaleza universal, otras serán exclusivas de particularidades específicas del operador y del contexto en el cual las actividades necesarias para la provisión de servicios tienen lugar. Esto le permite al operador adjudicar recursos para actividades relativas a la seguridad operacional que son respuesta a la identificación sobre la base de datos de problemas propios del operador.

24. Aun cuando la imposición normativa y su cumplimiento continuará siendo un imperativo y la base sobre la que se asienta el SMS, la disponibilidad de datos le permite al operador dar preponderancia a ciertos programas de seguridad operacional (y a la adjudicación de recursos para los mismos), con respecto a otros. En el futuro, cuando la implementación de SMS haya alcanzado madurez en la industria aeronáutica mundial, no es inimaginable el descarte, o por lo menos la minimización, de programas de seguridad operacional cuya imposición es de naturaleza normativa, cuando datos específicos del operador apoyen la conclusión que el problema de seguridad operacional para el cual el programa en cuestión es la respuesta no afecta la seguridad de la provisión de servicios para el operador particular.

25. Lo expuesto a partir del párrafo 20 brinda la respuesta a la segunda de las preguntas claves formuladas en el primer párrafo de esta sección capítulo (*"¿qué tiene SMS de nuevo o diferente con respecto a lo que anteriormente se hacía en cuanto a seguridad operacional?")*. La novedad que SMS trae en cuanto a actividades de seguridad operacional de otra naturaleza es que permite la concentración de los recursos para atacar problemas de seguridad operacional que son los que realmente afectan la seguridad de la provisión de servicios para el operador particular. El aspecto fundamental a no perder de vista es que como las decisiones sobre la asignación de recursos sobre actividades específicas están basadas sobre datos, son fácilmente *explicables y defendibles*.

26. Se presenta a continuación una visualización de lo expuesto en los párrafos precedentes en cuanto SMS y los programas de seguridad.



27. La visualización presenta al SMS como un generador. La analogía es apropiada, en cuanto SMS es un verdadero generador de información e inteligencia para la toma de decisiones sobre la adjudicación de recursos para actividades agrupadas como programas de seguridad operacional. El *input* que hace funcionar al "generador" son datos específicos del operador. Dado que se trata de un sistema de gestión de la seguridad operacional, la mayoría de los datos será de naturaleza operativa, pero habrá aporte de datos de naturaleza financiera, legal, de recursos humanos (RRHH), de calidad, etc. Dentro del "generador", los datos son evaluados y analizados teniendo en cuenta cuestiones normativas, de política (tanto institucional como nacional), de coste/beneficio, etc. El *output* del "generador" son decisiones, que se implementan por medio de programas de seguridad. Estos programas de seguridad representan una asignación de recursos formal y principista para la solución de problemas de seguridad que son los que el operador enfrenta en el contexto operativo en el cual tiene lugar la provisión de sus servicios. La vigilancia permanente de las actividades subyacentes a los programas de seguridad durante la provisión de servicios es a su vez una fuente de generación de datos que se convierte en input adicional al "generador", dando lugar así a un sistema de operación continúa.

28. En la visión de futuro, los programas de seguridad operacional de un operador implementados como consecuencia de decisiones estratégicas sobre adjudicación de recursos basadas en datos serán una combinación de programas en respuesta a problemas específicos del operador y programas implementados como respuesta a imposiciones normativas. Aun cuando hubiese preponderancia de programas de seguridad como consecuencia de imposiciones normativas, los mismos habrán sido ponderados y priorizados sobre la base de datos, para asegurar la mejor adjudicación de recursos posible.

4.3 DOS PROCESOS FUNDAMENTALES

29. Antes de iniciar la discusión introductoria sobre los dos procesos fundamentales sobre los cuales el operador construye su SMS, otra diferenciación es de importancia: la diferencia entre *procesos* y *actividades*.

30. Un *proceso* representa un marco de referencia conceptual que sirve de apoyo y proporciona una guía sistemática y ordenada para la puesta en marcha y ejecución de acciones específicas para lograr un objetivo predeterminado. Pero el proceso en sí mismo es una abstracción, no existe en forma visible en el mundo material.

31. Una *actividad*, por su lado, es una secuencia o serie de acciones que representan los medios materiales por medio de los cuales se logra el objetivo u objetivos pre-especificados por un proceso. Las actividades son acciones concretas y visibles en el mundo material, y pueden llevarse a cabo en forma individual y/o aislada, o pueden estar coordinadas bajo un rótulo común integrador, tal como es el caso con los programas de ejecución. Proponiendo una analogía deportiva, el proceso representaría los límites del campo donde se desarrollará el juego y las pautas bajos las cuales se jugará, mientras que las actividades (aisladas o agrupadas bajo un programa de ejecución) son los jugadores.

32. En el caso de la gestión de la seguridad operacional, los procesos guían el *cómo, cuándo* y *qué* de la colección y análisis de datos sobre los cuales se basarán las decisiones estratégicas sobre la adjudicación de recursos. Las actividades son el *cómo, cuándo* y *qué* de la práctica actual, de la puesta en marcha de las mitigaciones de situaciones que amenazan la capacidad de un sistema de alcanzar su objetivo mediante la entrega de servicios.

33. Un sistema de gestión se construye sobre dos *procesos* fundamentales: gestión de riesgo y garantía de entrega. En el caso específico de SMS como sistema de gestión de la seguridad operacional, estos dos procesos fundamentales son gestión del riesgo de seguridad operacional *(safety risk management, SRM)* y aseguramiento de la seguridad operacional *(safety assurance, SA).* Ambos procesos son discutidos en detalle en sus respectivos capítulos, y lo que sigue a continuación es solamente una introducción a sus fundamentos.

34. La *gestión de riesgos de seguridad operacional* se basa en la aplicación de *principios de seguridad operacional sistémica* a la mitigación de situaciones que amenazan la capacidad de un sistema de alcanzar su objetivo mediante la entrega de servicios. La gestión de riesgos de seguridad operacional abarca, específicamente, actividades para la *identificación* y el *control inicial* de deficiencias de seguridad operacional y peligros en el contexto operativo dentro del cual tiene lugar la entrega de servicios por parte del operador.

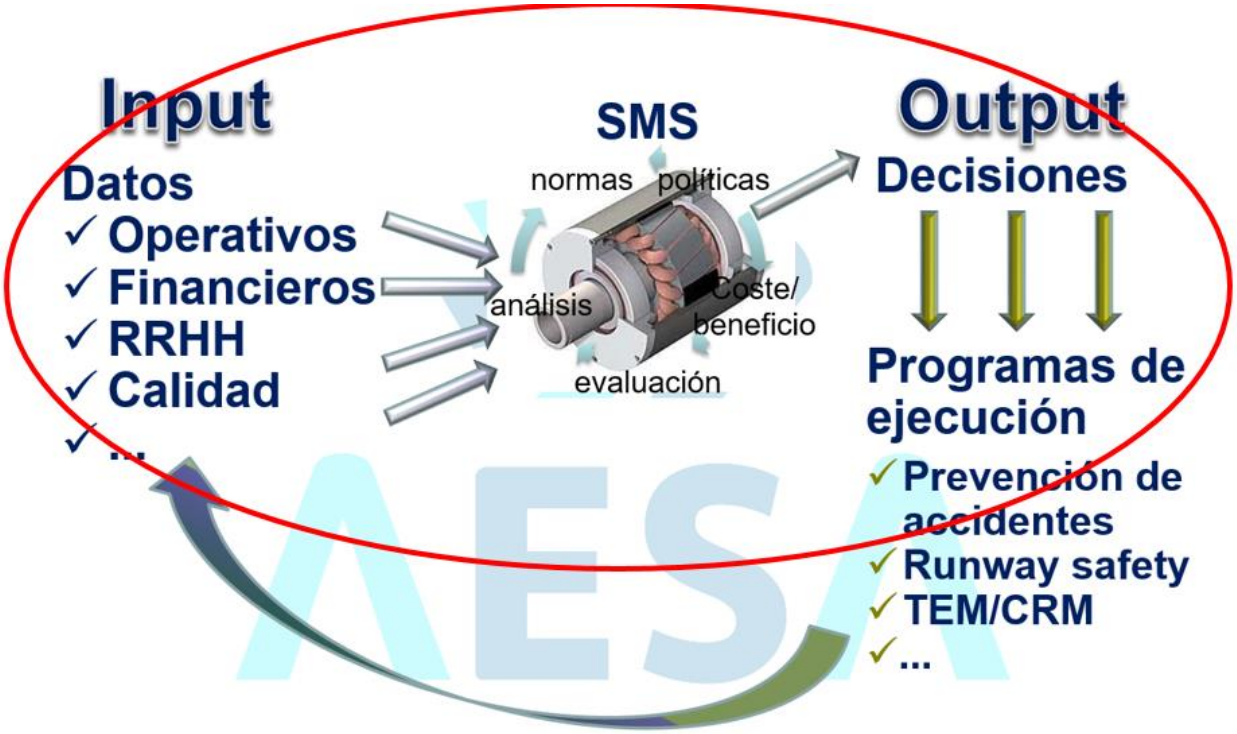
35. Los *objetivos* del proceso de gestión de riesgos de seguridad operacional son:

a. la captura de datos sobre deficiencias de seguridad y peligros en el contexto operativo;

b. el desarrollo de información inicial sobre deficiencias y peligros; y

c. el control inicial de los riesgos asociados a las deficiencias y peligros por medio de estrategias de mitigación.

36. A continuación se muestra la representación gráfica del proceso de gestión de riesgos de seguridad operacional sobre la visualización de SMS ya expuesta, el mismo abarcaría el *input* al "generador" (adquisición de datos), la transformación de los datos en información e inteligencia (análisis de datos y evaluación y priorización del riesgo), y el *output* (formulación de decisiones y su implementación por medio de programas de seguridad operacional como control inicial de deficiencias de seguridad y peligros en el contexto operativo).



37. *El aseguramiento de seguridad operacional* se basa en la aplicación de *principios de calidad – adaptados a las necesidades de la gestión de la seguridad operacional* – al control de la ejecución de las actividades de mitigación de situaciones que amenazan la capacidad de un sistema de alcanzar su objetivo mediante la entrega de servicios. Se trata, específicamente, de actividades que generan confianza que las actividades puestas en marcha para el control inicial de deficiencias de seguridad operacional y peligros en el contexto operativo *funcionan de acuerdo a lo esperado*.

38. Tal aseguramiento es necesario porque las actividades iniciales, puestas en marcha como consecuencia de la gestión de riesgos de la seguridad operacional, pueden ser los paliativos para las deficiencias y peligros que deben controlar o mitigar, pero pueden no serlo. Además, aunque lo fuesen, podría haber aspectos de las actividades de mitigación que no fuesen explotados en su pleno potencial, en cuanto a los objetivos buscados, al momento de la puesta en marcha tales actividades. Esto no significa, necesariamente, que la decisión sobre la puesta en marcha de las actividades de control o mitigación haya sido incorrecta. Más bien, hace evidente dos realidades de la gestión de la seguridad operacional:

    a. es imposible prever con anticipación todas las posibles interacciones operativas que se pueden dar en un contexto determinado. Por consiguiente, cualquier actividad de control o mitigación debe ser reevaluada tan pronto como la experiencia operativa así lo permita, como para introducir los retoques o ajustes necesarios para alcanzar los resultados deseados. Dicho de otra manera, i*mplementación* no es sinónimo de *solución*; y

    b. la calidad de las decisiones estratégicas sobre adjudicación de recursos para actividades de mitigación de deficiencias de seguridad y peligros en el contexto operativo, y la certeza de la eficiencia y eficacia de las actividades a tal efecto, son proporcionales a la calidad de los datos sobre los cuales las decisiones se basaron. De ahí la importancia de la realimentación al sistema de gestión por medio de la garantía de procesos; en el caso de SMS, la realimentación al SMS por medio del proceso de aseguramiento de la seguridad operacional.

39. Los objetivos del proceso de aseguramiento de la seguridad operacional son:

    a. el almacenamiento de datos sobre deficiencias de seguridad y peligros en el contexto operativo;

    b. el análisis permanente de datos sobre deficiencias de seguridad y peligros en el contexto operativo; y

    c. el control permanente de la eficiencia y eficacia de actividades de control o mitigación de las deficiencias de seguridad y peligros en el contexto operativo.

40. A continuación se muestra la representación gráfica del proceso de aseguramiento de la seguridad operacional sobre la visualización de SMS ya expuesta; el mismo estaría representado por la flecha que une a los programas de seguridad operacional con los datos que son el *input* al "generador". Se busca subrayar la importancia de la monitorización constante de las actividades de estos programas – por medio de datos – como para verificar desfases entre el logro de los resultados buscados al implementar los programas, y los resultados reales obtenidos. Esto permitirá al operador efectuar los retoques o cambios necesarios a los programas para mantener su eficiencia y eficacia.

Input
Datos
✓ Operativos
✓ Financieros
✓ RRHH
✓ Calidad
✓ ...
SMS
normas
políticas
análisis
Coste/
beneficio
evaluación
Output
Decisiones
Programas de ejecución
✓ Prevención de accidentes
✓ Runway safety
✓ TEM/CRM
...

5. CAPÍTULO 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

5.1 INTRODUCCIÓN

1. El capítulo 1 de esta Guía presenta una exposición inicial sobre los dos procesos básicos de SMS, de los cuales se derivan las actividades de mitigación de las deficiencias de seguridad y peligros en el contexto operativo. Tales procesos son la gestión de riesgos de seguridad operacional y el aseguramiento de seguridad operacional. Este capítulo trata sobre el primero de ellos: la gestión de riesgos de seguridad operacional.

2. Según la exposición inicial del capítulo 1, la *gestión de riesgos de seguridad operacional* se basa en la aplicación de *principios de seguridad operacional sistémica* al control y mitigación de situaciones que amenazan la capacidad de un sistema de alcanzar su objetivo mediante la entrega de servicios. Hay cuatro principios de la gestión de riesgo de seguridad operacional, derivados de principios básicos de seguridad operacional sistémica, que tienen la solidez de la roca, y cuya comprensión y apreciación son requisito fundamental para el gestor de seguridad operacional encargado con la implementación y mantenimiento de un SMS efectivo. Tales principios son de validez universal e incuestionables en cuanto a su importancia como marco de referencia para guiar conceptualmente el desarrollo de procesos e implementación de actividades subyacentes al SMS. Estos principios son:

- ✓ Todo sistema es **vulnerable**, desde el punto de vista de la seguridad operacional
- ✓ Las vulnerabilidades en materia de seguridad operacional de un sistema se **describen** en términos de
  - deficiencias de seguridad operacional
  - peligros
  - consecuencias
  - riesgos de seguridad operacional
- ✓ Los peligros son componentes **normales** e **identificables** de un sistema, y sus **consecuencias controlables**
- ✓ Los riesgos de seguridad operacional son una medida de **referencia** y **control**

3. El desarrollo de este capítulo sigue el "plan de vuelo" presentado por estos cuatro principios para entender la teoría y práctica subyacente a la gestión de riesgos de seguridad operacional como uno de los dos pilares sobre los cuales se basa la práctica y operación diaria de SMS por un operador.

5.2 LA VULNERABILIDAD DE LA SEGURIDAD OPERACIONAL DE LOS SISTEMAS

4. El primer principio de la gestión de riesgos de la seguridad operacional postula que

   ✓ *Todo sistema es **vulnerable**, desde el punto de vista de la seguridad operacional*

5. La vulnerabilidad de un sistema – desde el punto de vista de la seguridad operacional – es la susceptibilidad del mismo a sufrir deficiencias de seguridad y

estar expuesto a peligros. La vulnerabilidad desde el punto de vista de la seguridad operacional no es igual entre sistemas (en nuestro caso, entre líneas aéreas); hay sistemas que son más vulnerables a deficiencias y peligros que otros. Un número de factores influyen tal vulnerabilidad, tales como la complejidad del sistema, su tamaño, sus recursos, etc. Pero independientemente de estos factores, la premisa a rescatar es que no existe sistema diseñado por el ser humano que sea invulnerable; todos los sistemas exhiben un grado de vulnerabilidad, y las líneas aéreas de la aviación comercial no son una excepción.

6. La vulnerabilidad del sistema nace con el sistema mismo. Es producto de la imposibilidad, por parte de los diseñadores del sistema, de anticipar *todas* las posibles interacciones operativas que tendrán lugar en el contexto operativo en el cual se llevarán a cabo las operaciones necesarias para lograr el objetivo del sistema por medio de la entrega de servicios. El dinamismo típico de un sistema como la aviación comercial contemporánea hace que tal anticipación – que sólo puede ser realista si está basada en datos – sea una tarea que está más allá de las posibilidades de captación y análisis de los datos disponibles al presente en aviación comercial.

7. Aun cuando los diseñadores pudiesen anticipar todas las posibles interacciones que se darán en el contexto operativo durante las operaciones necesarias para la provisión de servicios, es altamente improbable que el sistema estuviese dotado con los recursos económicos necesarios para introducir defensas contra las potenciales consecuencias adversas de *todas* las interacciones operativas previstas. Al no poder anticipar – por el motivo que fuese, indisponibilidad de datos o de recursos económicos – todas las posibles interacciones operativas, habrá algunas para cuyas potenciales consecuencias adversas no se habrán introducido defensas durante el diseño del sistema. El lógico corolario es que el sistema no estará defendido – por diseño – contra deficiencias de seguridad y peligros consecuencia de estas interacciones, dando así lugar a la génesis de su vulnerabilidad.

8. Durante las primeras etapas del diseño de un sistema, dos preguntas principales ocupan la mente de sus diseñadores:

    a. ¿qué recursos se necesitan para lograr el objetivo (*output*) del sistema por medio de la entrega de servicios?; y

    b. ¿cómo puede protegerse el sistema contra deficiencias de seguridad y peligros durante las operaciones necesarias para la entrega de servicios?

9. Los diseñadores del sistema utilizan diversos métodos para dar respuesta a estas dos preguntas. Un método frecuentemente utilizado consiste en definir escenarios de interacciones operativas plausibles (tantos como sea posible) entre los operarios del sistema (en aviación, el personal operativo: pilotos, mecánicos, controladores de tránsito aéreo, etc.), la tecnología con la que se dotará al sistema, y el contexto operacional, a efectos de identificar posibles deficiencias y peligros producto de dichas interacciones. Tales escenarios se validan contra datos históricos (tantos

como sea posible) para determinar probabilidad, aceptándose algunos y descartándose otros.

10. El resultado final del proceso de aceptación y descarte de escenarios es un diseño inicial del sistema cuya defensa está basada en hipótesis sobre la correcta funcionalidad de las tres defensas básicas del sistema de aviación contra deficiencias de seguridad y peligros: a) la tecnología (también necesaria para lograr el objetivo del sistema por medio de la entrega de servicios); b) la instrucción o entrenamiento necesarios para que los profesionales aeronáuticos puedan operar adecuadamente la tecnología; y c) los reglamentos y procedimientos que rigen el comportamiento del sistema y de las personas. Estas hipótesis son el fundamento del funcionamiento defensivo del sistema desde el punto de vista teórico o ideal, es decir, son el fundamento hipotético de cómo el sistema *debería* funcionar, defensivamente hablando, una vez operativo. Se ensayan las hipótesis, se valida el funcionamiento teórico y, en última instancia, el sistema pasa a ser operacional.

11. Una vez iniciadas las operaciones, las defensas del sistema funcionan como deberían (es decir, siguiendo las hipótesis de diseño) la mayoría de las veces. No obstante, a menudo el funcionamiento operativo real es distinto de lo que debería ser en comparación con las hipótesis de funcionamiento teórico. Es verdad *sine qua non* de la vida de cualquier sistema que, junto con la iniciación de las operaciones, se produce una gradual pero inexorable y progresiva deriva entre el funcionamiento teórico previsto por las hipótesis de diseño del sistema y el funcionamiento real del mismo, una deriva hacia un funcionamiento dictado por los imperativos de las operaciones en la vida real. Dado que esta deriva es consecuencia de la práctica diaria, se la conoce como "deriva práctica".

12. La deriva práctica entre funcionamiento teórico y funcionamiento real, la deriva de *cómo deberían* funcionar las defensas durante las operaciones a *cómo funcionan*, es inevitable en cualquier sistema, independientemente de lo cuidadosa y esmerada que haya sido la planificación de su diseño. Si bien las razones profundas de la deriva práctica son las expuestas en los párrafos anteriores, ante los ojos de los operadores del sistema las razones de la deriva práctica son más simples y directas: tecnología que no siempre funciona de acuerdo con lo previsto o propuesto por sus fabricantes; procedimientos que no pueden ejecutarse en condiciones operacionales dinámicas según lo previsto o propuesto por sus diseñadores; reglamentos que no tienen plenamente en cuenta las limitaciones del contexto y se tornan por lo tanto en difíciles de cumplir; introducción de cambios sutiles y graduales en el sistema con posterioridad a su diseño sin la correspondiente reevaluación de su impacto en las hipótesis básicas del diseño; adición de nuevos componentes al sistema sin una adecuada evaluación de los peligros que dichos componentes pueden introducir; interacción no anticipada con otros sistemas, y así sucesivamente.

13. Lo importante a rescatar de esta exposición es que la vulnerabilidad de un sistema a deficiencias de seguridad operacional y peligros, y la deriva práctica resultante, no son de ninguna manera una sentencia ni acta de defunción del sistema. Más bien, se trata de algo normal y aceptable bajo las pautas de *system safety*. La deriva

práctica es controlable por un operador por medio de SMS. Para expresar los conceptos genéricos expuestos en los párrafos anteriores en términos aplicables a la operación de SMS, se formulan cinco postulados prácticos que son la esencia del control de la deriva práctica:

a. no hay ninguna operación para la cual las defensas necesarias pueden ser entera y completamente pre-especificadas de forma impecable;

b. siempre quedará un remanente de vulnerabilidades, desde el punto de vista de la seguridad operacional, que no habrán sido anticipadas, por lo tanto;

c. es ciertamente necesario llevar a cabo una planificación de las defensas necesarias para la operación de forma prescriptiva, pero

d. es necesario reconocer que habrá vulnerabilidades imprevistas durante la planificación al momento de la ejecución de las operaciones, vulnerabilidades que tienen el potencial de generar brechas en las defensas del sistema, por consiguiente;

e. bajo SMS, la preocupación no son las vulnerabilidades durante la ejecución de las operaciones, sino la ausencia o ineficacia de las actividades de gestión de control de las vulnerabilidades, para minimizar la posibilidad de brechas en las defensas.

5.3 LA DESCRIPCIÓN DE LAS VULNERABILIDADES DE SEGURIDAD OPERACIONAL DEL SISTEMA

14. El segundo principio de la gestión de riesgo de la seguridad operacional postula que

- ✓ *Las vulnerabilidades en materia de seguridad operacional de un sistema se* ***describen*** *en términos de*
  - *deficiencias de seguridad operacional*
  - *peligros*
  - *consecuencias*
  - *riesgos de seguridad operacional*

15. Una vez aceptado por el operador que su sistema (es decir, la línea aérea) es un sistema con vulnerabilidades de seguridad operacional como consecuencia de deficiencias de seguridad operacional y peligros de difícil anticipación durante su planificación, y que el rol de SMS, por medio de la gestión de riesgos de la seguridad operacional, es mantener el control de deficiencias y peligros durante las operaciones necesarias para el logro del objetivo del sistema por medio de la provisión de servicios, el paso siguiente es describir deficiencias de seguridad operacional y peligros en términos operativos, a efectos de poder gestionar su control.

16. La diferencia entre *deficiencias de seguridad operacional*, *peligros* y *riesgos de seguridad operacional* es a menudo fuente de confusión. Para desarrollar prácticas

de gestión de riesgos de seguridad operacional que sean pertinentes y efectivas, es esencial una clara comprensión sobre qué es una deficiencia de seguridad, qué es un peligro, y qué es un riesgo de seguridad operacional. Una clara comprensión de las diferencias entre estos tres componentes es también fundamental para la práctica de SMS.

17. Una *deficiencia de seguridad operacional* es *una condición en el sistema que permite o es la génesis de los peligros y de su perduración en el tiempo*. Se trata de condiciones que están presentes en el sistema en forma latente, muchas veces con significativa anticipación al suceso que las hace evidentes. Un ejemplo de una deficiencia de seguridad operacional es *"certificación de un aeródromo que no cumple con la normativa establecida"*. Un aeródromo puede operar bajo condiciones de certificación incorrectas/incompletas sin que ello necesariamente signifique la ocurrencia inmediata de sucesos de relevancia. No obstante, la deriva práctica, y una clara situación de vulnerabilidad, se han instalado en el sistema. Las deficiencias de seguridad operacional son de naturaleza institucional, y como consecuencia de ello, la solución de las mismas es de naturaleza institucional más que operativa.

18. Un *peligro* se puede definir como *una condición o un objeto que potencialmente puede causar lesiones al personal, daños al equipamiento o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita.* La definición que recoge actualmente OACI en el Anexo 19 es: "*Condición u objeto que entraña la posibilidad de causar un incidente o accidente de aviación o contribuir al mismo.*" No todos los peligros son consecuencia de deficiencias de seguridad operacional. Los peligros son – en gran medida – componentes naturales del contexto operativo y, como las deficiencias de seguridad operacional, están presentes en el sistema en forma latente. Un ejemplo de un peligro es la condición *"señalización confusa en el aeródromo"*. Un aeródromo puede operar bajo condiciones de señalización confusa sin que ello necesariamente signifique la ocurrencia inmediata de sucesos de significación. No obstante, la deriva práctica, y una clara situación de vulnerabilidad, se han instalado en el sistema. Los peligros son de naturaleza operativa, y su control es de competencia específica de SMS.

19. Una *consecuencia* se define como *el posible resultado de un peligro*. El potencial perjuicio – desde el punto de vista de la seguridad operacional – de un peligro se materializa mediante una o varias consecuencias. Una posible consecuencia del peligro *"señalización confusa en el aeródromo"* puede ser *"incursión en pista"*. Las consecuencias de un peligro pueden ser ponderadas a lo largo de un espectro en cuanto a la naturaleza de su severidad, en caso de materializarse, que va desde severidad de naturaleza catastrófica a severidad de naturaleza insignificante. La consecuencia *"incursión en pista"* puede resultar en una múltiple colisión entre aeronaves con cuantiosas pérdidas humanas y materiales, o bien puede resultar en una simple transgresión inconsecuente de la señalización de detención antes de la pista sin otra consecuencia que un desvío normativo.

20. Finalmente, *el riesgo de seguridad operacional* se define como: "*la probabilidad y la severidad previstas de las consecuencias o resultados de un peligro*". Normalmente,

los riesgos de seguridad operacional se evalúan y designan mediante una convención alfanumérica para permitir su medición. Por ejemplo, el riesgo de seguridad operacional de la consecuencia *"incursión en pista"* puede ser evaluado como de probabilidad *frecuente* y de consecuencias *catastróficas*. En función de ello, este riesgo de seguridad operacional particular sería designado (según la matriz de riesgo adoptada por el operador) como por ejemplo 5A (frecuente/catastrófico).

21. La exposición en los párrafos anteriores permite ejemplificar la secuencia apropiada del análisis subyacente a la gestión de riesgos de seguridad operacional, cuyo cumplimiento es esencial para la correcta operación de SMS por parte del operador:

    a. *deficiencia de seguridad*: certificación de un aeródromo que no cumple con la normativa establecida;

    b. *peligro:* señalización confusa en el aeródromo;

    c. *consecuencia*: incursión en pista;

    d. *riesgo de seguridad operacional*: 5A (frecuente/catastrófico)

5.4 LA IDENTIFICACIÓN DE LOS PELIGROS

22. El tercer principio de la gestión de riesgos de la seguridad postula que

    ✓ Los peligros son componentes **normales** e **identificables** de un sistema, y sus **consecuencias controlables**

23. Los peligros son componentes normales del contexto operativo en el que un sistema brinda la prestación de servicios para el logro de su objetivo. Por sí mismos, los peligros no son "cosas malas"; no son necesariamente componentes perjudiciales o negativos de un sistema. Sólo cuando los peligros interactúan con otros componentes del contexto operativo en las operaciones del sistema dirigidas a la prestación de servicios, su potencial perjudicial puede transformarse en un problema de seguridad operacional. Por ejemplo, el viento es un componente normal del entorno natural. No obstante, en ciertas condiciones operativas específicas, el viento tiene posibilidad de provocar lesiones al personal, daños al equipo o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita.

24. Un viento de 15 nudos, por sí mismo, no necesariamente tendría el potencial de provocar daños durante operaciones aeronáuticas. En realidad, un viento de 15 nudos orientado directamente en el sentido de la pista contribuye a mejorar la performance de las aeronaves durante el despegue. No obstante, cuando un viento de 15 nudos sopla en dirección perpendicular a una pista en la que se realizará un aterrizaje o un despegue, cuando se transforma en *viento cruzado* (una condición operativa específica), es sólo entonces que el viento tiene posibilidad de provocar lesiones al personal, daños al equipo o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita. Cuando una condición específica

de viento (cruzado a la pista) interactúa con las operaciones del sistema (despegue o aterrizaje de un avión) dirigidas a la prestación de un servicio (la necesidad de transportar pasajeros o carga hacia o desde el aeródromo particular *cumpliendo un horario*), es que su potencial de producir daños pasa a ser un problema de seguridad operacional (una salida lateral de la pista debido a la pérdida de control de la aeronave como consecuencia del viento cruzado).

25. Veamos otro sencillo ejemplo. El combustible es un componente técnico del sistema de aviación y, al igual que toda otra fuente de energía, constituye un peligro. Mientras está almacenado en tanques subterráneos y no se lo manipula, el potencial perjuicio del combustible como peligro es bajo. Las aeronaves son también componentes técnicos del sistema de aviación. El abastecimiento de combustible a las aeronaves lo hacen personas. Durante las operaciones de abastecimiento de combustible por personas (una interacción operacional esencial para la prestación del servicio), el potencial perjudicial del combustible como peligro aumenta considerablemente. Por ello, se implantan procedimientos de abastecimiento de combustible (mitigación) para llevar los riesgos de seguridad operacional de las consecuencias de las operaciones de abastecimiento bajo control de la organización. Estos procedimientos se basan en la identificación y el control de los elementos del peligro.

26. Vale la pena enfatizarlo, en especial debido a las connotaciones que el término genera: los peligros no deben considerarse necesariamente como "cosas malas" o algo con connotaciones negativas. Los peligros son parte integral de los contextos operacionales, y son también perfectamente identificables. El verdadero desafío, desde el punto de vista de la gestión de riesgos de la seguridad operacional, es el control de los riesgos asociados a sus potenciales consecuencias.

27. Las consecuencias de los peligros pueden contenerse mediante diversas estrategias de control o mitigación, de manera tal que se contenga el potencial perjuicio del peligro, lo que se analizará más adelante en esta Guía. El análisis de las estrategias de mitigación de las consecuencias de los peligros nos lleva a tener en cuenta varios puntos de importancia.

28. En primer lugar, los peligros se dan en el *presente*. En la mayoría de los casos, son parte del contexto operacional y por lo tanto están presentes en el lugar de trabajo antes de que el personal "se presente a trabajar". Como componentes físicos del contexto operacional o del lugar de trabajo, la mayoría de los peligros son, y deberían ser, detectables mediante auditorías. Por el contrario, las consecuencias pertenecen y se dan en el *futuro*. No se materializan hasta que los peligros interactúan en ciertas operaciones del sistema dirigidas a la prestación de servicios. Como consecuencia de esta interacción, los peligros pueden desencadenar su potencial perjuicio. Esto trae a colación un aspecto esencial de la gestión de la seguridad operacional: las estrategias de mitigación deberían dirigirse a contener de forma proactiva el potencial perjuicio de los peligros y no esperar hasta que las consecuencias de éstos se materialicen y posteriormente tratarlas de forma reactiva.

29. En segundo lugar, las consecuencias de los peligros no son eventos de azar, en los cuales interviene el destino y la suerte, sino eventos predecibles y controlables. No son eventos sin causa aparente, sino el resultado del potencial no controlado de los peligros, cuyas causas antecedentes son generalmente bien conocidas y de relativamente fácil rastreo en archivos de seguridad operacional debidamente constituidos. Aun cuando hubiese un elemento de incertidumbre en el pronóstico de las consecuencias, tal elemento puede reducirse considerablemente a través del análisis y estimación de estadísticos.

30. En tercer lugar, un peligro puede tener una gama de consecuencias, cuya ponderación puede variar entre extremos de significación. El peligro *"señalización confusa en el aeródromo"* puede llevar a la consecuencia *"incursión en pista de severidad catastrófica",* o bien a la consecuencia *"confusión entre vehículos terrestre en la plataforma"*, con todo un abanico de posibles consecuencias de distinta severidad entre medio. En el ejemplo anterior del viento cruzado, una consecuencia del peligro *"viento cruzado"* podría ser *"la pérdida de control lateral".* Otra consecuencia más severa podría ser la *"salida lateral de la pista sin consecuencias".* Una consecuencia más severa aún podría ser *"salida lateral de la pista con daños al tren de aterrizaje"*. Por consiguiente, es importante describir todas las consecuencias posibles de un peligro durante el análisis del peligro y no sólo las más obvias o inmediatas. No obstante, esta introspección debería quedar contenida en el límite de lo probable y en lugar de en el límite de lo imaginable, con el fin de evitar malgastar recursos en el análisis de consecuencias "posibles" pero "altamente improbables".

31. Finalmente, para fines de gestión de riesgos de seguridad operacional, las consecuencias de los peligros deben describirse en términos operacionales. Muchos peligros tienen el potencial de producir la consecuencia final y más extrema: la pérdida de vidas humanas. La mayoría de los peligros tienen el potencial de pérdida de bienes, daños ecológicos y consecuencias similares de alto nivel. No obstante, describir las consecuencias de los peligros en términos extremos hace difícil diseñar estrategias de mitigación, excepto la cancelación de la operación. Para diseñar estrategias de mitigación que defiendan contra los problemas de seguridad operacional subyacentes en las consecuencias operacionales no extremas del peligro (por ejemplo, el viento cruzado), dichas consecuencias deben describirse en términos operacionales (salida lateral de la pista), y no en términos extremos (pérdida de vidas).

32. La descripción de los peligros que puedan afectar una operación particular es parte de la evaluación de los riesgos de seguridad operacional de las consecuencias de los peligros (analizados en la próxima sección del capítulo). La evaluación de los riesgos de seguridad operacional de las consecuencias de los peligros permite a la organización tomar decisiones informadas sobre si puede lograr la mitigación de las consecuencias del peligro y así continuar la operación. Si las consecuencias del peligro (viento transversal) se describen en términos extremos (pérdida de vidas) en vez de términos operacionales (salida lateral de la pista), la evaluación del riesgo

de seguridad operacional no tiene demasiado sentido dado que la mitigación de tal consecuencia no se podrá lograr a menos que haya una adjudicación astronómica de recursos, y la única mitigación efectiva sería la cancelación de la operación.

33. La potencial de confusión entre deficiencias de seguridad operacional, peligros, consecuencias y riesgos de seguridad operacional ya ha sido expuesto. En particular, existe una tendencia a confundir los peligros con sus consecuencias. Cuando esto sucede, la descripción del peligro en términos operacionales refleja las consecuencias más bien que el propio peligro. En otras palabras, no es raro ver que los peligros se describen como una de sus consecuencias. Describir un peligro como una de sus consecuencias no sólo oculta el carácter verdadero y el potencial perjudicial del peligro en cuestión, sino que también interfiere con la identificación de otras posibles consecuencias de importancia del peligro. Por otro lado, la correcta descripción de los peligros permite identificar la naturaleza y el potencial perjuicio del peligro, deducir correctamente el origen o la fuente del peligro y, lo que es más importante, evaluar las consecuencias en términos de la magnitud de las pérdidas posibles, lo que constituye uno de los objetivos finales de la gestión de riesgos de la seguridad operacional según se analiza en la sección siguiente.

34. Para enfatizar la diferencia entre peligros y consecuencias, considérese la siguiente ampliación del ejemplo del aeródromo que opera con su sistema de señalización en estado deficiente. Esto complica la tarea de la navegación en tierra para los usuarios del aeródromo, tanto aeronaves como vehículos terrestres. En este caso, la denominación correcta del peligro podría ser *"señalización confusa en el aeródromo"* o bien *"señalización del aeródromo en mal estado",* según fuese el enunciado que describiese más exactamente la condición (es decir, la condición con potencial de provocar lesiones al personal, daños al equipo o estructuras, pérdidas de material o reducción de la capacidad de realizar una función prescrita). Como resultado de este peligro, son posibles un número de consecuencias. Una consecuencia del peligro (*señalización de confusa en el aeródromo/señalización del aeródromo en mal estado)* podría ser *"incursión en la pista".* Pero puede haber también otras consecuencias: vehículos terrestres que entren en áreas restringidas, aeronaves en rodaje hacia calles de rodaje erróneas, colisiones entre aeronaves, colisión entre vehículos terrestres, colisión entre aeronaves y vehículos terrestres, y así sucesivamente. Así pues, denominar el peligro como *"incursión en la pista"* en vez de *"señalización de confusa en el aeródromo/señalización del aeródromo en mal estado"* oculta el carácter del peligro e interfiere con la identificación de otras consecuencias importantes. Esto conducirá probablemente a estrategias de mitigación parciales o incompletas, con el consiguiente derroche de recursos.

35. A los efectos de su identificación y el control de sus consecuencias, los peligros pueden agruparse en tres familias genéricas: peligros naturales, peligros técnicos y peligros económicos.

36. Los *peligros naturales* son consecuencia del contexto natural en el que se llevan a cabo las operaciones necesarias para la prestación de servicios. Los ejemplos peligros naturales abarcan:

a) condiciones meteorológicas o sucesos climatológicos violentos (huracanes, tormentas invernales, tornados, tormentas eléctricas, rayos y relámpagos, viento de cizalladura, etc.);

b) condiciones meteorológicas adversas (formación de hielo, lluvia congelante, lluvia fuerte, nieve, viento, restricciones a la visibilidad, etc.);

a) sucesos geofísicos (terremotos, erupciones volcánicas, tsunamis, inundaciones y deslizamientos de tierra, etc.);

d) condiciones geográficas (terreno adverso, orografía, grandes masas de agua, etc.);

e) sucesos medio-ambientales (incendios, actividades de fauna silvestre, aves, etc.); y

f) sucesos de salud pública (epidemias, pandemias de gripe u otras enfermedades).

37. Los *peligros técnicos* tienen su origen en fuentes energéticas (electricidad, combustible, presión hidráulica, presión neumática y así sucesivamente) o en materiales críticos para la seguridad operacional (tecnología) necesarios para las operaciones relacionadas con la provisión de servicios. Los ejemplos peligros técnicos abarcan *condiciones* respecto de:

a) aeronaves y componentes, sistemas, subsistemas y equipo relacionado de aeronaves;

b) instalaciones, herramientas y equipo relacionado de la organización; o

c) instalación de sistemas, subsistemas y equipo relacionado externos a la organización.

38. Finalmente, los *peligros económicos* son consecuencia del entorno sociopolítico en el que se realizan las operaciones relacionadas con la provisión de servicios. Los ejemplos de peligro económico comprenden condiciones relacionadas con crecimiento; recesión; coste de materiales y equipos, etc.

39. Las actividades de gestión de la seguridad operacional dirigidas a controlar las consecuencias los peligros estarán dirigidas con carácter casi exclusivo a los peligros técnicos y naturales.

40. El análisis de peligros es un procedimiento en tres etapas:

a) *Primera etapa:* identificar el *peligro genérico* (también conocido como peligro de máximo nivel o TLH, *Top Level Hazard*). El término peligro genérico se emplea en el contexto de esta Guía para dar una perspectiva simplificada que apoye el seguimiento y la clasificación de los componentes más específicos del peligro que se desprendan del peligro genérico.

b) *Segunda etapa:* desglosar el peligro genérico en componentes específicos. Cada peligro específico tendrá probablemente un conjunto distinto y particular de condiciones causales, lo que hace que cada peligro específico tenga carácter diferente y particular.

c) *Tercera etapa:* relacionar los peligros específicos con todas las consecuencias específicas posibles, es decir, eventos o sucesos específicos.

41. A continuación, se proporciona un ejemplo para ilustrar las nociones de peligro genérico, peligro específico y consecuencias. Un aeropuerto internacional con cien mil movimientos por año inicia un proyecto de construcción para ampliar y repavimentar una de sus dos pistas cruzadas. El siguiente mecanismo aplicaría:

a) Formular el peligro genérico (o *TLH*)
   - ✓ construcción en aeropuerto;

b) Identificar peligros específicos o componentes específicos del peligro genérico
   - ✓ equipos de construcción;
   - ✓ calles de rodaje cerradas;
   - ✓ …

c) Relacionar peligros específicos con consecuencias específicas
   - ✓ colisión de aeronaves con equipo de construcción (equipo de construcción);
   - ✓ entrada de aeronaves en la calle de rodaje equivocada (calle de rodaje cerrada);
   - ✓ ...

42. Para concluir esta sección, conviene subrayar que, en todo sistema, no importa cuál sea la industria que se considere, su personal realiza las actividades necesarias para la provisión de servicios *dentro de la deriva*, vale decir, en un sistema imperfecto – defensivamente hablando – con respecto a sus hipótesis de diseño en cuanto a su funcionamiento. Por ende, el personal operativo desarrolla sus actividades en un sistema vulnerable. En virtud de ello, el personal operativo convive diariamente con deficiencias de seguridad operacional, peligros y en muchos casos sus consecuencias, que a su vez en muchos casos no han sido formalmente gestionadas.

43. Por otro lado, también conviene subrayar que, a pesar de la deriva entre diseño y operación, a pesar de las limitaciones de las hipótesis de diseño del sistema que condujeron a la deriva, el personal, que "vive" diariamente dentro de la deriva, se las ingenia para hacer que el sistema *funcione efectivamente* de manera cotidiana. El personal aplica adaptaciones locales y estrategias personales (que encarnan la experiencia colectiva de los profesionales de la aviación) para lograr el objetivo del sistema por medio de la entrega de servicios, superando así las carencias del sistema, en cuanto a las deficiencias de seguridad operacional y los peligros que no han sido formalmente gestionados.

44. La captación de lo que ocurre diariamente dentro de la deriva práctica, incluyendo prácticas locales y adaptaciones, mediante mecanismos formales (es decir, obteniendo formalmente el conocimiento colectivo que refleja la experiencia profesional de los distintos grupos de trabajo) tiene un considerable potencial de aprendizaje sobre adaptaciones exitosas para reducir la deriva entre el funcionamiento teórico y el funcionamiento real del sistema, y por lo tanto para el control de deficiencias de seguridad operacional y peligros en el contexto operativo. La captación formal de experiencia colectiva puede transformarse en intervenciones formales para la reformulación de hipótesis de diseño o el rediseño o mejora del sistema, si dicho potencial de aprendizaje se adquiere y aplica en forma organizada y principista. En el lado negativo, la proliferación descontrolada de adaptaciones locales y estrategias personales pueden dar lugar a situaciones de inestabilidad en el sistema, generando el potencial de un incidente o accidente.

45. El corolario es obvio: los programas de notificación de sucesos de seguridad operacional (tratados en el capítulo siguiente) son una herramienta primordial; y la protección de las fuentes de información sobre seguridad operacional es una condición fundamental, para la gestión de riesgos de seguridad operacional, y para la implementación y efectivo mantenimiento de SMS por un operador.

5.5 MEDICIÓN Y CONTROL

46. El cuarto y último principio de la gestión de riesgos de la seguridad postula que

- ✓ Los riesgos de seguridad operacional son una medida de **referencia** y **control**

47. Es un axioma básico de los procesos de gestión que no se puede gestionar lo que no se puede medir. Por consiguiente, es fundamental establecer alguna forma de ponderación o medición de la severidad y probabilidad de las consecuencias de los peligros. Esta es la contribución esencial del proceso de gestión de riesgos de seguridad operacional a la gestión de la seguridad operacional por medio de SMS. Mediante la "asignación de un ranking" a las consecuencias de los peligros, SMS proporciona al operador un fundamento principista para la priorización en la adopción de decisiones estratégicas sobre los riesgos de seguridad operacional, y la consiguiente asignación de recursos del operador para actividades destinadas a contener el potencial perjuicio de los peligros en el contexto operativo durante la provisión de servicios.

48. La noción de riesgo, en su sentido más amplio, ha sido objeto de mucho estudio, y la literatura sobre el tema es copiosa. Al igual que los otros términos asociados con la gestión de riesgos de seguridad operacional, es esencial que el uso del término sea dogmático, ya que existe la posibilidad de confusión debido al uso popular del término, que es frecuente, amplio y generalmente vago. La primera precaución para evitar la confusión es afinar el uso del término genérico "riesgo" al más específico término "riesgo de seguridad operacional". Esto es importante porque "riesgo" es una medida que se aplica a múltiples actividades, tales como: riesgo de inversión,

riesgo financiero, riesgo de calidad, riesgo laboral, riesgo medioambiental, riesgo legal, riesgo de seguridad física (*security*), etc. Más allá de ello, es esencial desde un principio establecer una clara definición de riesgo de seguridad operacional y relacionar dicha definición con los conceptos de peligro y consecuencias expresados en términos operacionales.

49. Aún después de afinar el uso del término genérico "riesgo" al término más específico "riesgo de seguridad operacional", las confusiones pueden seguir existiendo. Esto se debe a que la noción de riesgo es artificial. Los riesgos de seguridad operacional no son componentes tangibles o visibles de un contexto físico o natural; es necesario pensar acerca de riesgos de seguridad operacional para comprender o formarse una imagen de los mismos. Por el contrario, los peligros y las consecuencias son componentes tangibles o visibles de un contexto físico o natural y, por consiguiente, intuitivos en términos de comprensión y visualización.

50. La noción de riesgo de seguridad operacional es lo que se conoce como una abstracción intelectual, es decir, una convención artificial creada por los seres humanos. Dicho simplemente, mientras que los peligros y las consecuencias son componentes físicos del mundo natural, los riesgos de seguridad operacional no existen realmente en el mundo natural. El riesgo de seguridad operacional es un producto de la mente humana a los efectos de medir, de "asignar un valor o serie de valores" a las consecuencias de los peligros.

51. El riesgo de seguridad operacional se define como la probabilidad y la severidad previstas de las consecuencias o resultados de un peligro. Normalmente, los riesgos de seguridad operacional se designan mediante una convención alfanumérica que permite su medición. Volviendo al ejemplo del viento cruzado presentado en la sección anterior, puede verse que la definición propuesta de riesgo de seguridad operacional permite relacionar riesgos de seguridad operacional con peligros y consecuencias, cerrando así el círculo de la trilogía peligro-consecuencia-riesgo de seguridad operacional:

    a) un viento de 15 nudos cruzado a la pista es un peligro;

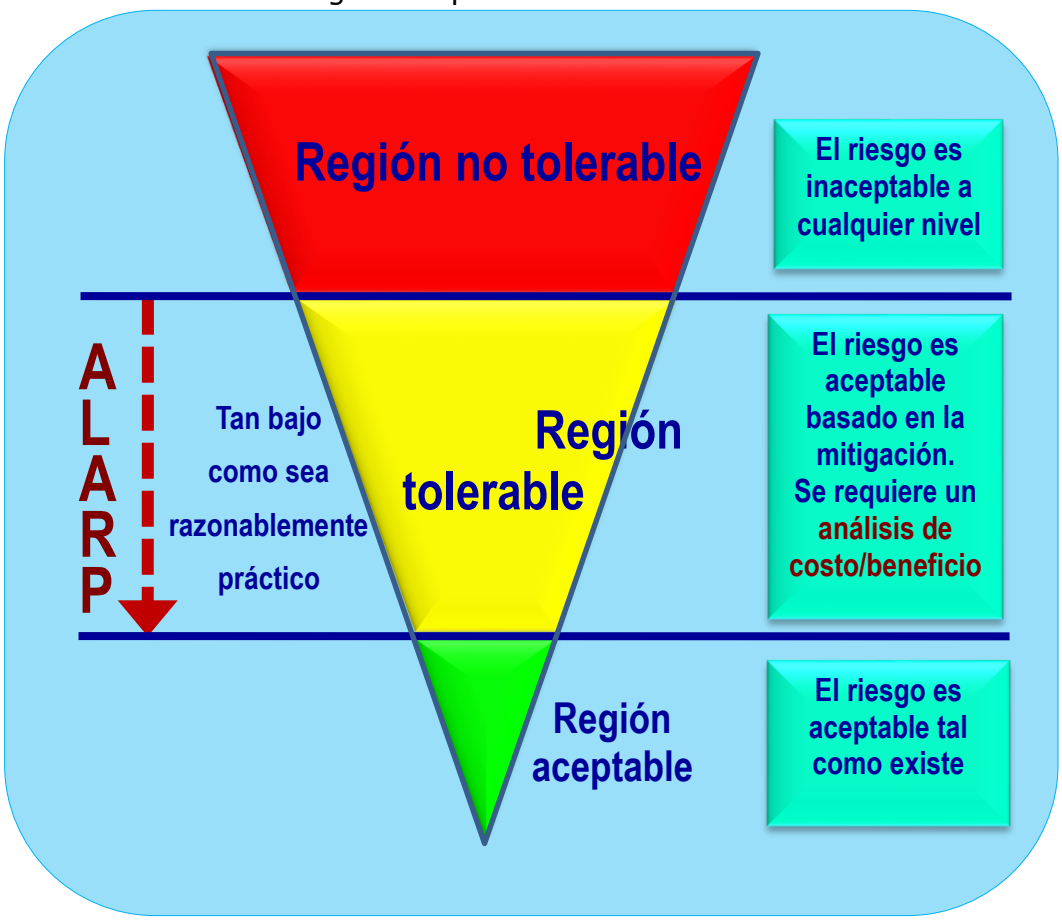
    b) la posibilidad de salida lateral de la pista por pérdida de control de la aeronave durante el despegue o el aterrizaje es una de las posibles consecuencias del peligro;

    c) la evaluación de las consecuencias de una salida lateral de la pista, expresada en términos de probabilidad y severidad como convención alfanumérica, constituye la medición del riesgo de seguridad operacional.

52. La expresión gestión de los riesgos de seguridad operacional es un término genérico que engloba la evaluación y priorización de adjudicación de recursos para el control o mitigación de las consecuencias de los peligros que amenazan el logro del objetivo del sistema por medio de las operaciones necesarias para la provisión de servicios. Se trata de reducir las consecuencias de los peligros a un nivel tan bajo como sea

razonable practicable (As Low As Reasonably Practicable, o ALARP). El objetivo de la gestión de riesgos de seguridad operacional es proporcionar el fundamento para una asignación equilibrada de recursos para contener el potencial negativo de todas las consecuencias evaluadas de los peligros a los que se enfrenta el operador durante la provisión de sus servicios, y aquéllas para las cuales es viable la mitigación. La gestión de riesgos de seguridad operacional es, por consiguiente, un componente fundamental del proceso de gestión de la seguridad operacional. Fundamentalmente, su valor agregado corresponde al hecho que es un enfoque basado en datos para asignación de recursos, y por lo tanto fácil de defender y de explicar.

53. La figura adjunta presenta una representación visual genérica ampliamente adoptada del proceso de gestión de los riesgos de seguridad operacional. El triángulo se presenta en posición invertida, lo que sugiere que la aviación (al igual que cualquier otro sistema de producción) está plagada potencialmente de riesgos de seguridad operacional que son ponderados como de "intolerables": la mayoría de los riesgos de seguridad operacional de las consecuencias de los peligros se evaluarán como cayendo inicialmente en la región intolerable. Un número menor de riesgos de seguridad operacional de las consecuencias de los peligros será evaluado en forma tal que dicha evaluación caiga directamente en la región tolerable; y un número aún menor – ínfimo realmente – se evaluará de forma que la evaluación caiga directamente en la región aceptable.



54. Las consecuencias cuyos riesgos de seguridad operacional son evaluados como que corresponden inicialmente a la región intolerable (roja) son inaceptables bajo

cualquier circunstancia. La probabilidad y/o severidad de las consecuencias de los peligros son de tal magnitud, y el potencial perjuicio del peligro plantea un conflicto tal a la viabilidad de la entrega de servicios por el operador, que se requieren medidas inmediatas de mitigación para la continuación de las operaciones. En términos generales, el operador tiene dos alternativas para llevar las consecuencias de los peligros a las regiones tolerable o aceptable:

a) asignar recursos para reducir la exposición al potencial perjuicio de las consecuencias de los peligros o su magnitud; o

b) si la mitigación no es posible, cancelar la operación.

55. Las consecuencias cuyos riesgos de seguridad operacional evaluados como que corresponden inicialmente a la región tolerable (amarilla) son aceptables sobre la base de estrategias de control o mitigación que garanticen, en la medida previsible, que las consecuencias de los peligros se mantienen bajo control del operador. Los mismos criterios de mitigación se aplican a las consecuencias cuyos riesgos de seguridad operacional inicialmente corresponden a la región intolerable y son mitigados a la región tolerable. Una consecuencia cuyo riesgo de seguridad operacional se evalúa inicialmente como intolerable, y que se mitiga hasta caer en la región tolerable debe permanecer "protegida" mediante estrategias de mitigación que garanticen su control. En ambos casos, hay consideraciones de coste-beneficio que son inevitables, y que se reducen a dos preguntas básicas:

a) ¿hay un retorno razonable de la inversión necesaria para la asignación de recursos para llevar la probabilidad o severidad de las consecuencias de los peligros bajo control del operador?

b) ¿es necesaria una asignación de recursos de tal magnitud que plantea una mayor amenaza a la viabilidad del operador que operar bajo las condiciones de probabilidad o severidad existentes?

56. El acrónimo ALARP se utiliza para describir una consecuencia cuyo riesgo de seguridad operacional se ha reducido a un nivel tan bajo como sea razonablemente práctico. Para determinar lo que es "razonablemente práctico" en el contexto de la gestión de riesgo de seguridad operacional; deben considerarse tanto la viabilidad técnica de continuar reduciendo el riesgo de seguridad operacional como el coste. Si se llega a la conclusión que el riesgo de seguridad operacional de una consecuencia es ALARP, ello significa que toda ulterior reducción del riesgo de seguridad operacional es impracticable o está ampliamente superada por el coste. No obstante, debe tenerse en cuenta que cuando un operador "acepta" un riesgo de seguridad operacional ALARP, ello no significa que el mismo haya sido eliminado, sino que hay un cierto nivel residual de riesgo de seguridad operacional que permanece presente; no obstante, el operador ha aceptado que dicho riesgo de seguridad operacional residual es suficientemente bajo como para continuar las operaciones.

57. Las consecuencias cuyos riesgos de seguridad operacional han sido evaluados como que corresponden inicialmente a la región aceptable son aceptables en su estado actual y no requieren medidas para llevar o mantener la probabilidad o la severidad de las consecuencias de los peligros bajo control del operador.

58. El procedimiento para la cuantificación de los riesgos de seguridad operacional de las consecuencias de los peligros, como primer paso para llevar a las mismas bajo control del operador, se inicia evaluando la probabilidad que las consecuencias de los peligros se materialicen durante las operaciones necesarias para la provisión de servicios. Esto se conoce como evaluación de la probabilidad del riesgo de seguridad operacional. La probabilidad del riesgo de seguridad operacional se define como la posibilidad de que una consecuencia en cuestión pueda ocurrir. Al evaluar la probabilidad de la consecuencia (o evento), es esencial referirse a los datos históricos contenidos en la base de datos de seguridad operacional del operador, a efectos de tomar decisiones informadas. Se desprende que un operador que no cuente con una base de datos de seguridad operacional sólo puede realizar evaluaciones de probabilidad basadas en la experiencia de su personal (juicio experto), en tendencias globales de la industria y/o, en la menos deseable de las alternativas, en opiniones.

59. Sobre la base de las consideraciones que surjan del análisis de datos históricos u otras fuentes, puede establecerse la probabilidad que pueda ocurrir una consecuencia determinada y evaluarse su importancia aplicando una tabla de probabilidad de riesgos de seguridad operacional. En la figura adjunta se presenta una tabla típica de probabilidad de los riesgos de seguridad operacional, en este caso, con una matriz de cinco puntos. La tabla abarca cinco categorías para indicar la probabilidad de ocurrencia de una consecuencia o evento, el significado de cada categoría y una asignación de valor a cada categoría. Debe subrayarse que este es un ejemplo presentado solamente con fines didácticos. Esta tabla, así como la tabla de severidad y las matrices de evaluación de riesgos de seguridad operacional y los criterios de tolerancia que se analizarán en los párrafos siguientes son, desde el punto de vista conceptual, comunes a la industria. No obstante, el nivel de detalle y complejidad de las tablas y matrices debe adaptarse en forma correspondiente a las necesidades particulares y complejidades de diferentes operadores. Hay operadores que incluyen definiciones cualitativas y cuantitativas. Análogamente, algunas tablas se extienden hasta quince categorías de probabilidades. Las tablas de cinco puntos y las matrices de cinco por cinco no constituyen de modo alguno una norma. Sólo se presentan porque tienen una complejidad adecuada a los fines didácticos así como a las necesidades de la presente Guía.

Probabilidad del evento		
Definición cualitativa	**Significado**	**Valor**
Frecuente	Probable que ocurra muchas veces *(ha ocurrido frecuentemente)*	**5**
Ocasional	Probable que ocurra algunas veces *(ha ocurrido infrecuentemente)*	**4**
Remoto	Improbable, pero es posible que ocurra *(ocurre raramente)*	**3**
Improbable	Muy improbable que ocurra *(no se conoce que haya ocurrido)*	**2**
Extrema-damente improbable	Casi inconcebible que el evento ocurra	**1**

60. Una vez evaluada la probabilidad del riesgo de seguridad de una consecuencia o evento, la segunda etapa de su cuantificación es la de severidad de la consecuencia del peligro si su potencial perjuicio se materializa durante operaciones dirigidas a la prestación de servicios. Esto se conoce como evaluación de la severidad de riesgos de seguridad operacional.

61. La severidad de riesgos de seguridad operacional se define como los posibles efectos de una consecuencia, tomando como referencia la situación más probable. Cabe acotar que se trata de la situación más probable creíble, es decir, que no se exagera al expresar las condiciones extremas anticipadas. A tal efecto, la disponibilidad de datos es esencial, para evaluar la severidad en términos realistas y no caer en la situación más extrema (accidente). La severidad de los posibles efectos de una consecuencia se evalúa utilizando una tabla de severidad de los riesgos de seguridad operacional. En la figura adjunta se presenta una tabla típica de severidad de riesgos de seguridad operacional, también de cinco puntos. Comprende cinco categorías para indicar el nivel de severidad de la consecuencia o evento, el significado de cada categoría y la asignación de un valor a cada categoría. Al igual que con la tabla de probabilidad de riesgos de seguridad operacional, esta tabla constituye un ejemplo presentado solamente con fines didácticos, y se aplican los mismos comentarios expresados anteriormente.

Severidad de los eventos		
Definiciones de aviación	**Significado**	**Valor**
Catastrófico	➢Destrucción de equipamiento ➢Muertes múltiples	**A**
Peligroso	➢Una reducción importante de los márgenes de seguridad, daño físico o una carga de trabajo tal que los operadores no pueden desempeñar sus tareas en forma precisa y completa. ➢Lesiones serias. ➢Daños mayores al equipamiento.	**B**
Mayor	➢Una reducción significativa de los márgenes de seguridad, una reducción en la habilidad del operador en responder a condiciones operativas adversas como resultado del incremento de la carga de trabajo, o como resultado de condiciones que impiden su eficiencia. ➢Incidente serio. ➢Lesiones a las personas.	**C**
Menor	➢Interferencia. ➢Limitaciones operativas. ➢Utilización de procedimientos de emergencia. ➢Incidentes menores.	**D**
Insignificante	➢Consecuencias leves	**E**

62. La cuantificación de la probabilidad que una consecuencia tenga lugar, y de su severidad en tal caso, permite determinar la tolerabilidad del riesgo de seguridad operacional de las consecuencias del peligro si el potencial perjuicio del peligro se materializa durante operaciones necesarias para la provisión de servicios. Esto se conoce como evaluación de la tolerabilidad de riesgos de seguridad operacional. Se trata de un procedimiento en dos pasos.

63. En el primer paso, es necesario obtener una evaluación general del riesgo de seguridad operacional. Esto se logra combinando las tablas de probabilidad de los riesgos de seguridad operacional y de severidad de los riesgos de seguridad operacional en una matriz de evaluación de los riesgos de seguridad operacional, de la cual se muestra un ejemplo en la figura adjunta.

64. Por ejemplo, se ha evaluado la probabilidad del riesgo de seguridad operacional como ocasional (4). La severidad del riesgo de seguridad operacional se ha evaluado como peligroso (B). La combinación alfanumérica de la probabilidad y la severidad (4B) constituye el riesgo de seguridad operacional de la consecuencia del peligro que se considera. Ampliando un concepto previamente mencionado, puede verse, mediante este ejemplo, que un riesgo de seguridad operacional es solamente una combinación alfanumérica y no un componente visible o tangible del mundo natural. La codificación en colores de la matriz de la figura refleja las regiones de tolerabilidad del triángulo invertido anteriormente presentado.

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

65. En el segundo paso, el índice de riesgo de seguridad operacional obtenido de la matriz de evaluación de riesgos de seguridad operacional debe exportarse a una matriz de tolerabilidad de riesgos de seguridad operacional que describe los criterios de tolerabilidad. El criterio para un riesgo de seguridad operacional evaluado como 4B es, de acuerdo con la matriz de tolerabilidad de la figura "inaceptable en las circunstancias actuales". En este caso, el riesgo de seguridad operacional cae en la región intolerable del triángulo invertido. El riesgo de seguridad operacional de las consecuencias del peligro es inaceptable. La organización debe:

a) asignar recursos para reducir la exposición a las consecuencias de los peligros;

b) asignar recursos para reducir la severidad, probabilidad o el potencial perjuicio de las consecuencias de los peligros; o

c) cancelar la operación, si ni a) ni b) son factibles.

Gestión del riesgo	Índice de evaluación del riesgo	Criterio sugerido
Región no tolerable	5A, 5B, 5C, 4A, 4B, 3A	Inaceptable bajo las circunstancias existentes
Región tolerable	5D,5E, 4C, 4D, 4E, 3B, 3C, 3D 2A, 2B, 2C	Aceptable en base a mitigación del riesgo Puede requerir una decisión de la dirección
Región aceptable	3E, 2D, 2E, 1A, 1B 1C, 1D, 1E	Aceptable

66. El paso final en la gestión de riesgos de seguridad operacional para poner bajo control del operador los riesgos de seguridad operacional de las consecuencias de los peligros es la puesta en marcha de estrategias de mitigación. En términos generales, control y mitigación son términos que pueden usarse indistintamente. Ambos tienen el significado de designar medidas para enfrentar el peligro y llevar bajo control de la organización la probabilidad y la severidad de las consecuencias del peligro.

67. Considérese el siguiente ejemplo: un operador está planificando iniciar operaciones en un aeródromo ubicado en una zona de geografía compleja y que cuenta con ayudas a la navegación limitadas. El riesgo de seguridad operacional global de las consecuencias de los peligros analizados se ha evaluado como 4B ("inaceptable en las circunstancias actuales"). Por lo tanto, deben asignarse recursos para llevarlo hacia abajo en el triángulo, a la región tolerable, donde los riesgos de seguridad operacional son ALARP. Si esto no puede hacerse, entonces debe cancelarse la operación dirigida a la provisión de un servicio que expone al operador a peligros de consecuencias inaceptables.

68. Hay tres estrategias genéricas para el control/mitigación de las consecuencias de del peligro:

    a) *evitar:* se cancela la operación debido a que los riesgos de seguridad operacional exceden los beneficios de continuarla;

    b) r*educir:* se reduce la frecuencia de la operación, o se adoptan medidas para reducir la severidad de las consecuencias de los peligros identificados, por ejemplo, se limitan las operaciones en el aeródromo ubicado en una geografía compleja y sin las ayudas de navegación necesarias a condiciones diurnas y de vuelo visual;

    c) s*egregar la exposición: s*e adoptan medidas para aislar los efectos de las consecuencias de los peligros o crear redundancia para protegerse de los mismos; por ejemplo, las operaciones en el aeródromo ubicado en una geografía compleja y sin las ayudas de navegación necesarias se limitan a aeronaves con capacidades específicas de performance de navegación, o bien con capacidades de navegación autónomas.

69. Cuando se evalúan las opciones específicas en cuanto a estrategias de mitigación, debe tenerse en cuenta que no todas ofrecen el mismo potencial de reducción de los riesgos. Es necesario evaluar la eficacia de cada opción antes de adoptar una decisión. Es importante considerar toda la gama de posibles medidas de mitigación así como el compromiso entre las diversas estrategias medidas para llegar a la mejor solución posible. Cada estrategia de mitigación considerada debe ser examinada desde la siguiente perspectiva:

a) *eficacia:* ¿en qué medida las mitigaciones previenen la consecuencia en cuestión? La eficacia puede considerarse como un continuo:

1) *mitigaciones de ingeniería:* eliminan la posibilidad de la consecuencia;

2) *mitigaciones de control:* aceptan la posibilidad de la consecuencia, pero reducen probabilidad y/o severidad, imponiendo condiciones de utilización/operación restrictivas.

   Ambas mitigaciones, ingeniería y control, se consideran mitigaciones "duras" dado que no asumen desempeño operativo humano impecable.

3) *mitigaciones de personal:* se delega en el personal operativo el control de las consecuencias del peligro, por ejemplo, por medio de advertencias, listas de verificación, SOPs (*standard operating procedures*) o instrucción. Las mitigaciones de personal son consideradas "medidas blandas", dado que confían en un desempeño operativo humano impecable.

b) *coste-beneficio:* ¿superan los costes los beneficios percibidos?

c) *practicidad:* ¿es factible y apropiada la mitigación en términos de tecnología disponible, factibilidad financiera y administrativa, legislación y reglamentos, voluntad política, etc.?

d) *aceptación de cada interesado:* ¿cuánta aceptación (o resistencia) puede esperarse de las partes interesadas?

e) *cumplimiento obligatorio:* si se ponen en vigor nuevas reglas (SOP, reglamentos, etc.) ¿pueden hacerse cumplir?

f) d*uración:* ¿resistirá la mitigación la prueba del tiempo? ¿Será de beneficio temporario o será útil a largo plazo?

g) *nuevos problemas:* ¿qué nuevos problemas, o nuevas (quizás peores) consecuencias podría introducir la mitigación propuesta?

70. Las medidas de mitigación más efectivas son lógicamente las mitigaciones duras. Debido a que éstas son a menudo las más costosas, la tendencia es a recurrir con frecuencia a las medidas de mitigación blandas (como la instrucción). En tales casos, debe quedar claro que el operador está probablemente delegando en el personal operativo y en otros subordinados la responsabilidad de la gestión de los riesgos de seguridad operacional.

71. En resumen, las estrategias de control/mitigación de las consecuencias de los peligros se basan principalmente en la introducción de defensas de seguridad o en el refuerzo de las existentes. Las defensas del sistema aeronáutico básicamente se agrupan bajo una de las tres categorías generales:

a) tecnología

b) instrucción

c) normativa (incluyendo reglamentos, políticas y procedimientos internos)

72. Como parte de la mitigación de las consecuencias de los peligros, es importante determinar por qué se necesitan nuevas defensas o por qué deben reforzarse las existentes. Las preguntas siguientes pueden contribuir a dicha determinación:

a) ¿existen defensas para proteger contra las consecuencias de los peligros en cuestión?

b) ¿funcionan las defensas como estaba previsto?

c) ¿son las defensas prácticas como para usarlas en condiciones operativas reales?

d) ¿son necesarias medidas adicionales de mitigación de las consecuencias de los peligros?

73. Se presentan a continuación dos apéndices a este capítulo, con dos ejercicios de gestión de riesgo de la seguridad operacional. El apéndice 1 contiene un ejemplo de gestión de riesgos de seguridad operacional de un operador de tamaño medio-grande, mientras que el apéndice 2 contiene un ejemplo similar para un operador pequeño.

5.6 APÉNDICE 1 AL CAPÍTULO 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL – OPERADOR DE GRAN TAMAÑO O COMPLEJIDAD

Caso de estudio – Operación en un aeropuerto en obras de construcción.

5.6.1 SITUACIÓN OPERATIVA

Un operador de tamaño medio-grande que utiliza aeronaves de gran porte para la provisión de sus servicios recibe notificación del operador del aeropuerto que es su base principal – que tiene dos pistas paralelas, una principal y otra secundaria – sobre la instalación de un sistema de drenaje cerca de una de las cabeceras de la pista secundaria. Los vehículos de construcción deberán cruzar la pista principal para llegar al sitio de construcción.

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

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

5.6.2 DESCRIPCIÓN DEL SISTEMA

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

a) el contexto físico de las pistas durante las obras nocturnas, que incluye un significativo volumen de tránsito de vehículos de construcción entre la rampa y el lugar de la obra;

b) la torre de control de tránsito aéreo y el hecho de que no existen radiocomunicaciones con los vehículos de construcción que no están equipados para ello; y

c) carteles, señales e iluminación para las calles de rodaje, pistas y zona de obras.

5.6.3 IDENTIFICACIÓN DE PELIGROS

Peligro genérico – Obras de construcción en el aeropuerto.

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

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

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

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

5.6.4 EVALUACIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

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

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

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

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

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

5.6.5 CONTROL/MITIGACIÓN DE LOS RIESGOS DE SEGURIDAD OPERACIONAL

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

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

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

5.6.6 REGISTRO DE IDENTIFICACIÓN DE PELIGROS Y GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

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

5.6.7 REGISTRO DE IDENTIFICACIÓN PELIGROS Y GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

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

5.7 APÉNDICE 2 AL CAPÍTULO 2: GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL – OPERADOR PEQUEÑO

Caso de estudio – Iniciación de operaciones en pistas pedregosas

5.7.1 INFORME SOBRE EL ANÁLISIS DE LA OPERACIÓN DEL BAE JETSTREAM 31 EN PISTAS PEDREGOSAS

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

El siguiente personal integró el equipo de análisis:

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

5.7.2 RESUMEN DEL ANÁLISIS

5.7.2.1 Planificación y operación

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

Cualquier requerimiento de vuelo a una pista pedregosa que no se encuentre en la lista de pistas aprobadas requerirá una evaluación del riesgo de seguridad operacional específico antes del vuelo. Esta coordinación demandará un tiempo adicional, pero se

considera indispensable para asegurar el control adecuado de riesgos de seguridad operacional.

5.7.2.2 Instrucción

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

5.7.2.3 Mantenimiento

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

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

5.7.2.4 Documentación

Se completan los cambios para el procedimiento estandarizado de operación (SOP) y el Memorando Provisional de Operaciones con los procedimientos y prácticas detalladas.

5.7.2.5 Mitigación del riesgo

Ver la matriz adjunta

5.7.2.6 Responsabilidades por la gestión de la seguridad operacional

Se mantendrá una reunión de información con el Gerente Responsable antes del comienzo de la operación en pistas pedregosas.

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

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

6. CAPÍTULO 3: ASEGURAMIENTO DE SEGURIDAD OPERACIONAL

6.1 INTRODUCCIÓN

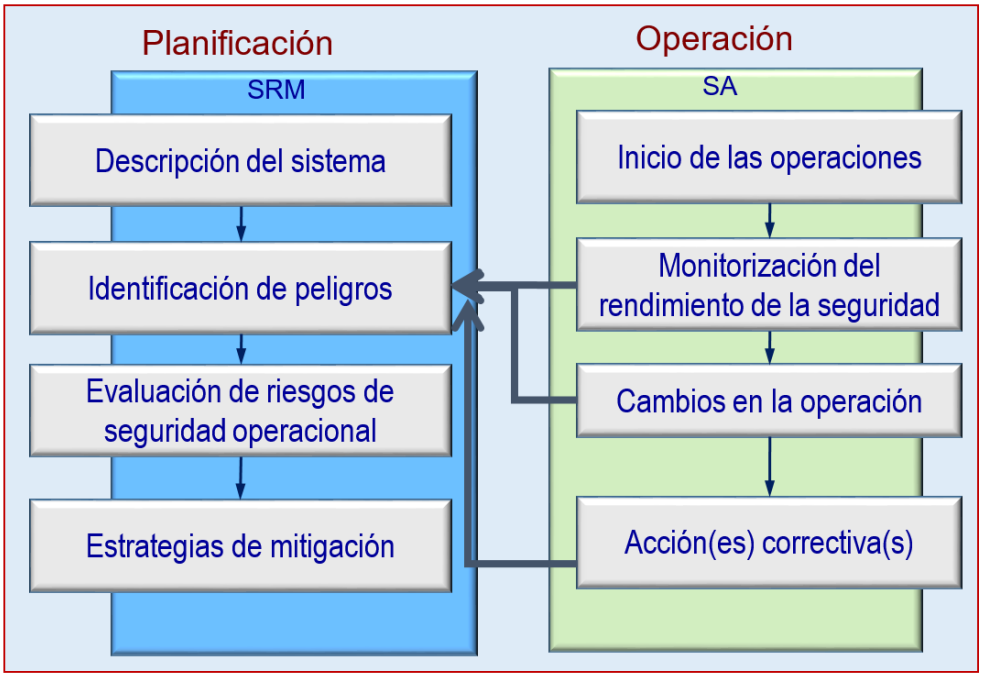
1. El capítulo 1 de esta Guía presenta una exposición inicial sobre los dos procesos básicos de SMS, de los cuales se derivan las actividades de mitigación de las deficiencias de seguridad y peligros en el contexto operativo: gestión de riesgo de seguridad operacional y aseguramiento de seguridad operacional. El capítulo 2 de la Guía se concentra sobre el primero de los dos procesos (gestión de riesgo de seguridad operacional). Este capítulo presenta el segundo proceso: aseguramiento de seguridad operacional.

2. El capítulo 2 es de considerable extensión, comparado con el presente capítulo. Esto obedece a una razón histórica: la aviación civil tiene un largo historial de excelencia en cuanto a gestión de riesgos de seguridad operacional, no en el sentido estricto del proceso propuesto por SMS, pero sí entendiendo el mismo en su sentido más amplio. Al fin y al cabo, la investigación de accidentes, una actividad que se iniciara con la aviación misma, es una forma de gestión de riesgos de seguridad operacional, la más practicada tradicionalmente y – complementada en años recientes por la investigación de incidentes – quizás aún la principal hoy en día si se toma en cuenta a la industria a nivel mundial. Las recomendaciones de seguridad operacional producto de tales investigaciones, y los programas de seguridad operacional que como consecuencia de las mismas se han implementado por décadas, son formas innegables de gestión de riesgo de seguridad operacional.

3. Tal largo historial no es el caso con el aseguramiento de seguridad operacional. Probablemente debido a la robustez de la convicción sobre la investigación de accidentes e incidentes – eventos de gran relevancia pero infrecuentes y de escasez estadística – como el mecanismo primario de aseguramiento de seguridad operacional, es que la tasa de accidentes ha sido el parámetro de garantía de seguridad operacional seleccionado por la industria, a expensas de otros parámetros de menor relevancia, pero de mayor frecuencia y abundancia estadística. Dicho de otra manera, en la medida que no se experimente un accidente o incidente, la presunción es que las medidas de mitigación contra las consecuencias de las deficiencias de seguridad operacional y los peligros funcionan al nivel esperado, es decir, que hay aseguramiento de seguridad operacional. En función de lo dicho anteriormente, la bibliografía sobre aseguramiento de la seguridad operacional no es copiosa como lo es la bibliografía sobre gestión de riesgos de seguridad operacional. No es impropio sugerir, parafraseando un poema popular, que en lo que a aseguramiento de seguridad operacional desde un punto de vista contemporáneo se refiere, no hay un claro camino, y se está haciendo camino al andar.

4. Según la exposición del capítulo 1, el aseguramiento *de seguridad operacional* se basa en la aplicación de *principios de calidad – adaptados a las necesidades de la gestión de la seguridad operacional* – al control de la ejecución de las actividades de mitigación de las consecuencias de peligros que comprometen la capacidad de un sistema de alcanzar su objetivo mediante la entrega de servicios. La simple

representación gráfica incluida a continuación, apoyada por texto explicativo, sirve para ilustrar la diferencia entre la visión tradicional de aseguramiento de seguridad operacional basada en el accidente/incidente como parámetro, y la visión de aseguramiento de la seguridad operacional bajo el marco del SMS, según lo articulado en la definición propuesta. Esto es necesario porque las sutilezas en las diferencias en relación entre la gestión de riesgos de seguridad operacional (*safety risk management, SRM*) y el aseguramiento de seguridad operacional (*safety assurance, SA*) son a menudo fuente de confusión.



5. La función de gestión de riesgos de seguridad operacional de un SMS es esencialmente una función asociada a la *planificación de las operaciones*. Se describe el sistema, es decir, se identifican los componentes y las condiciones del contexto operativo en el cual tendrán lugar las operaciones necesarias para la provisión de servicios con vista al logro del objetivo y las interacciones previstas entre tales componentes y condiciones; se completa la identificación inicial de peligros y la evaluación de los riesgos de seguridad operacional de las consecuencias que surjan de los peligros, en base a las interacciones previstas entre los componentes y condiciones; y se implementan mitigaciones contra las consecuencias. En este punto, se inician las operaciones cotidianas, bajo el supuesto que las mitigaciones incorporadas en el diseño son garantía suficiente de seguridad durante la operación.

6. Bajo la visión tradicional de aseguramiento de seguridad operacional basada en el accidente/incidente como parámetro, los supuestos empleados durante la planificación o diseño no sufrían modificación alguna; es decir, no había modificaciones en las mitigaciones incorporadas en el diseño, excepto que se experimentase un accidente o incidente. La columna de la derecha de la ilustración anterior, verdaderamente no existía.

7. Bajo la visión propuesta por SMS, la función de aseguramiento de seguridad operacional es una actividad íntimamente asociada a la *operación*. Se inicia en el momento que se inician las operaciones, para asegurar – por medio de la monitorización continua de las operaciones – que las mitigaciones contra las consecuencias de los peligros inicialmente identificadas funcionan de acuerdo a lo previsto y que logran sus objetivos previstos. Como consecuencia de la monitorización continua de las operaciones, el aseguramiento de seguridad operacional también permite la identificación de otros peligros que pudieron no haber sido identificados inicialmente, así como de otros debidos a la introducción de cambios en el entorno operacional, lo que a su vez lleva a la puesta en marcha de mitigaciones adicionales. Todo ello, *sin necesidad de experimentar un accidente o incidente.*

8. *El proceso de Gestión de riesgos de seguridad operacional*, entonces, permite al operador la evaluación de los riesgos de seguridad operacional en las operaciones que apoyan la prestación de servicios, y apoya las decisiones de seguridad operacional para la puesta en marcha de mitigaciones para mantener las consecuencias de los peligros a nivel ALARP. El proceso de *Aseguramiento de seguridad operacional* se concentra en actividades que permiten que el operador se demuestre a sí mismo y a los terceros con los que tiene relación durante las operaciones necesarias para la provisión de servicios, mediante recolección y análisis de evidencias objetivas, que las mitigaciones funcionan satisfactoriamente.

9. Por consiguiente, bajo un SMS, la gestión de riesgos de seguridad operacional (SRM) debe ser considerada como un proceso *inicial,* de diseño y planificación, mientras que el de aseguramiento de seguridad operacional es un proceso *continuo*, de vigilancia y control, que nunca se interrumpe mientras duren las operaciones. La sección final de este capítulo ofrece un ejemplo que permite visualizar a través de un simple escenario la interacción SRM/SA bajo un SMS.

10. Bajo la perspectiva englobada por el párrafo anterior, dos interrogantes son probables: ¿cuáles son las condiciones a partir de las cuales un operador ya establecido debe desencadenar el proceso gestión de riesgos de seguridad operacional? ¿Puede dar por buenos todos los controles y mitigaciones operativas actuales (sujeto a las actividades de aseguramiento de la seguridad operacional) y lanzar el proceso de gestión de riesgos de seguridad operacional sólo en base a cambios internos o externos relevantes? La respuesta es un rotundo sí. Un operador establecido condicionará sus actividades ya en marcha a los mecanismos de aseguramiento de la seguridad operacional, y lanzará el proceso de gestión de riesgos de seguridad operacional al abrir nuevas rutas, al operar en nuevos aeródromos, al incorporar nueva tecnología, al implementar nueva normativa; en definitiva, ante cualquier situación que implique cambios en el sistema establecido que puedan disminuir la validez de controles y mitigaciones en pie.

11. De la misma manera que los cuatro principios básicos de la gestión de riesgos de la seguridad operacional proporcionaron un "plan de vuelo" para el desarrollo del

capítulo 2, la exposición sobre aseguramiento de seguridad operacional en este capítulo sigue el "plan de vuelo" proporcionado por la columna derecha de la ilustración sobre la relación SRM/SA ya expuesta. Este capítulo también incluye dos apéndices, que exponen dos perspectivas o alternativas para la medición de la actuación en materia de seguridad operacional.

6.2 INICIO DE LAS OPERACIONES

12. No se considera necesario abundar sobre este aspecto, dado que es obvio. Iniciadas las operaciones, el aseguramiento de seguridad operacional en SMS funciona en forma similar a la garantía de la calidad en QMS (*Quality Management Systems*). Las actividades de aseguramiento de seguridad operacional de SMS se han derivado de la norma ISO 9001-2000; norma internacional de gestión de la calidad. No obstante, existe una diferencia importante: los requisitos de QMS están orientados al cliente y su satisfacción; los requisitos de SMS son requisitos de seguridad operacional y están orientados a la satisfacción de la misma.

6.3 OBSERVACIÓN Y MEDICIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL

13. *Aseguramiento* puede definirse, de la forma más sencilla, como "*algo que da confianza*". Una vez que se han puesto en marcha las mitigaciones contra las consecuencias de los peligros en el contexto operativo en el cual tienen lugar las operaciones necesarias para la entrega de servicios, es responsabilidad del operador asegurar que funcionan según lo previsto. En el marco de la sencilla definición anterior de "aseguramiento", esto consiste en que el operador debe llevar a cabo actividades para brindar confianza sobre la eficacia y efectividad de las mitigaciones. El operador debe supervisar de manera continua y rutinaria sus operaciones para identificar:

    a) cambios que puedan producirse en el contexto operativo y que podrían indicar el potencial de peligros nuevos o consecuencias no mitigadas; y/o

    b) eventual deterioro en los procedimientos operacionales, instalaciones, condiciones del equipo, que pudieran reducir la efectividad de las mitigaciones vigentes contra consecuencias de peligros.

14. Cualquiera de las dos condiciones enumeradas en el párrafo anterior indicaría la necesidad de lanzar un nuevo ejercicio de gestión de riesgos de seguridad operacional para examinar y, si es necesario, modificar las mitigaciones existentes o poner en marcha nuevas mitigaciones. El análisis y la evaluación permanentes de estas mitigaciones a través de la observación y medición del rendimiento en materia de seguridad operacional deben continuar durante la operación cotidiana del sistema, de forma análoga a los análisis y a las evaluaciones de garantía de la calidad, con requisitos relativos al análisis, auditoría, verificación, y documentación por el operador de la efectividad de las mitigaciones. Las actividades de aseguramiento de seguridad operacional deben también incluir procedimientos que

aseguren la puesta en marcha de medidas correctivas en respuesta a los resultados de los análisis de datos, notificaciones de sucesos, encuestas, auditorías, etc.

15. La tarea principal de la observación y medición del rendimiento en materia de seguridad operacional es el control. A continuación se presenta una lista de aspectos o áreas genéricas que han de considerarse para lograr tal control, para "asegurar la seguridad operacional", mediante la observación y medición del rendimiento en materia de seguridad operacional:

    a) *responsabilidad:* quién es responsable de la gestión de las actividades de aseguramiento de seguridad operacional (planificación, organización, dirección, control) en apoyo de las operaciones y su logro final;

    b) *autoridad:* quién puede dirigir, controlar o modificar los procedimientos operativos y quién no, así como quién puede adoptar decisiones clave con respecto a las decisiones de aceptación de riesgos de seguridad operacional de las consecuencias de los peligros;

    c) *procedimientos:* cuáles son las formas específicas de realizar las actividades operacionales que transforman el "qué" (objetivos) en "cómo" (actividades prácticas);

    d) *recursos:* cuáles son los recursos del operador, incluyendo instalaciones, soporte informático, procedimientos especiales, así como prácticas de supervisión, necesarios para la realización correcta de las actividades operacionales;

    e) *interfaces:* ¿cuáles son las líneas de autoridad entre departamentos, y líneas de comunicación entre personal operativo? Hay coherencia de procedimientos y clara delimitación de responsabilidades entre departamentos, sectores y personal operativo; y

    f) *medidas de control:* cuáles son los medios que proporcionan información a las partes responsables que las actividades operacionales se están realizando y los resultados previstos se están alcanzando.

16. La observación y medición del rendimiento en materia de la seguridad operacional se basa fundamentalmente en la adquisición de datos de naturaleza operativa, a través de cuyo análisis el operador puede medir la eficacia de las mitigaciones de las consecuencias de los peligros e identificar peligros adicionales durante la provisión de servicios, y determinar de tal manera el rendimiento en materia de seguridad operacional de su sistema.

17. Los datos para alimentar la observación y medición del rendimiento en materia de seguridad operacional proceden de varias fuentes, que en términos generales incluyen aportes del personal operativo a través de los programas de notificación de sucesos; programas de análisis de datos de vuelo y observación directa de las

operaciones cotidianas relacionadas con la prestación de servicios; auditorías formales; encuestas de seguridad operacional al personal; e investigaciones internas de seguridad operacional. Cada una de estas fuentes de datos existe en alguna medida en todos los operadores, dejando a cada operador que las adapte al ámbito y escala adecuados al tamaño y tipo de su organización.

18. ***Programas de notificación de sucesos.*** Las notificaciones de sucesos son elementos esenciales para la observación y medición del rendimiento en materia de seguridad operacional, así como para el aseguramiento de seguridad operacional como un todo. Nadie conoce mejor cómo funciona *realmente* un sistema que el personal operativo. Para saber cómo funciona el día a día de las operaciones, *realmente*, no como dice "el manual", más vale preguntarle al personal operativo que leer el "manual". El capítulo 2 presenta la noción de la *deriva práctica* y señala que el personal operativo realiza las actividades necesarias para la prestación de servicios dentro de la deriva práctica. En virtud de ello, convive diariamente con deficiencias de seguridad, peligros y sus consecuencias, que en muchos casos, a su vez, no han sido formalmente gestionados. Por ende, la exposición en el capítulo 2 sobre identificación de peligros concluye con un claro corolario sobre la importancia primordial de los programas de notificación de sucesos como elemento fundamental para la captación de la *deriva práctica* y la implementación y efectivo mantenimiento del SMS por un operador.

19. De acuerdo con las disposiciones que emanan de OACI, se puede distinguir tradicionalmente dos tipos de programas de notificación de sucesos: programas de notificaciones obligatorias y programas de notificaciones voluntarias. En Europa, las disposiciones de OACI se han transpuesto mediante el Reglamento (UE) No 376/2014 del Parlamento Europeo Y del Consejo de 3 de abril de 2014 relativo a la notificación de sucesos en la aviación civil, que modifica el Reglamento (UE) no 996/2010 del Parlamento Europeo y del Consejo, y por el que se derogan la Directiva 2003/42/CE del Parlamento Europeo y del Consejo y los Reglamentos (CE) no 1321/2007 y (CE) no 1330/2007 de la Comisión. Una breve descripción de cada tipo de programa sigue a continuación:

a) En los programas de notificaciones obligatorias (Art. 4 del Reglamento (UE) No 376/2014), el personal operativo debe notificar ciertos tipos de sucesos que están claramente especificados en normas internacionales, que a su vez han sido traspuestas a normas nacionales. Esto exige directivas detalladas que establezcan quiénes deberán notificar y qué deberá notificarse. En el caso de Europa, el Reglamento de Ejecución (UE) 2015/1018 de la Comisión de 29 de junio de 2015 por el que se establece una lista de clasificación de los sucesos en la aviación civil de notificación obligatoria de conformidad con el Reglamento (UE) no 376/2014 del Parlamento Europeo y del Consejo. Los programas de notificaciones obligatorias informan sobre eventos de cierta gravedad, aunque no necesariamente catastróficos, y por sus orígenes y naturaleza recogen primariamente información sobre fallos técnicos. En Europa, de acuerdo con las disposiciones del Reglamento (UE) No 376/2014, los Estados miembros, EASA y los operadores no pondrán a disposición ni utilizarán los datos de sucesos: 1)

para determinar la culpa o responsabilidad; o 2) para ninguna finalidad distinta de mantener y mejorar la seguridad aérea. Además, excepto en casos de dolo o negligencia grave, de entablarse procedimientos disciplinarios o administrativos en aplicación del Derecho nacional, la información contenida en las notificaciones de sucesos no se utilizará contra: 1) los notificantes; o 2) las personas que aparezcan mencionadas en las notificaciones de sucesos.

b) En los *programas de notificaciones voluntarias* (Art. 5 del Reglamento (UE) No 376/2014), el personal operativo, sin ninguna obligación normativa, proporciona voluntariamente información y datos sobre sucesos que puedan no ser captados por el sistema de notificación obligatoria u otra información relacionada con la seguridad que el notificante perciba como un peligro real o potencial para la seguridad aérea. En estos programas, el operador y el Estado, incentivan la notificación de sucesos, ofreciendo una medida de protección a quienes reportan de la aplicación de medidas disciplinarias, siempre y cuando no haya negligencia grave ni intención dolosa. En Europa, la reglamentación protege tanto los sistemas de notificación voluntaria como los sistemas de notificación obligatoria: "*Art. 16.6 del Reglamento (UE) No 376/2014: Sin perjuicio del Derecho penal nacional aplicable, los Estados miembros se abstendrán de entablar procedimientos en relación con infracciones no premeditadas o realizadas por descuido que hayan llegado a su conocimiento solo por haber sido notificadas en virtud de los artículos 4 (notificación obligatoria) y 5 (notificación voluntaria).*" La información notificada no se usa contra quienes notifican; es decir, que estos programas brindan protección a las fuentes de información para fomentar la disponibilidad de dicha información. Debido a esto, los programas de notificaciones voluntarias informan sobre eventos de menor gravedad (aunque con significativo potencial de daño) y recogen primariamente información sobre deficiencias de seguridad operacional, peligros, procedimientos y desempeño humano operativo.

20. ***Observación directa de las operaciones cotidianas***. Estos programas captan el funcionamiento de las operaciones en tiempo real, y se fundamentan sobre la misma justificación que los programas de notificación de sucesos: captar datos sobre lo que ocurre diariamente en el contexto operativo durante el transcurso de las operaciones necesarias para la entrega de servicios, para verificar el funcionamiento real de controles y mitigaciones, y su empleo por el personal operativo, así como identificar peligros no previstos. Se trata de captar la operación tal como realmente tiene lugar, y no como debería ser según lo especificado, para analizar las diferencias y realimentar controles y mitigaciones en función de ellas. En otras palabras, se trata de captar lo que ocurre diariamente dentro de la *deriva práctica.* Existen dos tipos de observación directa de operaciones diarias:

a) *Análisis de datos de vuelo:* son programas electrónicos que capturan parámetros de vuelo en tiempo real, y su análisis es una valiosa ayuda para el diagnóstico de situaciones que tienen que ver con desviaciones de parámetros operacionales establecidos y el funcionamiento de los sistemas de las aeronaves. Un uso típico del análisis de datos de vuelo es la

monitorización de aproximaciones no estabilizadas. Es importante tener en cuenta que los programas de análisis de datos de vuelo sólo proporcionan parámetros, es decir, datos en el más estricto sentido de la palabra. Por lo tanto, estos programas informan qué pasó, pero no del porqué. El establecimiento por parte del operador de un programa de análisis de datos de vuelo es una norma internacional promulgada por OACI y recogida en el Reglamento (UE) No 965/2012 de la Comisión de 5 de octubre de 2012, ORO.AOC.130 Análisis de los datos de vuelo — aviones, por lo tanto, de cumplimiento obligatorio.

b) *Programas de observación directa:* estos programas capturan aspectos específicos del contexto operativo, incluyendo el rendimiento real de controles y mitigaciones, así como el del personal operativo, también en tiempo real. Esto se logra a través de la observación directa de las operaciones por observadores, que han sido rigurosamente entrenados y respetan un estricto protocolo de observación. En virtud de ello, estos programas no solamente generan datos sino también información sobre el contexto en el cual los datos se originan, informando por lo tanto no solamente del *qué* pasó, sino también del *porqué*. Debido a ello, los programas de observación directa son un complemento ideal de los programas de análisis de datos de vuelo. Un ejemplo de programa de este tipo existente para operadores es conocido como *Line Operations Safety Audit (LOSA).* La OACI avala este programa, y ha publicado un manual sobre el mismo *(Auditoría de la seguridad de las operaciones de línea aérea (LOSA) (Doc. 9803).*

21. ***Auditorías formales.*** La contribución de las auditorías a la observación y medición del rendimiento en materia de seguridad operacional se concentra en velar por la integridad de los elementos constitutivos del SMS del operador. Mientras que los programas expuestos anteriormente son de operación continua, las auditorías se llevan a cabo a intervalos puntuales. Bajo la perspectiva de la observación y medición del rendimiento en materia de seguridad operacional, la contribución real de las auditorías no es tanto profundizar en los procedimientos técnicos sino más bien proporcionar garantías de la integridad de las funciones del proceso de aseguramiento de seguridad operacional, así como de la integridad de las actividades y recursos de los departamentos operativos directamente involucrados en las actividades de entrega de servicios. Asimismo, las auditorías se utilizan para asegurar que la estructura de SMS es sólida en términos de niveles de recursos, cumplimiento de los procedimientos, niveles de competencia e instrucción para operar equipos e instalaciones y mantener niveles de rendimiento requeridos, etc. Si bien las auditorías son "externas" a las dependencias involucradas en las actividades directamente relacionadas con la provisión de servicios, son "internas" al operador en su totalidad.

22. ***Encuestas de seguridad operacional al personal.*** Las encuestas de seguridad operacional examinan elementos particulares o procedimientos de una operación específica; por ejemplo, áreas con problemas o cuellos de botella en las operaciones

diarias, para los cuales los datos de los otros programas de observación y medición del rendimiento en materia de seguridad operacional no proporcionan una respuesta. Una encuesta de seguridad operacional consiste simplemente en solicitar la opinión del personal operativo directamente involucrado en la operación en cuestión, sus percepciones y las áreas de confusión. Las encuestas de seguridad operacional pueden apoyarse en el uso de listas de verificación, cuestionarios y/o entrevistas confidenciales informales. Dado que la información de las encuestas de seguridad operacional es subjetiva, es necesaria una depuración antes de poner en marcha medidas correctivas. Las encuestas de seguridad operacional al personal suponen una fuente importante de información de seguridad operacional, y de bajo coste.

23. ***Investigaciones internas de seguridad operacional.*** Se llevan a cabo para ciertos eventos de seguridad operacional de notificación obligatoria de acuerdo con requisitos internos o regulatorios. Los accidentes e incidentes graves, investigados por las autoridades de aviación civil, también pueden desencadenar investigaciones internas por parte del operador.

6.4 CAMBIOS EN EL CONTEXTO OPERATIVO Y/O LAS OPERACIONES

24. Si hay una constante a la que está expuesto un operador en la aviación comercial, tal constante es: el cambio. Los operadores experimentan cambios permanentes debido a expansión, contracción, cambios en los sistemas existentes, equipos, programas, productos y servicios, introducción de nuevos equipos o procedimientos, etc. Cada vez que se introduce un cambio en el sistema del operador, por minúsculo que sea, se abre la puerta a la introducción inadvertida de nuevos peligros. El cambio puede introducir nuevos peligros, impactar en la adecuación de las estrategias de mitigación de las consecuencias de los peligros existentes, o afectar a la eficacia de esas estrategias. Los cambios pueden ser externos al operador o internos. Ejemplos de cambios externos serían cambios de los requisitos reglamentarios, cambios en los requisitos de seguridad aeroportuaria y reorganización del control del tránsito aéreo, por citar unos pocos. Ejemplos de cambios internos serían cambios de administración, introducción de nuevas operaciones, cambios de equipamiento o procedimientos, etc. Es función de las actividades de aseguramiento de la seguridad operacional, por medio de la gestión del cambio, asegurar que los peligros que son resultados secundarios de los cambios sean sistemática y proactivamente identificados, y que se pongan en funcionamiento mitigaciones contra las consecuencias de los mismos.

25. En el Capítulo 4 de esta Guía se analiza la importancia de describir el sistema (descripción del sistema) como una de las actividades preliminares fundamentales en la planificación de un SMS. El objetivo de la descripción del sistema es establecer un análisis inicial de referencia sobre peligros para el futuro del sistema. Este análisis de peligros de referencia sirve como matriz, ya que a medida que el sistema evoluciona con el tiempo, se van acumulando cambios graduales y aparentemente pequeños en el contexto operativo, que harán que la descripción inicial del sistema deje de ser una referencia adecuada. Por consiguiente, como parte del protocolo de gestión del cambio, la descripción del sistema y el análisis inicial de peligros de

referencia deberían re-examinarse periódicamente, incluso si no existen circunstancias obvias o evidentes de cambio, para determinar su validez. Cuando se introducen cambios en las operaciones, y periódicamente *a posteriori*, el operador debería examinar el contexto operativo anticipado y el contexto real, para asegurar que continúa existiendo un panorama claro de las circunstancias bajo las cuales tiene lugar la prestación de servicios.

26. Por consiguiente, como parte del proceso de aseguramiento de seguridad del SMS, el operador debería establecer un procedimiento formal gestión del cambio para identificar los cambios en la organización que puedan afectar a los procedimientos y a los servicios establecidos. Antes de implantar cambios, el procedimiento de gestión del cambio debería asegurar la puesta en marcha de mitigaciones para asegurar la actuación en materia de seguridad operacional tras los cambios, al efecto de mantener bajo control las consecuencias de los nuevos peligros que podrían haber sido introducidas por el cambio durante el suministro de servicios.

27. Al establecer un procedimiento formal para la gestión del cambio, el operador debería tener en cuenta las tres consideraciones siguientes:

a) *Criticidad del equipamiento y actividades.* La criticidad se relaciona estrechamente con el control de las consecuencias de los peligros. La criticidad se refiere a las consecuencias potenciales en caso que el equipo sea inadecuadamente operado o que un procedimiento se ejecute en forma incorrecta, y esencialmente responde a la pregunta: *"¿cómo afecta este equipo/procedimiento para las operaciones seguras del sistema?"* Si bien esta es una consideración que debería tenerse en cuenta durante el diseño del sistema, se hace más evidente durante una situación de cambio. Por otro lado, cuando se introducen cambios es como que se está diseñando un nuevo sistema. Claramente, algunos procedimientos son más esenciales para la prestación segura de servicios que otros. Por ejemplo, los cambios en procedimientos relativos al retorno al servicio de una aeronave después de un mantenimiento mayor en un operador que ha implantado por primera vez su propia organización de mantenimiento después de subcontratar previamente dicho mantenimiento a terceros, es indudablemente más crítica para la seguridad operacional que un escenario similar respecto de cambios en los procedimientos de los servicios de comidas para pasajeros (*catering*). El equipo y los procedimientos que tienen una criticidad más elevada respecto de la seguridad operacional deberían ser objeto central de examen después de cambios para facilitar la eventual adopción de medidas correctivas a fin de controlar posibles riesgos de seguridad operacional emergentes.

b) *Estabilidad de las operaciones y el contexto operativo.* Los cambios en las operaciones pueden ser resultado de cambios programados como crecimiento, operaciones a nuevos destinos, cambios en las flotas, cambios en los servicios contratados u otros cambios directamente bajo control de la organización. Los cambios en el contexto empresarial son también importantes, tales como cambios en la situación económica o financiera, la

situación laboral, cambios en entornos políticos o normativos. De no menor importancia son los cambios en el entorno físico como los que se producen cíclicamente en los sistemas meteorológicos. Si bien estos factores no están bajo control directo del operador, éste debe adoptar medidas para responder a ellos. Los cambios frecuentes en las operaciones, el entorno empresarial o físico hacen que el operador deba actualizar información clave con mayor frecuencia que en situaciones más estables. Esta es una condición esencial para la gestión del cambio.

c) *Funcionamiento previo.* El funcionamiento previo (vale decir, antes de la introducción de cambios en las operaciones) del equipamiento crítico es un indicador válido del funcionamiento futuro, tras cambios en las operaciones. Es aquí donde entra en juego el carácter de "cierre del círculo" del aseguramiento de seguridad operacional. El empleo de análisis de tendencias, en el proceso de aseguramiento de seguridad operacional, para hacer el seguimiento en el tiempo de la medición del rendimiento en materia de la seguridad operacional, proporciona valiosa información para la planificación de actividades futuras en situaciones de cambio. Además, donde se hayan encontrado y corregido deficiencias como resultado de auditorías, evaluaciones, investigaciones o informes anteriores, es esencial que dicha información se tenga en cuenta para asegurar la efectividad de las medidas correctivas.

6.5 ACCIÓN CORRECTIVA

28. Como cierre del círculo de aseguramiento de seguridad operacional, el operador debe tomar acción correctiva para rectificar cualquier desfase entre el funcionamiento anticipado de las mitigaciones de las consecuencias de los peligros anticipados, o bien de nuevos peligros introducidos por situaciones de cambio, y para eliminar sus causas con objeto de evitar, de ser posible, que situaciones similares vuelvan a darse en el futuro.

29. Las medidas de acción correctiva como consecuencia de actividades de aseguramiento de seguridad operacional serán similares a las medidas adoptadas como consecuencia de la gestión de riesgos de seguridad operacional (expuestas en el capítulo 2 bajo el título *Medición y control*). Estas medidas estarán basadas en la puesta en marcha o el refuerzo de variantes de las tres defensas básicas del sistema aeronáutico: tecnología, instrucción y normativa (incluyendo los procedimientos del operador). La diferencia básica es que la gestión de riesgos de seguridad operacional es una actividad de planificación, y como tal, mira hacia el futuro. Por lo tanto, se diseña una arquitectura básica, que debe ser convalidada por la práctica operativa, tras el inicio de las operaciones. El aseguramiento de la seguridad operacional, en cambio, es una actividad de ejecución, y tiene lugar en el presente. Por lo tanto, corrige desfases entre el funcionamiento previsto de las operaciones y el real (si aquél fuese insatisfactorio), acomoda aspectos específicos de la operación que la práctica diaria evidencia que no han sido adecuadamente considerados durante las hipótesis de planificación, o bien propone controles o mitigaciones para las

consecuencias de los peligros que son producto de cambios en las operaciones con respecto a la planificación inicial.

6.6 SRM Y SA – UN EJEMPLO CONJUNTO

30. Como cierre ilustrativo de los pasos conjuntos a observar en la gestión de riesgos de seguridad operacional (SRM) y aseguramiento de seguridad operacional (SA) según lo expuesto en los capítulos 2 y 3, se presenta un simple ejemplo que se refiere a una operación bajo lista de equipamiento mínimo (*Minimum Equipment List, MEL).* El operador en cuestión va a iniciar una nueva operación, para la cual es necesario establecer los procedimientos operativos, incluyendo el uso de la MEL. Una preocupación particular es el tipo de piloto automático con el cual están dotados las aeronaves del operador, que tiene un historial de fallos intermitentes de difícil identificación *a priori*, durante las inspecciones periódicas. Por lo tanto, y a los efectos de acotar el ejemplo, el mismo está limitado solamente al análisis de la operación MEL con piloto automático inoperativo. Un análisis desde la perspectiva del operador debería observar los siguientes pasos.

6.7 PLANIFICACIÓN – SRM

31. *Descripción del sistema.* En este paso, se debe analizar el tipo de operación, el personal que la ejecutará, el contexto operativo, y las mitigaciones de riesgos de seguridad operacional ya existentes, bajo la forma de normas, estándares y procedimientos. Se trata de un operador que opera aeronaves bimotores de mediano porte en operaciones regulares de transporte de pasajeros. El operador dispone de una lista *Master* de equipamiento mínimo *(Master Minimum Equipment List, MMEL)* para el tipo de aeronave, que debe transformar en una MEL propia para la nueva operación a iniciarse. La normativa exige que haya un copiloto para operaciones IFR cuando el piloto automático se encuentra inoperativo. Todas las aeronaves del operador están equipadas, y sus pilotos entrenados y habilitados, para operaciones con un solo piloto, por lo que el operador desea operar con un solo piloto aún en el caso que el piloto automático esté inoperativo.

32. *Identificación de peligros y sus consecuencias*. En este paso, se individualizan los peligros que son inherentes a operaciones IFR con un solo piloto y con el piloto automático inoperativo, y sus consecuencias. Siendo el peligro genérico *"operación con un solo piloto con piloto automático inoperativo"*, un componente o peligro específico del mismo es la *"operación en condiciones de vuelo instrumentales reales"*. Las consecuencias posibles de este peligro, por ejemplo, pérdida de control de la aeronave por el piloto, están en principio mitigadas bajo la normativa existente por los requerimientos de un copiloto cuando el piloto automático está inoperativo. En todo caso, todas y cada una de las posibles consecuencias deben ser analizadas para determinar su significación operativa, el riesgo de seguridad operacional que generan, y las mitigaciones existentes. Ejemplos de otras consecuencias incluyen la ejecución incorrecta de procedimientos con y sin piloto automático, y con y sin copiloto. Hay muchas actividades de la cabina de mando

en las cuales el piloto automático no puede ser sustituto del copiloto (seleccionar ayudas a la navegación, radiocomunicaciones, lectura de listas de verificación, etc.). También, en una tripulación compuesta pueden generarse cuestiones de coordinación entre la tripulación. A los efectos del ejemplo, nos limitaremos a dos posibles consecuencias del peligro específico "*operación en condiciones de vuelo instrumentales reales"*: la ya mencionada pérdida de control en vuelo, y accidentes de vuelo controlado contra el terreno (CFIT).

33. *Evaluación de riesgos de seguridad operacional*. En este paso, se evalúa y cuantifica la relevancia de cada una de las consecuencias de los peligros identificados. Respetando las pautas del ejemplo, el operador considera que las dos consecuencias operativas del peligro específico "*operación en condiciones de vuelo instrumentales reales" (*accidentes de vuelo controlado contra el terreno (CFIT) o pérdida de control en vuelo) son de elevada severidad, ambas potencialmente catastróficas. Utilizando la matriz de riesgos de seguridad operacional de su SMS, el operador evalúa el riesgo de seguridad operacional como *remoto* (3) pero *catastrófico* (A). La combinación 3A es *inaceptable bajo las circunstancias existentes*. Es por lo tanto necesario introducir adaptaciones de la MMEL para la operación (MEL) por el operador con un solo piloto y piloto automático inoperativo para determinar si es posible reducir el riesgo de seguridad operacional de las consecuencias a un nivel ALARP.

34. *Estrategias de mitigación*. En este paso se definen procedimientos para ser incorporados en la MEL del operador. Los procedimientos a incorporar en la MEL abarcan:

- el piloto automático debe ser desactivado y retirado de la aeronave por personal de mantenimiento debidamente cualificado;
- los pilotos deben ser notificados que el piloto automático se encuentra inoperativo por medio del sistema de registro técnico de la aeronave, así como por un cartel en el *cockpit*; y
- no se puede operar sin piloto automático por más de 10 (diez) días.

La re-evaluación del operador utilizando la matriz de riesgo concluye que el riesgo de seguridad operacional de las consecuencias *CFIT* y *pérdida de control en vuelo* siguen siendo 3ª; es decir, que las mitigaciones propuestas no disminuyen ni la probabilidad ni la severidad de las consecuencias. La conclusión del operador es que es necesario integrar un copiloto a la tripulación en caso de operación con piloto automático inoperativo. Los procedimientos a incorporar a la MEL se expanden de la siguiente manera:

- el piloto automático debe ser desactivado y retirado de la aeronave por personal de mantenimiento debidamente cualificado;
- los pilotos deben ser notificados que el piloto automático se encuentra inoperativo por medio del sistema de registro técnico de la aeronave, así como por un cartel en el *cockpit*;
- no se puede operar sin piloto automático por más de 10 (diez) días; y

- debe programarse un copiloto que esté habilitado en la aeronave y con los requerimientos de vigencia al día.

Es fundamental establecer claramente y sin ambigüedades que la operación MEL con el piloto automático inoperativo será aceptable solamente si los nuevos procedimientos a incorporarse como mitigación se respetan, de lo contrario la operación en tales condiciones debe ser re-evaluada.

6.8 OPERACIÓN – SA

35. *Inicio de las operaciones.* En este paso, las aeronaves comienzan las operaciones, y el operador debe determinar las áreas de su sistema sobre las cuales deberá prestar particular atención en su monitorización de las operaciones, para verificar que las estrategias de mitigación funcionan de acuerdo con lo esperado. Tales áreas incluyen:

- *Operaciones e instrucción*. Debe verificarse la disponibilidad en tiempo y forma de copilotos habilitados, así como que los copilotos han completado la formación en *Crew Resource Management (CRM)* que les permite operar como miembros de una tripulación según la normativa vigente. Todos los pilotos deben conocer la limitación del máximo de 10 días para la operación sin piloto automático.
- *Despacho*. Los despachadores de vuelo deben estar al tanto de los requerimientos MEL para el despacho con piloto automático inoperativo, incluyendo la limitación de los 10 días.
- *Mantenimiento*. Los mecánicos deben estar al tanto de los requerimientos MEL, y en especial del plazo máximo para reparar los pilotos automáticos para evitar la puesta fuera de servicio de las aeronaves una vez que haya expirado el plazo máximo.

36. *Observación y medición de la actuación en materia de seguridad operacional.* En este paso, el "*technical logbook*" de las aeronaves será una de las principales fuentes de datos para la observación y medición de la actuación en materia de seguridad de las operaciones MEL con el piloto automático inoperativo. También lo serán los informes de despacho, los registros de mantenimiento y las órdenes de compras de repuestos para los pilotos automáticos. Asimismo, los registros de actividad de pilotos son una fuente a considerar, dado que habrá vuelos que requieren dos pilotos. Tales registros permiten corroborar si se observa las mitigaciones (dos pilotos, 10 días) así como el eventual impacto en las operaciones (demoras, cancelaciones). Otra importante fuente de datos es el programa de notificaciones de sucesos, para constatar el estado de situación real de las mitigaciones.

37. *Cambios en la operación*. En este paso, a través del programa de notificaciones de sucesos, el operador toma conocimiento que el retiro de los componentes electrónicos del piloto automático para su reparación genera frecuentemente fallos intermitentes del sistema compás número 1 (del lado del comandante), lo que aumenta de manera significativa la carga de trabajo en condiciones instrumentales

reales. La interrelación entre componentes electrónicos del piloto automático y el sistema compás número 1 no es obvia ni evidente en los diagramas de mantenimiento, por lo cual no fue tenida en cuenta al definir los procedimientos MEL. Los procesos de SA del operador han así detectado una degradación en la eficacia de las mitigaciones propuestas, que de otra manera muy probablemente hubiera sido detectada con posterioridad a un evento significativo, por ejemplo, un incidente.

38. *Acción correctiva.* En este paso, sobre la base de los reportes de sucesos, mantenimiento consulta con el fabricante del piloto automático y recibe la información necesaria para introducir una modificación al procedimiento de retirar los componentes electrónicos del piloto automático que elimina los fallos intermitentes del sistema compás número 1.

39. Como conclusión de cierre, es apropiado convenir que el ejemplo presentado abarca actividades que no son ni nuevas en la práctica aeronáutica ni exclusivas de SMS. Sin embargo, SMS proporciona una secuencia estructurada y debidamente documentada de actividades por medio de sus dos procesos básicos (SRM y SA), y ofrece al operador un conjunto integral de prácticas que asegura el control a un grado razonablemente practicable de las consecuencias de los peligros que debe enfrentar durante la provisión de sus servicios.

6.9 APÉNDICE 1 AL CAPÍTULO 3: OBSERVACIÓN Y MEDICIÓN DEL RENDIMIENTO EN MATERIA DE SEGURIDAD OPERACIONAL DE SMS

Se recomienda como lectura adicional el Material guía de la OACI, Manual de gestión de la seguridad operacional (Doc. 9859) en su 4ª Edición.

La introducción de un conjunto de indicadores de rendimiento en materia de seguridad operacional (*safety performance indicators - SPIs*) responde a la necesidad de complementar el enfoque tradicional de la gestión de la seguridad operacional basada en el cumplimiento normativo, con un enfoque basado en el desempeño. Tal enfoque evaluará la eficacia real de las actividades críticas para la gestión de la seguridad operacional con respecto a los controles organizacionales existentes. La combinación de ambos enfoques es necesaria para una eficaz implantación de SMS que permita alcanzar el objetivo de mejora continua de la seguridad operacional en que se basa la gestión de la seguridad operacional.

El desarrollo de un conjunto de indicadores cuantificables relacionados con el rendimiento en materia de seguridad operacional de SMS se basa en ciertos conceptos, cuya comprensión es un fundamento esencial para la elaboración de los parámetros. Los conceptos involucrados, y sus jerarquías correspondientes, son los siguientes:

a) **Seguridad operacional –** Estado en el que los riesgos asociados a las actividades de aviación relativas a la operación de las aeronaves, o que apoyan directamente dicha operación, se reducen y controlan a un nivel aceptable.

b) **Rendimiento en materia de seguridad operacional –** Logro de un Estado o un proveedor de servicios en lo que respecta a la seguridad operacional, de conformidad con lo definido mediante sus metas e indicadores de rendimiento en materia de seguridad operacional.

c) **Indicadores de rendimiento en materia de seguridad operacional** – Parámetro basado en datos que se utiliza para observar y evaluar el rendimiento en materia de seguridad operacional.

d) **Metas de rendimiento en materia de seguridad operacional** – La meta proyectada o prevista del Estado o proveedor de servicios que se desea conseguir, en cuanto a un indicador de rendimiento en materia de seguridad operacional, en un período de tiempo determinado que coincide con los objetivos de seguridad operacional.

Por tanto, resulta necesario definir un conjunto de indicadores de rendimiento en materia de seguridad operacional y su cuantificación, como elementos que permiten determinar si el sistema funciona de acuerdo con los objetivos de su diseño durante las operaciones de entrega de servicios, y no solamente que satisface requisitos normativos.

La definición de un conjunto de indicadores de rendimiento en materia de seguridad operacional y su cuantificación también permite identificar dónde pueden necesitarse correcciones para mantener o reencauzar el rendimiento en materia de seguridad operacional del sistema al nivel previsto por los objetivos de diseño del sistema.

En consecuencia, la identificación de los indicadores de rendimiento en materia de seguridad operacional debe ser realista, relevante y estar vinculada a los objetivos de seguridad, independientemente de su simplicidad o complejidad.

Además, un conjunto de indicadores de rendimiento en materia de seguridad operacional y su cuantificación también permite evaluar la eficacia real de los controles y mitigaciones de la gestión de la seguridad operacional, de modo que puedan adoptarse las medidas correctivas necesarias y controlarse las consecuencias de los peligros en el contexto operativo en el cual tienen lugar las operaciones necesarias para la provisión de servicios en un nivel ALARP.

La selección de indicadores de rendimiento en materia de seguridad operacional apropiados es fundamental para la observación y medición del rendimiento en materia de seguridad operacional de SMS. Dicha selección debe ser función del detalle con el cual se prevea representar el nivel aceptable de rendimiento en materia de seguridad operacional del sistema. Si se desea representar la medición del rendimiento en materia de seguridad operacional en términos amplios y genéricos, es apropiada la selección de indicadores de rendimiento en materia de

seguridad operacional que representen consecuencias de relativa relevancia. Si se desea representar la medición del rendimiento en materia de seguridad operacional en términos específicos y más definidos, entonces se requiere la selección de indicadores que representen consecuencias de muy escasa severidad. En ambos casos, para que los indicadores de rendimiento en materia de seguridad operacional sean significativos deben ser representativos de las operaciones asociadas a la entrega de servicios que caracterizan el contexto particular del operador.

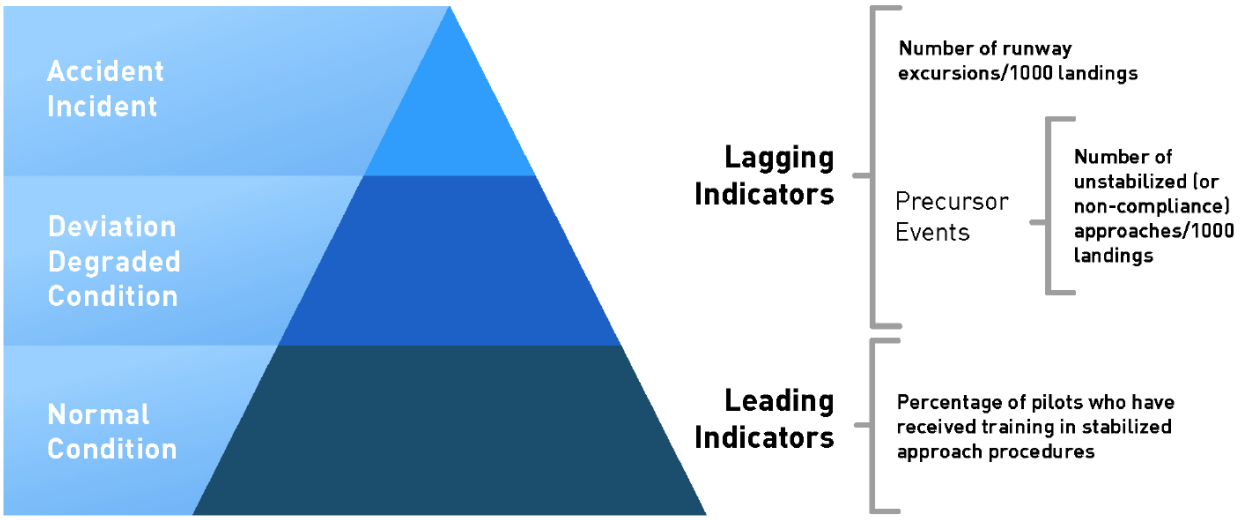
El primer paso en la definición de los indicadores de rendimiento en materia de seguridad operacional, y por ende, de la medición del rendimiento en materia de seguridad operacional de SMS por el operador, es decidir con respecto al detalle con que tal medición pretende representar el sistema particular del operador, y luego seleccionar indicadores de rendimiento en materia de seguridad operacional que caractericen o tipifiquen las operaciones asociadas a la entrega de servicios en el contexto particular del operador. *Es pauta básica en SMS que el detalle de representación debe ser de alta especificidad.* La disponibilidad de datos de seguridad operacional es un factor determinante en la decisión con respecto al detalle de la representación, así como en la selección de indicadores. Los operadores que han desarrollado capacidades de colección y análisis de datos de seguridad operacional estarán en condiciones de representar el nivel de actuación en materia de seguridad operacional con mayor detalle que los operadores que no lo han hecho.

A la hora de seleccionar indicadores de rendimiento en materia de seguridad operacional es relevante seleccionar un conjunto de indicadores que abarquen distintos tipos: a) indicadores reactivos o *lagging indicators,* incluyendo indicadores de tipo precursor (alta probabilidad/baja severidad); y b) indicadores preventivos o *leading indicators.* Los indicadores reactivos miden eventos que ya han ocurrido. También se los conoce como "indicadores basados en consecuencias" y normalmente (pero no siempre) miden las consecuencias negativas que la organización intenta evitar. Los indicadores preventivos miden procesos e inputs que se implementan para mejorar o mantener la seguridad.

Una vez definidos los indicadores de rendimiento en materia de seguridad operacional, el paso siguiente es definir las metas de actuación en materia de seguridad operacional, que pueden considerarse como mejoras específicas a ser logradas.

Una vez seleccionados los indicadores y las metas de rendimiento en materia de seguridad operacional, puede establecerse la medición del rendimiento en materia de seguridad operacional que representa la cuantificación de la eficacia y eficiencia de la gestión de la seguridad operacional en la práctica del SMS del operador en particular. Para ello, deben asignarse *valores* a los indicadores de actuación en materia de seguridad operacional y a las metas de actuación en materia de seguridad operacional.

En la figura se adjunta un ejemplo extraído del documento 9859 de la OACI:



Finalmente, para lograr el "salto" de los valores de indicadores de rendimiento en materia de seguridad operacional a los valores de las metas de rendimiento en materia de seguridad operacional de un SMS, son necesarios planes de acción, que son los medios y actividades necesarias para lograr tal "salto". Los planes de acción incluyen procedimientos operacionales, tecnología, sistemas y programas con respecto a los cuales pueden especificarse mediciones de fiabilidad, disponibilidad, eficacia o exactitud. Un ejemplo de plan de acción sería *implantar un programa de inspección en rampa tres veces por día, elaborar e implantar un curso de instrucción para conductores e instalar carteles en calles de rodaje (específicos del aeródromo)*.

7. CAPÍTULO 4: POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

7.1 INTRODUCCIÓN

1. Los tres capítulos iniciales de esta Guía abarcan la fundamentación dogmática y los dos procesos básicos para la operación de SMS, así como sus actividades subyacentes y los medios necesarios para las mismas. Sabido es que ningún proceso puede desarrollarse, no importa lo fuerte que sea su fundamentación dogmática, ni ninguna actividad puede funcionar, dentro de un vacío institucional. Deben existir arreglos institucionales y, fundamentalmente, recursos que son absolutamente necesarios para apoyar la implementación y mantenimiento efectivo del SMS por un operador.

2. El punto a no perder de vista es que, a pesar de la vital importancia que tienen los arreglos institucionales, los mismos son medios para lograr un fin: el establecimiento y mantenimiento de las actividades subyacentes a los dos procesos básicos de SMS; es decir, gestión de riesgos de seguridad operacional y aseguramiento de seguridad operacional. Los arreglos institucionales son los auspiciantes, pero los jugadores del partido son las actividades que se realizan dentro del campo de juego delimitado por los dos procesos básicos. Un operador que ha establecido solamente los arreglos institucionales pero no pone en práctica las actividades no tiene un SMS. Tal operador tiene, a lo sumo, las herramientas necesarias para practicar SMS, pero si las actividades subyacentes a los dos procesos no están establecidas y en funcionamiento, las herramientas están encerradas en un cajón.

3. La consideración del párrafo anterior no es menor. Para ponerlo en lenguaje inequívoco: el cumplimiento normativo, por sí solo, no es evidencia que el operador ha implementado un SMS efectivo y eficiente. El cumplimiento normativo es evidencia solamente que el operador cumple con un conjunto de normas. Pero la evidencia de que el objetivo de gestión de la seguridad operacional buscado por las normas se ha alcanzado sólo puede ser brindado por la verificación de la eficacia y eficiencia de los procesos de gestión de riesgos de seguridad operacional y aseguramiento de la seguridad operacional en tiempo real. Tal verificación, a su vez, solamente puede validarse a través de la definición del rendimiento en materia de la seguridad operacional específica del SMS del operador, con sus indicadores de rendimiento en materia de seguridad operacional típicamente representativos del contexto operativo donde las operaciones del operador necesarias para la entrega de servicios tienen lugar, y por el logro de las metas de rendimiento en materia de seguridad operacional del SMS (ver el capítulo 3). El logro de estas últimas en particular es la evidencia, más allá de cualquier posible cuestionamiento, que el operador tiene no solamente las herramientas necesarias para la práctica de las actividades subyacentes a los dos procesos básicos del SMS, sino también que sabe cómo utilizarlas.

4. El presente capítulo abarca dos aspectos. El primer aspecto abarca los cuatro arreglos institucionales globales que se consideran necesarios para auspiciar el establecimiento y funcionamiento efectivo y eficiente de SMS: la publicación de la

política de seguridad operacional del operador, el establecimiento de objetivos de seguridad operacional del operador, la asignación de responsabilidades dentro de la estructura de personal del operador para la gestión de la seguridad operacional, incluyendo la designación de personal con funciones al respecto, y la publicación de la documentación pertinente. Un quinto arreglo institucional, la promoción de la seguridad operacional, se expone en el próximo capítulo. Una vez completada la exposición sobre los arreglos institucionales, el segundo aspecto que aborda el capítulo es la secuencia de actividades a llevar a cabo para la paulatina y progresiva implementación de SMS por un operador.

7.2 POLÍTICA DE SEGURIDAD OPERACIONAL

5. El punto de partida para asegurar la existencia de los arreglos institucionales y por ende los recursos necesarios para asegurar la eficacia y la eficiencia de SMS para el operador es la publicación de una inequívoca política de seguridad operacional. La política de seguridad operacional es el equivalente institucional a la Constitución de un país; es la carta magna del operador en lo que a gestión de la seguridad operacional se refiere. Una vez elaborada la política de seguridad operacional, la alta dirección del operador debe comunicarla, con visible respaldo, a todo el personal. La política de seguridad operacional refleja el compromiso moral y material del operador, enunciada por su alta dirección, en cuanto a lo siguiente:

   a) reflejará el compromiso de la organización respecto de la seguridad operacional incluyendo el logro de los estándares más elevados de seguridad operacional y de su gestión además del cumplimiento de todos los requisitos normativos nacionales, y normas internacionales que fuesen aplicables a sus operaciones, así como de las prácticas diarias operativas más efectivas;
   b) incluirá una declaración clara acerca de la provisión de los recursos necesarios para una entrega de servicios segura, efectiva y eficiente;
   c) incluirá procedimientos de presentación de informes en materia de seguridad operacional;
   d) indicará claramente qué tipos de comportamientos son inaceptables en lo que respecta a las actividades de aviación del operador e incluirá las circunstancias en las que no se podrán aplicar medidas disciplinarias;
   e) estará firmada por el Gerente Responsable del operador
   f) se comunicará, apoyándola ostensiblemente, a toda la organización;
   g) se examinará periódicamente para asegurarse de que siga siendo pertinente y apropiada para el proveedor de servicios

6. El siguiente ejemplo de política de seguridad operacional ha sido adaptado del *Manual de gestión de la seguridad operacional* de la OACI (Doc. 9859):

DECLARACIÓN DE POLÍTICA DE SEGURIDAD OPERACIONAL

La gestión de la seguridad operacional es uno de los objetivos fundamentales desde el punto de vista institucional. Estamos comprometidos a elaborar, implantar, mantener y mejorar constantemente las actividades necesarias para asegurar que todas las operaciones necesarias para la provisión de nuestros servicios tienen lugar bajo el marco de una asignación equilibrada de recursos, dirigidos a lograr el nivel más elevado de eficacia de la gestión de la seguridad operacional y a satisfacer el cumplimiento de las normas nacionales e internacionales aplicables a la provisión de nuestros servicios.

Todos nuestros empleados son responsables del logro del nivel más elevado de eficacia de la gestión de la seguridad operacional, comenzando por el Gerente Responsable.

Nuestro compromiso es:

- *apoyar la gestión de la seguridad operacional mediante la adjudicación de los recursos necesarios, a efectos de generar una cultura corporativa que fomente prácticas operativas seguras, aliente la efectiva notificación y comunicación de cuestiones relativas a la seguridad operacional, y gestione activamente la seguridad operacional brindando la misma atención a los resultados buscados que la atención brindada a los resultados de los otros sistemas de gestión de la organización;*

- *incorporar – en la medida lógica y adecuada – la gestión de la seguridad operacional como responsabilidad de todos los empleados;*

- *definir claramente para todos los empleados – en la medida lógica y adecuada – las líneas de rendición de cuentas y responsabilidades para el logro del rendimiento en materia de la seguridad operacional del sistema de gestión de la seguridad operacional (SMS);*

- *establecer programas de identificación de deficiencias de seguridad operacional y peligros en nuestro contexto operativo, incluyendo un programa de notificación de sucesos, para generar la información necesaria a efectos de controlar o mitigar las consecuencias de las deficiencias de seguridad y de los peligros que resultan de las operaciones o actividades necesarias para la provisión de servicios, al nivel más bajo razonablemente práctico (ALARP);*

- *garantizar que no se adoptarán medidas contra los empleados que revelen deficiencias o problemas de seguridad operacional mediante el programa de notificación de sucesos, a menos que el reporte indique, más allá de toda duda razonable, que se ha cometido un acto ilícito, una negligencia grave, o un incumplimiento deliberado o voluntario de reglamentos o procedimientos;*

- *cumplir y, cuando sea posible, sobrepasar los requisitos y las normas legislativas y reglamentarias durante las operaciones necesarias para la provisión de servicios;*

- *asegurar la disponibilidad de recursos humanos con los conocimientos y la instrucción necesaria para poner en práctica los procesos y actividades de gestión de la seguridad operacional;*

- *asegurar que todo el personal posee información y ha recibido instrucción sobre seguridad operacional adecuada y apropiada; que es competente en cuestiones de gestión de la seguridad operacional; y que solamente se le asigna tareas sobre el particular que son acordes con su competencia;*

- *establecer y medir el rendimiento en materia de seguridad operacional de nuestro sistema de gestión de seguridad operacional (SMS) con respecto a los indicadores y metas de rendimiento en materia de seguridad operacional que son representativas del contexto operativo en el que tienen lugar las operaciones necesarias para la provisión de nuestros servicios;*

- *mejorar continuamente el rendimiento en materia de seguridad operacional de nuestro sistema de gestión de seguridad operacional (SMS), mediante procesos de gestión que aseguren que se adoptan las actividades pertinentes y que son eficaces; y*

- *asegurar que los servicios suministrados por terceras partes para apoyar las operaciones necesarias para la provisión de nuestros servicios satisfacen los*

estándares de actuación en materia de seguridad operacional de nuestro sistema de gestión de seguridad operacional (SMS).

_____

Gerente Responsable

7.3 OBJETIVOS DE SEGURIDAD OPERACIONAL

7. Íntimamente ligado a la definición de la política de seguridad operacional se encuentra el establecimiento de los objetivos de seguridad operacional del operador. Existe una tendencia a confundir los *objetivos de seguridad operacional* del operador con las *metas de rendimiento en materia de seguridad operacional* de SMS. Los *objetivos de seguridad operacional* del operador son declaraciones de alto nivel y frecuentemente de naturaleza conceptual que identifican, en términos globales y genéricos, lo que el operador desea lograr en términos de gestión de la seguridad operacional. Las *metas de rendimiento en materia de seguridad operacional* son parámetros que permiten medir, por medio de sus valores, la eficacia y la eficiencia de SMS *exclusivamente*. Si bien existe una relación genérica entre objetivos de seguridad operacional del operador y metas de rendimiento en materia de seguridad operacional de SMS, claramente se trata de entes diferentes.

8. El apéndice 1 al capítulo 3 presenta algunos ejemplos de metas de rendimiento en materia de seguridad operacional de SMS. De los mismos se desprende que las metas son representaciones cuantificables de eventos directamente relacionados con las operaciones necesarias para la provisión de servicios por el operador. Para aclarar las diferencias entre unos y otros, a continuación se presentan ejemplos de objetivos de seguridad operacional del operador, de los cuales se desprende la naturaleza global y conceptual, antes que métrica, de los mismos:

   a) minimizar los eventos adversos de seguridad operacional de todo tipo (incidentes, incidentes serios y accidentes);

   b) minimizar daños a las aeronaves y lesiones a las personas que pudieran resultar durante las operaciones;

   c) implementar un programa efectivo de análisis de datos de vuelo en todas las flotas;

   d) proporcionar instrucción en SMS que sea apropiada y de relevancia para todo el personal;

   e) implementar un programa efectivo de notificación de sucesos;

   f) poner en marcha canales de difusión de información de seguridad operacional para todo el personal apropiado;

   g) etc.

7.4 RENDICIÓN DE CUENTAS SOBRE LA SEGURIDAD OPERACIONAL

9. Indudablemente, el aspecto más importante de la rendición de cuentas sobre la seguridad operacional es la identificación del Gerente Responsable, quien debe ser una persona única e identificable, con la responsabilidad final de rendición de cuentas por el rendimiento efectivo y eficiente de SMS del operador.

10. La alternativa más frecuente es determinar quién debería ser el Gerente Responsable en base a la función asignada a la persona dentro de la organización del operador. No obstante, más importante que *quién* debería ser el Gerente Responsable, son las facultades que éste debería tener para poder cumplir con su responsabilidad de rendir cuentas adecuadamente por el rendimiento efectivo y eficiente de SMS del operador. Estas facultades comprenden, sin estar necesariamente limitadas a:

    a) autoridad en cuestiones de recursos humanos;

    b) autoridad en cuestiones financieras significativas;

    c) responsabilidad directa en la conducción de los asuntos de la organización;

    d) autoridad final sobre las operaciones autorizadas en el certificado del operador;

    e) establecimiento y promoción de la política de seguridad operacional;

    f) establecimiento de los objetivos y de las metas de rendimiento en materia de seguridad operacional;

    g) actuar como el defensor de la seguridad operacional y

    h) responsabilidad final sobre todos los asuntos de seguridad operacional.

11. Lo anterior subraya que las facultades (y por ende, las responsabilidades) del Gerente Responsable se refieren a la asignación de recursos para el control de actividades, casi exclusivamente. Por consiguiente, un operador que designe a un Gerente Responsable que no tenga estas facultades y responsabilidades coloca a la persona designada en una posición tal en que no cuenta con los atributos esenciales para desempeñar su función.

12. El Gerente Responsable puede delegar el día a día de la gestión de SMS a otra persona o personas, siempre que dicha asignación esté adecuadamente documentada y descripta en el documento pertinente del operador. La responsabilidad por la rendición de cuentas del Gerente Responsable no se ve afectada, no obstante, por la asignación de la gestión de SMS a otra persona: recuérdese que se pueden delegar responsabilidades, pero no se puede delegar el acto de rendición de cuentas. El Gerente Responsable conserva la responsabilidad final de rendición de cuentas por el rendimiento efectivo y eficiente de SMS del operador aun cuando delegue el día a día de las actividades de SMS.

13. La asignación de responsabilidades de gestión de seguridad operacional a los niveles superiores de la gestión del operador es también un elemento clave de los arreglos institucionales necesarios para auspiciar los dos procesos básicos de SMS. Se trata de la inclusión, en la descripción de tareas de cada persona encargada de una

dependencia funcional, de las responsabilidades relativas al funcionamiento del SMS en la medida apropiada, además de las responsabilidades específicas por el funcionamiento de la dependencia funcional en cuestión. En el marco de la gestión de la seguridad operacional como función institucional, cada persona responsable de una dependencia funcional tendrá un grado de participación en la operación de SMS. Esta participación será por cierto más profunda para los encargados de las dependencias funcionales que tienen asignadas las operaciones directamente relacionadas con la entrega de servicios de la organización (operaciones, mantenimiento, ingeniería, instrucción y despacho de vuelo, generalmente conocidos como "post-holders" o "personal responsable") que para los encargados de las funciones de apoyo a las operaciones (recursos humanos, administración, asuntos jurídicos, calidad y financieros).

14. Las responsabilidades de rendición de cuentas, responsabilidades generales y facultades de las personas encargadas de dependencias funcionales, y en particular de los "post-holders", deben estar documentadas y descriptas en el documento pertinente del operador. Las responsabilidades de rendición de cuentas, responsabilidades generales y facultades deben estar representadas en un organigrama institucional que permita visualizar las interfaces e interrelaciones en términos de la gestión de la seguridad operacional entre las diversas dependencias del operador.

15. El centro operativo para el funcionamiento de SMS del operador debe estar ubicado en una dependencia única e identificable – aun cuando se nutra del conocimiento y experiencia que puedan aportar las dependencias operacionales – que a los efectos de esta Guía se denominará "oficina de servicios de gestión de seguridad operacional". El concepto de la oficina de servicios de gestión de seguridad operacional es clave para la noción de gestión de la seguridad operacional como proceso institucional, y de SMS como el sistema de gestión que el operador cuenta para tal fin. La oficina de servicios de gestión de seguridad operacional es independiente y neutral con respecto a las decisiones adoptadas y las actividades operativas puestas en marcha en relación al apoyo de la provisión de servicios por los "post-holders" de las dependencias operacionales. En un entorno SMS, la oficina de servicios de gestión de seguridad operacional realiza cuatro funciones corporativas esenciales, que son absolutamente consistentes con la noción de SMS como "generador" de datos expuesta en los capítulos 1 al 3:

    a) gestiona y supervisa el sistema de identificación de deficiencias de seguridad operacional y peligros en el contexto operativo donde tienen lugar las operaciones necesarias para la provisión de servicio para el logro del objetivo, y proporciona información sobre los mismos a las dependencias operacionales a cargo de la provisión de servicios cuyas actividades pudiesen verse afectadas por deficiencias y peligros (*gestión de riesgos de seguridad operacional*);

    b) supervisa, a través del análisis y la monitorización continua de datos, la eficacia de las mitigaciones contra las consecuencias de los peligros puestas en marcha por las dependencias operacionales a cargo de la provisión de servicios (*aseguramiento de la seguridad operacional*);

c) asiste a los "post-holders" – a requerimiento – en asuntos de gestión de la seguridad operacional (*aseguramiento de la seguridad operacional*); y

d) asesora a la alta dirección en asuntos de gestión de la seguridad operacional (*aseguramiento de la seguridad operacional*).

16. En el enfoque tradicional de la seguridad operacional, la dependencia con el rótulo "seguridad operacional" (o "prevención de accidentes") era el "propietario" exclusivo de todas las actividades que se consideraban relacionadas con la seguridad operacional dentro del operador. El responsable de seguridad operacional, a menudo conocido como el responsable del programa de prevención de accidentes, era la persona a cargo de identificar los problemas de seguridad operacional, proponer soluciones, participar en la implantación de las mismas, y supervisar la eficacia de las soluciones.

17. En años recientes, la noción de que la "propiedad" de las actividades de seguridad operacional era exclusiva de la dependencia con el rótulo "seguridad operacional" o "prevención de accidentes" se vio involuntariamente reforzada por una práctica adoptada a gran escala en toda la industria, que establecía un canal directo de comunicación entre el responsable de seguridad operacional y el gerente responsable del operador.

18. La intención de esta práctica, de gran acepción en numerosos segmentos de la industria, era doble. En primer lugar, trataba de elevar el nivel jerárquico y la visibilidad de la dependencia a cargo de la seguridad operacional, estableciendo un enlace directo entre ésta y el gerente responsable. En segundo lugar, el enlace directo trataba de generar neutralidad, apartando a los encargados de gestionar las actividades operacionales directamente relacionadas con la provisión de servicios ("post-holders") de la evaluación y resolución de problemas de seguridad operacional. La composición de lugar era que existía una gran probabilidad de que los "post-holders" pudieran, en diverso grado, ser partes interesadas, lo que llevaría a un posible conflicto de intereses en la evaluación y resolución de problemas de seguridad operacional. La relación directa entre el responsable de seguridad operacional y el gerente responsable suponía la eliminación de este presunto conflicto de intereses.

19. Aunque claramente bien intencionada, esta práctica presenta dos carencias de significación. En primer lugar, al otorgar la propiedad del proceso de seguridad operacional enteramente a la dependencia de seguridad operacional, se eliminaba a los "post-holders" del proceso de toma de decisiones de seguridad operacional, y del aporte que pudiesen generar en base a sus conocimientos y experiencia. Esto nutría la percepción que "*los problemas de seguridad operacional no son problemas de los "post-holders"; los problemas de seguridad operacional pertenecen a la dependencia de seguridad operacional y al responsable de la misma".* De esta manera, la línea de rendición de cuentas se reducía en la práctica a un diálogo entre el gerente responsable y el responsable de seguridad operacional. Considerando la carga de trabajo de un gerente responsable, este diálogo tenía todas las posibilidades de transformarse en monólogo. En segundo lugar, y muy importante,

dejaba de lado el valioso aporte, en términos de conocimiento y experiencia, que las dependencias operacionales podrían brindar a la toma de decisiones sobre soluciones a problemas de seguridad operacional del operador.

20. El contexto SMS plantea una perspectiva diferente. El nombre de la "oficina de seguridad operacional" u "oficina de prevención" se ha modificado a *oficina de servicios de gestión de la seguridad operacional* (o departamento SMS), para reflejar que tal dependencia proporciona un servicio al operador, tanto a la alta dirección como a los "post-holders", con respecto a la gestión de la seguridad operacional como proceso institucional. La oficina de servicios de gestión de seguridad operacional es fundamentalmente una dependencia de colección y análisis de datos de seguridad operacional; es decir, está a cargo del "generador" ejemplificado en el capítulo 2. Mediante una combinación de métodos, la oficina de servicios de gestión de seguridad operacional capta lo que sucede dentro de la deriva operacional (ver el capítulo 2), mediante la colección continua y regular de datos de seguridad operacional sobre deficiencias de seguridad operacional y peligros durante las actividades de provisión de servicios.

21. Una vez identificados los peligros, evaluadas sus consecuencias y estimados los riesgos de seguridad operacional de tales consecuencias (es decir una vez que se ha extraído información de seguridad operacional de los datos captados), la información de seguridad operacional se transmite a los "post-holders" para la resolución de los problemas de seguridad identificados. Los "post-holders" son los verdaderos expertos temáticos en sus respectivos sectores y, por consiguiente, los que están en la mejor posición para diseñar soluciones efectivas y eficientes e implantarlas. Además, los "post-holders" pueden encargarse de la última etapa del proceso de análisis de datos de seguridad operacional, transformando la información en inteligencia, dándole contexto a la información sobre peligros obtenida por la oficina de servicios de gestión de seguridad operacional.

22. De tal manera, la responsabilidad principal de la gestión de la seguridad operacional corresponde a los "dueños" de las actividades necesarias para la provisión de servicios. Es durante estas actividades de producción cuando los peligros pueden desencadenar su potencial perjuicio, cuando las deficiencias en los procedimientos contribuyen a desencadenar las consecuencias perjudiciales de los peligros, y donde el control de supervisión directo y la asignación de recursos pueden mitigar las consecuencias de los peligros a un valor ALARP. Además, los propietarios de las actividades son los expertos técnicos temáticos de las operaciones específicas del operador y, por lo tanto los que tienen mayores conocimientos y experiencia en los procedimientos técnicos para proponer soluciones.

23. Una vez que la información de seguridad operacional ha sido entregada a los "post-holders" apropiados, la oficina de servicios de gestión de seguridad operacional reanuda sus actividades regulares de colección y análisis de datos de seguridad operacional. A intervalos regulares convenidos entre la oficina de servicios de gestión de seguridad operacional y los "post-holders" en cuestión, la oficina de servicios de gestión de seguridad operacional presenta a los "post-holders" de las áreas en que hubiese un problema de seguridad operacional un nuevo paquete de datos sobre el problema que se está tratando de solucionar. El nuevo paquete de datos indicará si las soluciones de mitigación implantadas por los "post-holders" han solucionado el problema de seguridad operacional, o si éste persiste. En este último caso, se introducen más soluciones de mitigación, se conviene un nuevo intervalo de tiempo, se recogen y analizan más datos de seguridad operacional, se entrega

la información de seguridad a los "post-holders", y este ciclo se repite tantas veces como sea necesario hasta que el análisis de los datos de seguridad operacional demuestra que el problema de seguridad operacional se ha resuelto. En todo este proceso, los "post-holders" no responden por la solución del problema de seguridad operacional en cuestión a la oficina de servicios de gestión de seguridad operacional, sino al Gerente Responsable, como persona con responsabilidad final por la rendición de cuentas por la eficacia y eficiencia de SMS del operador.

24. La oficina de servicios de gestión de seguridad operacional será, en la mayoría de las organizaciones, la dependencia en la cual el Gerente Responsable ha asignado las funciones cotidianas de gestión de SMS, y será la dependencia responsable y el punto focal para la puesta en práctica y mantenimiento de un SMS efectivo. La oficina de servicios de gestión de seguridad operacional también asesora al Gerente Responsable y a los "post-holders" en asuntos relativos a la gestión de la seguridad operacional, y es responsable de coordinar y comunicar asuntos de seguridad operacional dentro del operador, así como con agencias externas, contratistas y partes interesadas, según corresponda.

25. La oficina de servicios de gestión de seguridad operacional se comunica directamente con los "post-holders" o personal responsable de operaciones, mantenimiento, ingeniería, instrucción, etc. Si debido al tamaño del operador, los "post-holders" cuentan con personal de seguridad operacional especializados en áreas operativas específicas, y tales personas tienen responsabilidades delegadas para la gestión de problemas de seguridad operacional en un área operativa en cuestión, tales personas serán el primer punto de contacto para la oficina de servicios de gestión de seguridad operacional en la comunicación con las áreas específicas.

26. En circunstancias normales, la oficina de servicios de gestión de seguridad operacional tiene acceso al Gerente Responsable o se comunica con éste mediante dos canales: el Grupo de Acción de seguridad operacional y/o el Comité de Control de seguridad operacional. Estos grupos se discuten continuación en este capítulo. En circunstancias excepcionales o urgentes, la oficina de servicios de gestión de seguridad operacional tiene acceso directo de emergencia al Gerente Responsable. Este canal de comunicación debería utilizarse con gran cautela y, en tal caso, debe justificarse y documentarse adecuadamente.

27. La distribución de información sobre seguridad operacional por la oficina de servicios de gestión de seguridad operacional es sólo la primera etapa del proceso de gestión de riesgos de seguridad operacional. Los "post-holders" deben actuar sobre esta información. La mitigación de problemas de seguridad operacional inevitablemente exige recursos. A veces estos recursos son directamente accesibles por los "post-holders". Otras veces, se requieren recursos adicionales, cuya asignación puede no estar entre las facultades del "post-holder", y debe ser aprobada por niveles superiores de la organización.

28. El Comité de Control de la seguridad operacional (*safety review committee, SRC*) proporciona la plataforma para lograr los objetivos de asignación de recursos y evaluación neutral de la eficacia y eficiencia de las estrategias de mitigación de problemas de seguridad operacional. Se trata de un comité de muy alto nivel, presidido por el Gerente Responsable e integrado por los "post-holders" o responsables de las áreas funcionales. El encargado de la oficina de gestión de la seguridad operacional participa en el SRC solamente como asesor. El SRC tiene

carácter eminentemente estratégico, trata problemas de alto nivel en relación con las políticas, asignación de recursos y supervisión del rendimiento de SMS del operador, y se reúne con poca frecuencia, a menos que circunstancias excepcionales impongan otra cosa.

29. Una vez que el SRC ha elaborado una dirección estratégica, la implantación de las estrategias decididas debe realizarse en forma coordinada en toda la organización del operador. Esta es la función principal del Grupo de Acción de seguridad operacional (*safety advisory group, SAG*). El SAG es un comité de alto nivel, integrado por los "post-holders" y representantes del personal operativo, y presidido en turnos por "post-holders" designados. El responsable de la oficina de servicios de gestión de seguridad operacional es el secretario del SAG. El SAG tiene carácter eminentemente táctico y se ocupa de los asuntos de implantación para satisfacer las directivas estratégicas del SRC. Mientras el SAG trata de aspectos de implantación a nivel operativo relativos a actividades específicas para asegurar la mitigación de las consecuencias de los peligros durante las operaciones de línea, el SRC trata de la coordinación de esos aspectos, para asegurar la coherencia en la dirección estratégica.

7.5 DOCUMENTACIÓN SMS

30. La literatura sobre SMS es unánime en asignarle tres características distintivas, proponiendo que SMS es:
    a) sistemático;
    b) preventivo; y
    c) explícito

31. Se considera a SMS *sistemático* porque las actividades de gestión de la seguridad operacional se ejecutan de acuerdo a un plan predeterminado y se aplican de manera coherente a través de toda la organización del operador. Las actividades de SMS apuntan a mejoras graduales pero constantes, y no a cambios radicales e instantáneos. Se considera a SMS *preventivo* porque se basa en un enfoque que enfatiza la identificación de deficiencias de seguridad operacional y peligros, y la mitigación de las consecuencias de los peligros antes que los mismos queden en evidencia a través de sucesos que afectan en forma significativa la seguridad operacional. Para mantener la efectiva identificación de los peligros, se realiza una supervisión constante de las actividades operacionales necesarias para la provisión de los servicios. Por último, se considera a SMS *explícito* porque todas las actividades de gestión de la seguridad operacional están debidamente documentadas. Las actividades de gestión de la seguridad operacional y la subsiguiente experiencia que se acumula como resultado de las mismas están registradas en documentos formales del operador. Se trata de una situación en la cual la memoria colectiva de seguridad operacional del operador reside en una estructura formal y no en las mentes de determinados individuos. Por lo tanto, la documentación es un elemento esencial del SMS.

32. La documentación SMS debe incluir y hacer referencia, según corresponda, a todos los reglamentos pertinentes y aplicables, tanto nacionales como internacionales. También debe incluir registros y documentación específica de SMS, como formularios de notificación de sucesos, líneas de rendición de cuentas, responsabilidades y facultades relativas a la gestión de la seguridad operacional y la estructura del operador para la gestión de la seguridad operacional. Además deben documentarse directrices explícitas para el tratamiento, almacenamiento y conservación de los registros.

33. Distintos operadores tendrán distintos sistemas de manejo de la documentación, dentro del marco de referencia normativo establecido. Por ello, se hace mención solamente a los dos documentos más específicos de SMS: el plan de implementación SMS, y el manual SMS (SMSM).

34. El *plan de implementación SMS* constituye la formulación de una estrategia realista por el operador para el diseño y puesta en marcha de las actividades necesarias para SMS, de manera tal de satisfacer los objetivos de seguridad operacional del operador, incluyendo la prestación efectiva y eficiente de los servicios. El plan de implementación es una descripción de *cómo* el operador logrará la puesta en marcha de las actividades subyacentes a SMS de forma organizada y siguiendo pautas establecidas, *quiénes* las ejecutarán, y *cuál* será el *cronograma q*ue guiará tal puesta en marcha. Dependiendo del tamaño del operador y la complejidad de sus operaciones, el plan de implementación SMS puede ser elaborado por una persona, o por un grupo de planificación que abarque una base de experiencia apropiada. El grupo de planificación debe disponer de recursos necesarios acorde con la tarea que debe realizar (incluyendo el tiempo para las reuniones). Asimismo, debe reunirse regularmente con la alta dirección para evaluar el progreso del plan de implementación. Una vez completado, la alta dirección del operador debe aprobar el plan de implementación de SMS.

35. El *manual SMS* (*SMS Manual, SMSM*) define el enfoque del operador respecto de la gestión de la seguridad operacional. El SMSM es el instrumento clave para comunicar tal enfoque a toda la organización. En él se documentan, en forma permanente y actualizada, todos los aspectos de SMS que fueron objeto del plan de implementación SMS. El SMSM puede integrarse como parte del manual de operaciones del operador. Típicamente, el contenido del SMSM comprende:
    a) control del documento para asegurar que se mantiene actualizado;
    b) los requisitos regulatorios aplicables al SMS del operador;
    c) ámbito de aplicación del SMS e integración con otros sistemas de gestión;
    d) la política y los objetivos de seguridad operacional, que se mantienen actualizados en forma permanente;
    e) líneas de rendición de cuentas respecto de la gestión de la seguridad operacional;
    f) el personal clave para la gestión de la seguridad operacional, sus funciones, atribuciones y responsabilidades;
    g) el sistema de reporte de seguridad operacional
    h) actividades de gestión de riesgos de seguridad operacional, incluyendo identificación de peligros y la evaluación de los riesgos de seguridad operacional;
    i) actividades de aseguramiento de seguridad operacional, incluyendo la observación y medición del rendimiento en materia de seguridad operacional y los procedimientos para la gestión del cambio;
    j) investigaciones de seguridad operacional y acciones correctivas;
    k) instrucción y comunicación de la seguridad operacional;
    l) mejora continua y auditoría del SMS;
    m) procedimientos de control de documentación con respecto a procesos y actividades de gestión de la seguridad operacional;
    n) coordinación de la planificación de respuesta ante emergencias;
    o) control de las actividades contratadas; y

p) el "análisis de carencias" o gap analysis del operador con respecto a los requerimientos de implementación de SMS establecidos, que se mantiene actualizado en forma permanente.

7.6 LA IMPLEMENTACIÓN DE SMS EN LA PRÁCTICA – OCHO ACTIVIDADES CLAVE

36. El consenso de opinión actual en la industria es que la implementación de SMS debe ser llevada a cabo en forma gradual, escalonando las actividades a ser completadas a lo largo de un período de tiempo. Esto obedece a la necesidad de manejar adecuadamente la carga de trabajo asociada a la implementación de SMS, así como de permitir una adjudicación de recursos a las actividades de implementación que sea paulatina en vez de abrupta.

37. Para facilitar una implementación de SMS que satisfaga tanto los requisitos de OACI como los de EASA, esta Guía, en vez de replicar el material OACI, expone en forma conceptual las actividades fundamentales iniciales que son condición *sine qua non* para la implementación de SMS por un operador. De tal manera, los operadores podrán cotejar el estado de situación de sus SMS contra estas actividades, adoptar las que fueren necesarias y desechar las que no lo fuesen.

7.7 GRUPO DE PLANIFICACIÓN SMS

38. El establecimiento de un *grupo de planificación SMS* es la primera actividad de la implementación o actualización, según sea el caso, de SMS por el operador. Dado que SMS es el sistema de gestión de la seguridad operacional de toda la organización del operador, es fundamental que el grupo de planificación tenga conocimientos multidisciplinares, y que integre a todos los sectores del operador responsables de las distintas actividades relacionadas con la provisión de servicios. El grupo de planificación debe incluir, sin estar necesariamente limitado a, operaciones (incluyendo cabina de pasajeros y despacho); instrucción; mantenimiento; rampa; finanzas; legal; calidad, y recursos humanos. El grupo de planificación desarrollará sus tareas respetando un cronograma definido, y deberá reunirse con una periodicidad apropiada con la alta dirección del operador para evaluar el progreso de las actividades de implementación. Se deberán definir los términos de referencia y mandato del grupo, y asignar los recursos necesarios para que el grupo desarrolle sus tareas (incluyendo el tiempo para las reuniones), de manera de satisfacer las tareas que debe realizar dentro del cronograma de actividades aprobado.

7.8 DESCRIPCIÓN DEL SISTEMA

39. La primera actividad a completar por el grupo de planificación es la *descripción del sistema* del operador. Dogmáticamente, la descripción del sistema, es decir, del contexto operativo global al cual el sistema de gestión de seguridad operacional se aplicará, permite al grupo de planificación identificar las fuentes potenciales de vulnerabilidades en lo que se refiere a seguridad operacional durante la provisión de servicios por el operador. Básicamente, se trata de identificar el volumen y complejidad de las interrelaciones operativas durante la provisión de servicios, evaluar cuales son las defensas *ya existentes* contra deficiencias de seguridad operacional y las consecuencias de peligros, y determinar la necesidad de defensas adicionales. Como consecuencia de ello, el grupo de planificación esbozará un panorama global en cuanto a la asignación de los recursos necesarios para operar

y proteger al sistema durante las actividades relacionadas con la provisión de servicios, en función del volumen y complejidad de las interacciones operativas, y las defensas necesarias. En términos formales o técnicos, la descripción del sistema de un operador debería incluir lo siguiente:

a) las funciones del sistema del operador (operaciones, mantenimiento, instrucción, etc.);

b) las interacciones del sistema del operador con otros sistemas en el sistema de transporte aéreo (ATC, aeródromos, etc.);

c) los componentes tecnológicos del sistema;

d) los componentes normativos, del sistema, incluyendo los procedimientos que definen o guían la operación y el uso de la tecnología;

e) los aspectos más característicos del entorno operacional (geografía, condiciones meteorológicas especiales, etc.); y

f) los productos y servicios necesarios para la provisión de los servicios propios del operador contratados a terceros.

7.9 ANÁLISIS DE CARENCIAS

40. Concretada la descripción del sistema, la actividad inmediata siguiente del grupo de planificación debe ser la concreción del *análisis de carencias de SMS*. La puesta en práctica de SMS requiere que el operador haga un balance de su organización para determinar cuáles son los componentes y elementos constitutivos de SMS que están actualmente funcionando en el sistema del operador, y qué componentes y elementos se deben agregar o modificar para alcanzar la puesta en práctica de SMS de forma tal de dar cumplimiento a los requisitos del mismo reflejados en la normativa vigente. Este análisis se conoce como análisis de las carencias (*gap analysis*) e implica la comparación entre requisitos normativos de SMS y los recursos existentes en el operador. Al presente, el marco de referencia internacional para efectuar la comparación entre los requisitos de SMS y los recursos existentes en el operador es la estructura SMS de la OACI (ver el apéndice a este capítulo). Los contenidos del análisis propiamente dicho, según lo propone OACI, se encuentran en el *Manual de gestión de la seguridad operacional* (Doc. 9859). Otras guías que se pueden emplear son las elaboradas por el Grupo de colaboración internacional denominado SM ICG, al cual pertenece AESA: https://www.skybrary.aero/index.php/SM_ICG_SMS_Evaluation_Tool . Algunas de estas guías se encuentran traducidas en la página Web de AESA: https://www.seguridadaerea.gob.es/lang_castellano/g_r_seguridad/actividades_grupos/default.aspx y guías adicionales elaboradas por AESA se puede consultar en: https://www.seguridadaerea.gob.es/lang_castellano/g_r_seguridad/drgi/default.aspx

41. A Cada elemento de la estructura SMS de la OACI – o las estructuras alternativas de acuerdo a normativas especificas – debe ser evaluado para determinar si el operador

debe crear o modificar directivas o procedimientos para satisfacer los requerimientos del elemento en cuestión, para determinar si es necesario desarrollar el mecanismo requerido por SMS, o si los mecanismos ya existentes en el operador satisfacen los requerimientos del elemento en cuestión. Una vez que el análisis de carencias haya sido completado y documentado, los mecanismos identificados como faltantes o deficientes formarán la base del plan de implementación de SMS.

41. No debe considerarse al análisis de carencias como un ejercicio contable administrativo de disponibilidad de elementos. El análisis de carencias es un primer y fundamental paso para identificar fuentes de vulnerabilidad de la seguridad operacional, que son especificadas como peligros en las interfaces operativas entre los componentes del sistema. Una vez que el sistema se describe en términos de componentes e interacciones, la segunda etapa es tratar estas vulnerabilidades de seguridad operacional, especificadas como peligros en las interfaces entre los componentes del sistema, mediante un análisis de los recursos ya presentes en el mismo.

42. Ampliando lo ya expuesto, el análisis de carencias tiene dos objetivos. El primero es identificar las posibles disparidades en las interfaces entre los diferentes componentes identificados en la descripción del sistema. Estas disparidades son fuentes de vulnerabilidades de seguridad operacional. El segundo objetivo consiste en identificar los recursos adicionales que podrían considerarse necesarios para "emparejar" las interfaces desfasadas. Desde la perspectiva de SMS, un análisis de carencias es básicamente un análisis de los arreglos de seguridad operacional que ya existen dentro del operador comparados con los arreglos necesarios para el funcionamiento de SMS. El análisis de las carencias es importante porque un número de las estructuras básicas de organización necesarias para comenzar a elaborar un SMS pueden ya existir en la organización: rara vez será necesario construir un SMS "a partir de cero", debido a que la mayoría de los operadores tendrán varias actividades relacionadas a SMS establecidas y funcionando. El desarrollo de SMS debería aprovechar y construirse sobre las estructuras del operador existentes.

7.10 IDENTIFICACIÓN DEL GERENTE RESPONSABLE Y RENDICIÓN DE CUENTAS SOBRE LA SEGURIDAD OPERACIONAL

43. Concretadas la descripción del sistema y el análisis de carencias, el paso siguiente para el grupo de implementación es *la identificación del Gerente Responsable*, y la definición de las *líneas de rendición de cuentas sobre la seguridad operacional.* Esto incluye a la oficina de servicios de gestión de seguridad operacional, el SRC y el SAG, según la base expuesta bajo el título pertinente en este capítulo. Cabe destacar – según sean los términos de referencia establecidos – que es altamente improbable que el grupo de implementación tenga autoridad para *designar* al Gerente Responsable o *asignar* responsabilidades por la gestión de la seguridad operacional. El rol del grupo es más bien para *identificar y proponer* al Gerente Responsable. De la misma manera, es probable que la autoridad del grupo de implementación esté limitada a *proponer* los fundamentos para la asignación de responsabilidades para la gestión de la seguridad operacional.

7.11 POLÍTICA DE SEGURIDAD OPERACIONAL

44. La cuarta actividad del grupo de implementación es la definición y propuesta, para su aprobación y posterior publicación, del borrador de la *política de seguridad operacional* del operador, según lo indicado bajo el título pertinente en este capítulo.

7.12 PROGRAMA INTERNO DE INSTRUCCIÓN EN SMS

45. La siguiente actividad del grupo de implementación es el establecimiento de los contenidos y el cronograma de un *programa interno de instrucción* sobre SMS. El alcance de la instrucción interna sobre SMS será proporcional al nivel de participación individual del personal del operador en las actividades de SMS, de acuerdo con las funciones y responsabilidades en materia del funcionamiento del mismo. El programa de instrucción interno debe abarcar conocimientos acerca de la normativa vigente, los dos procesos básicos del sistema (gestión de riesgos de seguridad operacional y aseguramiento de seguridad operacional), y las actividades y medios con que cuenta el operador en apoyo a tales procesos.

7.13 COMUNICACIÓN SOBRE LA INICIACIÓN DEL PROYECTO DE IMPLANTACIÓN DE SMS

46. La sexta actividad a acometer por el grupo de implementación es el establecimiento de un programa de *comunicación sobre la iniciación del proyecto de implantación de SMS*. El grupo debe evaluar y arbitrar los medios necesarios más adecuados (circulares internas, boletines informativos, sitio web, *briefings*, etc.) para comunicar, a todo el personal pertinente del operador, el inicio y periódico progreso de las actividades para el desarrollo de las actividades de implantación de SMS. El programa de comunicación inicial se convertirá en un programa permanente de comunicación sobre la gestión de la seguridad operacional, que se expone en el capítulo siguiente de esta Guía.

7.14 EVALUACIÓN Y PROPUESTA DE PUESTA EN MARCHA DE LAS FUENTES DE ADQUISICIÓN DE DATOS SOBRE DEFICIENCIAS DE SEGURIDAD OPERACIONAL Y PELIGROS

47. La siguiente actividad es posiblemente una de las más importantes y de cuya correcta conclusión depende en gran medida el éxito o el fracaso de SMS del operador: *la evaluación de las fuentes de adquisición de datos sobre deficiencias de seguridad operacional y peligros que existen en el operador y propuesta de puesta en marcha de las adicionales que fuesen necesarias*. Al fin y al cabo, ya se ha expuesto la noción de SMS como esencialmente un sistema de apoyo a la toma de decisiones sobre gestión de la seguridad operacional sobre la base de datos. La ecuación es muy simple: sin datos, no hay SMS. Por lo tanto, el grupo de implementación debe hacer una evaluación de las distintas formas de adquisición de datos con que cuenta el operador, y proponer la institución de aquellas fuentes de adquisición de datos con las que no contase el operador, según lo expuesto en el capítulo 3 de esta Guía.

7.15 PLAN DE IMPLEMENTACIÓN

48. La actividad final, como culminación del desarrollo de la fase de planificación, una vez completadas las actividades listadas en los párrafos 37 a 48 anteriores, el grupo de implementación estará en condiciones de formular del *plan de implementación* de SMS del operador, según lo expuesto bajo el título pertinente en este capítulo.

49. En resumidas cuentas, las ocho actividades propuestas abarcan:

    1. Integración del grupo de planificación SMS
    2. Descripción del sistema
    3. Análisis de carencias de SMS
    4. Identificación del Gerente Responsable y líneas de rendición de cuentas sobre la gestión de la seguridad operacional
    5. Propuesta de política de seguridad operacional
    6. Propuesta de programa interno de instrucción sobre SMS
    7. Comunicación sobre la iniciación del proyecto de implantación de SMS
    8. Evaluación y propuesta de puesta en marcha de las fuentes de adquisición de datos sobre deficiencias de seguridad operacional y peligros

50. En este punto, al haber concretado las ocho actividades descriptas en los párrafos anteriores (que no son poca cosa ni de poca monta), el operador estará en condiciones de comenzar a "hacer SMS", es decir, a desarrollar las actividades operacionales necesarias para la provisión de servicios bajo la tutela de SMS. Esto es porque, al alcanzar este punto, el operador tendrá en marcha los *arreglos institucionales* básicos para apoyar las actividades subyacentes a los dos procesos básicos de la gestión de la seguridad operacional: gestión de riesgos de seguridad operacional, y aseguramiento de la seguridad operacional. Es ahora una cuestión de *comenzar a ejecutar las actividades*, según las pautas conceptuales y dogmáticas proporcionadas por esta Guía en los capítulos 1 al 3.

7.16 APÉNDICE 1 AL CAPÍTULO 4: ESTRUCTURA SMS DE LA OACI

En este apéndice se introduce un marco estructural para la implantación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS) por un operador. La implantación del marco será proporcional al tamaño del operador y la complejidad de los servicios proporcionados. El marco incluye cuatro componentes y doce elementos que representan los requisitos mínimos para la implantación de un SMS.

1. Política y objetivos de seguridad operacional
1.1 Compromiso de la dirección
1.2 Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional
1.3 Designación del personal clave de seguridad operacional
1.4 Coordinación de la planificación de respuestas ante emergencias
1.5 Documentación SMS
2. Gestión de riesgos de seguridad operacional
2.1 Identificación de peligros
2.2 Evaluación y mitigación de riesgos de seguridad operacional

3. Aseguramiento de la seguridad operacional
3.1 Observación y medición del rendimiento en materia de seguridad operacional
3.2 Gestión del cambio
3.3 Mejora continua del SMS
4. Promoción de la seguridad operacional
4.1 Instrucción y educación
4.2 Comunicación de la seguridad operacional.

7.16.1 POLÍTICA Y OBJETIVOS DE SEGURIDAD OPERACIONAL

1.1 Compromiso de la dirección
El operador definirá su política de seguridad operacional de conformidad con los requisitos nacionales e internacionales pertinentes. La política de seguridad operacional:

a) reflejará el compromiso de la organización respecto de la seguridad operacional;
b) incluirá una declaración clara acerca de la provisión de los recursos necesarios para su puesta en práctica;
c) incluirá procedimientos de presentación de informes en materia de seguridad operacional;
d) indicará claramente qué tipos de comportamientos son inaceptables en lo que respecta a las actividades de aviación del operador e incluirá las circunstancias en las que no se podrían aplicar medidas disciplinarias;
e) estará firmada por el Gerente Responsable del operador
f) se comunicará, apoyándola ostensiblemente, a toda la organización;
g) se examinará periódicamente para asegurarse de que siga siendo pertinente y apropiada para el operador

1.2 Obligación de rendición de cuentas y responsabilidades en materia de seguridad operacional.
El operador identificará al Gerente Responsable quien, independientemente de sus otras funciones, será el responsable final y rendirá cuentas, en nombre del operador, respecto de la implantación y mantenimiento de SMS.
El operador definirá claramente las líneas de rendición de cuentas sobre la seguridad operacional para toda la organización incluida la responsabilidad directa de rendición de cuentas sobre seguridad operacional de la alta dirección (incluyendo a los "post-holders").
El operador determinará la responsabilidad de rendición de cuentas de todos los miembros de la dirección (incluyendo a los "post-holders"), independientemente de sus otras funciones, así como la de los empleados, en relación con el rendimiento en materia de seguridad operacional de SMS.
El operador documentará y comunicará la información relativa a las responsabilidades, la rendición de cuentas y las autoridades de seguridad operacional a toda la organización.
El operador definirá los niveles de gestión con autoridad para tomar decisiones sobre la tolerabilidad de riesgos de seguridad operacional.

1.3 Designación del personal clave de seguridad operacional
El operador designará un gerente o gestor de seguridad operacional que será responsable de la implantación y el mantenimiento de un SMS eficaz.

1.4 Coordinación de la planificación de respuestas ante emergencias

El operador garantizará que el plan de respuesta ante emergencias se coordine en forma apropiada con los planes de respuesta ante emergencias de las organizaciones con las que deba interactuar al prestar sus servicios.

1.5 Documentación SMS

El operador elaborará un plan de implantación del SMS, aprobado formalmente por la organización, en el que se definirá el enfoque de la organización respecto de la gestión de la seguridad operacional, de manera que se cumplan los objetivos de la organización en materia de seguridad operacional.

El operador preparará y mantendrá documentación SMS en la que se describan:

a) la política y los objetivos de seguridad operacional,
b) los requisitos del SMS,
c) los procesos y procedimientos del SMS,
d) la rendición de cuentas, las responsabilidades y las autoridades que tienen que ver con los procesos y procedimientos del SMS,
e) los resultados esperados del SMS.

El operador preparará y mantendrá un manual de sistemas de gestión de la seguridad operacional (SMSM) como parte de su documentación SMS (podrá integrarse como parte del Manual de Operaciones).

7.16.2 GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

2.1 Identificación de peligros

El operador definirá y mantendrá un proceso que garantice la identificación de los peligros asociados a sus operaciones.

La identificación de los peligros se basará en una combinación de métodos reactivos y preventivos para recopilar datos sobre seguridad operacional.

2.2 Evaluación y mitigación de riesgos de seguridad operacional

El operador definirá y mantendrá un proceso que garanticen el análisis, la evaluación y el control de los riesgos de seguridad operacional asociados a los peligros identificados.

7.16.3 3. ASEGURAMIENTO DE LA SEGURIDAD OPERACIONAL

3.1 Observación y medición del rendimiento en materia de la seguridad operacional

El operador desarrollará y mantendrá los medios para verificar el rendimiento en materia de seguridad operacional de la organización y para confirmar la eficacia de los controles de los riesgos de seguridad operacional.

El rendimiento en materia de seguridad operacional del operador se verificará con referencia a los indicadores y metas de rendimiento en materia de seguridad operacional del SMS.

3.2 Gestión del cambio

El operador definirá y mantendrá un proceso para identificar los cambios que puedan afectar al nivel de riesgo de seguridad operacional asociado a sus operaciones, así como para identificar y manejar los riesgos de seguridad operacional que puedan derivarse de esos cambios.

3.3 Mejora continua del SMS

El operador observará y evaluará la eficacia de sus procesos SMS para permitir el mejoramiento continuo de la actuación general del SMS.

7.16.4 PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

4.1 Instrucción y educación

El operador creará y mantendrá un programa de instrucción en seguridad operacional que garantice que el personal cuente con la instrucción y las competencias necesarias para cumplir con sus funciones en el marco de SMS.

El alcance del programa de instrucción en seguridad operacional será apropiado para el tipo de participación que cada persona tenga en el SMS.

4.2 Comunicación de la seguridad operacional

El operador creará y mantendrá un medio formal de comunicación en relación con la seguridad operacional que:

- garantice que el personal conozca el SMS, con arreglo al puesto que ocupe dentro de la organización;
- difunda información crítica para la seguridad operacional;
- explique por qué se toman determinadas medidas de seguridad operacional y
- explique por qué se introducen o modifican procedimientos de seguridad operacional.

8. CAPÍTULO 5: PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

8.1 INTRODUCCIÓN

1. Los tres primeros capítulos de esta Guía reflejan, respectivamente, la fundamentación dogmática para la puesta en marcha de SMS, y los dos procesos básicos subyacentes a su operación: gestión de riesgo de seguridad operacional y aseguramiento de seguridad operacional, así como las actividades y los medios necesarios para la ejecución de los mismos. El capítulo anterior abarca los cuatro arreglos institucionales primarios para auspiciar el establecimiento y funcionamiento efectivo y eficiente de SMS: la publicación de la política de seguridad operacional, el establecimiento de objetivos de seguridad operacional, la asignación de responsabilidades para la gestión de la seguridad operacional, incluyendo la designación de personal con funciones al respecto, y la publicación de la documentación pertinente. El capítulo anterior también describe las ocho actividades iniciales para la puesta en marcha de SMS, presentadas en su orden secuencial. El contenido de este capítulo abarca el quinto arreglo institucional necesario para auspiciar el establecimiento y funcionamiento efectivo y eficiente de SMS: promoción de la seguridad operacional.

2. Las actividades de gestión de seguridad operacional de un operador bajo SMS difícilmente resultarán exitosas si se pretende que funcionen por mandato o mediante la implantación mecánica de directivas. La promoción de la seguridad operacional es una actividad fundamental, en cuatro nítidos aspectos:

   a) como instrumento que genera y apoya las pautas que predisponen hacia actitudes y conductas individuales y colectivas acorde con los imperativos de funcionamiento de SMS;

   b) como auspicio al desarrollo de prácticas operativas conducentes a la cristalización de los procesos de gestión de la seguridad operacional durante las operaciones necesarias para la provisión de servicios del operador;

   c) para cubrir eventuales vacíos que pudiesen darse en la comprensión de directivas y/o ejecución de procedimientos; y finalmente

   d) como medio que genera sentido de propiedad de SMS a todo el personal involucrado, y le otorga finalidad a las actividades de gestión de la seguridad operacional del operador bajo SMS.

8.2 ACTIVIDADES DE PROMOCIÓN DE SEGURIDAD OPERACIONAL

3. Hay tres actividades básicas de promoción de la seguridad operacional que el operador debe poner en marcha como parte de SMS:

   a) debe establecer un programa de comunicación sobre gestión de la seguridad operacional;

b) debe auspiciar, por medio del programa de comunicación sobre gestión de seguridad operacional, educación sobre ésta; y

c) debe proveer instrucción sobre gestión de seguridad operacional, incluyendo el establecimiento de competencias en seguridad operacional.

8.3 COMUNICACIÓN

4. La comunicación es el ingrediente esencial de la promoción de la seguridad operacional. Son frecuentes los casos en los que las ideas, aún las mejor concebidas, fallan en su traslado a la práctica porque quienes las conciben no las comunican efectivamente a quienes las deben llevar a cabo en la práctica. Esto genera dos alternativas: por un lado, desconocimiento del objetivo buscado, lo que lleva a grietas y desviaciones en su puesta en marcha. Por otro, y quizás lo más contraproducente, indiferencia cuando no actitudes cínicas. Lo antedicho es aplicable a todos los campos del comportamiento humano, y la gestión de la seguridad operacional no es una excepción.

5. El operador debe por lo tanto establecer procedimientos que permitan la comunicación más efectiva posible al personal operativo y a la alta dirección, que hagan posible a esta última comunicar:

   a) los objetivos globales en cuanto a la gestión de la seguridad operacional;

   b) la situación actual de las actividades específicas al respecto; y

   c) el logro de hitos significativos.

6. Análogamente, el operador debe establecer procedimientos que permitan la comunicación "hacia arriba", es decir, del personal operativo a dirección, sobre aspectos referidos a la gestión de la seguridad operacional, en un entorno flexible y libre de restricciones burocráticas.

7. El vehículo de comunicación más importante con el que cuenta el operador para la comunicación sobre la gestión de la seguridad operacional bajo SMS es el manual del sistema de gestión de la seguridad operacional (SMSM), según lo expuesto en el capítulo anterior. El SMSM es el instrumento clave para comunicar el enfoque del operador sobre la gestión de la seguridad operacional a toda la organización.

8. En orden de importancia, el otro vehículo fundamental de comunicación del operador a los efectos de la gestión de la seguridad operacional, al que históricamente no se le ha dado la dimensión de importancia que verdaderamente tiene, son los procedimientos operativos estandarizados (*SOPs*). Los *SOP*s son mucho más que una guía mecánica de cómo ejecutar acciones. En su sentido final, son un mandato sobre como la dirección ha establecido que deben realizarse las operaciones necesarias para la provisión de servicios.

9. Otros ejemplos de formas de comunicación sobre gestión de la seguridad operacional a disposición del operador incluyen sesiones periódicas de información (no hay sustituto para la comunicación cara a cara), boletines informativos y anuncios de seguridad operacional, cuya difusión en la actualidad ha sido notablemente facilitada por los portales web y el correo electrónico.

10. La unidad del operador a cargo de la gestión diaria de SMS será quien proporcione la materia prima necesaria para un programa de comunicación sobre gestión de la seguridad operacional. Se trata de información actualizada que haga que el SMS sea visible en todos los aspectos de las operaciones del operador que apoyan la provisión de servicios. Esto incluye no solo la comunicación actualizada sobre los objetivos de seguridad operacional del operador, sino también comunicación periódica sobre la evaluación del rendimiento en materia de seguridad operacional del SMS, incluyendo indicadores y metas de actuación en materia de seguridad operacional y sus logros, según lo expuesto en el capítulo 3. Igualmente, las enseñanzas y lecciones en cuanto a seguridad operacional obtenidas de investigaciones oficiales o internas, casos de estudio, o intercambio de experiencias, tanto internamente como con otros operadores, son materia prima para la comunicación y deben ser objeto de divulgación.

11. En síntesis, el operador debe tener en marcha un programa de comunicación sobre gestión de la seguridad operacional, gestionado por la unidad del operador a cargo de la gestión diaria del SMS, dirigido al personal operativo de toda la organización, que tenga como objetivos:

    a) asegurar que todo el personal tiene pleno conocimiento del SMS;

    b) transmitir información crítica para la gestión de la seguridad operacional;

    c) explicar por qué se adoptan medidas particulares;

    d) explicar por qué se introducen o modifican procedimientos de seguridad operacional; y

    d) transmitir información que pueda ser útil.

8.4 FORMACIÓN

12. La formación sobre gestión de la seguridad operacional se refiera a la provisión periódica, por parte del operador y por medio de su programa de comunicación sobre gestión de la seguridad operacional, así como de material de interés general sobre novedades y tendencias en la aviación civil internacional en todos sus campos operativos. El objetivo de la formación es poner al alcance del personal operativo, y de los niveles gerenciales operativos, conocimiento sobre cómo aspectos humanos, técnicos y organizacionales determinan la seguridad operacional del sistema como un todo, y así facilitar la comprensión de la información sobre gestión de la seguridad operacional distribuida por el operador por medio de su programa de comunicación.

13. Una contribución frecuentemente infravalorada de la formación sobre gestión de la seguridad operacional tiene que ver con su fundamental influencia como impulso de un programa de reporte de seguridad operacional efectivo. Se trata de una muy simple ecuación: personal operativo debidamente formado sobre el *porqué* y el *cómo* de la gestión de la seguridad operacional es sinónimo de personal operativo *motivado* para proveer información esencial para la gestión de la seguridad operacional.

14. Hoy día, un portal web y el correo electrónico son los medios ideales para circular información que auspicie la formación sobre gestión de la seguridad operacional.

8.5 INSTRUCCIÓN

15. A diferencia de la formación, cuyo objetivo es el desarrollo intelectual por medio de la provisión de fundamentos y conocimientos conceptuales de naturaleza amplia, la instrucción tiene por objetivo la provisión de conocimientos técnicos específicos y el desarrollo de habilidades o actitudes específicas necesarias para la ejecución de tareas determinadas.

16. La unidad del operador a cargo de la gestión diaria de SMS será quien proporcione la información actualizada necesaria como materia prima para el desarrollo de los materiales de instrucción. Según sea el caso de los arreglos internos del operador, la misma unidad se hará también cargo de la entrega de la instrucción relacionada con los aspectos de gestión de seguridad operacional pertinentes a las unidades operacionales específicas del operador. El dictado de instrucción en gestión de la seguridad operacional apropiada a todo el personal operativo, independientemente de su nivel en la organización del operador, es no solamente una indicación del compromiso de la alta dirección de contar con un SMS efectivo, sino también uno de los cimientos del mismo, desde la perspectiva de los arreglos institucionales.

17. La instrucción en gestión de la seguridad operacional debe incluir un método, debidamente documentado, para identificar los requisitos de instrucción, así como un método de validación que permita evaluar la efectividad de la misma. Los requisitos y actividades de instrucción en materia de gestión de la seguridad operacional deberían documentarse para cada área o unidad de actividad relacionada con las operaciones necesarias para la provisión de servicios. El programa de instrucción en gestión de la seguridad operacional debe ser acorde a las necesidades y complejidad de la organización.

18. El manual SMS (SMSM) es el depositario natural de los métodos y programas de instrucción en gestión de la seguridad operacional. El SMSM debe incluir las directivas específicas de instrucción inicial y periódica en gestión de la seguridad operacional para todo el personal técnico u operativo, post-holders y otros cargos, así como la necesidad de un *briefing* para el Gerente Responsable. El volumen de instrucción en gestión de la seguridad operacional para cada grupo profesional debe adecuarse a la responsabilidad de sus miembros y su participación en el SMS. El SMSM también debe especificar responsabilidades de instrucción en seguridad,

incluyendo contenido, frecuencia, validación y gestión de registros de instrucción en gestión de la seguridad operacional.

19. La identificación y seguimiento, para verificar que el personal ha recibido la instrucción prevista de los requisitos de instrucción en gestión de la seguridad operacional deben formar parte de los registros del personal operativo, junto con el resto de los requisitos de instrucción. La instrucción en gestión de la seguridad operacional debe asegurar que el personal está instruido y es competente para realizar sus tareas de gestión de la seguridad operacional.

8.6 PERSONAL TÉCNICO U OPERATIVO

20. La instrucción en gestión de la seguridad operacional para el personal técnico u operativo debería abarcar la política de seguridad operacional, los roles y las responsabilidades de seguridad operacional; los principios del SMS asociados a la gestión de riesgos de seguridad operacional y el aseguramiento de la seguridad operacional; junto con el uso y los beneficios de los sistemas de reporte de seguridad operacional del operador.

8.7 POST-HOLDERS (O PERSONAL RESPONSABLE) Y OTROS CARGOS

21. La instrucción en gestión de seguridad operacional para los post-holders y otros cargos que así lo requieran debería abarcar además el cumplimiento de los requisitos de seguridad operacional nacionales por la organización, la asignación de recursos y la promoción activa del SMS incluyendo una efectiva comunicación inter-departamental sobre seguridad operacional. Además, ha de incluirse instrucción sobre el establecimiento de las metas de rendimiento en materia de seguridad operacional.

8.8 BRIEFING ESPECIAL PARA EL GERENTE RESPONSABLE

22. Por último, la instrucción en seguridad operacional debería incluir un *briefing* especial para el Gerente Responsable. Esta sesión debe ser breve (inferior a 2 horas), a los efectos de proporcionar al Gerente Responsable un panorama amplio y global sobre SMS del operador. El *briefing* para el Gerente Responsable debe proporcionar una respuesta clara y sin ambigüedad a dos preguntas que indudablemente estarán en la mente del Gerente Responsable: "¿qué se hace de forma diferente bajo el marco del SMS con respecto a lo que hacíamos antes?", y "¿qué me toca hacer a mí?". Ambas preguntas fueron discutidas en el capítulo 1 de esta Guía.

9. BIBLIOGRAFÍA

9.1 ICAO

- *Anexo 19 Gestión de la seguridad operacional de OACI*
- *Manual de gestión de la seguridad operacional de OACI* (Doc. 9859)
- *Auditoría de la seguridad de las operaciones de línea aérea (LOSA)* (Doc. 9803)
- *Estudio de la seguridad de las operaciones normales (NOSS)* (Doc. 9910)
- *Compendio sobre factores humanos Núm. 17 — Manejo de amenazas y errores (TEM) en el control de tránsito aéreo* (Circular 314)

9.2 EASA

- *Safety Management System and Safety Culture Working Group (SMS WG)*
- *Aircraft ground handling and human factors. A comparative study of the perceptions by ramp staff and management*
- *Just culture and human factors training in ground service providers*
- *Guidance on organisational structures*
- *Guidance on hazards identification*
- *Guidance on operational risk assessment*

9.3 CASA

- *Civil Aviation Advisory Publication CAAP SMS 1(0) – Safety management systems for regular public transport operations*
- *Advisory circular AC 119-165(0) – Safety management training*
- *Advisory circular AC 139-16(0) – Developing safety management systems at your aerodrome*
- *Civil Aviation Advisory Publication CAAP SMS 2(0) – Integration of Human Factors (HF) into safety management systems (SMS)*
- *Safety management and the CEO (CASA brochure)*
- *Managing change in the aviation industry (CASA brochure)*
- *Safety management systems – Industry best practice (CASA brochure)*

9.4 EUROCONTROL

- *Generic safety management manual*

9.5 IATA

- *Safety management systems – The senior airline manager's implementation guide*
- *Safety management systems (SMS) for airline operations*

9.6 IBAC

- *SMS toolkit for business aircraft operators*

9.7 IBA

- *Safety management systems (SMS) implementation guide*
- *Safety management systems (SMS) framework*
- *Safety management systems (SMS) assurance guide*
- *Advisory Circular AC 120-92A – Safety management systems for aviation service providers*
- *Advisory Circular AC150/5200-37 – Introduction to safety management systems (SMS) for airport operators*

9.8 TRANSPORT CANADA

- *Safety management systems for small aviation operations – A practical guide to implementation* (TPE14135)
- *Safety management systems: Assessment guide* (TP14326)
- *Safety management systems – Implementation procedures guide for Air Operators and Approved Maintenance Organizations* (TP14343)
- *Risk management and decision-making in civil aviation* (TP13095)
- *Risk management and decision-making in civil aviation – Short process* (TP13095B)
- *Safety management systems for flight operations and aircraft maintenance organizations* (TP13881)
- *Guidance on Safety Management System Development* (Advisory Circular 107-001)

9.9 UK CAA

- *Safety management systems – Guide to organizations*
- CAP 712 – *Safety Management Systems for Commercial Air Transport Operations*
- CAP 642 – *Airside safety management*
- CAP 730 – *Safety management systems for air traffic management*
- CAP 760 - *Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers*

9.10 SM ICG

- A Common Approach to Safety Performance Measurement (SPMA) Paper
- Determining the Value of SMS
- How to Support a Successful SSP and SMS Implementation – Recommendations for Regulators
- Measuring Safety Performance Guidelines for Service Providers
- Risk Based Decision Making Principles
- SM ICG SMS Evaluation Tool
- SMS for Small Organizations
- SMS Inspector Competency Guidance
- SMS Integration – Points to Consider