ANAC
Administración Nacional
de Aviación Civil

SMS
Safety Management System

Fundamentos para la implementación del SMS

2012

Administración Nacional de Aviación Civil

República Argentina

Prólogo

El presente Manual es el medio seleccionado por la Administración Nacional de Aviación Civil (ANAC) para la difusión del concepto de gestión de la seguridad operacional dentro del ámbito de la aviación civil argentina. Para ello, se exponen con profundidad los conceptos y fundamentos que deben incorporar dentro de sus organizaciones todos aquellos proveedores de servicios a los cuales las Regulaciones Argentinas de Aviación Civil (RAAC) les requieren la implementación de un sistema de gestión de la seguridad operacional (SMS). Esta exigencia surge de las mencionadas Regulaciones Nacionales que, a la vez, incorporan las normas y métodos recomendados (SARPs) contenidos en los respectivos Anexos al Convenio de Chicago.

ANAC
Administración Nacional
de Aviación Civil

ESTA PÁGINA FUE DEJADA INTENCIONALMENTE EN BLANCO

Introducción

1. La responsabilidad por la implementación de un sistema de gestión de la seguridad operacional (SMS, *safety management system*) por parte de un proveedor de servicios surge de 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 la Administración Nacional de Aviación Civil, así como de múltiples autoridades internacionales como La Agencia Europea de Seguridad Aeronáutica (EASA), y la Agencia Federal de Aviación (FAA).

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 sistemas*, 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 del sistema, cualquiera sea el sistema en cuestión, una vez que éste se torna operativo, introduciendo seguridad *a priori*, es decir, "diseñando" seguridad en el sistema durante su concepción y desarrollo.

3. Para lograr tal objetivo, *system safety* le presta en principio seria atención a factores que son de consideración típica durante el diseño de un sistema, y que a veces entran en competencia – cuando no en conflicto – entre sí. Estos factores incluyen costos de desarrollo, cronogramas, confiabilidad del diseño propuesto, etc. La aplicación de conceptos de *system safety* apunta a lograr un equilibrio balanceado entre la atención depositada en cada uno de estos factores. 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 *herramientas* en el más amplio sentido) que necesita el sistema y los operadores del mismo interactúan en formas que pudieron no haber sido anticipadas – o que hubiese sido inimaginable anticipar – por los diseñadores, con el consiguiente impacto en la seguridad de las operaciones una vez que el sistema se pone en marcha.

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, las actividades *en system safety* estaban basadas en la ingeniería en forma casi excluyente; 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. En este sentido, recuérdese como anécdota histórica que la primera versión de la cápsula espacial *Mercury* no tenía ventanillas para el ocupante, y solo la inalterable posición de los astronautas llevó a la instalación de una, con gran desgano por parte de los diseñadores. En cambio, la gestión de la

seguridad operacional a través de SMS amplía la perspectiva (y por consiguiente el dogma) de *system safety* 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 y/o productos, sin importar la naturaleza del sistema ni de sus servicios y/o productos. Estos dos 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 riesgos de seguridad operacional* y *garantía de la seguridad operacional* respectivamente.

6. En la literatura sobre *system safety* hay también coincidencia en cuanto a que el desarrollo y operación en forma continuada de los dos procesos básicos de un sistema de gestión que apoya la provisión de servicios y/o productos no puede tener lugar en el vacío institucional. A no ser que se hayan establecido arreglos institucionales que proporcionen los cimientos y faciliten la implementación y el mantenimiento efectivo – en el caso del SMS – de la gestión de riesgos de la seguridad operacional y de la garantía 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 de los arreglos institucionales adaptados para el caso de SMS sugiere dos rótulos genéricos para los arreglos institucionales que funcionan como los de cimientos de SMS: *política y objetivos de seguridad operacional*, y *promoción de la seguridad operacional*.

7. Las normativas sobre el SMS emitidas por OACI y por otras autoridades 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 las de otras autoridades. 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 del SMS, hace que el material contenido en este documento satisfaga las necesidades de implementación de SMS no sólo de los proveedores de servicios argentinos que brindan servicios domésticos sino que también de los que prestan servicios internacionales, bajo el imperativo de las normas OACI.

8. Las normas de OACI son de cumplimiento obligatorio para operaciones internacionales. Su no cumplimiento significaría que, por ejemplo, las aeronaves de un explotador aéreo estarían operando sin un certificado de operación válido – aún cuando tuviese uno concedido por su autoridad de registro – fuera del ámbito de competencia de la autoridad certificadora. Aún cuando un Estado en cuestión hubiese notificado una diferencia a la OACI sobre cualquier aspecto de la normativa SMS, o cual-

quier otra normativa, tal notificación es a *efectos informativos solamente* y no exime del cumplimiento de la norma por el proveedor de servicios 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 este documento en lineamientos de validez universal, en vez de en lineamientos particulares adoptados por una autoridad u otra. Un proveedor de servicios que implemente su SMS siguiendo los lineamientos ofrecidos por este documento cumplirá con la normativa OACI así como otras normativas vigentes.

9. Estos *Fundamentos para la Implementación de SMS por los proveedores de servicios* de la Administración Nacional de Aviación Civil (ANAC) se divide en cinco capítulos, que abarcan respectivamente la fundamentación dogmática, los dos procesos básicos y los dos arreglos institucionales necesarios para apoyar la implementación y el mantenimiento efectivo del SMS por un proveedor de servicios. El capítulo de apertura presenta la fundamentación sobre la cual se construye el SMS. Los dos capítulos subsiguientes abarcan los dos procesos básicos del SMS (gestión de riesgo de seguridad operacional y garantía 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.

10. El material contenido en el documento incluye ejemplos prácticos de aplicación a los efectos de facilitar no solamente la comprensión sino también la implementación. Los procesos y arreglos institucionales, y sus actividades subyacentes, presentan un verdadero plan de vuelo para la puesta en marcha del SMS, o para la reacomodación de procesos, arreglos institucionales, actividades y mecanismos ya existentes dentro de un proveedor de servicios para satisfacer los requerimientos combinados de implementación del SMS. El documento incluye un apéndice que contiene bibliografía así como portales informáticos referidos al SMS.

11. Para concluir esta introducción, es necesario reconocer que el cuadro relativo al SMS en la escena internacional es uno de sumo dinamismo. Se trata de una situación en evolución, en la medida en que la industria mundial adquiere realimentación producto de las experiencias diarias de los proveedores de servicios en actividades de desarrollo, implementación y operación del SMS. Por ello, este documento es un documento viviente, que será modificado según lo impongan las circunstancias de manera tal que su contenido mantenga constante validez y vigencia.

12. Las consultas y comentarios sobre este documento y sus contenidos deben ser dirigidos a:

Unidad de Planificación y Control de Gestión
Administración Nacional de Aviación Civil (ANAC)
ssp-sms@anac.gov.ar

ESTA PÁGINA FUE DEJADA INTENCIONALMENTE EN BLANCO

Índice

Capítulo I

Los Fundamentos

Capítulo I

Los Fundamentos

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 por intermedio del axioma más atesorado – o por lo menos más proclamado – por la comunidad aeronáutica 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 trasladar en forma efectiva a la práctica diaria de las operaciones de la industria aeronáutica, sin que esta afirmación signifique formular un juicio inmoral. Las razones del tan difícil sustento de la visión que el axioma transmite y su aplicación diaria se hacen evidentes cuando se las considera bajo la perspectiva provista por la literatura sobre *system safety* a que se ha hecho alusión en la Introducción a este documento. Como prólogo a tal consideración, una premisa es medular y de rigor: *las cuestiones de seguridad operacional de la aviación no son ni inherentes ni condición natural de las operaciones de vuelo. Tales cuestiones son el producto colateral de la necesidad y la concreción, por parte de las organizaciones de la industria, de las actividades que deben desarrollar, y que son necesarias para la provisión de servicios a los efectos de lograr un producto de rédito.*

3. La literatura sobre *system safety* postula categóricamente que todo sistema se concibe y crea con un objetivo de producción, vale decir, para generar un producto (*output*) mediante la entrega de un servicio o un producto. El sistema en cuestión puede abarcar desde una biblioteca pública (cuyo producto es el enriquecimiento intelectual de la población, por intermedio 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 intermedio del transporte aéreo de personas y/o mercancías).

4. A los efectos de un análisis neutro y desapasionado de cuál es la ubicación jerárquica de la seguridad operacional entre las prioridades de las organizaciones de aviación, el *producto* no es tan importante como la *provisión de servicios*. Esta provisión tiene lugar dentro de contextos operativos específicos que incluyen componentes naturales, tales como la meteorología, eventos geofísicos, orografía, etc. Por otro lado, la provisión de servicios demanda (y por lo tanto los contextos operativos específicos incluyen) 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 operacionales específicas, según ciertas *interacciones operativas*, 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, el equipamiento puede fallar, el combustible para el 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 durante la etapa de diseño o planificación – 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 *controles o mitigaciones* contra las posibles consecuencias de interacciones entre los diversos componentes, que pueden generar situaciones adversas a la provisión de servicios. Para ello, debe *adjudicar recursos* que se conviertan en el sustento para la puesta en marcha y el mantenimiento de las actividades de control y mitigación.

7. Las situaciones adversas generadas por las consecuencias de las interacciones entre los diversos componentes naturales y técnicos del contexto operativo tienen el potencial de poner en peligro la capacidad de un sistema de brindar su producto mediante la entrega de servicios. La adjudicación de recursos para el control o 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. Más frecuentemente que no, las decisiones sobre la adjudicación de recursos no son las óptimas que la visión filosófica/estereotípica de la seguridad operacional hubiese deseado o propuesto (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 al adoptar una decisión en cuanto a la adjudicación de recursos es inevitable porque no existe sistema cuyos administradores y gestores 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 una santo para vestir a otro.

9. La complejidad de las situaciones que deben ser tenidas en cuenta, la confluencia de factores de muy distinta naturaleza, y la siempre presente limitación en la disponibilidad de recursos para asig-

nar a actividades de control o mitigación de las consecuencias de las interacciones entre componentes del sistema, son de gran significación al momento de la decisión. Por lo tanto, la única posibilidad que el compromiso en la toma de decisiones para la adjudicación de recursos esté lo más realísticamente posible cercano 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 del SMS, y su real contribución al logro de los objetivos globales de un proveedor de servicios: 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 controlar o mitigar las consecuencias de las interacciones entre diversos componentes del sistema con potencial de generar situaciones que ponen en peligro la capacidad del proveedor de servicios de brindar su producto mediante la entrega de servicios.

Dos preguntas claves

11. Hay dos preguntas que se formulan frecuentemente sobre el SMS. Una pregunta es: *"¿cuál es la diferencia entre el SMS y un programa de prevención de accidentes?"* La compañera inseparable de la anterior es: *"¿qué tiene el 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 proveedor de servicios 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 dedicada a la provisión de servicios 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 medio ambiente
c) Sistema de gestión de seguridad *(security)*
d) Sistema gestión financiero
e) Sistema de gestión legal
f) Sistema de gestión de recursos humanos
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 tal sistema, 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 institucionales para contrarrestar deficiencias que tienen el potencial de poner en peligro la capacidad del proveedor de servicios en cuanto a 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 de gestión que se considere. Así, un sistema de gestión financiero es un sistema de recolección 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 recolección 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 productos 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 recolección 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.

¿Cuál es la diferencia entre el SMS y un programa de prevención de accidentes?

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

17. Una vez que los datos han sido analizados y se ha extraído información e inteligencia de los mismos, la conducción superior del proveedor de servicios 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 intermedio 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*. Típicos ejemplos de programas de seguridad (es decir, programas que ejecutan decisiones formuladas por los niveles gerenciales del proveedor de servicios) incluyen:

a) Programa de seguridad de vuelo y prevención de accidentes;
b) Programa de instrucción en gestión del los recursos de la cabina de mando (Crew Resource Management, CRM);
c) Programa de instrucción en gestión de amenazas y errores (Threat and Error Management, TEM);
d) Programa de instrucción sobre mercancías peligrosas;

e) Programa de competencias lingüísticas;

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

g) Programa de prevención de accidentes durante aproximación y aterrizaje (Approach and Landing Accident Reduction, ALAR)

h) 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 el SMS y un programa de prevención de accidentes?"). El* SMS es el sistema de gestión que le permite al proveedor de servicios 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 durante la operación de aeronaves, que están agrupadas bajo un programa de seguridad operacional específico. En síntesis, el SMS es un sistema de gestión, prevención de accidentes es un programa de ejecución.

¿Qué tiene el SMS de nuevo o diferente con respecto a lo que anteriormente se hacía en cuanto a seguridad operacional?

20. Al presente, la implementación por un proveedor de servicios de programas de seguridad 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 la respuesta a deficiencias de seguridad de naturaleza global. Estas deficiencias pueden ser de primacía en determinados ámbitos nacionales o regionales específicos, mientras que pueden no serlo en otros, por lo menos al nivel en el 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 proveedores de servicios no cuenta con un mecanismo formal que permita evaluar, sobre la base de datos, la importancia específica que tiene una deficiencia particular dentro de su contexto operativo, su impacto en la seguridad operacional durante la provisión de servicios, y por ende el valor agregado que podría aportar al proveedor de servicios la eventual normativa en vigor sobre el tema en cuestión. Ausente tal mecanismo, el proveedor de servicios 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 necesariamente son una respuesta a deficiencias de seguridad operacional que afectan específicamente al proveedor de servicios puede obstaculizar la identificación de deficiencias que *sí* afectan directamente al proveedor de servicios, generando una situación de precariedad en la gestión de la seguridad operacional. Segundo, puede forzar la adjudicación de recursos a actividades de relativa significación específica para la seguridad operacional, distrayéndolos de otras actividades de real significación específica, potencializando aun más la aparición de grietas en la gestión de la seguridad operacional.

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

24. Aún cuando la imposición normativa y su cumplimiento continuará siendo un imperativo, la disponibilidad de datos le permite al proveedor de servicios 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 del 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 proveedor de servicios 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 proveedor de servicios particular.

25. Lo expuesto a partir del párrafo 33 brinda la respuesta a la segunda de las preguntas claves formuladas en el primer párrafo de este Capítulo (*"¿qué tiene el SMS de nuevo o diferente con respecto a lo que anteriormente se hacía en cuanto a seguridad operacional?").* La novedad que el 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 proveedor de servicios particular. El aspecto fundamental a no perder de vista es que como las decisiones sobre la concentración de recursos sobre actividades específicas están basadas sobre datos, son fácilmente *explicables y defendibles*.

"El Generador SMS"

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

27. La visualización presenta al SMS como un generador (ver fig. 1). La analogía es apropiada, en cuanto el SMS es un verdadero generador de información e inteligencia para la toma de decisiones estratégicas sobre la adjudicación de recursos para actividades agrupadas bajo el rotulo *programas de seguridad operacional*. El *input* que hace funcionar al "generador" son datos específicos del proveedor de servicios. 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 calidad, etc. Dentro del "generador", los datos son evaluados y analizados teniendo en cuenta cuestiones normativas, de política (tanto institucional como nacional), de costo/beneficio, etc. El *output* del "generador" son decisiones estratégicas, que se implementan por intermedio de programas de seguridad. Estos programas de seguridad representan una adjudicación de recursos formal y principista para la solución de problemas de seguridad que son los que el proveedor de servicios específicamente 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 proveedor de servicios implementados como consecuencia de decisiones estratégicas sobre la adjudicación de recursos basadas en datos serán una combinación de programas en respuesta a problemas específicos del proveedor de servicios 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.

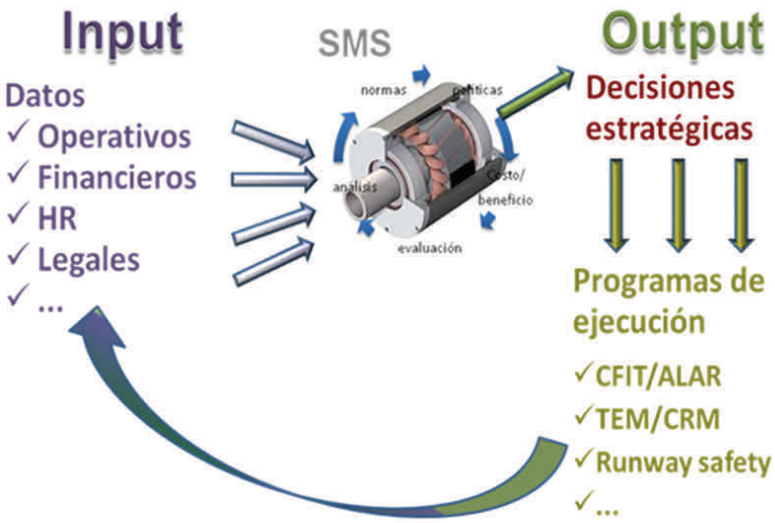

Fig. 1 "El generador SMS"

Dos procesos fundamentales

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

30. Un *proceso* es un marco de referencia conceptual. Sirve de apoyo y proporciona una guía sistemática y ordenada para la puesta en marcha y ejecución de acciones específicas necesarias para lograr un objetivo pre-especificado. Pero el proceso en sí mismo es una abstracción, una idea, y no existe en forma visible o concreta en el mundo material.

31. Una *actividad*, por su lado, es una secuencia o serie de acciones específicas o actividades que representan los medios materiales por intermedio 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 los controles y mitigaciones para las situaciones que ponen en peligro la capacidad de un proveedor de servicios de brindar su producto 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 del SMS como sistema de gestión de la seguridad operacional, estos dos procesos fundamentales se denominan gestión del riesgo de seguridad operacional *(safety risk management, SRM)* y garantía de la seguridad operacional *(safety assurance, SA).* Ambos procesos son presentados en detalle en sus respectivos capítulos, y lo que sigue a continuación es solamente una breve introducción a sus fundamentos.

34. La *gestión de riesgo de seguridad operacional* se basa en la aplicación de *principios de seguridad operacional sistémica* al control y mitigación de situaciones que ponen en peligro la capacidad de un proveedor de servicios de brindar su producto mediante la entrega de servicios. La gestión de riesgo 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 proveedor de servicios.

35. La gestión de riesgos de seguridad operacional involucra esencialmente actividades que *miran*

hacia el futuro. Sus *objetivos* 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 deficiencias y peligros por intermedio de estrategias de control o mitigación.

36. Graficando el proceso de gestión de riesgo de seguridad operacional sobre la visualización del SMS ya expuesta, el mismo abarcaría el *input* al "generador" (adquisición de datos), el "generador" mismo (transformación de los datos en información e inteligencia) y el *output* (formulación de decisiones estratégicas y su implementación por intermedio de programas de seguridad operacional como control inicial de deficiencias de seguridad y peligros en el contexto operativo).

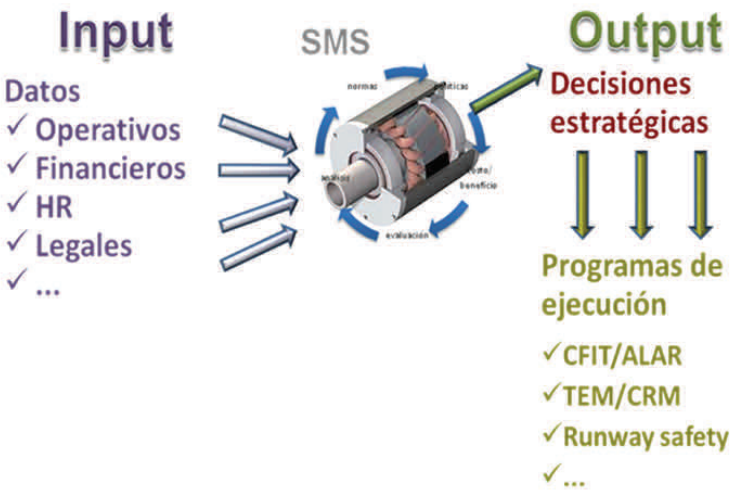

Fig. 2 "El generador SMS"

37. La *garantía de la 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 control y mitigación (es decir, de los programas de seguridad operacional) para las situaciones que ponen en peligro la capacidad de un proveedor de servicios de brindar su producto mediante la entrega de servicios. Un aspecto esencial de este control es la verificación que los programas implementados son la respuesta apropiada para las deficiencias de seguridad operacional y peligros para cuya contención fueron puestos en marcha. Se trata, específicamente, de actividades que generan confianza que las actividades puestas en marcha por medio de la gestión de riesgo de seguridad operacional para el control inicial de deficiencias de seguridad operacional y peligros en el contexto operativo *cumplen su objetivo* y *funcionan de acuerdo a lo esperado*.

38. Tal reaseguro es necesario porque las actividades iniciales, puestas en marcha como consecuencia

de la gestión de riesgo 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 control o 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. Mas 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 operativo determinado. Por consiguiente, cualquier actividad de control o mitigación debe ser reevaluada y validada 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, y contrario a la percepción establecida entre la comunidad aeronáutica, implementación no es sinónimo de solución; y

b) la calidad de las decisiones estratégicas sobre adjudicación de recursos para actividades de control o 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. “Buenos” datos permiten tomar “buenas” decisiones”; mientras que “malos” datos generan “malas” decisiones. De ahí, la importancia de la realimentación, producto de la experiencia operativa, al sistema de gestión por intermedio de la garantía de entrega; en el caso del SMS, la realimentación al SMS por intermedio de la garantía de la seguridad.

39. A diferencia de la gestión del riesgo de seguridad operacional, cuyas actividades *miran al futuro*, la garantía de la seguridad operacional involucra actividades que *se ocupan del presente.* Sus objetivos 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 (es decir, de los programas de seguridad operacional) para las deficiencias de seguridad y peligros en el contexto operativo.

40. Graficando el proceso de garantía 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 destacar la importancia del monitoreo constante de las actividades de estos programas – por intermedio de datos – como para verificar desfasajes entre el logro de los resultados buscados al implementar los programas, y los resultados reales obtenidos. Esto permitirá al proveedor de servicios efectuar los retoques o cambios necesarios a los programas para mantener su eficiencia y eficacia.

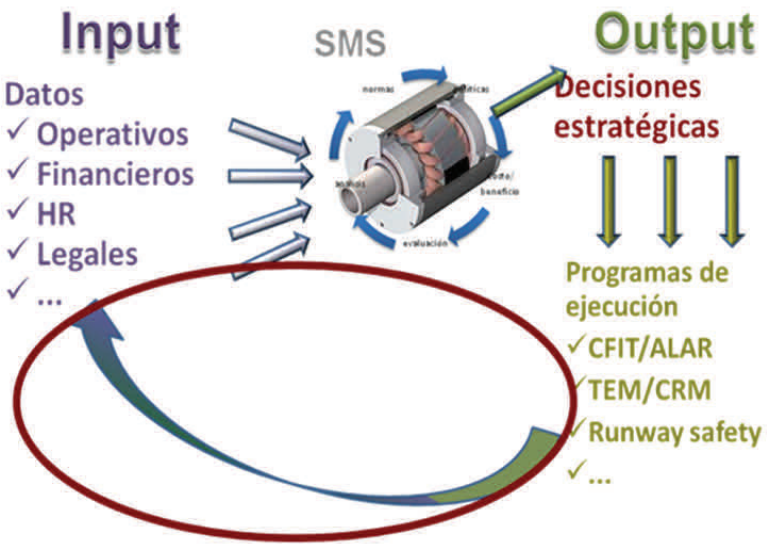

Fig. 3 “El generador SMS”

ESTA PÁGINA FUE DEJADA INTENCIONALMENTE EN BLANCO

Capítulo II

Gestión de Riesgo de Seguridad Operacional (SRM)

Capítulo II

Gestión de Riesgo de Seguridad Operacional (SRM)

Introducción

1. El Capítulo I de este documento presenta una exposición inicial sobre los dos procesos básicos del SMS, de los cuales se derivan las actividades de control o mitigación de las deficiencias de seguridad operacional y peligros en el contexto operativo. Tales procesos son la gestión de riesgo de seguridad operacional y la garantía de la seguridad operacional. Este Capítulo trata sobre el primero de ellos: la gestión de riesgo de seguridad operacional.

2. Según la exposición inicial del Capítulo I, la *gestión de riesgo de seguridad operacional* se basa en la aplicación de *principios de seguridad operacional sistémica* al control y mitigación de situaciones que ponen en peligro la capacidad de un proveedor de servicios de brindar su producto mediante la entrega de servicios.

3. 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 de la implementación y mantenimiento efectivos de un SMS. Tales principios son de validez universal, e incuestionables en cuanto a su importancia como marco de referencia para guiar conceptualmente la 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**

4. 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 riesgo de seguridad operacional como uno de los dos

pilares sobre los cuales se basa la práctica y operación diaria de SMS por un proveedor de servicios.

Principios del SMS

Principio N° 1: La vulnerabilidad de los sistemas en cuanto a seguridad operacional

5. El primer principio de la gestión de riesgo de la seguridad operacional postula que

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

6. La vulnerabilidad de un sistema – desde el punto de vista de la seguridad operacional – es la susceptibilidad del mismo a deficiencias de seguridad y peligros. La vulnerabilidad desde el punto de vista de la seguridad operacional no es igual para cada sistema (en nuestro caso, entre líneas aéreas); hay sistemas que son más vulnerables a deficiencias y peligros que otros. Un número de factores influyen sobre tal vulnerabilidad 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 la aviación comercial con sus componentes: líneas aéreas, servicios de tránsito, explotadores aeroportuarios, etc. no son una excepción.

7. La vulnerabilidad del sistema nace con el diseño del 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 llevaran a cabo las operaciones necesarias para lograr el producto 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.

8. Aún 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 de 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 una cierta magnitud de deficiencias de seguridad y peligros consecuencia de estas interacciones, dando así lugar a la génesis de su vulnerabilidad.

9. 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 producto (*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?

10. Los diseñadores del sistema utilizan diversos métodos para encontrar respuestas 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.

11. 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 operacional y peligros: la tecnología (también necesaria para lograr el producto del sistema por intermedio de la entrega de servicios), la instrucción necesaria para que los operarios puedan operar adecuadamente la tecnología, y las políticas, los reglamentos y procedimientos que rigen las conductas operativas 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.

12. 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”.

13. La deriva práctica entre funcionamiento teórico y funcionamiento real, la deriva de *cómo deberían* funcionar las defensas durante las operaciones a *cómo funcionan realmente*, 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 limi-

taciones del contexto y se tornan por lo tanto difíciles de observar; introducción de cambios sutiles y graduales en el sistema luego de 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.

14. 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 para un proveedor de servicios por intermedio de su SMS. Como para expresar los conceptos genéricos expuestos en los párrafos anteriores en términos aplicables a la operación del 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 especificadas con anticipación 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 fisuras en las defensas del sistema, por consiguiente;

e) bajo el 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 fisuras en las defensas.

Principio N° 2: La descripción de las vulnerabilidades de seguridad operacional del sistema

15. 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**

16. Una vez aceptado por el proveedor de servicios que su sistema (es decir, la línea aérea, el taller de mantenimiento, el aeródromo, etc.) tiene vulnerabilidades de seguridad operacional como consecuencia de deficiencias de seguridad y peligros de difícil anticipación durante su planificación, y que el rol del SMS, por intermedio de la gestión de riesgos de la seguridad operacional, es proporcionar el control de deficiencias y peligros durante las operaciones necesarias para el logro del producto del sistema por medio de la provisión de servicios, el paso siguiente es describir deficiencias de seguridad y peligros en términos operativos, a efectos de poder gestionar su control.

17. La diferencia entre *deficiencias de seguridad*, *peligros* y *riesgos de seguridad operacional* es a menudo fuente de confusión. Para desarrollar prácticas de gestión de riesgo de la 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 del SMS.

18. 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 significación. 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.

19. Un *peligro* se define 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.* 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 del SMS.

20. Una *consecuencia* se define como *el posible resultado de un peligro*. La capacidad de provocar daño – desde el punto de vista de la seguridad operacional – de un peligro se materializa mediante una o varias consecuencias. Una 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 extenso espectro en cuanto a la naturaleza 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 trasgresión inconsecuente de la señalización de detención antes del ingreso a pista sin otra consecuencia que un desvío normativo menor.

21. Finalmente, *el riesgo de seguridad operacional* se define como *la evaluación, expresada en términos de probabilidad y severidad previstas, de cada una de las consecuencias de un peligro, tomando en cuenta la peor situación previsible*. 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 proveedor de servicios) como por ejemplo 5A (frecuente/catastrófico).

22. La exposición en los párrafos anteriores permite ejemplificar la secuencia apropiada del análisis subyacente a la gestión de riesgos de seguridad operacional, cuya observancia es esencial para la correcta operación de SMS por parte del proveedor de servicios:

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)

Principio N° 3: La identificación de peligros

23. El tercer principio de la gestión de riesgo de la seguridad postula que

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

24. Los peligros son componentes normales del contexto operativo en el que un sistema brinda la prestación de servicios para el logro de su producido. 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 de provocar daño 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.

25. Un viento de 15 nudos, en 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 especifica del 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 excursión lateral de la pista debido a la pérdida de control de las aeronaves como consecuencia del viento cruzado).

26. Veamos otro ejemplo sencillo. 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, ella potencial de provocar daño 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 de provocar daño del combustible como peligro aumenta considerablemente. Por ello, se implantan procedimientos de abastecimiento de combustible (controles) para llevar los riesgos de seguridad operacional de las consecuencias de las operaciones de abastecimiento bajo control de la organización (mitigación). Estos procedimientos se basan en la identificación y el control de los elementos del peligro.

27. Vale 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 riesgo de la seguridad operacional, es el control de sus consecuencias.

28. La consecuencias de los peligros pueden contenerse mediante diversas estrategias de control o mitigación, de manera tal de contener el potencial de provocar daño del peligro, lo que se analizará más adelante en este documento. El análisis de las estrategias de mitigación de las consecuencias de los peligros nos lleva a tener en cuenta varios puntos de importancia.

29. 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 poner de manifiesto su potencial de provocar daño. Esto trae a colación un aspecto esencial de la gestión de la seguridad operacional: las estrategias de mitigación deberían dirigirse a contener en forma proactiva el potencial de provocar daño de los peligros y no esperar hasta que las consecuencias de éstos se materialicen y posteriormente tratarlas en forma reactiva.

30. 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 estadísticos.

31. 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 *"excursión lateral de la pista sin consecuencias".* Una consecuencia más severa aún podría ser *"excursión 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. Esto es porque, al momento de la ponderación de los riesgos de seguridad operacional, el dogma impone la consideración de la *peor* consecuencia *previsible* que sea *creíble.*

32. 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 control o mitigación, excepto la cancelación de la operación. Para diseñar estrategias de control o 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 (excursión lateral de la pista), y no en términos extremos (pérdida de vidas).

33. La descripción de las consecuencias 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 operacio-

nal de las consecuencias de los peligros permite a la organización tomar decisiones informadas sobre si puede lograr el control o 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 (excursión lateral de la pista), la evaluación del riesgo de seguridad operacional no tiene demasiado sentido dado que el control o 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.

34. El potencial de confusión entre deficiencias de seguridad, 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 de oculta el carácter verdadero y el potencial de provocar daño 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 de provocar daño 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 riesgo de la seguridad operacional según se analiza en la sección siguiente.

35. 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. La señalización en estado deficiente complica la tarea de la navegación en tierra para los usuarios del aeródromo, tanto aeronaves como vehículos terrestres. En este caso, la nominación 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 ingresen 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 control o mitigación parciales o incompletas, con el consiguiente derroche de recursos.

36. 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.

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

a) condiciones meteorológicas o sucesos climáticos violentos (huracanes, tormentas invernales, tornados, tormentas eléctricas, rayos y relámpagos, cortante de viento, etc.);
b) condiciones meteorológicas adversas (formación de hielo, lluvia congelante, lluvia fuerte, nieve, viento, restricciones a la visibilidad, etc.);
c) sucesos geofísicos (terremotos, volcanes, 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).

38. 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. Ejemplos de peligros técnicos comprenden *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.

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

40. Las actividades de gestión de la seguridad operacional dirigidas a controlar las consecuencias de los peligros estarán dirigidas principalmente, pero no necesariamente con carácter exclusivo, a los peligros técnicos y naturales.

41. 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 para ayudar y simplificar el análisis y la clasificación de los componentes 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.

42. 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 el aeropuerto internacional;

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);
- ✓ ingreso de aeronaves en despegue a la calle de rodaje equivocada (calle de rodaje cerrada);
- ✓ ...

43. Para concluir esta sección, es un hecho de la realidad que, en todo sistema, no importa cuál sea la industria que se considere, sus operarios realizan 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 conduce sus actividades en un sistema vulnerable. En virtud de ello, el personal operativo convive diariamente con deficiencias de seguridad, peligros y en muchos casos sus consecuencias, que a su vez, en muchos casos, no han sido formalmente gestionadas.

44. Por otro lado, es también un hecho de la realidad 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, los operarios, que “viven” diariamente dentro de la deriva, se las ingenian para hacer que el sistema *funcione efectivamente* de manera cotidiana. Los operarios aplican adaptaciones locales y estrategias personales (que encarnan la experiencia colectiva de los profesionales operativos de la aviación) para lograr el producto del sistema por intermedio de la entrega de servicios, superando así las carencias del sistema, en cuanto a las deficiencias de seguridad y los peligros que no han sido formalmente gestionados.

45. La captación, mediante mecanismos formales, (es decir, obteniendo formalmente el conocimiento colectivo que refleja la experiencia profesional de los distintos grupos de trabajo) de lo que ocurre diariamente dentro de la deriva práctica, incluyendo prácticas locales y adaptaciones, tiene un considerable potencial de aprendizaje sobre adaptaciones exitosas, de forma de reducir la deriva entre el funciona-

miento teórico y el funcionamiento real del sistema, y por lo tanto para el control de deficiencias de seguridad 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 y descontrol en el sistema, generando el potencial de un incidente o accidente.

46. El corolario es obvio: los programas de reportaje 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 riesgo de seguridad operacional, y para la implementación y efectivo mantenimiento de SMS por un proveedor de servicios.

Principio N° 4: Medición y control

47. El cuarto y último principio de la gestión de riesgo de la seguridad postula que

"Los riesgos de seguridad operacional son una medida de referencia y control"

48. 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 probabilidad y severidad 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 número" a las consecuencias de los peligros, SMS proporciona al proveedor de servicios un fundamento principista para la adopción de decisiones estratégicas sobre los riesgos de seguridad operacional, y la consiguiente asignación de recursos del proveedor de servicios para actividades destinadas a contener el potencial de provocar daño de los peligros en el contexto operativo durante la provisión de servicios para el logro del producto.

49. 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 riesgo 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, de ahí que hay riesgo de inversión, riesgo financiero, riesgo de calidad, riesgo legal, etc. Más allá de esto, 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.

50. 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.

51. 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 la severidad, de “asignar un número” a las consecuencias de los peligros.

52. El *riesgo de seguridad operacional* se define como *la evaluación, expresada en términos de la probabilidad y la severidad previstas, de las consecuencias de un peligro, tomando como referencia la peor situación previsible.* Normalmente, los riesgos de seguridad operacional se designan mediante una convención alfanumérica que permite su cuantificación. 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 excursión lateral de la pista por pérdida de control de la aeronave durante el despegue o el aterrizaje es una de las *consecuencias* del peligro;

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

53. 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 ponen en peligro el logro del producto del sistema por intermedio 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 los 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 que enfrenta el proveedor de servicios durante la provisión de servicios, y aquéllas para las cuales son viables el control y la mitigación. La gestión de los 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.

54. La Figura 4 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 "cargada" de potencial de consecuencias cuyos riesgos de seguridad operacional son ponderados como de severidad: la mayoría de los riesgos de seguridad operacional de las consecuencias de los peligros se evaluarán como cayendo inicialmente a 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.

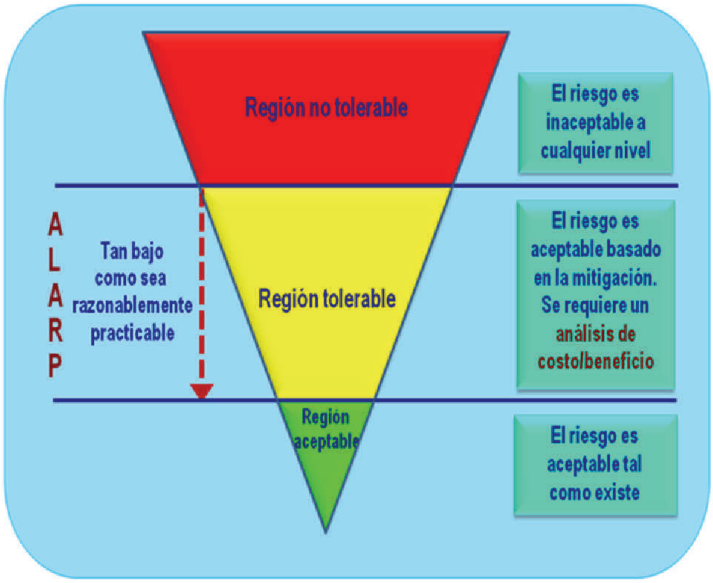

Fig. 4

55. 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 de provocar daño del peligro plantea una amenaza tal a la viabilidad de la entrega de servicios por el proveedor de servicios, que se requieren medidas inmediatas de control o mitigación para la continuación de las operaciones. En términos generales, el proveedor de servicios 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 de daño de las consecuencias de los peligros o su magnitud; o

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

56. 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 de lo previsible, que las consecuencias de los peligros se mantengan bajo el control del proveedor de servicios. Los mismos criterios de control se aplican a las consecuencias cuyos riesgos de seguridad operacional inicialmente corresponden a la región intolerable y se mitigan para llevarlos a la región tolerable. Una consecuencia cuyo riesgo de seguridad operacional se evalúa inicialmente como intolerable, y que se mitiga para ubicarlo en la región tolerable debe permanecer "protegido" mediante estrategias de mitigación que garanticen su control. En ambos casos, hay consideraciones de costo-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 el control del proveedor de servicios?

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

57. El acrónimo ALARP se utiliza para describir una consecuencia cuyo riesgo de seguridad operacional se ha reducido a un nivel tan bajo como es razonablemente práctico. Para determinar lo que es "razonablemente practicable" en el contexto de la gestión de los riesgos de seguridad operacional, deben considerarse tanto la viabilidad técnica de continuar reduciendo el riesgo de seguridad operacional como el costo. Si se llega a la conclusión que el riesgo de seguridad operacional de una consecuencia es "tan bajo como sea razonablemente practicable" (ALARP), ello significa que toda ulterior reducción del riesgo de seguridad operacional es impracticable o está ampliamente superada por el costo. No obstante, debe tenerse en cuenta que cuando un proveedor de servicios "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 proveedor de servicios ha aceptado que dicho riesgo de seguridad operacional residual es suficientemente bajo como para continuar las operaciones.

58. Las consecuencias cuyos riesgos de seguridad operacional han sido evaluados como que corresponden inicialmente a la región aceptable (verde) son aceptables en su estado actual y no requieren medidas para llevar o mantener su probabilidad o su severidad bajo el control del proveedor de servicios.

59. El procedimiento para la cuantificación de los riesgos de seguridad operacional, 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.

60. La probabilidad del riesgo de seguridad operacional se define como la posibilidad que una consecuencia en cuestión pueda ocurrir. Al evaluar la probabilidad de ocurrencia, es esencial referirse a

los datos históricos contenidos en la base de datos de seguridad operacional del proveedor de servicios, a efectos de tomar decisiones "informadas". Se desprende que un proveedor de servicios que no cuente con una base de datos de seguridad operacional sólo puede realizar evaluaciones de probabilidad basadas en la experiencia de su personal, en tendencias globales de la industria y/o, en la menos deseable de las alternativas, en opiniones.

61. Sobre la base de las consideraciones que surjan del análisis de datos históricos u otras fuentes, puede establecerse la probabilidad que ocurra una consecuencia determinada y evaluarse su importancia aplicando una tabla de probabilidad de riesgos de seguridad operacional. En la figura 5 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, 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 la matriz de evaluación de los 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 los diferentes proveedores de servicios. Hay proveedores de servicios 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 son una posible alternativa y se presentan porque tienen una complejidad adecuada a los fines didácticos así como a las necesidades del presente documento.

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**
Extremadamente improbable	Casi inconcebible que el evento ocurra	**1**

Fig. 5

62. Una vez evaluada la probabilidad del riesgo de seguridad operacional asociado a una consecuencia, la segunda etapa de su cuantificación es la de severidad de la consecuencia del peligro si su poten-

cial de provocar daño se materializa durante operaciones dirigidas a la prestación de servicios. Esto se conoce como evaluación de la severidad de los riesgos de seguridad operacional.

63. La severidad de los riesgos de seguridad operacional se define como: los posibles efectos de una consecuencia, tomando como referencia la peor situación previsible. Cabe acotar que se trata de la peor situación previsible pero creíble, es decir, que no se exagera al describir las condiciones extremas anticipadas. 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 6 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, el significado de cada categoría y la asignación de un valor a cada categoría. Al igual que con la tabla de probabilidad de los riesgos de seguridad operacional, esta tabla constituye sólo una posible alternativa y sirve como 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**

Fig. 6

64. 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 de provocar daño de éste se materializa durante las operaciones necesarias para la provisión de los servicios. Esto se conoce como la evaluación de la tolerabilidad de los riesgos de seguridad operacional. Se trata de un procedimiento en dos pasos.

65. 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 7.

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
Extremadamente improbable 1	1A	1B	1C	1D	1E

Fig. 7

66. 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 ya vertido, 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 7 refleja las regiones de tolerabilidad del triángulo invertido anteriormente presentado.

67. 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 7 “inaceptable en las circunstancias actuales”. En este caso, el riesgo de seguridad operacional cae en la región intolerable del triángulo invertido de la Figura 8. 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 o el potencial de provocar daño de las consecuencias de los peligros; o

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

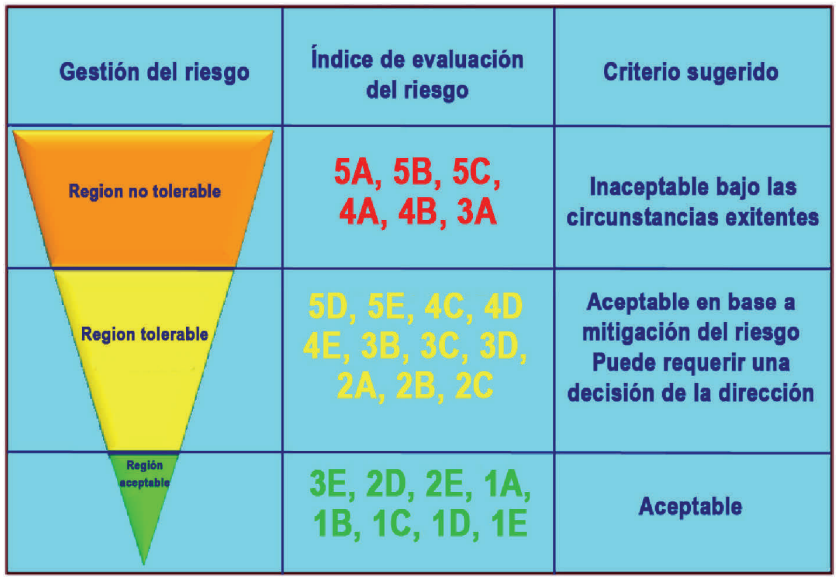

Fig. 8

68. El paso final en la gestión de riesgos de seguridad operacional para poner bajo control del proveedor de servicios los riesgos de seguridad operacional de las consecuencias de los peligros es la puesta en marcha de estrategias de control y/o mitigación. En términos generales, control y mitigación son términos que pueden usarse indistintamente. Ambos tienen por significado el de diseñar medidas para enfrentar el peligro poniendo bajo el control de la organización la probabilidad y/o la severidad de las consecuencias del peligro.

69. Considérese el siguiente ejemplo: un explotador aéreo 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 explotador aéreo a peligros de consecuencias inaceptables.

70. Hay tres estrategias genéricas para el control/mitigación de las consecuencias 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 exposición a las consecuencias, o se adoptan medidas

para reducir la severidad de las mismas, por ejemplo, se limitan las operaciones en el aeródromo, ubicado en una geografía compleja y sin las ayudas a la 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.

71. Cuando se evalúan las opciones específicas de cada una de las 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 la relación entre las diversas 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.

3) mitigaciones de personal: se delega en el personal operativo el control de las consecuencias del peligro, por ejemplo, por intermedio de advertencias, listas de verificación, estandarización de procedimientos operativos o instrucción.

b) *costo-beneficio:* ¿superan los costos 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?

Las mitigaciones de ingeniería y control, se consideran mitigaciones “duras” dado que no asumen desempeño operativo humano impecable. Las mitigaciones de personal son consideradas mitigaciones “blandas”, dado que confían en un desempeño operativo humano impecable.

72. 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 proveedor de servicios está probablemente delegando en el personal operativo y en otros subordinados la responsabilidad de la gestión de los riesgos de seguridad operacional.

73. 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

74. Como parte del control/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 ser usadas en condiciones operativas reales?
d) ¿son necesarias medidas adicionales de mitigación/control de las consecuencias de los peligros?

75. 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 riesgo de seguridad operacional de una línea aérea que opera aeronaves grandes (según RAAC Parte 121), mientras que el apéndice 2 contiene un ejemplo similar para un explotador aéreo de aeronaves pequeñas (según RAAC Parte 135).

ESTA PÁGINA FUE DEJADA INTENCIONALMENTE EN BLANCO

Apéndice I al Capítulo II

Gestión de riesgos de seguridad operacional – Explotador aéreo según RAAC Parte 121

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

Situación operativa

Un explotador aéreo que utiliza aeronaves de gran porte para la provisión de sus servicios recibe la notificación del explotador del aeropuerto en donde tiene instalada su base principal (el cual tiene dos pistas paralelas, una principal y una 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 explotador del aeropuerto ha decidido trabajar por la noche, cuando el volumen de tránsito es menor, para evitar disrupciones de cuantía en las operaciones diurnas. El análisis del plan de construcción propuesto por el explotador 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 en pista.

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

Descripción del sistema

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

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

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

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

Identificación de peligros

Peligro genérico – Obras de construcción en el aeropuerto.

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

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

a) Los vehículos de construcción pueden desviarse de los procedimientos prescriptos y cruzar la pista principal sin escolta;
b) Puede haber conflicto entre aeronaves y vehículos que crucen la pista principal.

Nota: *Del análisis del sistema surgirá más de un peligro, y cada peligro puede tener asociada más de una consecuencia.*

Evaluación de riesgos de seguridad operacional

La evaluación del explotador aéreo 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 explotador aéreo evalúa que, en caso de ocurrir dicho conflicto, la consecuencia podría ser de severidad *catastrófica*.

El explotador aéreo evalúa las defensas (medidas de control/mitigación) propuestas por el explotador 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.

Control / mitigación de los riesgos de seguridad operacional

El explotador aéreo decide que es necesario proponer al explotador 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 explotador aéreo 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 continuaría siendo 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 explotador aéreo el uso del camino perimetral no elimina enteramente el peligro (los vehículos de construcción todavía pueden atravesar la pista principal debido a varias circunstancias), no obstante reduce la probabilidad de que se manifiesten 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 practicable (ALARP).

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 explotador aéreo 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.

Registro de identificación de 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:* ***Aceptable (extremadamente improbable)***

Apéndice II al Capítulo II

Gestión de riesgos de seguridad operacional – Explotador aéreo según RAAC Parte 135

Caso de estudio – Iniciación de operaciones en pistas de pedregullo

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

Un explotador aéreo que opera según las reglas de la Parte 135 de las RAAC va a iniciar sus operaciones en pistas de pedregullo con aeronaves BAe Jestream 31. Por ello, debe desarrollar e implementar las medidas necesarias para permitir las operaciones con tales aeronaves en tales pistas. Completadas las averiguaciones y acciones del caso, dando curso a esta necesidad, se llega a una propuesta, que es aprobada. Se enmienda el Manual de Operaciones de la empresa (MOE) y el Manual General de Mantenimiento (MGM) para reflejar la propuesta, y se remiten para su impresión, que llevará tres semanas. El cambio del Manual de Instrucción para incorporar la enmienda sobre operación en pistas de pedregullo es aprobada por la Autoridad de Aviación Civil, y hasta tanto los procedimientos estandarizados de operación (SOPs) para tal operación sean incorporados a la enmienda del Manual de Operaciones, se publica un Memorando Provisorio de Operaciones de inmediata aplicación firmado por el Gerente de Operaciones. Se completa el entrenamiento teórico terrestre, y se archiva el registro de la instrucción.

El siguiente personal integró el equipo de análisis:

- Oficial de Seguridad Operacional
- Supervisor de la flota BA31
- Comandante de BA31
- Supervisor de mantenimiento de la flota BA31
- Encargado de instrucción
- Representante de la Gerencia Comercial
- Primer Oficial de BA31
- Ex Comandante de BA31 (2000 hrs. de experiencia en operaciones en pista de pedregullo en BA31)

Planificación y operación

Se compiló un listado de las pistas de pedregullo utilizables, para la evaluación y aprobación de las operaciones en las mismas. Inicialmente la operación comenzará con pistas de pedregullo compactadas de 5000 pies de longitud. El tiempo de servicio de las tripulaciones se iniciará con una presentación de dos (2) horas de anticipación antes de la salida para prever la planificación adecuada de la operación y el

briefing de la tripulación. Deberá ponerse una escoba en las aeronaves durante todo el año a fin de limpiar el área debajo de las hélices previo a la puesta en marcha.

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

Instrucción

La instrucción/adoctrinamiento inicial en vuelo será realizada por dos comandantes supervisados por un comandante con gran experiencia en pistas de pedregullo. El Oficial de Seguridad Operacional los acompañará durante el primer vuelo. No se programarán copilotos hasta que los dos comandantes hayan acumulado 10 despegues y aterrizajes cada uno en pistas de pedregullo. A menos que se combine la instrucción inicial en vuelo con los vuelos arrendados, esto significará aproximadamente 7 horas de vuelo. El encargado de instrucción coordinará la instrucción con el representante de la Gerencia Comercial antes del comienzo de la operación en pista de pedregullo.

Mantenimiento

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

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

Documentación

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

Mitigación del riesgo

Ver la matriz adjunta (tabla de la siguiente página)

Responsabilidades por la gestión de la seguridad operacional

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

Registro de identificación del peligro y gestión del riesgo de seguridad (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 e índice del riesgo de seguridad resultante
1	Operaciones de vuelo	Operación en pista de pedregullo	Largo de pista	Excursión de pista	• Pista mínima 5000 pies • Calificación especial de aeródromo para las tripulaciones • Instrucción teórica y de vuelo • Enmienda al Manual de Operaciones • Establecimiento de una lista de pistas con pedregullo autorizadas para su operación • Revisión del tiempo de servicio de las tripulaciones por una presentación anticipada de dos (2) horas antes de la salida del vuelo • Toda nueva operación en pistas con pedregullo no listadas requerirá una evaluación de riesgo de seguridad operacional *Índice de riesgo de seguridad:* ***2A*** *Tolerabilidad del riesgo de seguridad:* ***Tolerable en base a la mitigación***
2	Operaciones de vuelo	Operación de pista de pedregullo	Condición de la pista	• Daño a la luz anti-colisión inferior • Daño a cubiertas • Daño a los flaps • Daño a las palas de las hélices • Daño a los amortiguadores de tren de aterrizaje • Daño a las botas deshieladoras	• Remover luz anti-colisión inferior • Cubierta de tren de aterrizaje extra en el alojamiento inferior • Protector de flaps aplicado antes de cada operación • Instalar palas Mk. II • Servicio a los amortiguadores luego de cada operación • Inspección del borde de ataque y de las botas deshieladoras luego de cada operación *Índice de riesgo de seguridad:* ***2A*** *Tolerabilidad del riesgo de seguridad:* ***Tolerable en base a la mitigación***

ESTA PÁGINA FUE DEJADA INTENCIONALMENTE EN BLANCO

Capítulo III

Garantía de la Seguridad Operacional

Capítulo III

Garantía de la Seguridad Operacional

Introducción

1. El Capítulo I de este documento presenta una exposición conceptual sobre los dos procesos básicos del SMS, de los cuales se derivan las actividades de control o mitigación de las deficiencias de seguridad y peligros en el contexto operativo. Estos son la gestión de riesgo de seguridad operacional, y la garantía de la seguridad operacional. El Capítulo II de este documento se concentra sobre el primero de los dos procesos (la gestión de riesgo de seguridad operacional). Este Capítulo presenta el segundo proceso: la garantía de la seguridad operacional.

2. El Capítulo II 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 la gestión de riesgos de seguridad operacional, si bien no en el sentido estricto del proceso propuesto por el SMS, pero si 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, la principal aún hoy en día, si se toma en cuenta a la industria a nivel mundial. Las recomendaciones sobre 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. Tan largo historial no existe en lo relativo a la garantía de la seguridad operacional. Probablemente debido a la fuerte convicción en cuanto a que el proceso de la investigación de accidentes e incidentes – eventos de significación pero infrecuentes y – era el mecanismo primario de la garantía de la seguridad operacional, llevó a que la tasa de accidentes haya sido el parámetro de garantía de la seguridad operacional, favorecido esto por la industria, a expensas de otros parámetros de menor significación, pero de mayor frecuencia y abundancia estadística. Dicho de otra manera, en la medida en que no se experimente un accidente o incidente, la presunción es que las medidas de mitigación contra las consecuencias de los peligros funcionan al nivel esperado, es decir, que hay garantía de la seguridad operacional. En función de lo antedicho, la bibliografía sobre garantía de la seguridad operacional no es tan copiosa como lo es la bibliografía sobre gestión de riesgos de seguridad operacional. No es impropio sugerir, parafraseando una canción popular, que en lo que a garantía de la seguridad operacional (desde un punto de vista contemporáneo) se refiere, no hay un claro camino, y se está haciendo camino al andar.

La relación SRM/SA

4. La función de gestión de los riesgos de seguridad operacional de un SMS, como lo ilustra la figura 9, está esencialmente asociada a la planificación de las operaciones. Se describe el sistema, es decir, se identifican los componentes y condiciones del contexto operativo en el cual tendrán lugar las operaciones necesarias para la provisión de servicios con vista al logro del producto y las interacciones previstas entre tales componentes y las condiciones; posteriormente se identifican los peligros y se realiza la evaluación de los riesgos de seguridad operacional asociados a las consecuencias que surjan de dichos peligros, en base a las interacciones previstas entre los componentes y las condiciones; y se implementan mitigaciones contra las consecuencias. En este punto, se inician las operaciones cotidianas bajo el supuesto que las mitigaciones en vigor son garantía suficiente de seguridad en la operación.

5. Bajo la visión tradicional de garantía de la seguridad operacional basada en el accidente/incidente como parámetro, los supuestos de planificación no sufrían modificación alguna, vale decir, no había modificaciones en las mitigaciones, excepto que se experimentase un accidente o incidente. La columna de la derecha de la figura 9 no existía, en la realidad.

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

7. La gestión de riesgos de seguridad operacional, entonces, permite al proveedor de servicios la evaluación de los riesgos de seguridad operacional en las operaciones que apoyan la prestación de sus servicios, y apoya las decisiones de seguridad operacional para la puesta en marcha de controles y mitigaciones para mantener las consecuencias de los peligros a un nivel ALARP). Por su parte, la Garantía de seguridad operacional se concentra en actividades que permiten que el proveedor de servicios se demuestre a sí mismo y a terceros con los que tiene relación durante las operaciones necesarias para la provisión de sus servicios, que dichos controles y mitigaciones funcionan satisfactoriamente; mediante la recolección y el análisis de pruebas objetivas

8. Por consiguiente, bajo el entorno SMS, la gestión de riesgos de seguridad operacional (SRM) debe ser considerada como un proceso inicial, de diseño y planificación, mientras que la garantía de la seguridad operacional es un proceso continuo, de vigilancia y control, que nunca se detiene mientras duren las operaciones. La sección final de este Capítulo ofrece un ejemplo que permite visuali-

zar a través de un simple escenario la interacción SRM/SA bajo el entorno SMS.

9. 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 II, la exposición sobre garantía de la 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 un apéndice, que expone la perspectiva de la OACI para la medición de la performance de seguridad operacional.

10. Según la exposición del Capítulo I, la garantía de la 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 control y mitigación de las consecuencias de peligros que ponen en riesgo la capacidad de un sistema de lograr su producto mediante la entrega de servicios. La simple presentación gráfica de la figura 9, apoyada por texto explicativo, sirve para ilustrar la diferencia entre la visión tradicional de la garantía de la seguridad operacional basada en el accidente/incidente como parámetro, y la visión de garantía de la seguridad operacional bajo el entorno del SMS. Asimismo esto es necesario porque las sutilezas en las diferencias en la relación entre la gestión de riesgos de seguridad operacional (safety risk management, SRM) y la garantía de la seguridad operacional (safety assurance, SA) son a menudo fuente de confusión.

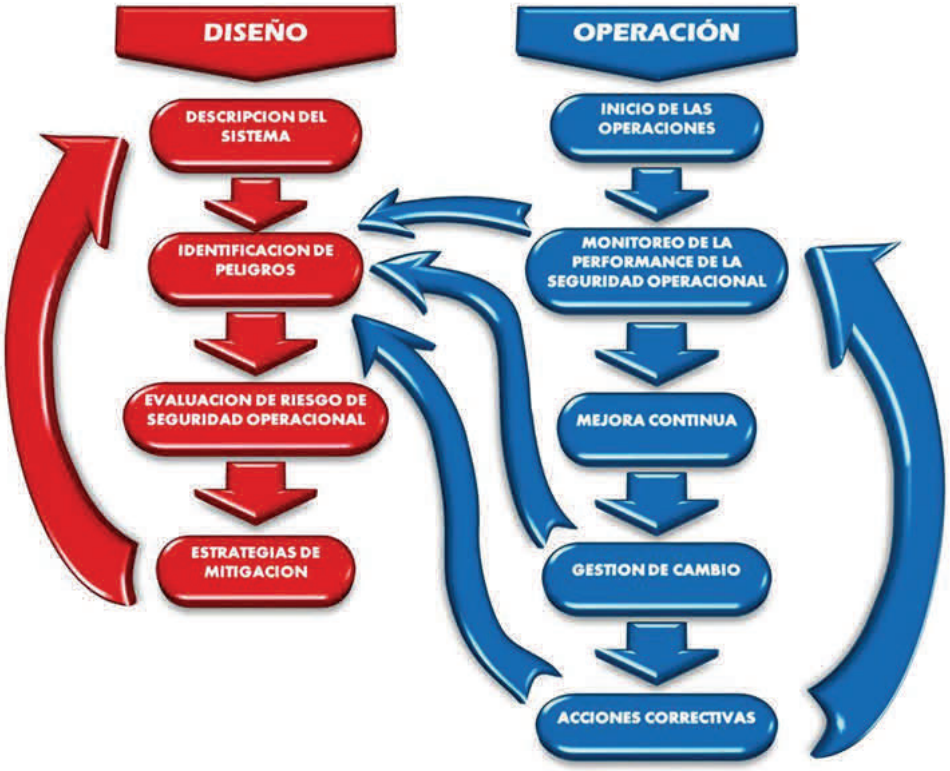

Fig. 9

SA – Puesta en marcha

Inicio de las operaciones

11. No se considera necesario abundar sobre este aspecto, dado que es obvio. Iniciadas las operaciones, la garantía de la seguridad operacional en el SMS funciona en forma similar a la garantía de la calidad en el QMS (Quality Management Systems). Las actividades de garantía de la 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, y a la identificación de defectos; los requisitos de SMS son requisitos de seguridad operacional y están orientados a la satisfacción de la misma, y a la identificación de deficiencias de seguridad operacional y peligros en el contexto operativo.

Monitoreo de la performance de seguridad operacional

12. Garantía puede definirse, de la forma más sencilla, como “algo que da confianza”. Una vez que los controles y 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 han sido instalados y puestos en marcha, es responsabilidad del proveedor de servicios asegurar que continúan instalados y que funcionan según lo previsto. En el marco de la sencilla definición anterior de “garantía”, esto consiste en que el proveedor de servicios debe llevar a cabo actividades para brindar confianza sobre la eficacia y efectividad de los controles y mitigaciones. El proveedor de servicios debe supervisar de manera continua y rutinaria sus operaciones para identificar:

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

b) El eventual deterioro en los procedimientos operacionales, las instalaciones, las condiciones del equipo o el desempeño humano, que pudieran reducir la efectividad de los controles y mitigaciones contra consecuencias de peligros en vigencia.

13. Cualquiera de las dos condiciones enumeradas en el párrafo inmediato anterior indicaría la necesidad de lanzar un nuevo ejercicio de gestión de riesgos de seguridad operacional para examinar y, si es necesario, modificar los controles y mitigaciones existentes o poner en marcha nuevos controles y/o mitigaciones. El análisis y la evaluación permanentes de estos controles y mitigaciones son actividades que son parte tanto del monitoreo de la performance de seguridad operacional y de la mejora continua del SMS. Estas actividades deben continuar durante la operación cotidiana del sistema y, en lo que a la mejora continua del SMS se refiere, son actividades análogas a las de garantía de la calidad con requisitos relativos al análisis, auditoría, verificación, y documentación por el proveedor de servicios de la efectividad de las estructuras del SMS. Las actividades de la garantía de la seguridad operacional deben también incluir procedimientos que aseguren la puesta en marcha de

medidas correctivas en respuesta a conclusiones surgidas del análisis de datos, reportajes, encuestas y auditorías, como parte del monitoreo de la performance de seguridad operacional.

14. La tarea principal del monitoreo de la performance de seguridad operacional es el control. A continuación se presenta una lista de aspectos o áreas genéricos que han de considerarse para lograr tal control, para "asegurar la seguridad operacional", mediante el monitoreo de la performance de seguridad operacional:

a) *responsabilidad:* quién es responsable de la gestión de las actividades de garantía 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 proveedor de servicios, que incluyen 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 las líneas de comunicación entre el personal operativo. Hay coherencia de procedimientos y clara delineación de responsabilidades entre departamentos, sectores y personal operativo; y

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

15. El monitoreo de performance de la seguridad operacional se basa fundamentalmente en la adquisición de datos de naturaleza operativa, a través de cuyo análisis el proveedor de servicios puede medir la eficiencia de las mitigaciones de control de las consecuencias de los peligros e identificar peligros adicionales durante la provisión de servicios, y determinar de tal manera la performance de seguridad operacional de su sistema.

16. Los datos para alimentar el monitoreo de la performance de seguridad operacional proceden de varias fuentes, que en términos generales incluyen aportes del personal operativo a través de los programas de reportaje de seguridad operacional; 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 al personal; e investigaciones internas de seguridad operacional. Cada una de estas fuentes de datos existe en alguna medida en todos los proveedores de servicios. Por ello, la exposición con respecto a qué es lo que cada fuente debería adoptar corresponde a un nivel operacional, dejando a cada proveedor de servicios que las adapte al ámbito y escala adecuados al tamaño y tipo de organización.

Programas de reportaje de seguridad operacional.

17. Los reportajes de seguridad operacional son elementos esenciales para el monitoreo de la performance de seguridad operacional así como para la garantía de la 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 referirse al "manual". El Capítulo II 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 en muchos casos sus consecuencias, que en muchos casos, a su vez, no han sido formalmente gestionados. Por ende, la exposición en el Capítulo II sobre identificación de peligros concluye con un claro corolario sobre la importancia primordial de los programas de reportaje de seguridad operacional como elemento fundamental para la captación de la deriva práctica y la implementación y efectivo mantenimiento del SMS por un proveedor de servicios.

18. Hay tres tipos de programas de reportaje de seguridad operacional: programas de reportajes obligatorio, programas de reportajes voluntario; y programas de reportajes confidencial. Una breve descripción de cada uno se expone a continuación:

a) En los *programas de reportaje obligatorios*, el personal operativo debe notificar ciertos tipos de sucesos que están claramente especificados en las regulaciones nacionales e internacionales, que a su vez han sido traspuestas a normas nacionales. Esto exige directivas detalladas que establezcan quienes deberán notificar, qué deberá notificarse y como deberá hacerse. Los programas de reportaje obligatorios informan sobre eventos de cierta gravedad, aunque no necesariamente catastróficos, y por sus orígenes y naturaleza recogen primariamente información sobre fallas técnicas.

b) En los *programas de reportaje voluntarios*, el personal operativo, sin ninguna obligación normativa, presenta información voluntariamente sobre sucesos operativos que han experimentado o presenciado. En estos sistemas, el proveedor de servicios (o el Estado, según sea el caso) incentiva el reportaje de sucesos, ofreciendo una medida de protección a quienes reportan de la aplicación de medidas disciplinarias, siempre y cuando no haya negligencia ni intención aviesa. La información notificada no se usa contra quienes informan, es decir, que estos programas brindan protección a las fuentes de información para fomentar el reporte de dicha información. Debido a esto, los programas de reportes voluntarios generan información sobre eventos de baja o escasa gravedad (aunque con significativo potencial de daño) y recogen primariamente información sobre deficiencias de seguridad operacional, peligros, procedimientos y desempeño humano operativo.

c) Los *programas de reportaje confidenciales* son una variación de los programas de reportaje voluntarios, en cuanto a que además de proteger hasta cierta medida a quienes informan contra posibles medidas disciplinarias, se protege la identidad de los mismos. Esta es una forma cabal de asegurar que la información proporcionada no se utiliza contra quien informa.

La confidencialidad (no el *anonimato*) se logra normalmente restringiendo la identificación de quien informa, y cualquier otra información que permitiera dar a conocer la identificación del mismo, quedando disponible dicha información solamente para los “guardianes” designados por común acuerdo entre las partes involucradas, quienes serán los encargados de hacer el seguimiento o complementar con información extra, si fuese necesario, en los sucesos notificados. Debido a esto, los programas de reportaje generan información de más considerable detalle sobre deficiencias de seguridad operacional, peligros, procedimientos y desempeño humano operativo que los programas de reportes voluntarios.

Observación directa de las operaciones cotidianas.

19. Estos programas captan el funcionamiento de las operaciones en tiempo real, y se fundamentan sobre la misma justificación que los programas de reportaje de seguridad operacional: 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 para identificar peligros no previstos. Se trata de captar la operación tal como realmente tiene lugar, y no como debería ser según lo especificado, como para analizar las diferencias entre “el ser y el deber ser” y realimentar los controles y las 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:* estos son sistemas 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 respecto de los parámetros operacionales establecidos y el funcionamiento de los sistemas de las aeronaves. Un uso típico del análisis de datos de vuelo es el monitoreo de aproximaciones estabilizadas. Es importante tener en cuenta que los sistemas de análisis de datos de vuelo sólo proporcionan parámetros, es decir, datos en el más estricto sentido de la palabra. Por lo tanto, estos sistemas informan *qué* pasó, pero no *porqué*. El establecimiento por parte del proveedor de servicios de un programa de análisis de datos de vuelo es una es un requerimiento regulatorio para los explotadores aéreos (RAAC Parte 121, secc. 121.14) y, por lo tanto, de cumplimiento obligatorio.

b) *Programas de observación directa:* estos programas capturan aspectos específicos del contexto operativo, incluyendo el desempeño real de los controles y mitigaciones establecidos así como el del personal operativo, también en tiempo real. Esto se logra a través de la observación directa de las operaciones por observadores humanos, que han sido rigurosamente entrenados y respetan un estricto protocolo de observación. En virtud de ello, estos sistemas no solamente generan datos sino también información sobre el contexto en el cual los datos se originan, informando por lo tanto no solamente *qué* pasó, sino también *porqué*. Debido a ello, los programas de observación directa son el complemento ideal de los programas de análisis de datos de vuelo. El único programa de este tipo existente para proveedores de servicios a la fecha 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).

Auditorías formales.

20. La contribución de las auditorías al monitoreo de la performance de seguridad operacional se concentra en velar por la integridad de los elementos constitutivos del SMS del proveedor de servicios y en la evaluación periódica de la efectividad de los controles y las mitigaciones sobre las consecuencias de los peligros. Mientras que los programas descriptos en el párrafo anterior son de operación continua, las auditorías se llevan a cabo a intervalos puntuales. Bajo la perspectiva del monitoreo de la performance de seguridad operacional, la real contribución 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 garantía de la 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 e instrucción, niveles de competencia e instrucción para operar equipos e instalaciones y mantener niveles requeridos de desempeño, etc. Si bien las auditorías son “externas” a las dependencias involucradas en las actividades directamente relacionadas con la provisión de servicios, aún son “internas” al proveedor de servicios en su totalidad.

Encuestas al personal sobre seguridad operacional.

21. 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 sistemas de monitoreo de la performance de seguridad no proporcionan una respuesta. La encuesta de seguridad consiste simplemente en solicitar la opinión del personal operativo directamente involucrado en la operación en cuestión, sus percepciones y las áreas de disenso o confusión. Las encuestas de seguridad pueden apoyarse en el uso de listas de verificación (tildar casilleros), cuestionarios y/o entrevistas confidenciales informales. Dado que la información de las encuestas es subjetiva, es necesaria una depuración antes de poner en marcha las medidas correctivas. Las encuestas de seguridad al personal son una fuente de importante información de seguridad operacional, y de bajo coste.

Investigaciones internas de seguridad.

22. Incluyen sucesos que no requieren ser investigados o notificados al Estado, por ejemplo, turbulencia en vuelo, fallas repetitivas de componentes o materiales, eventos de vehículos en la rampa, etc.

Gestión del cambio

23. Si hay una constante a la que está expuesto un proveedor de servicios en el momento actual de la

aviación comercial, tal constante es el cambio. Los proveedores de servicios experimentan cambios permanentes debido a expansión, contracción, cambios a 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 proveedor de servicios, 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 control o mitigación a las consecuencias de los peligros existentes, o afectar la eficacia de esas estrategias. Los cambios pueden ser externos al proveedor de servicios 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, para citar unos pocos. Ejemplos de cambios internos serían cambios de administración, introducción de nuevas operaciones, cambios de equipamiento o procedimientos, etc. Es función de la garantía de la seguridad operacional, por intermedio 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 controles y mitigaciones contra las consecuencias de tales peligros.

24. En el Capítulo IV de este documento se analiza la importancia de describir el sistema (descripción del sistema) como una de las actividades preliminares fundamentales en la planificación de un SMS. Dentro del contexto de la gestión del cambio, el objetivo de la descripción del sistema es establecer un análisis inicial de peligros de referencia para el futuro 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 reexaminarse 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 proveedor de servicios debería examinar el contexto operativo anticipado y el contexto real, para asegurar que continúa existiendo un panorama claro de las circunstancias bajos las cuales tiene lugar la prestación de servicios.

25. Por consiguiente, como parte de la garantía de seguridad de SMS, el proveedor de servicios debería establecer un procedimiento formal de gestión del cambio para identificar los posibles peligros que surjan debido a los cambios a implementar en la organización y que puedan afectar los procedimientos y servicios establecidos. Antes de implantar cambios, el procedimiento de gestión del cambio debería asegurar la puesta en marcha de controles o mitigaciones para asegurar la performance de seguridad operacional luego de los cambios, al efecto de mantener bajo control las consecuencias de los nuevos peligros que podrían haber sido introducidos por el cambio durante el suministro de servicios.

26. Al establecer un procedimiento formal para la gestión del cambio, el proveedor de servicios 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: *"¿qué tan importante es 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 mantenimiento mayor en un proveedor de servicios 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 proveedor de servicios, éste debe adoptar medidas para responder a ellos. Los cambios frecuentes en las operaciones, el entorno empresarial o físico hacen que el proveedor de servicios 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, luego de cambios en las operaciones. Es aquí donde entra en juego el carácter de círculo cerrado de la garantía de la seguridad operacional. El empleo de análisis de tendencias en el proceso de garantía de la seguridad operacional para hacer el seguimiento en el tiempo de las medidas de monitoreo de performance 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.

Mejora continua del SMS

27. Para ser exitoso, el SMS no puede ser estático. El hecho que los componentes y elementos del SMS estén implementados no significa necesariamente que el SMS está "completo". La provisión de servicios no es una actividad estática: el personal, el equipamiento, las rutas, las pistas y el entorno operativo cambian periódicamente. En la medida en se producen cambios en la provisión de servicios, la organización del proveedor de servicios cambia, y también deben cambiar y adaptarse las estructuras del SMS, que debe evolucionar haciendo uso de los resultados de la retroalimentación. Tal evolución es el objetivo de la mejora continua del SMS, que como parte de la garantía de seguridad operacional asegura el control de la eficiencia del sistema de gestión de la seguridad operacional, mediante una verificación y un mejoramiento constantes de los componentes del sistema operacional. La mejora continua del SMS aplica herramientas básicas de la gestión de calidad: evaluaciones internas y auditorías independientes (tanto internas como externas), que incluyen estrictos controles de los documentos y supervisión continuada de los recursos asignados para los controles de seguridad operacional y medidas de mitigación.

28. Las evaluaciones internas consisten en el análisis de las estructuras específicas del SMS. Las evaluaciones deben ser efectuadas por personas departamentos que sean funcionalmente independientes del proceso técnico que se evalúa (un departamento especializado según lo decida la administración superior). La función de evaluación interna también abarca la auditoría de las actividades propias de la gestión de la seguridad operacional, incluyendo la adopción de directivas, las actividades de gestión de riesgos de seguridad operacional, de garantía de seguridad operacional y de la promoción de la seguridad operacional, en lo que a la integridad de actividades y la apropiada asignación de recursos técnicos y humanos necesarios para lograr la eficacia de actividades se refiere.

29. Las auditorías permiten a los gerentes que poseen responsabilidades asignadas respecto del SMS hacer un relevamiento de las actividades del propio SMS.

30. Las auditorías internas son una herramienta importante para los administradores a fin de obtener información con la cual adoptar decisiones y mantener en marcha las actividades operacionales. La responsabilidad principal de la gestión de la seguridad operacional corresponde a aquellos a quienes "pertenecen" las actividades técnicas de la organización en apoyo de la prestación de servicios. Es aquí donde los peligros se encuentran con mayor frecuencia, así como donde las deficiencias de las actividades contribuyen a la posibilidad que los peligros desaten sus potenciales consecuencias y donde el control de supervisión directo y la asignación de recursos pueden mitigar los riesgos de seguridad operacional de las consecuencias de los peligros a un nivel ALARP. Las auditorías internas son una herramienta esencial para la garantía de la seguridad operacional, que ayuda a los gerentes a cargo de las actividades que apoyan la prestación de servicios a controlar que, una vez implantado los controles de las posibles consecuencias de los peligros, los recursos necesarios para que continúen funcionando y sean efectivos en el mantenimiento de la seguridad operacional.

31. Las auditorías externas del SMS, que persiguen los mismos fines que las internas, pueden ser efectuadas por la ANAC, socios de acuerdos de código compartido, clientes u otros terceros seleccionados por el proveedor de servicios. Estas auditorías no sólo proporcionan una sólida interfaz con el sistema de inspección sino también constituyen un sistema de garantía secundario.

32. Como conclusión, la mejora continua puede ocurrir solamente cuando la organización desarrolla una vigilancia constante respecto de la efectividad de los recursos asignados para el logro de sus operaciones técnicas y sus medidas correctivas para restaurar tal integridad, cuando corresponda. Sin una supervisión continua de los recursos necesarios para apoyar los controles de seguridad operacional y medidas de mitigación de deficiencias y peligros, no hay forma de medir si el SMS está cumpliendo su finalidad con eficiencia.

Las acciones correctivas generadas por la SA: corregir la "deriva práctica"

33. Como cierre del círculo de garantía de la seguridad operacional, el proveedor de servicios debe tomar acción correctiva para rectificar cualquier desfasaje entre el funcionamiento teóricamente previsto de los controles o mitigaciones sobre las consecuencias de los peligros ya existentes, o bien de nuevos peligros introducidos por situaciones de cambio para controlar o eliminar sus causas de manera de evitar, de ser posible, que situaciones similares vuelvan darse en el futuro.

34. Las medidas de acción correctiva como consecuencia de actividades de garantía de la seguridad operacional serán similares a las medidas adoptadas como consecuencia de la gestión de riesgos de seguridad operacional (expuestas en el Capítulo II bajo el titulo 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. La diferencia básica es que la gestión de riesgo de seguridad 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, luego del inicio de las operaciones. La garantía de la seguridad operacional, en cambio, es una actividad de ejecución, y tiene lugar en el presente. Por lo tanto, corrige desfasajes entre el funcionamiento previsto de las operaciones y el real (o sea, la "deriva práctica" que se expuso en el Capitulo 2) 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 peligros que son producto de cambios en las operaciones con respecto a la planificación inicial.

SRM y SA – Un ejemplo conjunto

35. Como cierre ilustrativo de los pasos conjuntos a observar en la gestión de riesgo de seguridad operacional (SRM) y la garantía de la seguridad operacional (SA) según lo expuesto en los Capítulos II y III, se presenta un simple ejemplo que se refiere a la operación de aeronaves de acuerdo con su Lista de Equipamiento Mínimo (Minimum Equipment List, MEL). El explotador aéreo en cuestión está

por iniciar una nueva operación (contrato para traslado de personal de una mina en vuelos VFR), 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 dotadas las aeronaves del explotador aéreo que serán afectadas a la nueva operación, ya que tiene un historial de fallas 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 explotador aéreo debería observar los siguientes pasos.

Planificación – SRM

36. Descripción del sistema. En este paso, se debe analizar el tipo de operación, el personal que la ejecutará, el contexto operativo, y las mitigaciones o controles de riesgos de seguridad operacional ya existentes, bajo la forma de normas, estándares y procedimientos.

37. Se trata de un explotador aéreo que conduce sus actividades bajo la Parte 135, y opera aeronaves bimotores con menos de diez asientos de pasajeros, en operaciones no regulares de transporte de pasajeros. El explotador aéreo dispone de una Lista Maestra de Equipamiento Mínimo (Master Minimum Equipment List, MMEL) para ese tipo de aeronave, que debe transformar en una MEL propia para la nueva operación a iniciarse (el traslado de personal de una mina en vuelos VFR). Todas las aeronaves del explotador están equipadas, y sus pilotos entrenados y habilitados, para operaciones con un solo piloto, por lo que el Proveedor de Servicios desea operar con un solo piloto aún en el caso que el piloto automático este inoperativo.

38. Identificación de peligros y sus consecuencias. En este paso, se individualizan los peligros que son inherentes a operaciones con un solo piloto y con el piloto automático inoperativo, y sus posibles consecuencias. Siendo el peligro genérico “operación con un solo piloto con piloto automático inoperativo”, un componente o peligro específico del mismo es la “sobrecarga de trabajo para el piloto durante estas operaciones”, lo que puede llevar a eventos operativos de significación. Las consecuencias posibles de este peligro, bajo la normativa existente, están en principio mitigadas 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, los riesgos de seguridad operacional que generan, y las mitigaciones que puedan existir. Ejemplos de posibles consecuencias incluyen la ejecución 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 “sobrecarga de trabajo para el piloto en condiciones de vuelo reales”: accidentes de vuelo controlado en el terreno (CFIT) o pérdida de control en vuelo.

39. Evaluación de riesgos de seguridad operacional. En este paso, se evalúa y cuantifica la significación de cada una de las consecuencias de los peligros identificados. Respetando las pautas del ejemplo, el explotador aéreo considera que las dos consecuencias operativas del peligro específico

"sobrecarga de trabajo para el piloto en condiciones de vuelo reales" (accidentes de vuelo controlado en el terreno (CFIT) o pérdida de control en vuelo), si bien de remota posibilidad, son de la máxima severidad, ambas potencialmente catastróficas. Utilizando la matriz de riesgos de seguridad operacional de su SMS, el Proveedor de Servicios evalúa el riesgo de seguridad operacional como remoto (3) pero catastrófico (A). La combinación 3A es inaceptable bajo las circunstancias existentes. Por lo tanto, es necesario introducir modificaciones en el MMEL para la operación MEL por el explotador con un solo piloto y piloto automático inoperativo en condiciones visuales según las necesidades de la operación bajo consideración, para determinar si es posible reducir el riesgo de seguridad operacional de las consecuencias a un nivel ALARP.

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

a) el piloto automático debe ser desactivado y retirado de la aeronave por personal de mantenimiento debidamente calificado;

b) los pilotos deben ser notificados que el piloto automático se encuentra inoperativo por medio del libro de novedades técnicas de la aeronave así como por un cartel en el cockpit; y

c) no se puede operar sin piloto automático por más de 10 (diez) días.

41. La reevaluación del explotador 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 explotador 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:

a) el piloto automático debe ser desactivado y retirado de la aeronave por personal de mantenimiento debidamente calificado;

b) los pilotos deben ser notificados que el piloto automático se encuentra inoperativo por medio del libro de novedades técnicas de la aeronave así como por un cartel en el cockpit;

c) no se puede operar sin piloto automático por más de 10 (diez) días; y

d) debe programarse, durante el entrenamiento periódico en simulador, una capacitación específica para los pilotos (maniobras con un solo piloto y diversas fallas en el piloto automático) que los prepare para completar exitosamente su vuelo con la falla del piloto automático.

e) debe programarse una capacitación específica y el suministro de una checklist para los pilotos que los prepare para continuar siempre el vuelo VFR hasta el aeropuerto de alternativa más cercano.

42. De la nueva cuantificación del riesgo de seguridad operacional surge que, si bien la severidad continua siempre la máxima (A), las nuevas medidas de mitigación reajustan la probabilidad que las consecuencias CFIT o pérdida de control en vuelo a "improbable" (2), lo que permite evaluar el riesgo de seguridad operacional como 2A. Por lo tanto, la operación es aceptable en tanto y en cuanto las mitigaciones se mantengan en pie. 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 reevaluada.

Operación – SA

43. Inicio de las operaciones. En este paso, se comienza la operación, y el explotador debe determinar las áreas de su sistema sobre las cuales deberá prestar particular atención en su monitoreo de las operaciones, para verificar que las estrategias de mitigación funcionan de acuerdo con lo esperado. Tales áreas incluyen:

a) *Operaciones e instrucción*. Debe verificarse la disponibilidad en tiempo 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.

b) *Despacho*. Los despachantes debe estar al tanto de los requerimientos MEL para el despacho con piloto automático inoperativo, incluyendo la limitación de los 10 días.

c) *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.

44. Monitoreo de la performance de seguridad. En este paso, el libro de de novedades técnicas de las aeronaves será una de las principales fuentes de datos para el monitoreo de la performance 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 notificación de sucesos del explotador, para constatar el estado de situación real de las mitigaciones.

45. Cambios en la operación. En este paso, a través del programa de notificación de sucesos, el explotador toma conocimiento que el retiro de los componentes electrónicos del piloto automático para su reparación genera frecuentemente fallas 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 explotador han detectado así una degradación en la eficacia de las mitigaciones propuestas que de otra manera muy probablemente hubiera sido detectada luego de un evento de significación, por ejemplo, un incidente.

46. Acción correctiva. En este paso, sobre la base de los reportes, 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 las fallas intermitentes del sistema compás número 1.

47. 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 intermedio de sus dos procesos básicos (SRM y SA), y ofrece al Proveedor de Servicios 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.

Apéndice I al Capítulo III

Medición de la performance de seguridad operacional de SMS

Material de orientación de la OACI

La información contenida en este Apéndice consiste en extractos del *Manual de gestión de la seguridad operacional* (Doc 9859).

En todo sistema de gestión, es necesario definir un conjunto de parámetros de performance operacional y su cuantificación, como elementos que permitan determinar si el sistema funciona de acuerdo con los objetivos de su diseño durante la realización de las actividades necesarias para la provisión de servicios, y no solamente que satisface requisitos normativos. La definición de un conjunto de parámetros de performance operacional y su cuantificación también permite identificar dónde pueden necesitarse correcciones para mantener o reencauzar la performance operacional del sistema al nivel previsto por los objetivos de diseño del sistema. Como consecuencia, un conjunto de parámetros de performance 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 mantenerse las consecuencias de los peligros en el contexto operativo en el cual tienen lugar la operaciones necesarias para la provisión de servicios en un nivel ALARP.

La introducción de un conjunto de parámetros de performance de seguridad operacional (*safety performance*) también 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 la performance. 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 mejoramiento continuo de la seguridad operacional en que se basa la gestión de la seguridad operacional.

El desarrollo de un conjunto de parámetros cuantificables relacionados con la performance 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 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.

b) *Nivel de performance de seguridad operacional* – Representación del sistema desde la perspectiva de la seguridad operacional, expresada por medio de indicadores de performance

seguridad operacional.

c) *Indicadores de performance de seguridad operacional* – Parámetros que tipifican el "estado" del desempeño del sistema de gestión de la seguridad operacional.

d) Valor de indicadores de performance de seguridad operacional – Cuantificación del indicador de seguridad operacional.

e) *Metas de performance de seguridad operacional* – Mejoras concretas a ser alcanzadas.

f) *Valor de metas de performance de seguridad operacional* – Cuantificación de la meta de seguridad.

g) *Medición de la performance de seguridad operacional* – Cuantificación de la eficacia y eficiencia de la gestión de la seguridad operacional de un sistema en la práctica. Esta medición se realiza a través del valor de los indicadores de performance de seguridad operacional

La selección de indicadores de performance de seguridad operacional apropiados es fundamental para la medición de la performance de seguridad operacional de SMS. Dicha selección debe ser función del detalle con el cual se prevea representar el nivel aceptable de performance de seguridad operacional del sistema. Si se desea representar la medición de la performance de seguridad operacional en términos amplios y genéricos, es apropiada la selección de indicadores de performance de seguridad operacional que representen consecuencias de relativa significación. Si se desea representar la medición de la performance de seguridad operacional en términos específicos y más definidos, entonces se requiere la selección de indicadores que representen consecuencias de "bajo nivel" es decir, que tengan una incidencia directa acotada pero que puedan influir en la performance del sistema. En ambos casos, para que los indicadores de performance de seguridad operacional sean significativos deben ser representativos de las operaciones asociadas a la entrega de servicios que caracterizan el contexto particular del proveedor de servicios.

Para elaborar adecuadamente los indicadores y las metas de performance de seguridad operacional de un SMS, es también fundamental comprender la diferencia entre dos conceptos estrechamente interrelacionados — y que por consiguiente a veces causan confusión — aunque bien distintos: la medición de la seguridad operacional y la medición de la performance de la seguridad operacional.

La medición de la seguridad operacional se refiere a la cuantificación de los resultados de consecuencias de significativa gravedad, como accidentes e incidentes graves. La medición de la seguridad operacional no es un proceso continuo sino más bien una verificación puntual, normalmente realizada con referencia a calendarios pre-especificados, por ejemplo, anualmente, semestralmente o trimestralmente. La medición de la seguridad operacional refleja la medida en la cual se han logrado los objetivos de seguridad operacional de alto nivel de los controles y/o estrategias de mitigación.

La medición de la performance de la seguridad operacional se refiere a la cuantificación de consecuencias de limitada gravedad respecto a la seguridad operacional, como el número de eventos relacionados

con objetos extraños (FOD) por número específico de operaciones en rampa, o el número de sucesos de presencia de vehículos terrestres no autorizados en las calles de rodaje por número específico de operaciones de aeropuerto o durante un período de tiempo especificado. La medición de la performance de seguridad operacional es una actividad permanente, que involucra supervisión y medición continuas por parte del operador, de determinadas actividades operacionales que son necesarias para prestar sus servicios. La medición de la performance de seguridad operacional proporciona una medida de la eficacia operacional real de un SMS, más allá de las medidas absolutas obtenidas con una medición de seguridad operacional (incluyendo el cumplimiento de las normas).

El primer paso en la definición de los indicadores de performance de seguridad operacional, y por ende de la medición de la performance de seguridad operacional de SMS por el proveedor de servicios, es decidir con respecto al detalle con que tal medición pretende representar el sistema particular del proveedor de servicios, y luego seleccionar indicadores de performance seguridad operacional que caractericen o tipifiquen las operaciones asociadas a la entrega de servicios en el contexto particular del Proveedor de servicios. Es pauta básica para el SMS que el detalle de esta 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 proveedores de Servicios que ya han desarrollado capacidades de colección y análisis de datos de seguridad operacional más específicos, estarán en condiciones de representar el nivel de performance de seguridad operacional con mayor detalle que los proveedores de servicios que no lo han hecho. En la Figura 10 se presentan ejemplos de valores de indicadores de performance de seguridad operacional de SMS.

Valores de indicadores de seguridad

1. *[Cantidad]* de desvíos de niveles de vuelo por *[cantidad]* de operaciones
2. *[Cantidad]* incursiones de pista de categoría B y C en 5 aeropuertos internacionales del *[Estado]* por *[cantidad]* de operaciones
3. *[Cantidad]* de eventos TCAS/ Airprox por *[cantidad]* de operaciones
4. *[Cantidad]* aproximaciones no-conformes (NCA) en 5 aeropuertos internacionales del *[Estado]* por *[cantidad]* de operaciones
5. *[Cantidad]* eventos FOD en 5 aeropuertos internacionales del *[Estado]* por *[cantidad]* de operaciones

Fig. 10

Una vez definidos los indicadores de performance de seguridad operacional, el paso siguiente es definir las metas de performance de seguridad operacional, que pueden considerarse como mejoras específicas a ser logradas. En la Figura 11 se presentan ejemplos de metas de performance de seguridad operacional de SMS asociadas a los indicadores previamente usados como ejemplo.

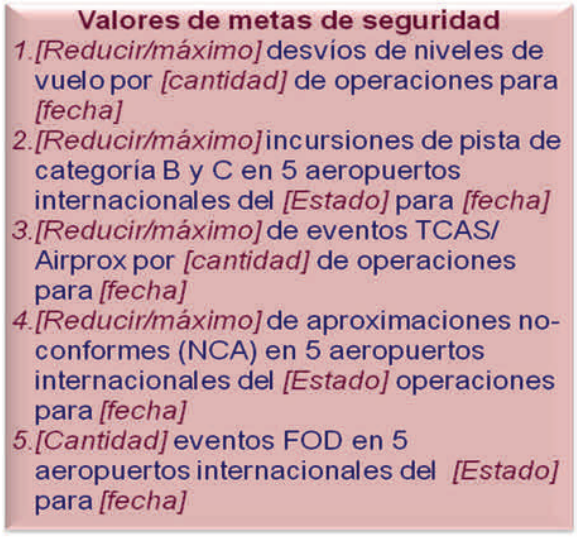

Fig. 11

Una vez seleccionados los indicadores y las metas de performance de seguridad operacional, puede establecerse la medición de la performance 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 proveedor de servicios en particular, durante las actividades necesarias para la provisión de los servicios que debe garantizar el SMS del proveedor de servicios en la práctica real. Para ello, deben asignarse *valores* a los indicadores de performance de seguridad operacional y las metas de performance de la seguridad operacional. En la Figura 12 se presenta un ejemplo de valores de medición de la performance de seguridad operacional específico al SMS de un proveedor de servicios.

Fig. 12

Finalmente, para lograr el “salto” de los valores de indicadores de performance de seguridad operacional a los valores de las metas de performance 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)*.

ESTA PÁGINA FUE DEJADA INTENCIONALMENTE EN BLANCO

Capítulo IV

Los arreglos institucionales

Capítulo IV

Los arreglos institucionales

Introducción

1. Los tres capítulos iniciales de este documento abarcan la fundamentación dogmática y los dos procesos básicos para la operación de un SMS, así como sus actividades subyacentes y los medios necesarios para las mismas. Aunque sea verdad de Perogrullo, sabido es que ningún proceso puede desarrollarse, no importa cuán fuerte sea su fundamentación dogmática, ni ninguna actividad puede ponerse en marcha, dentro de un vacío institucional. Deben existir arreglos institucionales y, fundamentalmente, recursos que los arreglos institucionales generan y encaminan, y que son absolutamente necesarios para apoyar la implementación y mantenimiento efectivo del SMS por un proveedor de servicios.

2. El punto a no perder de vista es que, no obstante la vital importancia que tienen los arreglos institucionales, los mismos son medios para lograr un fin, que es el establecimiento y mantenimiento de las actividades subyacentes a los dos procesos básicos del SMS, es decir, gestión de riesgo de seguridad operacional y garantía de la 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 proveedor de servicios que tiene en pie solamente los arreglos institucionales, pero no pone en práctica las actividades, no tiene un SMS. Tal proveedor de servicios tiene, a lo sumo, las “condiciones de contorno” necesarias para practicar SMS, pero si las actividades subyacentes a los dos procesos no están en pie y en funcionamiento, las herramientas están encerradas en un cajón.

3. La consideración que ofrece el párrafo anterior no es menor. Para ponerlo en lenguaje inequívoco: el cumplimiento normativo, por sí solo, no es evidencia que el proveedor de servicios ha implementado un SMS efectivo y eficiente. El cumplimiento normativo es evidencia solamente de eso: que el proveedor de servicios cumple con un conjunto de normas. Pero la evidencia 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 las actividades subyacentes a los procesos de gestión de riesgo de seguridad operacional y garantía de la seguridad operacional en tiempo real. Tal verificación, a su vez, solamente puede validarse a través de la definición de la performance de seguridad operacional específica del SMS del proveedor de servicios, descripta por sus indicadores de performance de seguridad operacional representativos del contexto operativo donde las operaciones del proveedor de servicios necesarias para la entrega de servicios tienen lugar, y por el logro de las metas de performance de seguridad operacional del SMS (ver el Capítulo III). El logro de estas últimas en particular es la evidencia, más allá de cualquier posible cuestionamiento, que el proveedor de servicios tiene no solamente las herramientas necesarias para la práctica de las actividades subya-

centes a los dos procesos básicos del SMS, sino 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 declaración de política de seguridad operacional del proveedor de servicios, el establecimiento de objetivos de seguridad operacional del proveedor de servicios, la asignación de responsabilidades dentro de la estructura de personal del proveedor de servicios por 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 del SMS por un proveedor de servicios.

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 del SMS del proveedor de servicios es la publicación de una clara e inequívoca declaración de política de seguridad operacional. La política de seguridad operacional es el equivalente institucional a la Constitución de un país: es la carta magna del proveedor de servicios en lo que a gestión de la seguridad operacional se refiere. Una vez elaborada la política de seguridad operacional, la administración superior del proveedor de servicios debe comunicarla, con visible endoso, a todo el personal. En lineamientos generales, la política de seguridad operacional refleja el compromiso moral y material del proveedor de servicios, enunciada por su administración superior, en cuanto a lo siguiente:

a) el logro de los estándares más elevados de seguridad operacional y de su gestión;

b) el 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;

c) la provisión de los recursos necesarios para una entrega de servicios segura, efectiva y eficiente;

d) la inclusión de la gestión de la seguridad operacional, con cánones debidamente valorizados, entre las responsabilidades principales de todos los integrantes de la administración superior; y

e) la adopción de las medidas necesarias para asegurar que la política sea comprendida, implantada y mantenida, según corresponda, a todos los niveles de las actividades del proveedor de servicios.

f) 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 del quehacer 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 tengan 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 los niveles de la administración y de la fuerza laboral deben asumir la responsabilidad y el compromiso del logro del nivel más elevado de eficacia en la gestión de la seguridad operacional, comenzando por el Director General.

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 fomenta prácticas operativas seguras, alienta la efectiva notificación y comunicación de cuestiones relativas seguridad operacional, y gestiona 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;*
- ***inscribir** – en la medida lógica y adecuada – a la gestión de la seguridad operacional como responsabilidad de todos los niveles de administración y de la fuerza laboral;*
- ***definir** claramente para todos los niveles de administración y de la fuerza laboral – en la medida lógica y adecuada – las líneas de rendición de cuentas y responsabilidades para el logro de la performance 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 reportes de seguridad operacional, 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 practicable (ALARP);*
- ***garantizar** que no se adoptarán medidas contra los empleados que informen sobre deficiencias o problemas de seguridad operacional mediante el programa de reportes de seguridad operacional, a menos que el reportaje 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 durante las operaciones necesarias para la provisión de servicios, los requisitos y las normas legislativas y reglamentarias;*
- ***asegurar** la disponibilidad de recursos humanos con conocimientos y capacitación suficientes para poner en práctica los procesos y actividades de gestión de la seguridad operacional;*
- ***asegurar** que todos los integrantes de la fuerza laboral poseen información y han recibido instrucción sobre seguridad operacional adecuada y apropiada; que son competentes en cuestiones de gestión de la seguridad operacional; y que solamente se les asignan tareas sobre el particular que son acorde con sus competencias;*
- ***establecer** y medir la performance de seguridad operacional de nuestro sistema de gestión de segu-*

ridad operacional (SMS) con respecto a los indicadores de performance de seguridad operacional y metas de performance 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 la performance de seguridad operacional de nuestro sistema de gestión de seguridad operacional (SMS), mediante procesos de gestión que aseguren que se adoptan, y son eficaces, las actividades pertinentes; y*
- ***asegurar** que los servicios suministrados por terceras partes para apoyar las operaciones necesarias para la provisión de nuestros servicios satisfacen los estándares performance de seguridad operacional de nuestro sistema de gestión de seguridad operacional (SMS).*

_____

Director General

Objetivos de seguridad operacional

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

7. El Apéndice al Capítulo III presenta ejemplos de metas de performance se 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 proveedor de servicios. Como para graficar las diferencias entre unos y otros, a continuación se presentan ejemplos de objetivos de seguridad operacional del proveedor de servicios, de los cuales se desprende la naturaleza global y conceptual, antes que métrica, de los objetivos de seguridad operacional:

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 capacitación en el SMS que sea apropiada y de relevancia para todo el personal;

e) implementar un programa efectivo de reportaje de seguridad operacional;

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

g) etc.

Asignación de responsabilidades por la gestión de la seguridad operacional

8. Indudablemente, el aspecto más importante de la asignación de responsabilidades de seguridad operacional es la identificación del Ejecutivo Responsable, quien debe ser una persona única e identificable, con la responsabilidad final de rendición de cuentas por la performance efectiva y eficiente del SMS del proveedor de servicios. Dependiendo del tamaño y complejidad del proveedor de servicios, el Ejecutivo Responsable puede ser:

a) el director general;

b) el presidente de la junta de directores;

c) un socio; o

d) el propietario.

9. El temperamento seguido más frecuentemente es determinar quién debería ser el Ejecutivo Responsable en base a la función asignada a la persona dentro de la organización del proveedor de servicios. No obstante, más importante que quién debería ser el Ejecutivo Responsable, son las facultades que éste debería tener para poder cumplir con su responsabilidad de rendir cuentas adecuadamente por la performance efectiva y eficiente del SMS del proveedor de servicios. Estas facultades comprenden, sin estar necesariamente limitadas a:

a) plena 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 proveedor de servicios; y

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

10. Lo anterior subraya que las facultades (y por ende, las responsabilidades) del Ejecutivo Responsable se refieren a la asignación de recursos o control de actividades, casi exclusivamente. Por consiguiente, un proveedor de servicios que designe al Ejecutivo Responsable en la persona de un funcionario 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.

11. El Ejecutivo Responsable puede delegar el día a día de la gestión del SMS a otra persona o personas, siempre que dicha asignación esté adecuadamente documentada y descripta en el documento

pertinente del proveedor de servicios. La responsabilidad por la rendición de cuentas del Ejecutivo Responsable no se ve afectada, no obstante, por la asignación de la gestión de SMS a otra persona: recuérdese que se pueden delegar funciones, pero no se pueden delegar responsabilidades por la rendición de cuentas. El Ejecutivo Responsable conserva la responsabilidad de rendición de cuentas por la performance efectiva y eficiente del SMS del proveedor de servicios aun cuando delegue el día a día de las actividades del SMS.

12. La asignación de las funciones y responsabilidades de gestión de seguridad operacional del personal a los niveles superiores de la administración del proveedor de servicios es también un elemento clave de los arreglos institucionales necesarios para auspiciar los dos procesos básicos del 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 del 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, generalmente conocidos como “gerentes operativos” o “gerentes de las áreas funcionales”) que para los encargados de las funciones de apoyo a las operaciones (recursos humanos, administración, asuntos jurídicos, calidad y financieros).

13. Las responsabilidades de rendición de cuentas, funciones y facultades de las personas encargadas de dependencias funcionales, y en particular de los gerentes de las áreas funcionales, deben estar documentadas y descriptas en el documento pertinente del proveedor de servicios. Las responsabilidades de rendición de cuentas, funciones y facultades deben estar graficadas 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 proveedor de servicios.

La Oficina de Servicios de Gestión de Seguridad Operacional

14. El centro operativo para el funcionamiento del SMS del proveedor de servicios debe estar ubicado en una dependencia única e identificable, que a los efectos de este documento se denominará “Oficina de Servicios de Gestión de la Seguridad Operacional”. El concepto de la Oficina de Servicios de Gestión de la Seguridad Operacional es clave para la noción de gestión de la seguridad operacional como proceso institucional, y para el SMS como el sistema de gestión que el proveedor de servicios cuenta para tal fin. La Oficina de Servicios de Gestión de la Seguridad Operacional es independiente y neutral con respecto a las decisiones operativas adoptadas y las actividades operativas puestas en marcha en relación con el apoyo a la provisión de servicios por los gerentes de las áreas funcionales. En un entorno SMS, la Oficina de Servicios de Gestión de la Seguridad Operacional realiza cuatro funciones corporativas esenciales, que son absolutamente consistentes con la noción del SMS como “generador” de datos expuesta en los Capítulos I al III:

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 servicios para el logro del producto, y proporciona información sobre los mismos a las dependencias funcionales 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 monitoreo continuo de datos, la eficacia de los controles o las mitigaciones contra las consecuencias de los peligros puestos en marcha por las dependencias funcionales a cargo de la provisión de servicios (*garantía de la seguridad operacional*);

c) asiste a los gerentes de las áreas funcionales, a requerimiento, en asuntos de gestión de la seguridad operacional (*garantía de la seguridad operacional*); y

d) asesora a la administración superior en asuntos de gestión de la seguridad operacional (*garantía de la seguridad operacional*).

15. 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 proveedor de servicios. El responsable de seguridad operacional, a menudo conocido como oficial 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.

16. En años recientes, la noción que la “propiedad” de las actividades de seguridad operacional eran exclusivamente 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 se establecía un canal directo de comunicación entre el responsable de seguridad operacional y el director general del proveedor de servicios.

17. 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 de seguridad operacional, estableciendo un enlace directo entre ésta y el director general. En segundo lugar, el enlace directo trataba de generar neutralidad, removiendo a los encargados de gestionar las actividades operacionales directamente relacionadas con la provisión de servicios (gerentes de las áreas funcionales) de la evaluación y resolución de problemas de seguridad operacional. La composición de lugar era que existía una gran probabilidad de que los gerentes de las áreas funcionales 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 director general suponía la eliminación de este presunto conflicto de intereses.

18. 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 gerentes de línea del proceso de toma de decisiones de seguridad operacional. Esto nutre la percepción que "los problemas de seguridad operacional no son problemas de los gerentes de las áreas funcionales; 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 reduce en la práctica a un diálogo entre el director general y el responsable de seguridad operacional. Considerando la carga de trabajo de un director general, este diálogo tiene todas las posibilidades de transformarse en monólogo. En segundo lugar, y muy importante, deja 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 proveedor de servicios.

19. 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, para reflejar que tal dependencia proporciona un servicio al proveedor de servicios, tanto a la administración superior como a los gerentes de las áreas funcionales, con respecto a la gestión de la seguridad como proceso institucional. La Oficina de Servicios de Gestión de la 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 II. Mediante una combinación de métodos, la Oficina de Servicios de Gestión de la Seguridad Operacional capta lo que sucede dentro de la deriva operacional (ver también el Capítulo II), 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.

20. 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 gerentes de las áreas funcionales para la resolución de los problemas de seguridad subyacentes. Los gerentes de las áreas funcionales 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 gerentes de las áreas funcionales 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 la Seguridad Operacional.

21. 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 de provocar daño, 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 controlar o 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 proveedor de servicios y, por lo tanto los que tienen mayores conocimientos y experiencia en los procedimientos técnicos como para proponer soluciones.

22. Luego que la información de seguridad operacional ha sido entregada a los gerentes de las áreas funcionales apropiadas, la Oficina de Servicios de Gestión de la 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 la Seguridad Operacional y los gerentes de las áreas funcionales en cuestión, la Oficina de Servicios de Gestión de la Seguridad Operacional presenta a gerentes de las áreas en que hubiese un problema de seguridad operacional un nuevo juego de datos sobre el problema que se está tratando de solucionar. El nuevo juego de datos indicará si las soluciones de mitigación implantadas por los gerentes de las áreas correspondientes 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 gerentes de las áreas correspondientes, y este ciclo se repite tantas veces como sea necesario hasta que el análisis de los datos de seguridad operacional comprueba que el problema de seguridad operacional se ha resuelto. En todo este proceso, los gerentes de las áreas involucradas no responden por la solución del problema de seguridad operacional en cuestión a la Oficina de Servicios de Gestión de la Seguridad Operacional, sino al Ejecutivo Responsable, como persona con responsabilidad final por la rendición de cuentas por la eficacia y eficiencia del SMS del proveedor de servicios.

23. La Oficina de Servicios de Gestión de la Seguridad Operacional será, en la mayoría de las organizaciones, la dependencia en la cual el Ejecutivo 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 la Seguridad Operacional también asesora al Ejecutivo Responsable y a los gerentes de las áreas funcionales en asuntos relativos a la gestión de la seguridad operacional, y es responsable de coordinar y comunicar asuntos de seguridad operacional dentro del proveedor de servicios, así como con agencias externas, contratistas y partes interesadas, según corresponda.

24. La Oficina de Servicios de Gestión de la Seguridad Operacional se comunica directamente con los gerentes de las áreas funcionales (operaciones, mantenimiento, ingeniería, instrucción, etc.). Si debido al tamaño del proveedor de servicios, estos gerentes cuentan con un funcionario de seguridad operacional especializado en un área operativa específica, y tal funcionario tiene responsabilidad delegada para la gestión de problemas de seguridad operacional en un área operativa en cuestión, ese funcionario será el primer punto de contacto para la Oficina de Servicios de Gestión de la Seguridad Operacional en la comunicación con el área específica.

25. En circunstancias normales, la Oficina de Servicios de Gestión de la Seguridad Operacional tiene acceso al Ejecutivo Responsable o se comunica con éste mediante dos canales: el grupo asesor de seguridad operacional y/o la junta de control de seguridad operacional. Las características de estos

grupos se discuten inmediatamente a continuación, en este Capítulo. En circunstancias excepcionales o urgentes, la Oficina de Servicios de Gestión de la Seguridad Operacional tiene acceso directo de emergencia al Ejecutivo Responsable. Este canal de comunicación debería utilizarse en contadísimas ocasiones y, en tal caso, debe justificarse y documentarse adecuadamente.

26. La distribución de información sobre seguridad operacional por la Oficina de Servicios de Gestión de la Seguridad Operacional es sólo la primera etapa del proceso de gestión de riesgos de seguridad operacional. Los gerentes de las áreas funcionales deben actuar sobre esta información. La mitigación de problemas de seguridad operacional inevitablemente exige recursos. A veces estos recursos son directamente accesibles por parte de los gerentes de las áreas funcionales. Otras veces, se requieren recursos adicionales, cuya asignación puede no estar entre las facultades de estos gerentes, y debe ser aprobada por los niveles superiores de la organización.

La Junta de la Seguridad (SRB) y el Grupo Ejecutivo de Seguridad Operacional (SAG)

27. La Junta de Control de la Seguridad Operacional (safety review board, SRB) 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 Ejecutivo Responsable e integrado por los gerentes superiores, incluyendo los gerentes responsables de las áreas funcionales. El encargado de la Oficina de Servicios de Gestión de la Seguridad Operacional participa en la SRB solamente como asesor. La SRB tiene carácter eminentemente estratégico, trata problemas de alto nivel en relación con las políticas, asignación de recursos y supervisión del desempeño de SMS del proveedor de servicios, y se reúne con poca frecuencia, a menos que circunstancias excepcionales impongan otra cosa.

28. Una vez que la SRB ha elaborado una dirección estratégica, la implantación de las estrategias decididas debe realizarse en forma coordinada en toda la organización del proveedor de servicios. Esta es la función principal del Grupo Ejecutivo de Seguridad Operacional (safety action group, SAG). El SAG es un comité de alto nivel, integrado por supervisores de línea y representantes del personal operativo, y presidido en turnos por gerentes de área designados. El responsable de la Oficina de Servicios de Gestión de la Seguridad Operacional es el secretario del SAG. El SAG tiene carácter eminentemente táctico y trata los asuntos de implementación para satisfacer las directivas estratégicas de la SRB. Mientras el SAG trata de aspectos de implementación a nivel operativo relativos a actividades específicas para asegurar la mitigación y/o control de las consecuencias de los peligros durante las operaciones, la SRB trata de la coordinación de esos aspectos, para asegurar la coherencia en la dirección estratégica.

Documentación SMS

29. La literatura sobre SMS es unánime en asignarle tres características distintivas, proponiendo que SMS es:

a) sistemático;

b) proactivo; y

c) explícito

30. Se considera al 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 proveedor de servicios. Las actividades del SMS apuntan a mejoras graduales pero constantes, y no a cambios radicales e instantáneos. Se considera al SMS proactivo porque se basa en un enfoque que enfatiza la identificación de deficiencias de seguridad operacional y peligros, y el control y 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 al 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 proveedor de servicios están al alcance de todo el personal involucrado. Se trata de una situación en la cual la memoria colectiva sobre seguridad operacional del proveedor de servicios reside en una estructura formal y no en las mentes de determinados individuos. Por lo tanto, la documentación es un elemento esencial del SMS.

31. 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 específicos del SMS, como formularios de notificación de sucesos, líneas de rendición de cuentas, responsabilidades y facultades relativas a la gestión de la seguridad operacional y a la estructura del proveedor de servicios para la gestión de la seguridad operacional. Además deben documentarse directrices explícitas para el tratamiento, almacenamiento y conservación de los registros.

32. Distintos proveedores de servicios 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 del SMS, y el manual del SMS (SMSM)

33. El plan de implementación SMS constituye la formulación de una estrategia realista por parte del proveedor de servicios para las actividades necesarias para el diseño y puesta en marcha del SMS, de manera tal de satisfacer los objetivos de seguridad operacional del proveedor de servicios, incluyendo la prestación efectiva y eficiente de los servicios. El plan de implementación es una descripción de cómo logrará el proveedor de servicios la puesta en marcha de las actividades subyacentes al SMS de forma organizada y siguiendo pautas establecidas, quiénes las ejecutarán, y cuál será el cronograma que guiará y documentará tal puesta en marcha. Dependiendo del tamaño del proveedor de servicios y la complejidad de sus operaciones, el plan de implementación del 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 conmensurables con la tarea que debe realizar (incluyendo el tiempo para las reuniones). Asimismo, debe reunirse regularmente con la administración superior para evaluar el progreso del plan de implementación. Una vez completado, la administración superior del proveedor de servicios debe endosar el plan de implementación del SMS.

34. El contenido de un plan de implementación del SMS abarca típicamente los aspectos enumerados inmediatamente a continuación en este párrafo. Como se menciona en el párrafo anterior, el plan de implementación SMS describe el cronograma que guiará y documentará el plan de implementación, y cómo y quiénes pondrán en marcha o se implementarán los siguientes requerimientos:

a) definición de la política y objetivos de gestión de la seguridad operacional;

b) definición de las funciones y responsabilidades de gestión de la seguridad operacional;

c) establecimiento de la política de reportes de seguridad operacional;

d) pautas para el establecimiento o adaptación de un programa de notificación de seguridad operacional;

e) pautas para la participación del personal operativo en las actividades de SMS en general y en el programa de reportajes de seguridad operacional;

f) pautas para medición de la performance de la seguridad operacional del SMS;

g) establecimiento de los medios de comunicación de la seguridad operacional;

h) necesidades de instrucción en gestión de la seguridad operacional; y

i) procedimientos para el control por el proveedor de servicios de la performance de la seguridad operacional del SMS.

35. El manual SMS (SMS Manual, SMSM) define el enfoque del proveedor de servicios 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. Típicamente, el contenido del SMSM comprende:

a) la descripción del sistema del proveedor de servicios, como ámbito del sistema de gestión de la seguridad operacional, que se mantiene actualizada en forma permanente;

b) el análisis de carencias del proveedor de servicios con respecto a los requerimientos de implementación de SMS establecidos, que se mantiene actualizado en forma permanente;

c) la política y los objetivos de seguridad operacional, que se mantienen actualizados en forma permanente;

d) las responsabilidades por la rendición de cuentas respecto de la gestión de la seguridad operacional;

e) el personal clave para la gestión de la seguridad operacional, sus funciones, atribuciones y responsabilidades;

f) procedimientos de control de documentación con respecto a procesos y actividades de ges-

tión de la seguridad operacional;

g) actividades de gestión de riesgo de seguridad operacional, incluyendo identificación de peligros;

h) actividades de garantía de la seguridad operacional, incluyendo monitoreo de la performance de seguridad operacional y los procedimientos para la gestión del cambio;

i) protocolos y procedimientos para auditorías y encuestas de seguridad operacional;

j) medios de promoción de la seguridad operacional;

k) coordinación de la planificación de respuesta ante emergencias; y

l) control de las actividades contratadas.

La implementación de SMS en la práctica – Ocho actividades clave

36. Actualmente hay consenso en la industria en cuanto a 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. Este consenso ha sido recogido en inmensa mayoría por las autoridades normativas, que ofrecen a los proveedores de servicios la opción de la implementación en fases de SMS. En términos globales, se proponen cuatro fases, cada una abarcando actividades que permitan la introducción de los elementos específicos del SMS. Así, la fase I se propone como fase de planificación, la fase II como la fase de introducción de los procesos reactivos, la fase III como la de los procesos proactivos y predictivos, y la fase IV como la de introducción de la garantía de la seguridad operacional.

37. El Manual de gestión de la seguridad operacional (Doc 9859) de la OACI contiene, en su Capítulo 10, una detallada descripción de los pasos a seguir en cada fase para la implementación del SMS, por lo que se sugiere como lectura de referencia, ya que este material constituye una verdadera lista de verificación, paso a paso, para el desarrollo de las cuatro fases. No obstante, el Doc 9859 parte del supuesto del desarrollo del SMS “desde cero”, es decir, contempla únicamente la situación en la cual el proveedor de servicios no tiene ninguno de los elementos necesarios. Se considera que tal situación es casi inexistente en la República Argentina. Finalmente, de acuerdo con lo expuesto se han identificado ocho actividades claves para la implementación del SMS, las cuales se describen a continuación.

Actividad No. 1: Establecimiento del Grupo de Planificación SMS

38. El establecimiento de un grupo de planificación SMS es, la primera actividad para la implementación o actualización, según sea el caso, del SMS por el proveedor de servicios. Dado que el SMS es el sistema de gestión de la seguridad operacional de toda la organización del proveedor de servicios, es fundamental que el grupo de planificación tenga una composición multidisciplinaria, y que se inte-

gre la participación a todos los sectores del proveedor de servicios responsables por 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); seguridad operacional; instrucción; mantenimiento; rampa; finanzas, legal y recursos humanos. El grupo de planificación desarrollará sus tareas respetando un cronograma definido, y deberá reunirse con una periodicidad apropiada con la administración superior del proveedor de servicios 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.

Actividad No. 2: Descripción del sistema

39. La segunda actividad a completar por el grupo de planificación es la descripción del sistema del proveedor de servicios. 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 proveedor de servicios. Básicamente, se trata de identificar el volumen y complejidad de la 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 proveedor de servicios (operaciones, mantenimiento, instrucción, etc.);

b) las interacciones del sistema del proveedor de servicios con otros sistemas en el sistema de transporte aéreo (por ej. si es el caso de una línea aérea, su relación con el ATC, los aeródromos, etc.);

c) las consideraciones de desempeño humano requeridas para la operación del sistema (es decir las actividades a ser desempeñadas por el personal operativo);

d) los componentes tecnológicos del sistema;

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

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

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

Actividad No. 3: Análisis de carencias del SMS

40. Concretada la descripción del sistema, la actividad inmediata siguiente del grupo de planificación debe ser la concreción del análisis de carencias del SMS. La puesta en práctica del SMS requiere que el proveedor de servicios haga un balance de su organización para determinar cuáles son los componentes y elementos constitutivos del SMS que están actualmente funcionando en el sistema del proveedor de servicios, 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 dogmáticos del mismo que hubiesen sido reflejados en la normativa vigente. Este análisis se conoce como análisis de carencias (gap analysis) e implica la comparación entre requisitos dogmáticos/normativos del SMS y los recursos existentes en el proveedor de servicios. Al presente, el marco de referencia internacional para efectuar la comparación entre los requisitos del SMS y los recursos existentes en el proveedor de servicios 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 detallados en la Lista de Chequeo para la Implementación del SMS de la ANAC. Cada elemento de la estructura del SMS debe ser evaluado para determinar si el proveedor de servicios debe crear o modificar políticas, directivas, o procedimientos para satisfacer los requerimientos del elemento en cuestión, si es necesario desarrollar una herramienta específica requerida por el SMS, o si las herramientas ya existentes en el sistema del proveedor de servicios satisfacen los requerimientos del elemento en cuestión. Una vez que el análisis de carencias haya sido completado y documentado, los instrumentos, políticas, procedimientos o directivas identificados como faltantes o deficientes formarán la base del plan de implementación del 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. Explayando 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 "alinear" 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 proveedor de servicios comparados con los necesarios para el funcionamiento del SMS. El análisis de las carencias es importante porque un número de las estructuras básicas de la organización necesarias para comenzar a elaborar un SMS, pueden ya existir en ella: rara vez será necesario construir un SMS "a partir de cero", debido a que la mayoría de los proveedores de servicios tendrán va-

rias actividades relacionadas con el SMS establecidas y funcionando. La elaboración del SMS debería aprovechar las estructuras existentes del proveedor de servicios y construir sobre ellas.

Actividad No. 4: Identificación del Ejecutivo Responsable y asignación de responsabilidades por la gestión de la seguridad operacional

43. Concretados la descripción del sistema y el análisis de carencias, el paso siguiente para el grupo de implementación es la identificación del Ejecutivo Responsable, y la definición de las responsabilidades a asignarse por la gestión de la seguridad operacional. Esto incluye a la Oficina de Servicios de Gestión de Seguridad Operacional, el SRB y el SAG, según los lineamientos expuestos bajo el título pertinente en este Capítulo. Cabe destacar que es altamente improbable que el grupo de implementación tenga autoridad para designar al Ejecutivo Responsable o asignar responsabilidades por la gestión de la seguridad operacional. El rol del grupo es más bien identificar y proponer al Ejecutivo Responsable. De la misma manera, es probable que la autoridad del grupo de implementación esté limitada a proponer los lineamientos para la asignación de responsabilidades por la gestión de la seguridad operacional. El ejecutivo responsable deberá ser designado oportunamente por el propietario o sociedad propietaria del proveedor de servicios definiendo, además de todas las funciones y responsabilidades de las que ya le hayan sido asignadas, aquellas relativas a la seguridad operacional según lo descripto en párrafos anteriores.

Actividad No. 5: Propuesta de declaración de política de gestión de la seguridad operacional

44. La quinta actividad del grupo de implementación es la definición y propuesta, para su aprobación y posterior publicación, del borrador de la declaración de política de gestión de la seguridad operacional del proveedor de servicios, según los lineamientos expuestos bajo el título pertinente en este Capítulo.

Actividad No. 6: Programa interno de capacitación sobre el SMS

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

Actividad No. 7: Comunicación sobre la iniciación del proyecto de implementación del SMS

46. La séptima actividad a acometer por el grupo de implementación es el establecimiento de un progra-

ma de comunicación sobre la iniciación del proyecto de implementación del 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 proveedor de servicios, el inicio y periódico progreso de las actividades para la implementación del 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 este documento.

Actividad No. 8: Evaluación y propuesta de puesta en marcha de los mecanismos para la adquisición de datos sobre deficiencias de seguridad operacional y peligros

47. La siguiente actividad es posiblemente una de las más fundamentales y de cuya correcta conclusión depende en gran medida el éxito o el fracaso de SMS del proveedor de servicios: la evaluación de los mecanismos para la adquisición de datos sobre deficiencias de seguridad operacional y peligros que existen en el proveedor de servicios y propuesta de puesta en marcha de los adicionales que fuesen necesarios. Al fin y al cabo, ya se ha expuesto la noción del 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 proveedor de servicios, y proponer la institución de aquellas con las que no contase el proveedor de servicios, según lo expuesto en el Capítulo III de este documento.

Plan de implementación del SMS

48. La actividad final, como culminación del desarrollo de la fase de planificación, una vez completadas las ocho actividades claves listadas en el párrafo 39, el grupo de implementación estará en condiciones de formular el Plan de Implementación del SMS del proveedor de servicios, según los lineamientos expuestos bajo el título pertinente en este Capítulo, el cual deberá estar aprobado por el Ejecutivo Responsable.

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

a) Establecimiento del grupo de planificación SMS

b) Descripción del sistema

c) Análisis de carencias del SMS

d) Identificación del Ejecutivo Responsable y asignación de responsabilidades por la gestión de la seguridad operacional

e) Propuesta de política de seguridad operacional

f) Propuesta de programa interno de capacitación sobre el SMS

g) Comunicación sobre la iniciación del proyecto de implementación del SMS

h) Evaluación y propuesta de puesta en marcha de los mecanismos para la 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 proveedor de servicios estará en condiciones de comenzar a "hacer SMS", es decir, a desarrollar las actividades operacionales necesarias para la provisión de servicios bajo el entorno SMS. Esto es porque, al alcanzar este punto, el proveedor de servicios tendrá en marcha los arreglos institucionales básicos para apoyar las actividades subyacentes a los dos procesos básicos de la gestión de la seguridad operacional: la gestión de riesgos de seguridad operacional, y la garantía de la seguridad operacional. Es ahora una cuestión de comenzar a ejecutar las actividades, según las pautas conceptuales y dogmáticas proporcionadas por este documento en los Capítulos I al III.

Apéndice al Capítulo 4

Estructura del SMS de la OACI

En este apéndice se introduce el marco estructural para la implantación y mantenimiento de un sistema de gestión de la seguridad operacional (SMS) por un proveedor de servicios impuesto por las Regulaciones RAAC. La implantación del marco será proporcional al tamaño del proveedor de servicios 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 Responsabilidad y compromiso de la administración

El proveedor de servicios definirá la declaración de política de gestión de la seguridad operacional de la

organización de conformidad con los requisitos nacionales e internacionales, y la misma llevará la firma del Ejecutivo Responsable de la organización. La política de seguridad operacional reflejará los compromisos de la organización respecto de la seguridad operacional; incluirá una declaración clara acerca de la provisión de los recursos necesarios para su puesta en práctica; y se comunicará, con visible endorso, a toda la organización. La política de seguridad operacional incluirá los procedimientos de reportes de seguridad operacional; indicará claramente qué tipos de comportamientos operacionales son inaceptables; e incluirá las condiciones en las que no se podrán aplicar medidas disciplinarias. La política de seguridad operacional se examinará periódicamente para garantizar que continúa siendo pertinente y apropiada para la organización.

1.2 Responsabilidades respecto de la seguridad operacional

El proveedor de servicios identificará al Ejecutivo Responsable quien, independientemente de sus otras funciones, será el responsable final y rendirá cuentas, en nombre del proveedor de servicios, respecto de la implantación y mantenimiento de SMS. El proveedor de servicios también identificará las responsabilidades de rendición de cuentas de todos los miembros de la administración superior, independientemente de las demás funciones que desempeñen, así como las de los empleados, en relación con la eficacia de la seguridad operacional de SMS. Las responsabilidades por la rendición de cuentas y las facultades de seguridad operacional se documentarán y comunicarán a toda la organización e incluirán una definición de los niveles de gestión que tienen autoridad para tomar decisiones relativas a la aceptabilidad de los riesgos de seguridad operacional.

1.3 Designación del personal clave de seguridad operacional

El proveedor de servicios identificará un gerente de seguridad operacional que será la persona responsable y punto focal para la implementación y el mantenimiento de un SMS eficaz.

1.4 Coordinación del plan de respuesta ante emergencias

El proveedor de servicios garantizará que el plan de respuesta ante emergencias, que permitirá la transición ordenada y eficiente de las operaciones normales a las operaciones de emergencia y el posterior restablecimiento de las operaciones normales, 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 proveedor de servicios elaborará un plan de implantación del SMS, endosado por la administración superior, que defina el enfoque de la organización respecto de la gestión de la seguridad operacional, de un modo que cumpla con los objetivos de la organización en materia de seguridad operacional. El proveedor de servicios elaborará y mantendrá actualizada la documentación de SMS, en la que se descri-

birán la política y los objetivos del SMS, sus requisitos, procesos y procedimientos, la rendición de cuentas, actividades y facultades respecto de los procesos y procedimientos, así como los resultados del SMS. También, como parte de la documentación relativa a SMS, el proveedor de servicios elaborará y mantendrá un manual de sistema de gestión de la seguridad operacional (SMSM) para comunicar a toda la organización su enfoque respecto de la gestión de la seguridad operacional.

2. GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

2.1 Identificación de peligros

El proveedor de servicios elaborará y mantendrá los medios que garanticen la identificación de los peligros. La identificación de los peligros se basará en una combinación de métodos reactivos, proactivos y predictivos de recopilación de datos sobre seguridad operacional.

2.2 Evaluación y mitigación de riesgos de seguridad operacional

El proveedor de servicios elaborará y mantendrá los medios que garanticen el análisis, la evaluación y el control de los riesgos de seguridad operacional en las operaciones del proveedor de servicios.

3. GARANTÍA DE LA SEGURIDAD OPERACIONAL

3.1 Supervisión y medición de la eficacia de seguridad operacional

El proveedor de servicios elaborará y mantendrá los medios para verificar la eficacia de la seguridad operacional de la organización y validar la efectividad de los controles de los riesgos de seguridad operacional. La eficacia de la seguridad operacional de la organización se verificará con referencia a los indicadores y las metas de performance de seguridad operacional del SMS.

3.2 Gestión del cambio

El proveedor de servicios elaborará y mantendrá los medios para identificar los cambios dentro de la organización que puedan afectar a los procesos y servicios establecidos; describir las disposiciones adoptadas para garantizar la performance de seguridad operacional de SMS antes de introducir cualquier cambio, y eliminar o modificar los controles de riesgos de seguridad operacional que ya no sean necesarios o efectivos debido a modificaciones del entorno operacional.

3.3 Mejora continua del SMS

El proveedor de servicios elaborará y mantendrá un protocolo para identificar las causas de performance

de seguridad operacional deficiente de SMS, determinar las consecuencias de las deficiencias de SMS en las operaciones y eliminar o mitigar las causas identificadas.

4. PROMOCIÓN DE LA SEGURIDAD OPERACIONAL

4.1 Capacitación y educación

El proveedor de servicios elaborará y mantendrá un programa de instrucción en seguridad operacional que asegure que el personal cuente con la instrucción y competencia necesarias para cumplir con sus funciones en el marco de SMS. El alcance de la instrucción en seguridad se adaptará al grado de participación en SMS de cada persona.

4.2 Comunicación de la seguridad operacional

El proveedor de servicios elaborará y mantendrá un medio formal para la comunicación sobre seguridad operacional que:

a) asegure que todo el personal tiene pleno conocimiento del SMS,
b) difunda información crítica respecto de la seguridad operacional
c) explique por qué se toman determinadas medidas de seguridad operacional y por qué se introducen o modifican procedimientos de seguridad operacional.

Capítulo V

Promoción de la Seguridad Operacional

Capítulo V

Promoción de la seguridad operacional

Introducción

1. Los tres primeros capítulos de este documento 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 garantía de la 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 declaración de política de seguridad operacional, el establecimiento de objetivos de seguridad operacional, la asignación de las funciones y responsabilidades por 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 del SMS: la promoción de la seguridad operacional.

2. Las actividades de gestión de seguridad operacional de un proveedor de servicios bajo el entorno del SMS difícilmente resulten exitosas si se pretende que funcionen por mandato o mediante la implementación 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 del SMS;

b) como impulso para el desarrollo de prácticas operativas conducentes a la integración de los procesos de gestión de la seguridad operacional con las operaciones necesarias para la provisión de los servicios, dentro de la organización;

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

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

Actividades de promoción de seguridad operacional

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

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

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

c) debe proveer capacitación sobre gestión de la seguridad operacional, incluyendo el establecimiento de competencias en lo relativo a seguridad operacional.

Comunicación

4. La comunicación es el ingrediente esencial de la promoción de la seguridad operacional. Es frecuentemente el caso 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 cabal del objetivo buscado, lo que lleva a grietas en la puesta en marcha. Por otro, y quizás lo más contraproducente, indiferencia cuando no actitudes cínicas. Lo antedicho es aplicable a todos los campos de accionar humano, y la gestión de la seguridad operacional no es una excepción.

5. El proveedor de servicios debe, por lo tanto, establecer procedimientos que permitan la comunicación más efectiva posible entre el personal operativo y la administración superior, 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 sobre temas al respecto; y

c) el logro de sucesos significativos.

6. Análogamente, el proveedor de servicios debe establecer procedimientos que permitan la comunicación “hacia arriba”, es decir, del personal operativo a la administración superior, 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 que cuenta el proveedor de servicios para la comunicación sobre la gestión de la seguridad operacional bajo el entorno del 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 proveedor de servicios sobre la gestión de la seguridad operacional a toda la organización.

8. En orden de importancia, el otro vehículo fundamental de comunicación del proveedor de servicios a los efectos de la gestión de la seguridad operacional, al que históricamente no se le ha dado la de importancia que verdaderamente tiene, por lo menos en el ámbito de los explotadores aéreos, son los procedimientos operativos estandarizados (SOPs). Los SOPs son mucho más que una guía mecánica de cómo ejecutar acciones. En su sentido final, son un mandato sobre como la administración superior ha establecido que deben conducirse las operaciones necesarias para la provisión de

servicios.

9. Otros ejemplos de formas de comunicación sobre gestión de la seguridad operacional a disposición del proveedor de servicios 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 sitios web y el correo electrónico.

10. La dependencia del proveedor de servicios a cargo de la administración 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 conspicuamente visible en todos los aspectos de las operaciones del proveedor de servicios que apoyan la provisión de servicios. Esto incluye no solo la comunicación actualizada sobre los objetivos de seguridad operacional del proveedor de servicios, sino también la comunicación periódica sobre la evaluación de la performance de seguridad operacional del SMS, incluyendo indicadores y metas de performance 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 proveedores de servicios, son materia prima para la comunicación y deben ser objeto de divulgación.

11. En síntesis, el proveedor de servicios debe tener en marcha un programa de comunicación sobre gestión de la seguridad operacional, administrado por la dependencia del proveedor de servicios a cargo de la administración diaria del SMS que esté, dirigido al personal operativo de toda la organización, y 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
e) transmitir toda otra información que pueda ser útil.

Educación

12. La educación sobre gestión de la seguridad operacional se refiere a la provisión periódica, por parte del proveedor de servicios y por intermedio 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 educación es poner al alcance del personal operativo y 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 proveedor de servicios por intermedio de su programa de comunicación.

13. Una contribución frecuentemente sub-valorizada de la educación sobre gestión de la seguridad operacional tiene que ver con su fundamental influencia como aliento de un programa de reportajes de seguridad operacional efectivo. Se trata de una muy simple ecuación: personal operativo educado 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 sitio web y el correo electrónico son los medios ideales para circular información que auspicie la educación sobre gestión de la seguridad operacional.

Capacitación

15. A diferencia de la educación, cuyo objetivo es el desarrollo intelectual por intermedio de la provisión de fundamentos y conocimientos conceptuales de naturaleza amplia, la capacitación 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 dependencia del proveedor de servicios a cargo de la administración diaria del SMS será quien proporcione la información actualizada necesaria como materia prima para el desarrollo de los materiales de instrucción. Según sea el caso de la organización interna del proveedor de servicios, la misma dependencia también se hará cargo de brindar la capacitación relacionada con los aspectos de gestión de la seguridad operacional pertinentes a las dependencias operacionales específicas del proveedor de servicios. El brindar capacitación en gestión de la seguridad operacional apropiada a todo el personal operativo, independientemente de su nivel en la organización del proveedor de servicios, es no solamente una indicación del compromiso de la administración superior 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 capacitación, así como un método de validación que permita evaluar la efectividad de la capacitación. Los requisitos y actividades de capacitación en gestión de la seguridad operacional deberían documentarse para cada área o dependencia que cumpla actividades relacionadas con las operaciones necesarias para la provisión de servicios. El programa de capacitación en gestión de la seguridad operacional debe ser acorde a las necesidades y la complejidad de la organización.

18. El manual SMS (SMSM) es propuesto como el depositario natural de los métodos y programas de capacitación en gestión de la seguridad operacional. El SMSM debe incluir las directivas específicas de capacitación inicial y periódica en gestión de la seguridad operacional para el personal operativo, supervisores y gerentes, así como la necesidad de un briefing para el Ejecutivo responsable. El volumen de capacitación 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 capacitación en seguridad operacional, incluyendo contenido, frecuencia, validación y gestión de registros de capacitación.

19. La identificación y seguimiento de los requisitos de capacitación en gestión de la seguridad operacional, para verificar que el personal ha recibido la capacitación prevista, deben ser parte del legajo técnico del personal operativo, junto con el resto de los requisitos de capacitación. La capacitación 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.

Personal operativo

20. La capacitación en gestión de la seguridad operacional para el personal operativo debería abarcar la asignación de responsabilidades por la gestión de la seguridad operacional, y los medios y las actividades para la identificación de peligros. Los objetivos de la capacitación en gestión de la seguridad operacional para el personal operativo deben incluir la definición de peligros, consecuencias y riesgos de seguridad operacional, el proceso de gestión de los riesgos de seguridad operacional, incluyendo funciones y responsabilidades y, fundamentalmente, la importancia de los reportes de seguridad operacional y el programa de reportes de seguridad operacional del proveedor de servicios. Esta capacitación asimismo debe abarcar los fundamentos de la gestión de la seguridad, un panorama general del SMS, y la política de seguridad operacional del proveedor de servicios.

Supervisores

21. La capacitación en gestión de la seguridad operacional para supervisores debería abarcar las responsabilidades por la gestión de la seguridad operacional, incluyendo medios para la promoción del SMS y para alentar y facilitar los reportes de seguridad operacional por el personal operativo. Por consiguiente, además de los objetivos de capacitación establecidos para el personal operativo, los objetivos de capacitación para supervisores incluyen un detallado conocimiento del proceso de gestión de la seguridad operacional, la identificación de peligros y la evaluación y mitigación de los riesgos de seguridad operacional, así como la gestión del cambio. Un aspecto fundamental a tratarse en la currícula de capacitación para supervisores es el análisis de datos de seguridad operacional.

Gerentes

22. La capacitación en gestión de la seguridad operacional para gerentes debe incluir responsabilidades por la gestión de la seguridad operacional. Esto incluye responsabilidades: por el cumplimiento de los requisitos de seguridad operacional nacionales, por la organización y asignación de recursos para la puesta en marcha y mantenimiento de un programa para fomentar una efectiva comunicación de seguridad operacional entre dependencias del proveedor de servicios, y por promover activamente el SMS. Además de los objetivos para los dos grupos anteriores, la capacitación en gestión de la seguridad operacional para gerentes debe incluir la garantía de la seguridad operacional y la

promoción de la seguridad operacional, funciones y responsabilidades de seguridad operacional y el establecimiento de la performance de seguridad operacional de SMS.

Briefing especial para el Ejecutivo Responsable

23. Por último, la capacitación en seguridad operacional debería incluir un briefing especial para el Ejecutivo Responsable. Esta sesión debe ser breve (no mayor de 2 horas), a los efectos de proporcionar al Ejecutivo Responsable un panorama amplio y global sobre el SMS del proveedor de servicios. El briefing especial para el Ejecutivo Responsable debe proporcionar una respuesta clara y sin ambigüedad a dos preguntas que indudablemente estarán en la mente del Ejecutivo Responsable: "¿qué es diferente en el SMS con respecto a lo que hacíamos antes?", y "¿qué me toca hacer a mí?". Ambas preguntas fueron discutidas en el capítulo 1 de este documento.

24. La Figura 13 presenta en forma gráfica y sintetizada la exposición brindada en los párrafos precedentes sobre capacitación en gestión de la seguridad operacional.

Fig. 13

Bibliografía

ICAO (http://www2.icao.int/en/ism/default.aspx)

- *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* (Cir 314)

CASA (http://casa.gov.au; bajo la pestaña “Education”)

- *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)*

EUROCONTROL (http://www.eurocontrol.int/)

- *Generic safety management manual*

IATA (http://www.iata.org/whatwedo/safety_security/Pages/index.aspx)

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

IBAC (http://www.ibac.org/safety-management)

- *SMS toolkit for business aircraft operators*

FAA (http://www.faa.gov/about/initiatives/sms/explained/components/#safety_policy)

- *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*

Transport Canada
(http://www.tc.gc.ca/eng/civilaviation/opssvs/aviationsafety-menu.htm;
http://www.tc.gc.ca/eng/civilaviation/standards/sms-guide3665.htm)

- *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)

UKCAA (http://www.caa.co.uk; bajo la pestaña “Safety Regulation Group”)

- *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*

www.anac.gob.ar

Azopardo 1405
(C1107ADY)
C.A.B.A. Argentina

MINISTERIO DE PLANIFICACIÓN
FEDERAL, INVERSIÓN PÚBLICA
Y SERVICIOS

Argentina