Capítulo 2

FUNDAMENTOS DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

2.1 EL CONCEPTO DE SEGURIDAD OPERACIONAL Y SU EVOLUCIÓN

2.1.1 Este capítulo proporciona una descripción general de los conceptos y prácticas fundamentales de la gestión de la seguridad operacional. Es importante comprender estos fundamentos antes de concentrarse en los aspectos específicos de la gestión de la seguridad operacional que figuran en los capítulos posteriores.

2.1.2 Dentro del contexto de la aviación, la seguridad operacional es “el estado en el que los riesgos asociados a las actividades de aviación relativas a la operación de aeronaves, o que apoyan directamente dicha operación, se reducen y controlan a un nivel aceptable”.

2.1.3 La seguridad operacional de la aviación tiene carácter dinámico. Continuamente surgen nuevos peligros y riesgos de seguridad operacional que deben mitigarse. Siempre y cuando los riesgos de seguridad operacional se mantengan en un nivel de control adecuado, un sistema tan abierto y dinámico como la aviación podrá seguir manteniéndose seguro. Es importante señalar que el nivel aceptable del rendimiento en materia de seguridad operacional está a menudo definido e influenciado por las normas y la cultura, tanto nacionales como internacionales.

2.1.4 El progreso en materia de seguridad operacional de la aviación puede describirse mediante cuatro enfoques, que a grandes rasgos corresponden a épocas de actividad. Dichos enfoques se indican a continuación y se ilustran en la Figura 2-1.

a) *Técnico* — Desde principios de la década de 1900 hasta fines de la década de 1960, la aviación surgió con una forma de transporte en masa, en la cual las deficiencias identificadas se relacionaban inicialmente con factores técnicos y fallas tecnológicas. El enfoque de las actividades de seguridad operacional fue, por tanto, orientado a la investigación y mejora de los factores técnicos (por ejemplo, las aeronaves). Para la década de 1950, las mejoras tecnológicas generaron una reducción gradual de la frecuencia de accidentes y los progresos de seguridad operacional se ampliaron para abarcar el cumplimiento reglamentario y la vigilancia.

b) *Factores humanos* — A principios de la década de 1970, la frecuencia de los accidentes de aviación se vio significativamente reducida gracias a los avances tecnológicos y a las mejoras de los reglamentos de seguridad operacional. La aviación se convirtió en un modo de transporte más seguro y el enfoque de las actividades de seguridad operacional se extendió para incluir problemas de factores humanos como la “interfaz hombre-máquina”. A pesar de la inversión de recursos en la mitigación de errores, el desempeño humano seguía citándose como el factor recurrente en los accidentes. El aspecto de factores humanos tendía a centrarse en la persona, sin considerar plenamente el contexto operacional e institucional. No fue sino hasta principios de la década de 1990 que se reconoció por primera vez que las personas operan en un entorno complejo, que incluye múltiples factores que tienen el potencial de afectar la conducta humana.

c) *Institucional* — Desde mediados de la década de 1990 hasta el fin del siglo, la seguridad operacional comenzó a verse desde una perspectiva sistémica que consistía en abordar los factores institucionales además de los factores humanos y técnicos. Se introdujo la noción de “accidente institucional”. Esta perspectiva consideraba el impacto de la cultura y las políticas institucionales

sobre la eficacia de los controles de riesgos de seguridad operacional. Además, el acopio y análisis rutinarios de datos de seguridad operacional aplicando metodologías reactivas y proactivas permitió a las organizaciones controlar los riesgos de seguridad operacional conocidos y detectar problemas de seguridad operacional emergentes. Estas mejoras proporcionaron los conocimientos y los fundamentos que permitieron avanzar hacia el enfoque actual de la gestión de la seguridad operacional.

d) *Sistema total* — Desde principios del siglo XXI, muchos Estados y proveedores de servicios habían adoptado los enfoques de seguridad operacional del pasado y evolucionado hacia niveles más elevados de desarrollo de la seguridad. Habían comenzado a implementar SSP o SMS y están ahora cosechando los beneficios de seguridad operacional. No obstante, hasta la fecha los sistemas de seguridad operacional se han concentrado principalmente en el rendimiento individual en materia de seguridad operacional y en el control local, con mínima consideración del contexto más amplio del sistema aeronáutico total. Esto ha llevado al creciente reconocimiento del carácter complejo del sistema de aviación y, por parte de las diferentes organizaciones, de que todas desempeñan un papel en la seguridad operacional de la aviación. Hay muchos ejemplos de accidentes e incidentes que indican que las interfaces entre organizaciones han contribuido a resultados negativos.

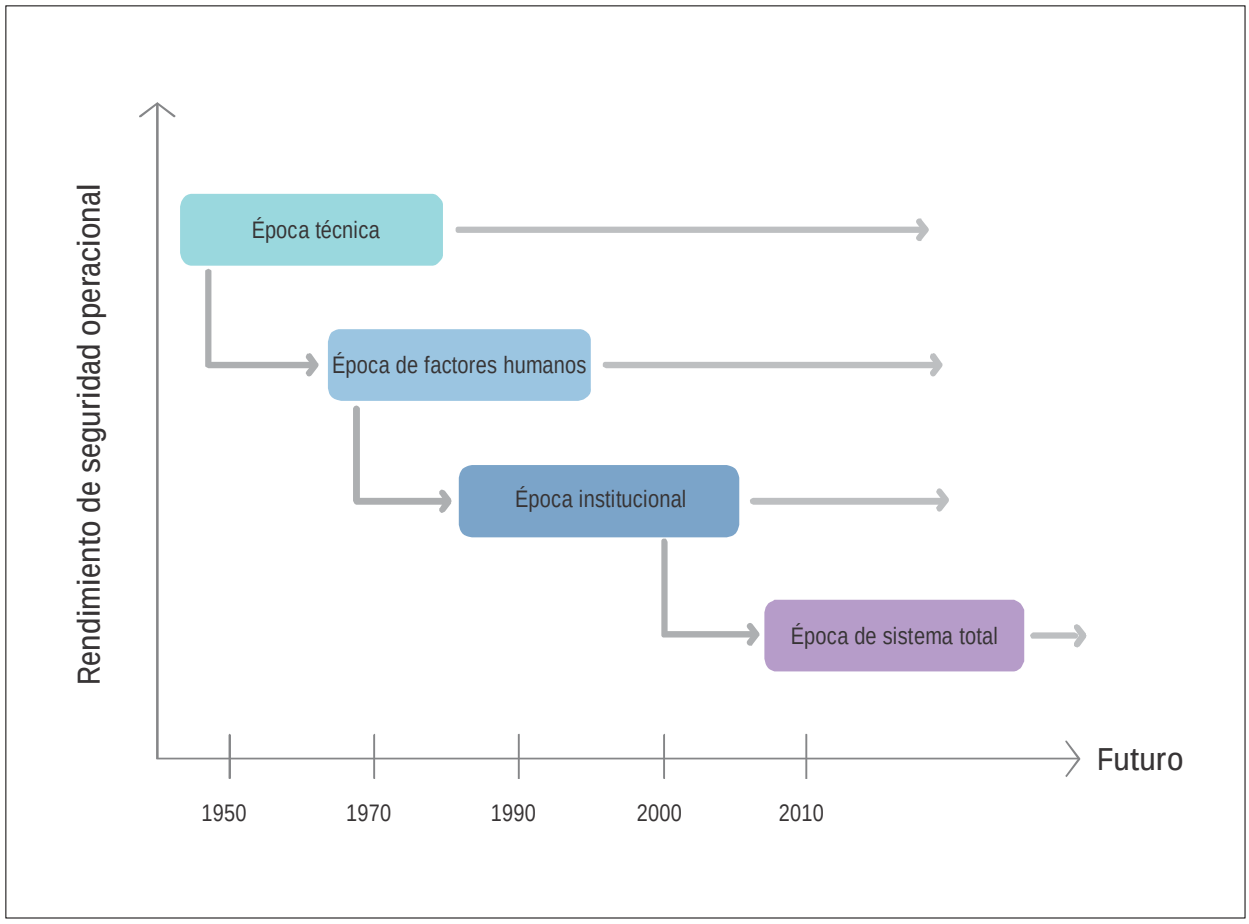

Figura 2-1. Evolución de la seguridad operacional

2.1.5 La evolución constante y complicada de la seguridad operacional ha llevado a los Estados y proveedores de servicios a un punto en el que están prestando seria consideración a las interacciones e interfaces entre los componentes del sistema: las personas, los procesos y las tecnologías. Esto ha conducido a un mayor reconocimiento de la función positiva que las personas desempeñen en el sistema. La colaboración entre los proveedores de servicios y entre éstos y los Estados trae aparejados beneficios en materia de seguridad operacional. Esta perspectiva ha alimentado a muchas iniciativas de colaboración entre proveedores de servicios y ha llevado al reconocimiento de los beneficios de la colaboración cuando se trata de problemas de seguridad operacional. Un buen ejemplo de ello es el Programa de seguridad operacional en la pista, de la OACI.

2.1.6 Para que el enfoque de sistema total en colaboración tenga éxito, deben comprenderse y gestionarse plenamente las interfaces e interacciones entre las organizaciones (incluidos los Estados). Los Estados también han comenzado a reconocer la función que puede desempeñar el enfoque de sistema total de la aviación en el desarrollo de sus SSP. Por ejemplo, dicho enfoque contribuye a gestionar los riesgos de seguridad operacional que abarcan varias actividades aeronáuticas.

2.2 LOS SERES HUMANOS EN EL SISTEMA

2.2.1 La forma en que las personas piensan acerca de sus responsabilidades con respecto a la seguridad operacional y la forma en que interactúan mutuamente para realizar sus tareas afectan considerablemente el rendimiento de la organización en materia de seguridad operacional. La gestión de la seguridad operacional debe abordar la forma en que las personas contribuyen, tanto positiva como negativamente, a la seguridad operacional de la organización. El aspecto factores humanos se refiere a comprender las formas en que las personas interactúan con el mundo, sus capacidades y limitaciones, e influir en la actividad humana para mejorar la forma en que las personas trabajan. Como resultado, la consideración de los factores humanos es parte integral de la gestión de la seguridad operacional, necesaria para comprender, identificar y mitigar riesgos así como para optimizar las contribuciones humanas a la seguridad operacional de la organización.

2.2.2 Las siguientes son maneras fundamentales en las que los procesos de gestión de la seguridad operacional consideran a los factores humanos:

a) compromiso de la administración superior para crear un entorno laboral que optimice el desempeño humano y aliente al personal a participar activamente y contribuir en los procesos de gestión de la seguridad operacional de la organización;

b) las responsabilidades del personal con respecto a la gestión de la seguridad operacional se aclaran para asegurar una comprensión y expectativas comunes;

c) la organización proporciona al personal información que:

   1) describe los comportamientos esperados con respecto a los procesos y procedimientos institucionales;

   2) describe las medidas que ha de adoptar la organización en respuesta a los comportamientos individuales;

d) los niveles de recursos humanos se vigilan y ajustan para asegurar que se cuenta con personal suficiente para satisfacer las demandas operacionales;

e) se establecen políticas, procesos y procedimientos para fomentar las notificaciones de seguridad operacional;

f) se analizan los datos de seguridad operacional y la información sobre seguridad operacional para permitir la consideración de los riesgos relacionados con el variable desempeño humano y las limitaciones humanas, con atención particular a los factores institucionales y operacionales conexos;

g) se elaboran políticas, procesos y procedimientos claros, concisos y viables, con miras a:

1) optimizar el desempeño humano;

2) prevenir errores involuntarios;

3) reducir las consecuencias no deseadas del variable desempeño humano; la eficacia de esto se vigila continuamente durante las operaciones normales;

h) la observación continua de las operaciones normales comprende la evaluación de si se aplican procesos y procedimientos y, cuando estos no se siguen, se realizan investigaciones para determinar la causa de ello;

i) las investigaciones de seguridad operacional comprenden la evaluación de los factores humanos contribuyentes, examinando no solamente comportamientos sino las razones de los mismos (contexto), en el entendido de que en la mayoría de los casos las personas tratan al máximo de realizar su trabajo;

j) el proceso de gestión de cambios incluye la consideración de la evolución de tareas y funciones de los seres humanos en el sistema;

k) el personal se capacita para asegurar su competencia en la ejecución de sus funciones, se examina la eficacia de la instrucción y se adaptan los programas de instrucción para satisfacer las necesidades cambiantes.

2.2.3 La eficacia de la gestión de la seguridad operacional depende en gran medida del grado de apoyo y del compromiso de la administración superior en cuanto a la creación de un entorno laboral que optimice el desempeño humano y aliente al personal a participar activamente y contribuir en los procesos de gestión de la seguridad operacional de la organización.

2.2.4 Para abordar la forma en que la organización influye en el desempeño humano debe existir un apoyo de alto nivel para implementar una gestión eficaz de la seguridad operacional. Esto comprende el compromiso de la administración para crear un entorno laboral correcto y una cultura de seguridad operacional correcta que tenga en cuenta los factores humanos. Esto también influirá en las actitudes y comportamientos de todas las personas en la organización. En el Capítulo 3 figura más información sobre la cultura de seguridad operacional.

2.2.5 Se han creado varios modelos para apoyar la evaluación de los factores humanos respecto del rendimiento de la seguridad operacional. El modelo SHELL es bien conocido y resulta útil para ilustrar el impacto y la interacción de los diferentes componentes del sistema con respecto a los seres humanos y hace hincapié en la necesidad de considerar a los factores humanos como parte integral de la SRM.

2.2.6 En la Figura 2-2 se ilustra la relación entre las personas (en el centro del modelo) y los componentes del lugar de trabajo. El modelo SHELL contiene los siguientes cuatro componentes:

a) soporte lógico (software-S): procedimientos, capacitación, asistencia técnica, etc.;

b) soporte físico (hardware-H): máquinas y equipo;

c) entorno (environment-E): el entorno laboral donde debe funcionar el resto del sistema L-H-S; y

d) elemento humano (liveware-L): otras personas en el lugar de trabajo.

Figura 2-2. Modelo SHELL

2.2.7 *Elemento humano*. En el centro del modelo SHELL se encuentran las personas en la primera línea de operaciones. No obstante, de todas las dimensiones del modelo, esta es la menos predecible y más susceptible a los efectos de influencias internas (hambre, fatiga, motivación, etc.) y externas (temperatura, iluminación, ruido, etc.). Aunque las personas son increíblemente adaptables, están sujetas a importantes variaciones del rendimiento. Los seres humanos no están estandarizados al mismo grado que el soporte físico, así que los bordes de este bloque no son simples ni rectos. Los efectos de las irregularidades en las interfaces entre los diversos bloques SHELL y el bloque central Elemento humano se deben entender para evitar tensiones que puedan comprometer el desempeño humano. Los bordes irregulares de los módulos representan el acoplamiento imperfecto de cada módulo. Esto resulta útil para visualizar las siguientes interfaces entre los diversos componentes del sistema de aviación:

a) *Elemento humano-soporte físico (L-H)*. La interfaz L-H hace referencia a la relación entre la persona y los atributos físicos del equipo, máquinas e instalaciones. Esto considera los aspectos ergonómicos de la operación del equipo por el personal, la forma en que se presenta la información de seguridad operacional y la forma en que se indican y operan los conmutadores y las palancas para que su funcionamiento resulte lógico e intuitivo.

b) *Elemento humano-soporte lógico (L-S)*. La interfaz L-S es la relación entre la persona y los sistemas de apoyo que se encuentran en el lugar de trabajo, por ejemplo, reglamentos, manuales, listas de verificación, publicaciones, procesos y procedimientos, y soporte lógico de computadora. Incluye temas tales como la experiencia reciente, precisión, formato y presentación, vocabulario, claridad y simbología. La interfaz L-S considera los procesos y procedimientos y la facilidad de comprenderlos y aplicarlos.

c) *Elemento humano-elemento humano (L-L)*. La interfaz L-L es la relación entre personas en el mismo entorno de trabajo. Algunas de estas interacciones corresponden al interior de la organización (colegas, supervisores, administradores), muchas otras se dan entre individuos de diferentes organizaciones con diferentes funciones (controladores de tránsito aéreo con pilotos, pilotos con mecánicos, etc.). En ella se considera la importancia de la comunicación y las habilidades interpersonales, así como la dinámica de grupo, para determinar la actuación humana.

El advenimiento de la gestión de recursos de tripulación y su ampliación a los servicios de tránsito aéreo (ATS) y operaciones de mantenimiento ha permitido a las organizaciones considerar el desempeño en equipo en la gestión de errores. También dentro del alcance de esta interfaz están las relaciones entre personal y administración así como la cultura institucional general.

d) *Elemento humano-entorno (L-E)*. Esta interfaz involucra la relación entre las personas y el entorno físico. Esto comprende aspectos como la temperatura, la luz ambiental, el ruido, las vibraciones y la calidad del aire. También considera factores del entorno externo, como las condiciones meteorológicas, la infraestructura y el terreno.

2.3 CAUSALIDAD DE ACCIDENTES

2.3.1 El modelo de “queso suizo” (o modelo de Reason), desarrollado por el profesor James Reason y bien conocido en la industria de la aviación, ilustra que los accidentes entrañan penetraciones sucesivas de múltiples defensas del sistema. Estas penetraciones o brtechas pueden generarse por muchos factores como fallas de los equipos o errores operacionales. El modelo de queso suizo sostiene que los sistemas complejos, como los de la aviación, están muy bien protegidos con capas de defensas (conocidas también como “barreras”). Las fallas de un solo punto rara vez traen consecuencias. Las brechas en las defensas de seguridad pueden ser una consecuencia atrasada de las decisiones tomadas en los niveles más altos de la organización, las que pueden permanecer latentes hasta que sus efectos o potencial de daño se activen por determinadas condiciones operacionales (conocidas como condiciones latentes). Bajo dichas circunstancias, las fallas humanas (o “fallas activas”), a nivel operacional actúan para violar las capas finales de la defensa de seguridad. El modelo de Reason propone que todos los accidentes incluyen una combinación de fallas activas y condiciones latentes.

2.3.2 Las fallas activas son medidas tomadas o no tomadas, como errores e infracciones, que tienen efectos adversos inmediatos. Por lo general, gracias a la retrospectiva, se consideran medidas inseguras. Las fallas activas se asocian normalmente con el personal de primera línea (pilotos, controladores de tránsito aéreo, mecánicos de mantenimiento de aeronaves, etc.) y pueden producir resultados perjudiciales.

2.3.3 Las condiciones latentes pueden existir mucho antes de que se experimente un resultado dañino. Las consecuencias de las condiciones latentes pueden permanecer ocultas por mucho tiempo. Inicialmente, estas condiciones latentes no se perciben como perjudiciales, pero serán evidentes luego de la violación de las defensas del sistema. Personas muy lejanas en tiempo y espacio del suceso pueden crear dichas condiciones. Las condiciones latentes en el sistema pueden incluir aquellas generadas por la falta de cultura de seguridad operacional, elecciones en cuanto a equipo o diseño de procedimientos, metas institucionales en conflicto, sistemas institucionales defectuosos o decisiones de la administración.

2.3.4 El paradigma de “accidente institucional” ayuda a minimizar fallas activas de individuos mediante la identificación de estas condiciones latentes en todo el sistema en vez de la realización de esfuerzos localizados. Es importante destacar que las condiciones latentes, cuando son creadas, normalmente tienen buenas intenciones. Los encargados de tomar decisiones en la organización a menudo tienen que equilibrar recursos finitos y prioridades y costos potencialmente conflictivos. Las decisiones adoptadas, normalmente a diario en las grandes organizaciones, podría, en circunstancias particulares, conducir involuntariamente a resultados perjudiciales.

2.3.5 En la Figura 2-3 se ilustra como el modelo del queso suizo ayuda a comprender la interacción de los factores institucionales y de gestión en la causalidad de accidentes. Allí se ilustra que varias defensas están incorporadas en el sistema de aviación para protegerlo contra variaciones en las decisiones o rendimientos humanos en todos los niveles del sistema. Pero normalmente cada capa de defensa presenta puntos débiles, indicados por los agujeros de las rebanadas de “queso suizo”. A veces todos los puntos débiles están alineados (representados por los agujeros alineados) conduciendo a una ruptura o brecha que penetra todas las barreras defensivas y puede provocar un resultado catastrófico. El modelo de queso suizo representa la forma en que las condiciones latentes siempre están presentes dentro del sistema y pueden manifestarse mediante factores activadores locales.

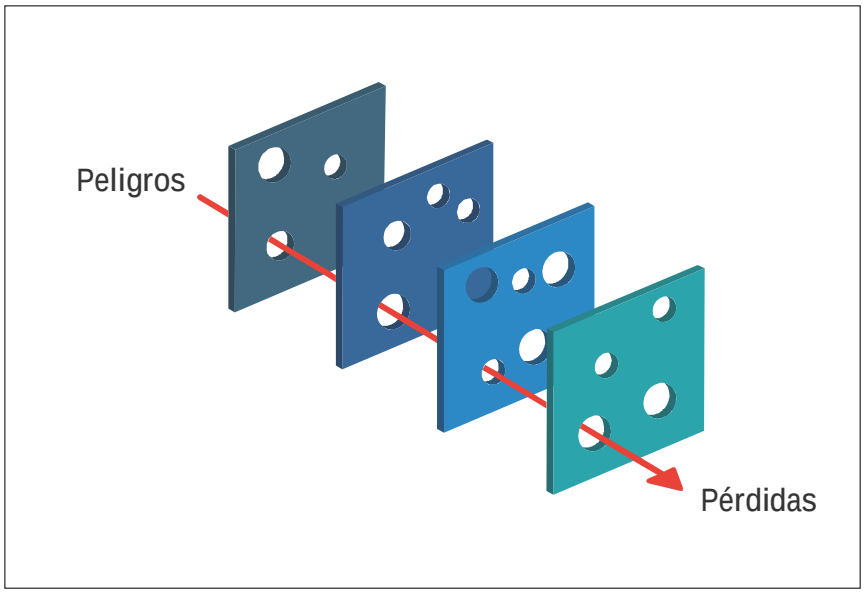

Figura 2-3. Concepto de causalidad de accidentes

2.3.6 Es importante reconocer que algunas de las defensas, o de las brechas, pueden estar influenciadas por una organización interactuante (en interfaz). Por lo tanto, es muy importante que los proveedores de servicios evalúen y gestionen dichas interfaces.

2.3.7 Aplicaciones del modelo "queso suizo" a la gestión de la seguridad operacional

2.3.7.1 El modelo de "queso suizo" puede utilizarse como guía de análisis tanto por los Estados como por los proveedores de servicios examinando más allá de los individuos involucrados en un incidente o peligro identificado, para determinar las circunstancias institucionales que pueden haber permitido que se manifestara la situación en cuestión. Puede aplicarse durante la SRM, la supervisión de la seguridad operacional, auditorías internas, gestión de cambios e investigaciones de seguridad operacional. En cada caso, el modelo puede aplicarse para considerar cuáles de las defensas de la organización son en verdad eficaces, cuáles podrían penetrarse o haberse penetrado y cómo podría beneficiarse el sistema mediante defensas adicionales. Una vez identificadas, cualesquiera debilidades en las defensas podrían reforzarse para proteger contra futuros accidentes a incidentes.

2.3.7.2 En la práctica, el suceso de que se trate penetrará las defensas en la dirección de la flecha (peligros a pérdida) según se muestra en la Figura 2-3. Las evaluaciones de la situación se realizarán en sentido opuesto, en este caso de pérdidas a peligros. Los accidentes de aviación reales normalmente comprenderán un cierto grado de complejidad adicional. Hay modelos más perfeccionados que pueden ayudar a Estados y proveedores de servicios a comprender cómo y por qué suceden los accidentes.

2.3.8 La desviación de la práctica

2.3.8.1 La teoría de Scott A. Snook sobre la desviación de la práctica se utiliza para comprender cómo la actuación de cualquier sistema se "desvía" respecto de su diseño original. Con frecuencia, las tareas, procedimientos y equipo se diseñan y planifican inicialmente en un entorno teórico, en condiciones ideales, con la hipótesis implícita de que casi todo puede predecirse y controlarse y que todo funciona según lo previsto. Normalmente esto se basa en tres suposiciones fundamentales, a saber:

a) está disponible la tecnología necesaria para lograr las metas de producción del sistema;

b) las personas están capacitadas, son competentes y están motivadas para operar correctamente la tecnología, según lo previsto; y

c) reglamentos y procedimientos indicarán el comportamiento humano y del sistema.

Estas suposiciones son el trasfondo del rendimiento del sistema base (o ideal), y pueden representarse gráficamente como una línea recta a partir de la fecha de implantación operacional, como se muestra en la Figura 2-4.

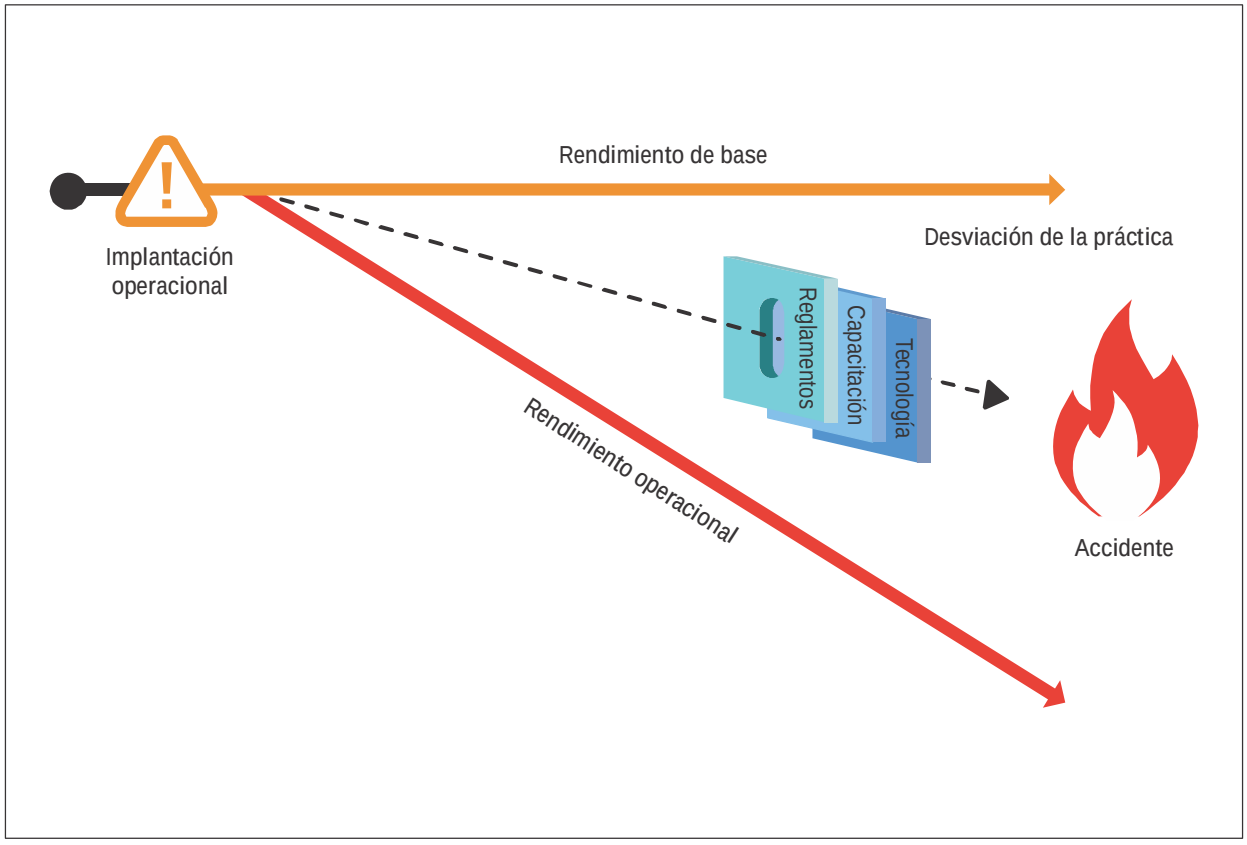

Figura 2-4. Concepto de desviación de la práctica

2.3.8.2 Una vez implantado operacionalmente, el sistema debería actuar idealmente según el diseño, siguiendo el rendimiento de base (línea naranja) la mayor parte del tiempo. En realidad, el rendimiento operacional es diferente del rendimiento de base, como consecuencia de las operaciones en un entorno complejo, siempre cambiante y normalmente exigente (línea roja). Dado que la desviación es una consecuencia de la práctica diaria, se le conoce como "desviación de la práctica". El término "desviación" se refiere en este contexto al alejamiento gradual desde un curso definido debido a influencias externas.

2.3.8.3 Snook afirma que la desviación de la práctica es inevitable en cualquier sistema, sin importar cuan cuidadosa y bien pensada haya sido la planificación del diseño. Los siguientes son algunos de los motivos de la desviación de la práctica:

a) tecnología que no siempre funciona como se predice;

b) procedimientos que no pueden ejecutarse según lo planificado bajo ciertas condiciones operacionales;

c) introducción de cambios al sistema, como la adición de nuevos componentes;

d) interacciones con otros sistemas;

e) cultura de seguridad operacional;

f) adecuación (o inadecuación) de los recursos (p. ej., equipo de apoyo);

g) enseñanzas obtenidas de éxitos y fallas para mejorar las operaciones, y así sucesivamente.

2.3.8.4 En realidad, a pesar de las deficiencias del sistema, las personas harán que el sistema funcione diariamente, aplicando adaptaciones (o soluciones) locales y estrategias personales. Estas soluciones pueden sortear o circunvalar la protección de controles de riesgo de seguridad operacional y defensas correspondientes existentes.

2.3.8.5 Las actividades de aseguramiento de la seguridad operacional, como auditorías, observaciones y vigilancia de los SPI pueden contribuir a revelar comportamientos que se desvían de la práctica. El análisis de la información sobre seguridad operacional para determinar las razones de dicha desviación contribuye a mitigar los riesgos de seguridad operacional. Cuanto más cerca del inicio de la implantación operacional se identifique la desviación de la práctica, más fácil será para la organización llevar a cabo una intervención. En los Capítulos 8 y 9, respectivamente, figura más información sobre aseguramiento de la seguridad operacional para Estados y proveedores de servicios.

2.4 EL DILEMA DE LA GESTIÓN

2.4.1 En una organización comprometida con el suministro de servicios, los riesgos de producción/rentabilidad y seguridad operacional están vinculados. Una organización debe mantener su rentabilidad para continuar funcionando mediante el equilibrio de la producción con riesgos de seguridad operacional aceptables (y los costos involucrados en la aplicación de controles de riesgos de seguridad operacional). Los controles de riesgos de seguridad operacional típicos son la tecnología, la instrucción, los procesos y los procedimientos. Para el Estado, los controles de riesgos de seguridad operacional son similares, es decir, la instrucción del personal, el uso adecuado de la tecnología, la vigilancia eficaz y los procesos y procedimientos internos que respaldan la vigilancia. La implementación de los controles de riesgos de seguridad operacional tiene un precio – dinero, tiempo, recursos – y el objetivo de los controles de riesgos de seguridad operacional es normalmente el mejoramiento del rendimiento en materia de seguridad operacional, y no el rendimiento en cuanto a la producción. No obstante, algunas inversiones en "protección" también pueden mejorar la "producción" mediante la reducción de accidentes e incidentes y, con ello, sus costos conexos.

2.4.2 El espacio de seguridad operacional es una metáfora para la zona donde una organización equilibra la producción y la rentabilidad deseadas manteniendo al mismo tiempo la protección de la seguridad operacional necesaria mediante controles de riesgos de seguridad operacional. Por ejemplo, un proveedor de servicios puede querer invertir en equipo nuevo. Este nuevo equipo puede proporcionar simultáneamente las necesarias mejoras de eficiencia así como mayor fiabilidad y rendimiento de seguridad operacional. Esta toma de decisiones entraña una evaluación de las ventajas para la organización así como de los riesgos de seguridad operacional involucrados. La asignación de recursos excesivos para la protección o los controles de riesgos puede causar que la actividad sea poco rentable, lo que pone en peligro la viabilidad de la organización.

2.4.3 Por otro lado, la asignación excesiva de recursos para la producción a expensas de la protección puede tener consecuencias sobre el producto o servicio y, en última instancia, puede producir un accidente. Por lo tanto, es fundamental que se defina un límite de seguridad operacional que proporcione la alerta temprana de la existencia o el desarrollo de una asignación de recursos desequilibrada. Las organizaciones utilizan sistemas de gestión financiera para reconocer cuando se están acercando demasiado a la bancarrota y aplican la misma lógica y herramientas empleadas en la gestión de la seguridad operacional para observar su rendimiento en materia de seguridad operacional. Esto permite que la organización funcione en forma rentable y segura dentro del espacio de seguridad operacional. En la Figura 2-5 se presenta una ilustración de los límites del espacio de seguridad operacional de una organización. Las organizaciones deben observar y gestionar continuamente su espacio de seguridad operacional dado que los riesgos de seguridad y las influencias externas cambian con el tiempo.

2.4.4 La necesidad de equilibrar la rentabilidad y la seguridad operacional (o la producción y protección) se ha convertido en un requisito fácilmente comprendido y aceptado desde la perspectiva del proveedor de servicios. Este equilibrio es igualmente aplicable a la gestión de la seguridad operacional por el Estado, dado que el requisito de equilibrar los recursos necesarios para las funciones de protección del Estado que incluyen la certificación y la supervisión.

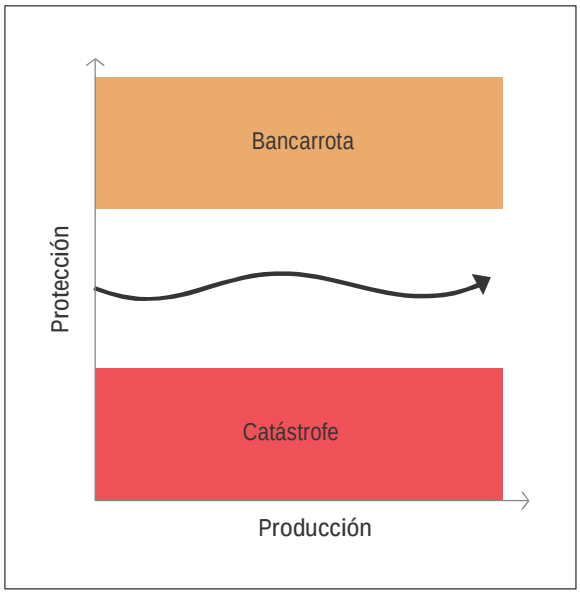

Figura 2-5. Concepto de espacio de seguridad operacional

2.5 GESTIÓN DE RIESGOS DE SEGURIDAD OPERACIONAL

La gestión de riesgos de seguridad operacional (SRM) es un componente fundamental de la gestión de la seguridad operacional y comprende la identificación de peligros, la evaluación de riesgos de seguridad operacional, la mitigación de dichos riesgos y la aceptación de los mismos. La SRM es una actividad continua debido a que el sistema de aviación cambia constantemente, pueden introducirse nuevos peligros y algunos peligros y riesgos de seguridad operacional conexos pueden cambiar con el tiempo. Además, la eficacia de las estrategias de mitigación de riesgos de seguridad operacional implementadas debe vigilarse para determinar si se requieren ulteriores medidas.

2.5.1 Introducción a los peligros

2.5.1.1 En la aviación, los peligros pueden considerarse como la posibilidad latente de que ocurran daños que está siempre presente en una forma u otra en el sistema o su entorno. Este potencial de daño puede aparecer en formas diferentes, por ejemplo como una condición natural (p. ej., terreno) o un aspecto técnico (p. ej., señalización de las pistas).

2.5.1.2 Los peligros constituyen una parte inevitable de las actividades aeronáuticas, pero su manifestación y posibles consecuencias adversas pueden abordarse mediante estrategias de mitigación que apuntan a contener la posibilidad de que el peligro conduzca a una condición insegura. La aviación puede coexistir con los peligros en la medida en que estos estén controlados. La identificación de peligros es el primer paso en el proceso SRM. Precede a la evaluación de los riesgos de seguridad operacional y requiere una clara comprensión de los peligros y sus consecuencias conexas.

2.5.2 Comprensión de los peligros y sus consecuencias

2.5.2.1 La identificación de los peligros se centra en las condiciones u objetos que podrían provocar o contribuir a la operación insegura de las aeronaves o del equipo relacionado con la seguridad operacional de la aviación, así como sus productos y servicios (en los párrafos siguientes se presenta orientación sobre la distinción de peligros directamente pertinentes a la seguridad operacional de la aviación respecto de otros peligros generales o industriales).

2.5.2.2 Por ejemplo, considérese un viento de quince kt, lo que no es necesariamente una condición peligrosa. De hecho, un viento de 15 kt que sopla directamente a lo largo de la pista mejora el despegue de la aeronave y la performance de aterrizaje. Pero si el viento de 15 kt sopla en una dirección perpendicular a la pista, se genera una condición de viento de costado o transversal que puede resultar peligrosa para las operaciones. Esto se debe a su potencial de contribuir a la inestabilidad de la aeronave. La reducción del control podría conducir a un incidente, como una salida de pista lateral.

2.5.2.3 Existe una tendencia común de confundir los peligros con sus consecuencias. Una consecuencia es un resultado que puede ser activado por un peligro. Por ejemplo, una salida de pista (aterrizaje largo) es una consecuencia posible relacionada con el peligro de una pista contaminada. Al definir claramente el peligro primero, se puede identificar más prontamente las posibles consecuencias.

2.5.2.4 En el ejemplo de viento de costado anterior, un resultado inmediato del peligro sería la pérdida de control lateral seguida de una posterior salida de la pista. La consecuencia final podría ser un accidente. El potencial de daño de un peligro se materializa mediante una o muchas consecuencias. Es importante que las evaluaciones de los riesgos de seguridad operacional identifiquen todas las consecuencias posibles. Las consecuencias más extremas, como la pérdida de vidas humanas, deberían diferenciarse de las que tienen carácter más leve, como los incidentes de aeronaves, el aumento de la carga de trabajo de la tripulación de vuelo o la incomodidad de los pasajeros. La descripción de las consecuencias facilita la evaluación de los riesgos y el ulterior desarrollo e implementación de estrategias de mitigación mediante la priorización y asignación de recursos. Una identificación de peligros adecuada genera una evaluación más precisa de los riesgos de seguridad operacional.

Identificación y priorización de peligros

2.5.2.5 Los peligros existen en todos los niveles de la organización y son detectables a partir de muchas fuentes como los sistemas de notificación, inspecciones, auditorías, reuniones de intercambio de ideas y opiniones de expertos. El objetivo es identificar en forma proactiva los peligros antes de que produzcan accidentes, incidentes u otros sucesos relacionados con la seguridad operacional. Un mecanismo importante para la identificación proactiva de peligros es un sistema de notificación voluntaria de seguridad operacional. En el Capítulo 5 figura orientación adicional sobre los sistemas de notificación voluntaria. La información recogida mediante tales sistemas puede complementarse con las observaciones o constataciones registradas durante inspecciones de rutina en el sitio o las auditorías de la organización.

2.5.2.6 Los peligros también pueden identificarse a partir de la revisión o el estudio de los informes de investigaciones tanto internas como externas. La consideración de los peligros al examinar informes de investigaciones de accidentes o incidentes es una buena manera de mejorar el sistema de identificación de peligros de la organización. Esto es particularmente importante cuando la cultura de seguridad operacional de la organización no está lo suficientemente madura como para respaldar un sistema de notificación voluntaria de peligros eficaz o en pequeñas organizaciones con sucesos o informes limitados. Una forma importante de obtener información sobre peligros específicos relacionados con operaciones y actividades es recurrir a fuentes externas como la OACI, asociaciones comerciales u otros órganos internacionales.

2.5.2.7 La identificación de peligros también puede considerar peligros generados fuera de la organización y peligros que escapan al control directo de la organización, como las condiciones meteorológicas extremas o las cenizas volcánicas. El conocimiento de peligros relacionados con los riesgos de seguridad operacional emergentes constituye también un aspecto importante para que las organizaciones puedan prepararse a fin de enfrentar situaciones que puedan ocurrir.

2.5.2.8 Al identificar peligros debería tenerse en cuenta lo siguiente:

a) descripción del sistema;

b) factores de diseño, incluyendo diseño de equipo y tareas;

c) limitaciones de la actuación humana (p. ej., fisiológicas, sicológicas, físicas y cognitivas);

d) procedimientos y prácticas operacionales, incluyendo documentación y listas de verificación y su validación en condiciones de operación reales;

e) factores de comunicación, incluyendo los medios de difusión, terminología e idioma;

f) factores institucionales, como los relacionados con la contratación, instrucción y retención de personal, compatibilidad de los objetivos de producción y de seguridad operacional, asignación de recursos, presiones de operación y cultura de seguridad operacional corporativa;

g) factores relacionados con el entorno operacional (p. ej., condiciones meteorológicas, ruido y vibraciones ambientales, temperatura e iluminación);

h) factores de vigilancia normativa, incluyendo la aplicación e imposición del cumplimiento de reglamentos así como la certificación de equipo, personal y procedimientos;

i) sistemas de observación del rendimiento que puedan detectar desviaciones de la práctica, desviaciones operacionales o un deterioro de la fiabilidad del producto;

j) factores de la interfaz humano-máquina; y

k) factores relacionados con las interfaces SSP/SMS con otras organizaciones.

Peligros de seguridad, salud y ambiente en el trabajo (OSHE)

2.5.2.9 Los riesgos de seguridad operacional asociados con peligros combinados, que tienen un impacto simultáneo en la seguridad operacional de la aviación, además de OSHE, pueden gestionarse en forma separada (paralela) mediante procesos de mitigación de riesgos con el fin de abordar las consecuencias separadas de la aviación y OSHE, respectivamente. O bien, se puede usar un sistema integrado de mitigación de riesgos de aviación y OSHE para abordar tales peligros combinados. Un ejemplo de peligro combinado es un rayo que impacta en una aeronave en la puerta de tránsito de un aeropuerto. Un inspector de OSHE podría considerar este peligro como "peligro en el lugar de trabajo" (seguridad operacional del personal de tierra/lugar de trabajo). Para un inspector de la seguridad operacional de la aviación, es también un peligro de aviación con el riesgo de dañar la aeronave y la seguridad de los pasajeros. Es importante considerar tanto las consecuencias para OSHE y para la seguridad operacional de la aviación de tales peligros combinados, dado que no son siempre las mismas. El propósito y enfoque de los controles preventivos para OSHE y para las consecuencias de seguridad operacional de la aviación pueden ser diferentes.

Metodologías de identificación de peligros

2.5.2.10 Las dos metodologías principales para identificar peligros son:

a) *Reactiva*. Esta metodología involucra el análisis de resultados o sucesos pasados. Los peligros se identifican mediante la investigación de sucesos de seguridad operacional. Los incidentes y accidentes son indicadores de deficiencias del sistema y, por lo tanto, pueden usarse para determinar los peligros que contribuyeron al suceso.

b) *Proactiva*. Esta metodología involucra el acopio de datos de seguridad de sucesos de consecuencias más leves o de rendimiento de procesos y el análisis de la información de seguridad operacional o de la frecuencia de los sucesos para determinar si un peligro podría conducir a un accidente o incidente. La información sobre seguridad operacional para la identificación proactiva de peligros procede principalmente de programas de análisis de datos de vuelo (FDA), sistemas de notificación de seguridad operacional y de la función de aseguramiento de la seguridad operacional.

2.5.2.11 Los peligros también pueden identificarse mediante análisis de datos de seguridad operacional que identifiquen tendencias adversas y permitan predecir posibles peligros emergentes, etc.

Peligros relacionados con interfaces del SMS con organizaciones externas

2.5.2.12 Las organizaciones deberían también identificar peligros relacionados con sus interfaces de gestión de la seguridad operacional. Siempre que sea posible, esto debería llevarse a cabo como actividad conjunta con las organizaciones interconectadas (en interfaz). La identificación de peligros debería considerar el entorno operacional y las diversas capacidades institucionales (personas, procesos, tecnologías) que podrían contribuir a la prestación segura del servicio o a la disponibilidad, funcionalidad o rendimiento del producto.

2.5.2.13 Como ejemplo, un servicio de escala para una aeronave involucra muchas organizaciones y personal de operaciones que trabajan en la aeronave o en torno a la misma. Probablemente existan peligros relacionados con las interfaces entre el personal de operaciones, su equipo y la coordinación de la actividad del servicio de escala.

2.5.3 Probabilidad del riesgo de seguridad operacional

2.5.3.1 La probabilidad del riesgo de seguridad operacional se define como la probabilidad de que pueda suceder una consecuencia o un resultado de seguridad operacional. Con las siguientes preguntas se puede ayudar a determinar dicha probabilidad:

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

b) ¿Qué otros equipos o componentes del mismo tipo presentan problemas similares?

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

d) ¿Cuál es la exposición del peligro que se considera? Por ejemplo, ¿durante qué porcentaje de la operación se utiliza el equipo o se realiza la actividad?

2.5.3.2 Tener en cuenta los posibles factores subyacentes a estas preguntas contribuirá a evaluar la probabilidad de las consecuencias del peligro en cualquier escenario previsible.

2.5.3.3 Un suceso se considera previsible si cualquier persona razonable podría haber esperado que sucediera dicho tipo de suceso en las mismas circunstancias. Es imposible identificar todos los peligros concebibles o teóricamente probables. Por lo tanto, se requiere un buen juicio para determinar un nivel de detalle apropiado en la identificación de los peligros. Los proveedores de servicios deberían actuar con la debida diligencia al identificar peligros importantes y razonablemente previsibles en relación con su producto o servicio.

Nota.— Con respecto al diseño de productos, se tiene la intención de que el término "previsible" corresponda a su uso en los reglamentos, políticas y orientaciones sobre aeronavegabilidad.

2.5.3.4 La Tabla 1 presenta una clasificación típica de la probabilidad de riesgos de seguridad operacional. La tabla incluye cinco categorías para denotar la probabilidad relacionada con un evento o condición inseguros, la descripción de cada categoría y una asignación de valor a cada una. Este ejemplo utiliza términos cualitativos; también pueden definirse términos cuantitativos a efectos de una evaluación más precisa. Esto dependerá de la disponibilidad de datos de seguridad operacional apropiados y del grado de desarrollo de la organización y la operación.

Tabla 1. Tabla de probabilidad de riesgos de seguridad operacional

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

Nota.— Este es solo un ejemplo. El nivel de detalle y complejidad de las tablas y matrices debe adaptarse a las necesidades y complejidades particulares de cada organización. También se debe tener presente que las organizaciones pueden incluir criterios tanto cualitativos como cuantitativos.

2.5.4 Gravedad del riesgo de seguridad operacional

2.5.4.1 Una vez completada la evaluación de probabilidad, el siguiente paso es evaluar la gravedad del riesgo de seguridad operacional teniendo en cuenta las posibles consecuencias relacionadas con el peligro. La gravedad del

riesgo de seguridad operacional se define como el grado de daño que puede suceder razonablemente como consecuencia o resultado del peligro identificado. La clasificación de la gravedad debería tener en cuenta:

a) muertes o lesiones graves que podrían ocurrir como resultado de:

1) encontrarse en la aeronave;

2) tener contacto directo con cualquier parte de la aeronave, incluyendo las que se hayan desprendido de la misma; o

3) exposición directa al chorro de los reactores; y

b) daños:

1) daños o fallas estructurales sufridos por la aeronave que:

i) afecten adversamente la resistencia estructural, performance o características de vuelo de la aeronave;

ii) requerirían normalmente importantes reparaciones o sustituciones del componente afectado;

2) daños sufridos por el equipo de ATS o aeródromo que:

i) afecten adversamente la gestión de la separación de aeronaves; o

ii) afecten adversamente la capacidad de aterrizaje.

2.5.4.2 La evaluación de la gravedad debería considerar todas las posibles consecuencias relacionadas con un peligro, teniendo en cuenta la peor condición previsible. En la Tabla 2 se presenta una clasificación típica de la gravedad del riesgo de seguridad operacional. Comprende cinco categorías para denotar el nivel de gravedad, la descripción de cada categoría y la asignación de valor a cada una de ellas. Al igual que con la tabla de probabilidad del riesgo de seguridad operacional, esta tabla es solo un ejemplo.

Tabla 2. Ejemplo de gravedad del riesgo de seguridad operacional

Gravedad	*Significado*	*Valor*
Catastrófico	• Aeronave o equipo destruidos • Varias muertes	A
Peligroso	• Gran reducción de los márgenes de seguridad operacional, estrés físico o una carga de trabajo tal que ya no se pueda confiar en que el personal de operaciones realice sus tareas con precisión o por completo • Lesiones graves • Daños importantes al equipo	B
Grave	• Reducción importante de los márgenes de seguridad operacional, reducción en la capacidad del personal de operaciones para tolerar condiciones de operación adversas, como resultado de un aumento en la carga de trabajo o como resultado de condiciones que afecten su eficiencia	C

Gravedad	*Significado*	*Valor*
	• Incidente grave • Lesiones a las personas	
Leve	• Molestias • Limitaciones operacionales • Uso de procedimientos de emergencia • Incidente leve	D
Insignificante	• Pocas consecuencias	E

2.5.5 Tolerabilidad del riesgo de seguridad operacional

2.5.5.1 El índice de riesgo de seguridad operacional se crea mediante la combinación de resultados de las evaluaciones de probabilidad y gravedad. En el ejemplo anterior, se trata de un designador alfanumérico. Las respectivas combinaciones de gravedad/probabilidad se presentan en la matriz de evaluación de riesgos de seguridad operacional de la Tabla 3. Dicha matriz se aplica para determinar la tolerabilidad del riesgo de seguridad operacional. Considérese, por ejemplo, una situación en que la probabilidad del riesgo de seguridad operacional se ha evaluado como ocasional (4), y la gravedad del riesgo de seguridad operacional se ha evaluado como peligrosa (B), la combinación de ambas es el índice de riesgo de seguridad operacional (4B).

Tabla 3. Ejemplo de matriz de riesgos de seguridad operacional

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

Nota.— En la determinación de la tolerabilidad del riesgo de seguridad operacional, deberían tenerse en cuenta la calidad y la fiabilidad de los datos utilizados para la identificación del peligro y la probabilidad del riesgo de seguridad operacional.

2.5.5.2 El índice obtenido de la matriz de evaluación del riesgo de seguridad operacional debe exportarse a la matriz de tolerabilidad del riesgo de seguridad operacional que describe — en forma narrativa — los criterios de tolerabilidad para la organización particular. La Tabla 4 es un ejemplo de tabla de tolerabilidad del riesgo de seguridad

operacional. Al usar el ejemplo anterior, el criterio del riesgo de seguridad operacional evaluado como 4B corresponde a la categoría de “intolerable”. En este caso, el índice de riesgo de seguridad operacional de la consecuencia es inaceptable. Por lo tanto, la organización debería tomar medidas de control de riesgos para reducir:

a) la exposición de la organización a un riesgo en particular, es decir reducir el componente de probabilidad del índice de riesgo a un nivel aceptable;

b) la gravedad de las consecuencias relacionadas con el peligro, es decir, reducir el componente de gravedad del índice de riesgo a un nivel aceptable; o

c) tanto la gravedad como la probabilidad para que el riesgo pueda gestionarse a un nivel aceptable.

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

Tabla 4. Ejemplo de tabla de tolerabilidad del riesgo de seguridad operacional

Rango del índice de riesgo de seguridad operacional	*Descripción del riesgo*	*Medida recomendada*
5A, 5B, 5C, 4A, 4B, 3A	INTOLERABLE	Tomar medidas inmediatas para mitigar el riesgo o suspender la actividad. Realizar la mitigación de riesgos de seguridad operacional prioritaria para garantizar que haya controles preventivos o adicionales o mejorados para reducir el índice de riesgos al rango tolerable.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1ª	TOLERABLE	Puede tolerarse sobre la base de la mitigación de riesgos de seguridad operacional. Puede necesitar una decisión de gestión para aceptar el riesgo.
3E, 2D, 2E, 1B, 1C, 1D, 1E	ACEPTABLE	Aceptable tal cual. No se necesita una mitigación de riesgos posterior.

2.5.6 Evaluación de riesgos relacionados con factores humanos

2.5.6.1 La consideración de los factores humanos tiene particular importancia en la SRM puesto que las personas pueden ser tanto una fuente como una solución de los riesgos de seguridad operacional, a saber:

a) contribuyendo a un accidente o incidente mediante una actuación variable debido a limitaciones humanas;

b) previendo y adoptando medidas apropiadas para evitar una situación peligrosa: y

c) resolviendo problemas, tomando decisiones y adoptando medidas para mitigar los riesgos.

2.5.6.2 Por consiguiente, es importante involucrar a personas con adecuada experiencia en factores humanos en la identificación, evaluación y mitigación de los riesgos.

2.5.6.3 La SRM requiere que se aborden todos los aspectos de los riesgos de seguridad operacional, incluyendo los relacionados con las personas. La evaluación de los riesgos asociados con el desempeño humano es más compleja que la de los factores de riesgo relacionados con la tecnología y el entorno dado que:

a) el desempeño humano es muy variable, con una amplia gama de influencias interactuantes tanto internas como externas al individuo. Muchos de los efectos de la interacción entre estas influencias son difíciles o imposibles de predecir; y

b) las consecuencias del variable desempeño humano serán diferentes según la tarea que se realice y el contexto de la misma.

2.5.6.4 Lo señalado anteriormente complica la forma en que se determina la probabilidad y la gravedad del riesgo. Por consiguiente, la experiencia en factores humanos es muy valiosa para identificar y evaluar los riesgos de seguridad operacional. [La gestión de la fatiga aplicando procesos SMS se aborda en el *Manual para la supervisión de los enfoques de gestión de la fatiga* (Doc 9966)].

2.5.7 Estrategias de mitigación de riesgos de seguridad operacional

2.5.7.1 La mitigación de riesgos de seguridad operacional se conoce a menudo como control de riesgos de seguridad operacional. Los riesgos de seguridad operacional deberían gestionarse a un nivel aceptable mitigándolos mediante la aplicación de adecuados controles de riesgos de seguridad operacional. Esto debería equilibrarse con respecto al tiempo, costos y dificultades de adoptar medidas para reducir o eliminar el riesgo. El nivel de riesgo de seguridad operacional puede disminuirse mediante la reducción de la gravedad de las posibles consecuencias, la probabilidad de que el suceso ocurra o la reducción de la exposición a ese riesgo de seguridad operacional. Es más sencillo y más común reducir dicha probabilidad que reducir la gravedad.

2.5.7.2 Las mitigaciones de riesgos de seguridad operacional son medidas que resultan a menudo en cambios de los procedimientos operacionales, equipo o infraestructura. Las estrategias de mitigación de riesgo de seguridad operacional corresponden a tres categorías:

a) *Evitar*: Se cancela o evita la operación o actividad debido a que los riesgos de seguridad operacional superan los beneficios de continuarla, eliminado así el riesgo de seguridad operacional en su totalidad.

b) *Reducir*: Se reduce la frecuencia de la operación o actividad o se adoptan medidas para reducir la magnitud de las consecuencias del riesgo.

c) *Segregar*: Se toman medidas para aislar los efectos de las consecuencias del riesgo o se introduce capas redundantes de protección contra los riesgos.

2.5.7.3 La consideración de los factores humanos es parte integral de la identificación de mitigaciones eficaces porque se requiere que las personas apliquen la mitigación o las medidas correctivas o contribuyan a las mismas. Por ejemplo, las mitigaciones pueden incluir el uso de procesos o procedimientos. Sin aportes de las personas que los utilizarán en situaciones del “mundo real” o de individuos con experiencia en factores humanos, los procesos o procedimientos elaborados pueden no ser adecuados al propósito en cuestión y resultar en consecuencias imprevistas. Además, deberían considerarse las limitaciones de la actuación humana como parte de toda mitigación de riesgos de seguridad operacional, desarrollando estrategias de captación de errores para tener en cuenta la variabilidad de dicha actuación. En última instancia, esta importante perspectiva de factores humanos tendrá como resultado mitigaciones más completas y eficaces.

2.5.7.4 Una estrategia de mitigación de riesgos de seguridad operacional puede involucrar uno de los enfoques descritos anteriormente o puede incluir múltiples enfoques. Es importante considerar la gama completa de posibles medidas de control para encontrar una solución óptima. La eficacia de cada estrategia alternativa debe evaluarse antes de adoptar decisiones. Cada alternativa de mitigación de riesgos de seguridad operacional propuesta debería examinarse a partir de las perspectivas siguientes:

a) *Eficacia*. El grado en que las alternativas reducen o eliminan los riesgos de seguridad operacional. La eficacia puede determinarse en términos de las defensas técnicas, de instrucción y normativas que puedan reducir o eliminar los riesgos.

b) *Costo/beneficio*. El grado en que las ventajas percibidas de la mitigación superan los costos.

c) *Practicidad*. El grado en que la mitigación puede implementarse y cuán apropiada resulta en términos de recursos tecnológicos, financieros y administrativos disponibles así como de legislación, voluntad política, realidades operacionales, etc.

d) *Aceptabilidad*. El grado en que la alternativa resulta aceptable para las personas que se espera la apliquen.

e) *Cumplimiento*. El grado en que pueda vigilarse el cumplimiento de nuevas reglas, reglamentos o procedimientos operacionales.

f) *Duración*. El grado en que la mitigación pueda ser sostenible y eficaz.

g) *Riesgos de seguridad operacional residuales*. El grado de riesgo de seguridad operacional que permanece después de la implementación de la mitigación inicial y que pueda requerir medidas adicionales de control de riesgos.

h) *Consecuencias involuntarias*. La introducción de nuevos peligros y riesgos de seguridad operacional conexos relacionados con la implementación de una alternativa de mitigación.

i) *Tiempo*. El tiempo requerido para implantar la alternativa de mitigación de riesgo de seguridad operacional.

2.5.7.5 Las medidas correctivas deberían tener en cuenta las defensas que existan y su capacidad o incapacidad de alcanzar un nivel aceptable de riesgo de seguridad operacional. Esto puede resultar en una revisión de evaluaciones de riesgos anteriores que puedan haber sido afectadas por la medida correctiva. Las mitigaciones y controles de riesgos de seguridad operacional deberán verificarse o auditarse para asegurar que son eficaces. Otra forma de observar la eficacia de las mitigaciones es aplicando los SPI. En el Capítulo 4 figura más información sobre la gestión del rendimiento en materia de seguridad operacional y los SPI.

2.5.8 Documentación de la gestión de riesgos de la seguridad operacional

2.5.8.1 Las actividades de gestión de riesgos de seguridad operacional deberían documentarse, incluyendo toda su posición subyacente a la evaluación de la probabilidad y la gravedad, las decisiones adoptadas, y toda medida de mitigación de riesgos emprendidas. Esto puede realizarse utilizando una hoja de cálculo o una tabla. Algunas organizaciones pueden utilizar una base de datos u otro soporte lógico donde puedan almacenarse y analizarse grandes volúmenes de datos de seguridad operacional o de información sobre seguridad operacional.

2.5.8.2 El mantenimiento de un registro de peligros identificados minimiza la probabilidad de que la organización pierda de vista sus peligros conocidos. Cuando se identifican nuevos peligros, pueden compararse con los peligros conocidos que figuran en el registro para ver si ya han sido registrados y qué medidas se adoptaron para mitigarlos. Los registros de peligros se presentan normalmente en forma de tablas y típicamente incluyen lo siguiente: el peligro, posibles consecuencias, evaluación de riesgos conexos, fecha de identificación, categoría del peligro, breve descripción, cuándo y dónde se aplica, quién o quiénes lo han identificado y qué medidas se adoptaron para mitigar los riesgos.

2.5.8.3 Las herramientas y procesos de toma de decisiones sobre riesgos de seguridad operacional pueden utilizarse para mejorar la repetición y justificación de las decisiones tomadas por los encargados de adoptar decisiones de seguridad operacional en la organización. En la Figura 2-6 se proporciona un ejemplo de ayuda para tomar decisiones sobre riesgos de seguridad operacional.

2.5.9 Análisis de costo-beneficios

El análisis de costo-beneficios o rentabilidad se realiza normalmente durante las actividades de mitigación de riesgos de seguridad operacional. Se asocia comúnmente con la gestión empresarial, como una evaluación de impactos normativos o procesos de gestión de proyectos. No obstante, puede que haya situaciones donde una evaluación de riesgos de seguridad operacional tenga consecuencias financieras de importancia. En tales situaciones, puede justificarse un análisis de costo-beneficios o un proceso de rentabilidad complementarios para respaldar la evaluación de los riesgos de seguridad operacional. Esto asegurará que el análisis de rentabilidad o la justificación de medidas de control de riesgos recomendadas han tenido en cuenta las repercusiones financieras conexas.

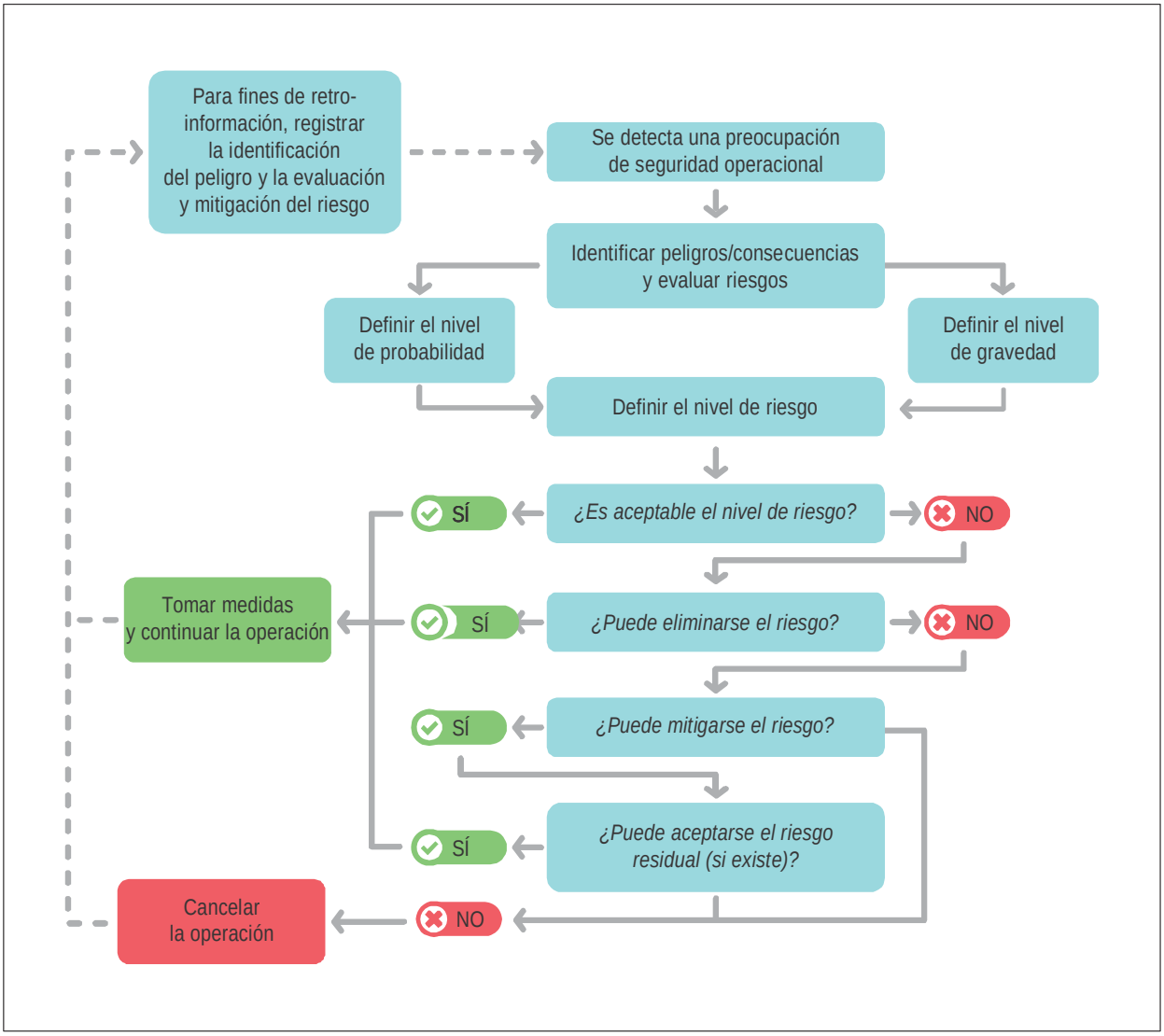

Figura 2-6. Ayuda para tomar decisiones sobre riesgos de seguridad operacional