

# Capítulo 1

## INTRODUCCIÓN

### 1.1 CONCEPTO DE SEGURIDAD OPERACIONAL

1.1.1 La seguridad operacional procura mitigar en forma proactiva los riesgos de seguridad operacional antes de que resulten en accidentes e incidentes de aviación. Mediante la implementación de la gestión de la seguridad operacional, los Estados pueden manejar sus actividades de seguridad operacional en forma más disciplinada, integradora y concentrada. La clara comprensión de su función y contribución respecto de la seguridad de las operaciones permite que el Estado y su industria de aviación prioricen medidas para enfrentar los riesgos de seguridad operacional y gestionar en forma más eficaz sus recursos para alcanzar el beneficio óptimo de la seguridad operacional de la aviación.

1.1.2 La eficacia de las actividades de gestión de la seguridad operacional del Estado se fortalece cuando se implementan en forma oficial e institucionalizada mediante un programa estatal de seguridad operacional (SSP) y sistemas de gestión de la seguridad operacional (SMS) para sus proveedores de servicios. El programa estatal de seguridad operacional, combinado con los SMS de sus proveedores de servicios, trata sistemáticamente los riesgos de seguridad operacional, mejora el rendimiento en materia de seguridad operacional de cada proveedor de servicios y, en forma colectiva, mejora el rendimiento en materia de seguridad operacional del Estado.

1.1.3 Cada Estado elabora y mantiene su SSP como enfoque estructurado para contribuir a la gestión de su rendimiento en materia de seguridad operacional de la aviación. El historial actual de seguridad operacional de la aviación se ha logrado mediante un enfoque tradicional basado en el cumplimiento y debería continuar tratándose como el fundamento del SSP. Como tal, los Estados deberían asegurar que cuentan con sistemas eficaces de vigilancia de la seguridad operacional. En el Capítulo 8 figura más información sobre el SSP.

1.1.4 Los Estados exigirán que los proveedores de servicios bajo su autoridad elaboren y mantengan un SMS, según se establece en el Anexo 19 — *Gestión de la seguridad operacional*, para mejorar en forma continua su rendimiento en materia de seguridad operacional mediante la identificación de peligros, acopio y análisis de datos, y evaluación y gestión continuas de los riesgos de seguridad operacional (véase el párrafo 1.2 por detalles sobre aplicabilidad del SMS). En el Capítulo 9 figura más información sobre la implementación de SMS.

1.1.5 Los objetivos del *Plan global para la seguridad operacional de la aviación* (GASP, Doc 10004) de la OACI estipulan que los Estados establezcan sistemas robustos y sostenibles de vigilancia de la seguridad operacional y que desarrollen los mismos en forma progresiva para alcanzar medios más perfeccionados de gestionar el rendimiento en materia de seguridad operacional. Estos objetivos corresponden a los requisitos de la OACI para la implementación de SSP por los Estados y de SMS por los proveedores de servicios.

1.1.6 Este enfoque de la seguridad operacional basado en el rendimiento ofrece mejoras dado que se concentra en el logro de resultados deseados en vez de concentrarse únicamente en determinar si el Estado cumple o no las disposiciones correspondientes. No obstante, es importante señalar que la aplicación de un enfoque del rendimiento en materia de seguridad operacional requiere colaboración puesto que requiere esfuerzos de parte de la industria de la aviación para elaborar medios apropiados de alcanzar los resultados especificados y, con respecto a los Estados, para evaluar el enfoque de cada proveedor de servicio.

### 1.1.7 BENEFICIOS DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

La implementación de la gestión de la seguridad operacional tiene muchos beneficios, entre ellos los siguientes:

- a) *Fortalecimiento de la cultura de seguridad operacional* – La cultura de seguridad operacional de una organización puede fortalecerse poniendo en evidencia el compromiso de la administración y haciendo que el personal participe activamente en la gestión de los riesgos de seguridad operacional. Cuando la administración otorga activamente carácter prioritario a la seguridad operacional ello es normalmente bien recibido por el personal y pasa a constituir parte de las operaciones normales.
- b) *Enfoque documentado y basado en procesos para garantizar la seguridad operacional* – Establece un enfoque claro y documentado para lograr operaciones seguras y que es comprendido por el personal y puede explicarse fácilmente a terceros. Además, una definición clara de un rendimiento básico permite introducir cambios controlados cuando se mejora continuamente el programa o sistema de seguridad operacional, lo que ayuda a la organización a optimizar los recursos necesarios para implantar cambios.
- c) *Mejor comprensión de interfaces y relaciones de seguridad operacional* – El proceso de documentar y definir interfaces en la gestión de la seguridad operacional puede beneficiar la comprensión por la organización de las relaciones entre procesos, lo que conduce a una mejor comprensión del proceso completo y a la presentación de oportunidades para aumentar la eficiencia.
- d) *Detección temprana mejorada de los peligros de seguridad operacional* – Mejora la capacidad del Estado o proveedor de servicios de detectar problemas de seguridad operacional emergentes, lo que puede prevenir accidentes e incidentes mediante la identificación proactiva de peligros y la gestión de los riesgos de seguridad operacional.
- e) *Toma de decisiones de seguridad operacional basada en datos* – Mejora la capacidad del Estado o proveedor de servicios de reunir datos de seguridad operacional con fines de análisis de ésta. Si se piensa en forma estratégica para determinar las preguntas que deben responderse, la información sobre seguridad operacional resultante puede ayudar a los encargados de tomar decisiones, en tiempo casi real, a adoptar decisiones válidas y mejor fundamentadas. Un aspecto importante de esta toma de decisiones es la asignación de recursos a las áreas de mayor preocupación o necesidad.
- f) *Comunicación mejorada sobre seguridad operacional* – Proporciona un lenguaje de seguridad operacional común a través de una organización y de la industria. Un lenguaje de seguridad operacional común es una herramienta fundamental para el desarrollo de una comprensión común de los objetivos y logros de la organización en materia de seguridad operacional. En particular, proporciona un reconocimiento de los objetivos de seguridad operacional de la organización y de sus indicadores de rendimiento en materia de seguridad operacional (SPI) y de las metas de rendimiento en materia de seguridad operacional (SPT), que establecen la orientación y la motivación para ésta. El personal será más consciente del rendimiento de la organización y de los progresos alcanzados hacia el logro de los objetivos de seguridad operacional definidos, así como de la forma en que contribuyen al éxito de la organización. El lenguaje de seguridad operacional común permite que los proveedores de servicios con múltiples actividades aeronáuticas reúnan información sobre seguridad operacional a través de entidades orgánicas. Esto es necesario para apoyar la gestión de interfaces a través de todo el sistema aeronáutico.
- g) *Pruebas de que la seguridad operacional constituye una prioridad* – Demuestran la forma en que la administración apoya y habilita la seguridad operacional, la forma en que se identifican y gestionan los riesgos de seguridad y la forma en que se mejora continuamente el rendimiento de la seguridad operacional, resultando en una mayor confianza de parte de la comunidad aeronáutica, tanto interna como externa a la organización. Esto también resulta en una confianza del personal respecto del

rendimiento en materia de seguridad operacional de la organización, que puede llevar a una creciente atracción y retención de personal de elevado calibre. También permite que los Estados y organizaciones regionales de vigilancia de la seguridad operacional (RSOO) desarrollen confianza en el rendimiento de los proveedores de servicios en materia de seguridad operacional.

- h) *Posibles ahorros financieros* – Puede permitir que algunos proveedores de servicios estén en condiciones de obtener descuentos en sus primas de seguros o una reducción de las primas de seguro de indemnización de sus empleados sobre la base de los resultados de sus SMS.
- i) *Aumento de la eficiencia* – Posible reducción del costo de las operaciones mediante la exposición de las ineficiencias en procesos y sistemas existentes. La integración con otros sistemas de gestión internos o externos puede también aportar economías sobre costos adicionales.
- j) *Posibilidad de evitar costos* – Mediante la identificación proactiva de peligros y la gestión de riesgos de seguridad operacional (SRM), pueden evitarse los costos en que se incurre debido a accidentes e incidentes. En tales casos, los costos directos pueden comprender: lesiones corporales, daños a la propiedad, reparación de equipo y retrasos. Los costos indirectos pueden comprender: acciones judiciales, lucro cesante y reputación dañada, excedentes de repuestos, herramientas e instrucción, aumento de las primas de seguro, disminución de productividad del personal, recuperación y limpieza de equipo, pérdida de uso de equipo que lleve a sustitución de equipo a corto plazo e investigaciones internas.

## 1.2 APLICABILIDAD DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

En el Capítulo 3 del Anexo 19 se esbozan las responsabilidades del Estado en materia de gestión de la seguridad operacional que incluyen exigir a los proveedores de servicios identificados en los SARPS que implementen SMS. Las disposiciones relativas a la implementación de SMS por proveedores de servicios figuran en el Capítulo 4 y en el Apéndice 2 del Anexo 19.

### 1.2.1 Aplicabilidad del SMS

1.2.1.1 La evaluación para determinar la aplicabilidad del SMS para la Enmienda 1 del Anexo 19 se basó en un conjunto de criterios. Se prevé que estos mismos criterios sean utilizados periódicamente por la OACI y por el Grupo de expertos sobre gestión de la seguridad operacional (SMP) para reevaluar la necesidad de extender la aplicabilidad a otras organizaciones aeronáuticas.

#### ***Enfoque de sistema total para la seguridad operacional***

1.2.1.2 El enfoque de sistema total para la seguridad operacional considera a la industria de la aviación en su totalidad como un sistema. Todos los proveedores de servicios y sus sistemas para la gestión de la seguridad operacional se consideran como subsistemas. Esto permite que el Estado considere las interacciones y las relaciones causa-efecto en la totalidad del sistema. A menudo resulta imposible o poco práctico construir todos los sistemas de seguridad operacional en la misma forma. Por lo tanto, una preocupación principal para Estados y proveedores de servicios es la mejor forma de gestionar las interfaces entre sistemas diferentes en interacción.

1.2.1.3 Al examinar la aplicabilidad de los SMS, se tuvo en cuenta la relación entre los proveedores de servicios que ya cuentan con un SMS con arreglo al Anexo 19 y otras organizaciones con actividades aeronáuticas. La aplicación del SMS debería reducir el riesgo de que existan brechas o superposiciones de seguridad operacional, y no aumentar los riesgos de seguridad operacional mediante un interfuncionamiento disminuido.

### **Consecuencias de la subcontratación**

1.2.1.4 Para que la SRM sea eficaz en el ámbito de los proveedores de servicios es importante definir con claridad las responsabilidades para la identificación de peligros y la gestión de los riesgos de seguridad operacional conexos en la totalidad de la cadena de servicios dentro del sistema, sin brechas ni superposiciones. Cuando un proveedor de servicios con SMS contrata una organización no sujeta a un SMS, los peligros y riesgos de seguridad operacional que podrían introducirse por el contratista son tratados por el SMS del proveedor de servicios. Esto impone responsabilidades SRM adicionales en el proveedor de servicios para asegurar que se tiene conocimiento de los riesgos de seguridad operacional inducidos por las actividades de sus contratistas. En el Capítulo 2 figura más información sobre la SRM.

### **Control normativo de los riesgos de seguridad operacional**

1.2.1.5 Los Estados deberían evaluar si la legislación y reglamentos existentes tratan eficazmente los peligros que la actividad entraña. Podría ocurrir que los requisitos existentes proporcionen suficiente mitigación de riesgos de seguridad operacional y la imposición del requisito de contar con SMS a las organizaciones a las que no se aplica el Anexo 19 puede no resultar en importantes beneficios en materia de seguridad operacional.

## **1.2.2 Ampliación de la aplicabilidad discrecional de SMS**

1.2.2.1 Los criterios de aplicabilidad mencionados anteriormente también pueden servir de orientación a los Estados cuando consideren una ampliación de la aplicabilidad del SMS más allá de la definición del Anexo 19 o la promoción de una implementación voluntaria. La aplicabilidad discrecional del SMS debería considerarse seriamente. La decisión de ampliar la aplicabilidad del SMS a sectores o proveedores de servicios debería tener en cuenta los riesgos de seguridad operacional identificados en el Estado y, si se toma la decisión de hacerlo, la implementación del SMS debería observarse como parte del SSP. Antes de exigir SMS, los Estados deben considerar si:

- a) existen otras opciones viables para alcanzar las mejoras deseadas en el rendimiento en materia de seguridad operacional; y
- b) se dispone de recursos suficientes para que el Estado y el sector industrial implementen y observen el SMS. En particular, debe considerarse las posibles consecuencias para el personal y el reto potencial de adquirir e integrar las habilidades y conocimientos necesarios.

1.2.2.2 Cada Estado debería considerar el nivel aceptable del rendimiento en materia de seguridad operacional (ALoSP) en toda su industria e instituir un plan de aplicabilidad del SMS que tenga la mayor probabilidad de alcanzar los objetivos de seguridad operacional del Estado. Es probable que el plan de aplicabilidad del SMS evolucione en forma paralela a los del Estado.

## **1.2.3 Responsabilidad de la gestión de la seguridad operacional**

No existen en el Anexo 19 disposiciones dirigidas a transferir al Estado las responsabilidades del proveedor o explotador de servicios de aviación. Los Estados cuentan con muchas herramientas para gestionar la seguridad operacional dentro de su sistema. Como parte de su SSP, cada Estado debería considerar las mejores opciones para la vigilancia de las actividades aeronáuticas que puedan no corresponder a la órbita de los actuales Anexos de la OACI así como la vigilancia de actividades nuevas o emergentes.

## **1.2.4 Aplicabilidad de los proveedores de servicios estatales o militares**

1.2.4.1 En algunos Estados, la función de proveedor de servicios es proporcionada por la administración pública civil o por el sector militar. Algunos proveedores de servicios civiles proporcionan servicios al sector militar bajo contrato, y algunas organizaciones militares proporcionan servicios civiles. Independientemente del arreglo en cuestión, debería

exigirse al proveedor de servicios para el sector civil del Estado que cumpla con todos los SARPS aplicables de la OACI, incluyendo los requisitos SMS del Anexo 19 sin importar el carácter específico de dicha organización. La descripción del sistema estatal o del proveedor de servicios debería tener en cuenta las funciones de esas organizaciones y sus relaciones mutuas. El ejecutivo responsable del proveedor de servicios, ya sea civil o militar, debería estar en condiciones de explicar los arreglos en cuestión y la forma en que se gestionan los riesgos de seguridad operacional. En pocas palabras, los proveedores de servicios deberían gestionar la seguridad operacional sin importar los arreglos organizativos.

1.2.4.2 Donde el Estado funciona como proveedor de servicios debería existir una clara separación entre sus funciones como proveedor de servicios y las correspondientes a la autoridad normativa estatal. Esto se logra mediante una clara definición de funciones y responsabilidades del personal de la autoridad estatal y de provisión de servicios para evitar posibles conflictos de intereses.

### 1.2.5 Seguridad, salud y ambiente en el trabajo y seguridad operacional de la aviación

La seguridad, salud y ambiente en el trabajo (OSHE) [también denominada salud y seguridad laboral (OHS) o salud y seguridad en el lugar de trabajo (WHS)] es un campo que abarca la seguridad, la salud y el bienestar de los trabajadores. La diferencia principal entre el sistema de gestión de la seguridad operacional de la aviación y el sistema OSHE es la intención de cada uno. En muchos Estados los empleadores tienen la obligación jurídica de ocuparse en forma razonable de la salud y seguridad de sus empleados. La intención de los programas OSHE es cumplir las obligaciones jurídicas y éticas de los empleadores mediante el fomento de un ambiente laboral seguro y saludable. Estos aspectos se tratan normalmente por un órgano gubernamental diferente del que se ocupa de los asuntos aeronáuticos. Por ello, el Anexo 19, Capítulo 2, *Aplicación*, se concentra intencionalmente en las “funciones de gestión de la seguridad operacional que atañen, o sirven de apoyo directo, a la operación segura de las aeronaves”.

## 1.3 IMPLEMENTACIÓN DE LA GESTIÓN DE LA SEGURIDAD OPERACIONAL

1.3.1 El establecimiento de una base sólida es fundamental para el logro de una implementación eficaz de la gestión de la seguridad operacional. Los aspectos siguientes deberían tratarse como primeros pasos para la implantación de SSP o SMS:

- a) *Compromiso de la administración superior*: Es fundamental que la administración superior de todos los órganos aeronáuticos del Estado se comprometa a implementar la gestión de la seguridad operacional en forma eficaz.
- b) *Cumplimiento de los requisitos prescriptivos*: El Estado debería asegurar que cuenta con un sistema de vigilancia de la seguridad operacional bien desarrollado para el otorgamiento de licencias, certificación, autorización y aprobación de individuos y organizaciones que realizan actividades aeronáuticas en el Estado, incluyendo personal técnico cualificado. Los proveedores de servicios deberían asegurar que cuentan con procesos para garantizar el continuo cumplimiento de los requisitos prescriptivos establecidos.
- c) *Régimen de cumplimiento*: El Estado debería establecer una política y marcos para imponer el cumplimiento a efectos de permitir que las partes gestionen y resuelvan desviaciones y transgresiones menores.
- d) *Protección de la información sobre seguridad operacional*: Es fundamental que los Estados instituyan un marco jurídico de protección para asegurar la disponibilidad continua de datos de seguridad operacional e información sobre seguridad operacional.

### 1.3.2 Descripción del sistema

La descripción del sistema consiste en un resumen de los procesos, actividades e interfaces de la organización (Estado o proveedor de servicios) que deben abordarse para la identificación de peligros y evaluación de riesgos de seguridad operacional abarcadas en sus sistemas de seguridad operacional. En ella se describe el sistema de aviación dentro del que funciona la organización así como las diversas entidades y autoridades involucradas. También comprende las interfaces dentro de la organización, así como aquellas con organizaciones externas que contribuyen a la prestación segura de los servicios. La descripción del sistema proporciona un punto de partida para la implementación del SSP/SMS. En los Capítulos 8 y 9, respectivamente, figura más información sobre la descripción del sistema para los Estados y los proveedores de servicios.

### 1.3.3 Interfaces

1.3.3.1 Cuando los Estados y los proveedores de servicios consideren la implementación de la gestión de la seguridad operacional es importante tener en cuenta los riesgos de seguridad operacional inducidos por las entidades interrelacionadas. Las interfaces pueden ser internas (p. ej., entre los departamentos de operaciones y de mantenimiento o los departamentos de finanzas, recursos humanos o asuntos jurídicos), o pueden ser externas (p. ej., otro Estado, proveedores de servicios o servicios contratados). Los Estados y los proveedores de servicios tienen mayor control sobre los riesgos de seguridad operacional conexos cuando se identifican y gestionan las interfaces. Estas se definen como parte de la descripción del sistema.

#### ***Evaluación de las consecuencias de las interfaces para la seguridad operacional***

1.3.3.2 Una vez que el Estado o el proveedor de servicios ha identificado sus interfaces, el riesgo de seguridad operacional planteado por cada interfaz se evalúa aplicando los procesos de evaluación de riesgos de seguridad operacional existentes en la organización (véanse detalles en el Capítulo 2). Sobre la base de los riesgos de seguridad operacional identificados, el Estado o el proveedor de servicios puede tener en cuenta trabajar con otras organizaciones para determinar una estrategia apropiada de control de riesgos de seguridad operacional. Las organizaciones que trabajan en colaboración pueden estar en condiciones de identificar más peligros de las interfaces, evaluar los riesgos de seguridad operacional conexos y determinar controles mutuamente apropiados. La colaboración es muy conveniente porque la percepción de los riesgos de seguridad operacional puede ser diferente entre diferentes organizaciones.

1.3.3.3 También es importante reconocer que cada organización involucrada es responsable de identificar y gestionar los peligros que puedan afectarla. El carácter crítico de la interfaz puede ser diferente para cada organización. Cada organización puede aplicar razonablemente diferentes clasificaciones del riesgo de seguridad operacional y tener diferentes prioridades en la materia (en términos de rendimiento de seguridad operacional, recursos, tiempo).

#### ***Observación y gestión de las interfaces***

1.3.3.4 Los Estados y los proveedores de servicios son responsables de la observación continua y la gestión de sus interfaces para asegurar que los servicios de proporcionan en forma segura. Un enfoque eficaz para las interfaces de la SRM es establecer acuerdos formales entre las organizaciones interrelacionadas con responsabilidades claramente definidas en cuanto a la observación y la gestión. Si se documentan y comparten todos los problemas de seguridad operacional de las interfaces, los informes de seguridad operacional y las enseñanzas obtenidas, así como los riesgos de seguridad operacional entre las organizaciones en cuestión se asegurará una comprensión clara de la gestión. La compartición permite transferir conocimientos y prácticas laborales que podrían mejorar la eficacia de cada organización en la materia.

### 1.3.4 Planificación de la implementación

1.3.4.1 La realización de un análisis de brechas antes de emprender la implementación de SSP/SMS permitirá a la organización identificar la brecha entre las estructuras y procesos organizativos actuales y los necesarios para el

funcionamiento eficaz del SSP o SMS. Para el SSP, es importante incluir un examen de las preguntas del protocolo del Programa universal de auditoría de la vigilancia de la seguridad operacional (USOAP) que se consideran como la base de dicho programa.

1.3.4.2 El plan de implementación del SSP o SMS es, como su nombre lo indica, un plan para la instrumentación del SSP/SMS. Proporciona una clara descripción de los recursos, tareas y procesos necesarios, y un cronograma y una secuencia indicativos de las tareas y responsabilidades fundamentales. En los Capítulos 8 y 9, respectivamente, figura más información sobre la implementación de la gestión de la seguridad operacional para los Estados y los proveedores de servicios.

### **Evaluación del grado de desarrollo**

1.3.4.3 Poco después de implementar los componentes y elementos fundamentales del SSP o SMS, deberían realizarse evaluaciones periódicas para observar cuán eficazmente está funcionando. A medida que se desarrolla el sistema, la organización debería procurar garantías de que está funcionando según lo previsto y que resulta eficaz para alcanzar sus objetivos y metas de seguridad operacional declarados. La gestión de la seguridad operacional lleva tiempo para alcanzar la madurez necesaria y el objetivo final debería ser el mantenimiento o la mejora continua del rendimiento de la organización en materia de seguridad operacional.

### **1.3.5 Consideraciones de tamaño y complejidad**

1.3.5.1 Cada Estado y cada proveedor de servicios es diferente de los demás. Los SSP y SMS están diseñados para adaptarse a las necesidades específicas de cada Estado o proveedor de servicios. Todos los componentes y todos los elementos de los SSP y SMS están interconectados y son interdependientes y son necesarios para un funcionamiento eficaz. Es importante de que los requisitos de SSP y SMS no se implementen solamente en forma prescriptiva. Los requisitos tradicionales de carácter prescriptivo deben complementarse con un enfoque basado en el rendimiento.

1.3.5.2 El programa o sistema está diseñado para producir los resultados deseados de cada organización sin cargas indebidas. Los SSP y SMS, si están bien implementados, tienen por objeto complementar y mejorar los sistemas y procesos existentes en la organización. La gestión efectiva de la seguridad operacional se alcanzará mediante una cuidadosa planificación e implantación, asegurando que cada requisito se enfoca de manera que corresponda a la cultura y entorno operacional de la organización. En los Capítulos 8 y 9, respectivamente, figura más información sobre los aspectos que han de considerarse al implementar SSP/SMS para Estados y proveedores de servicios.

### **1.3.6 Integración de los elementos básicos**

Es importante señalar que todos los sistemas están compuestos de tres elementos básicos: personas, procesos y tecnología. La gestión de la seguridad operacional no constituye una excepción. Al establecer o mantener los diferentes procesos, actividades y funciones, todos los Estados y proveedores de servicios deberían cerciorarse de que han tenido en cuenta la intención de cada requisito y, lo que es más importante, la forma en que trabajan conjuntamente para permitir que la organización satisfaga sus objetivos de seguridad operacional. Todos y cada uno de estos elementos de la gestión de la seguridad operacional, así como sus interrelaciones, se abarcarán a lo largo del presente manual.

## **1.4 GESTIÓN INTEGRADA DE LOS RIESGOS**

1.4.1 El sistema de aviación en su totalidad comprende muchos y diferentes sistemas funcionales como los financieros, ambientales, de seguridad operacional y de seguridad de la aviación. Estos dos últimos son los principales dominios operacionales del sistema de aviación global. Como conceptos comparten importantes características en tanto ambos se ocupan de los riesgos de que ocurran sucesos con consecuencias de diversa magnitud. No obstante, difieren respecto del importante elemento de la intencionalidad. La seguridad de la aviación se ocupa de actos maliciosos y

voluntarios para perturbar el funcionamiento de un sistema. La seguridad operacional se concentra en el impacto negativo para el funcionamiento de los sistemas en cuestión provocado por consecuencias no intencionales de una combinación de factores.

1.4.2 En el contexto operacional, todos los sistemas funcionales producen algún tipo de riesgo que debe gestionarse en forma apropiada para disminuir posibles consecuencias adversas. Tradicionalmente, cada sistema ha desarrollado marcos y prácticas de gestión de riesgos específicas de cada sector dirigidas a abordar las características propias de cada sistema. La mayoría de estas prácticas de gestión de riesgos comprenden análisis completos de las consecuencias dentro del sistema, a menudo conocidos como gestión de consecuencias imprevistas. Otro aspecto son las consecuencias entre sistemas que resultan de procesos de gestión de riesgos específicos del sistema. Esto se relaciona con el hecho de que una estrategia eficaz de gestión de riesgos de un sector específico puede tener consecuencias negativas sobre otro sector operacional de la aviación. En el contexto aeronáutico, la dependencia entre sistemas que se destaca con mayor frecuencia es el dilema entre seguridad operacional y seguridad de la aviación. Las medidas de seguridad de la aviación eficaces pueden tener consecuencias negativas para la seguridad operacional y a la inversa. Los dominios de seguridad operacional y seguridad de la aviación pueden diferir en la intención subyacente, pero convergen en el objetivo común de proteger a las personas y los bienes (p. ej., el tratamiento de las ciberamenazas y riesgos requiere coordinación a través de los dominios de seguridad operacional y seguridad de la aviación). En algunos casos, la gestión del riesgo inherente de un dominio puede afectar al otro en formas imprevistas, como en los ejemplos siguientes:

- a) el reforzamiento de las puertas del puesto de pilotaje, necesario por los riesgos de seguridad de la aviación, puede tener consecuencias de seguridad operacional en el funcionamiento de la aeronave;
- b) las restricciones impuestas al transporte en la cabina de dispositivos electrónicos personales puede desplazar el riesgo de seguridad de la aviación de la cabina a la bodega de carga, lo que aumentaría los riesgos de seguridad operacional; y
- c) el cambio de ruta para evitar el vuelo sobre zonas de conflicto puede provocar una congestión de los corredores aéreos, lo que constituiría un problema de seguridad operacional.

1.4.3 Una exitosa gestión de riesgos en la aviación debería apuntar a la reducción general de los riesgos en el sistema, incluyendo todos los sistemas funcionales involucrados. Este proceso requiere una evaluación analítica del sistema en su totalidad al más alto nivel de la entidad correspondiente (Estado, organizaciones regionales, proveedores de servicios). La evaluación e integración de las necesidades e interdependencias del sistema funcional se conoce como gestión integrada de los riesgos (IRM). La IRM se concentra en la reducción global de los riesgos de la organización. Esto se consigue mediante un análisis cuantitativo y cualitativo de los riesgos inherentes y de la eficacia y consecuencias de los procesos de gestión de riesgos específicos de cada sector. La IRM tiene la responsabilidad sistémica de coordinar, armonizar y optimizar los procesos de gestión de riesgos con el único objetivo de reducir el riesgo. La IRM no puede reemplazar las gestiones de riesgos específicas de los sistemas funcionales, y no pretende delegar funciones y responsabilidades adicionales a estos. La IRM es un concepto de alto nivel dirigido a aprovechar el asesoramiento de expertos en gestión de riesgos específicos de cada sector y proporcionar información holística para alcanzar el más alto nivel de rendimiento del sistema a un nivel socialmente aceptable. Más amplia información sobre gestión de riesgos de seguridad operacional, dentro del alcance del presente manual, figura en los Capítulos 2, 8 (para Estados) y 9 (para proveedores de servicios).

*Nota.— La estructura y las áreas de responsabilidad del gobierno dentro del Estado pueden afectar la vigilancia de cada área. Por ejemplo, la autoridad de aviación civil (CAA) es responsable de la seguridad operacional de la aviación, mientras que el órgano de protección del medio ambiente es responsable de la vigilancia ambiental. Cada entidad de vigilancia puede tener diferentes requisitos y metodologías.*