guía

El Sistema de gestión de la seguridad (SMS)

Guía para la implementación del SMS en Organizaciones de Diseño, Producción y Mantenimiento

2024

TEDAE
Defense, Security, Aeronautics and Space

GRUPO DE TRABAJO

Dña. Leire González. ACITURRI

D. José Luis Carretero. ACITURRI

Dña. Ana Isabel Álvarez. HEROUX DEVTEK

D. David Álvarez. INDRA

D. David Guzmán . ITP AERO

D. Jesús Bussión. TEMAI Ingenieros S.L

EDITA: TEDAE, Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio.

ARTE: EXPOMARK (www.expomark.es)

Índice

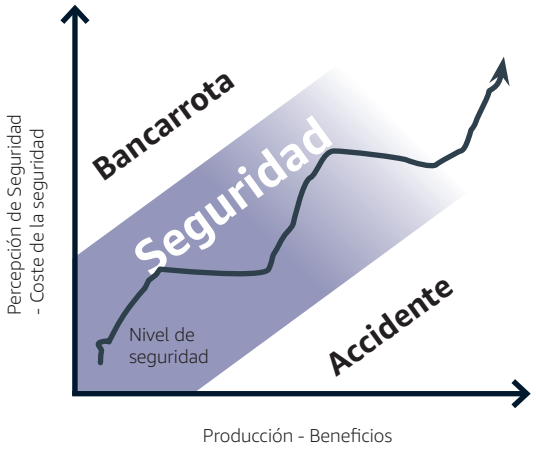
01 ¿Qué es el Sistema de Gestión de la Seguridad (SMS)?

La seguridad en la aviación, y en particular la seguridad de las operaciones (vuelo) ha sido desde los inicios de la aviación comercial el objetivo principal de todos los esfuerzos realizados en todas las organizaciones y participantes, incluyendo por supuesto, operadores, reguladores, diseñadores, fabricantes y mantenedores.

¿Qué entendemos por seguridad de la aviación?

Se entiende como un estado, en continua evolución, en la que los riesgos asociados con las actividades de la aviación, relacionadas con ella, o en soporte directo de la operación de una aeronave, son reducidos y controlados hasta un cierto nivel aceptable.

Ese nivel de seguridad es propio de cada organización y establece el compromiso entre el nivel de protección y la producción, o, en otras palabras, el beneficio y la seguridad, estableciendo el espacio de seguridad en el que se mueve la seguridad aceptable para dicha organización.



A lo largo de la historia, se han dado diferentes estrategias para hacer el transporte aéreo cada vez más seguro:

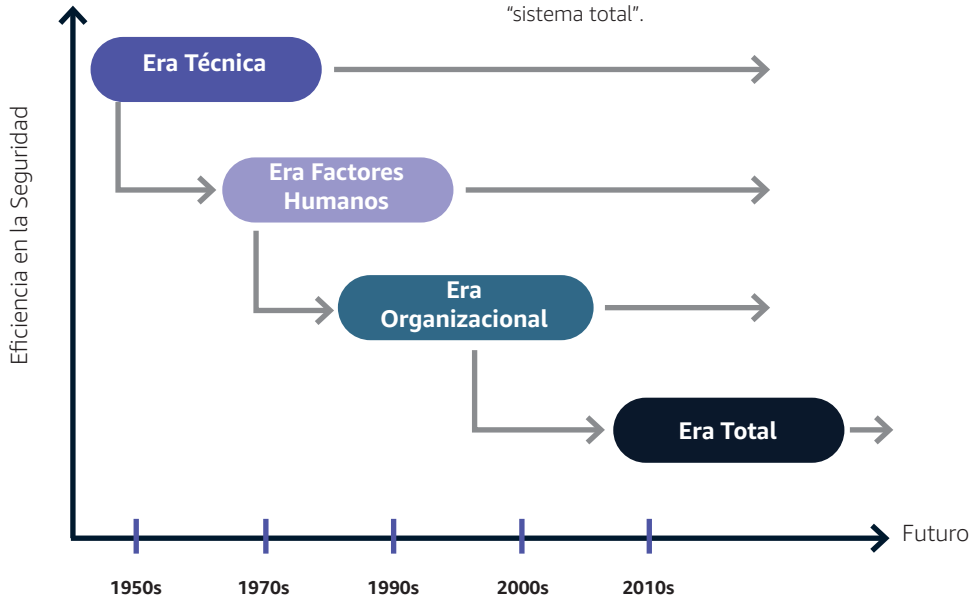
- Desde los inicios hasta finales de los 60, las deficiencias de seguridad estaban relacionadas con factores técnicos y fallos tecnológicos. Los esfuerzos en materia de seguridad se centraron en la investigación y la mejora de los factores técnicos (por ejemplo, la aeronave) y el cumplimiento de la normativa y la supervisión regulatoria. Es lo que se denomina época "técnica", y de ella derivan toda las regulaciones, manuales, normativas y estándares aplicados en aviación.

- A principios de los 70, los esfuerzos realizados convirtieron a la aviación en un modo de transporte más seguro, reduciendo la frecuencia de los accidentes. Sin embargo, algunos accidentes de este momento mostraban la influencia de los errores humanos. Consecuentemente, los esfuerzos en materia de seguridad empezaron a considerar los factores humanos, en particular la «interfaz hombre/máquina», centrados en el individuo, sin considerar el contexto operativo y organizativo que pueden afectar al comportamiento (época del "factor humano").

- A mediados de los 90, la seguridad empezó a considerarse de manera sistémica y a englobar factores organizativos, humanos y técnicos, in-

troduciéndose el concepto de «accidente organizativo» que tiene en cuenta el impacto de la cultura y las políticas de la organización en la eficacia de los controles de los riesgos para la seguridad. Adicionalmente, el análisis reactivo y proactivo de los datos de seguridad permitieron supervisar los riesgos conocidos y la aparición de nuevos riesgos (tendencias). Estas mejoras (era "organizacional") suponen los cimientos que llevaron a la actual gestión de la seguridad, SMS.

- Finalmente, a inicios del siglo XXI, ya se había ganado madurez en los sistemas de seguridad, implantando SMS, y recibiendo sus beneficios. Hasta este momento, los SMS se habían centrado en resultados individuales y en el control local, con mínima atención a la aviación en su conjunto. Un creciente reconocimiento de la complejidad del sistema de aviación y de las diferentes organizaciones que desempeñan un papel en la seguridad aérea ha ampliado el ámbito del SMS en lo que se denomina era de "sistema total".



En este contexto, el Sistema de Gestión de la Seguridad (SMS, por sus siglas en inglés: Safety Management System) es un conjunto de políticas, procesos y prácticas diseñadas para identificar, gestionar y mitigar los riesgos que puedan comprometer la seguridad de la aviación. De este modo, el SMS es similar al familiar sistemas de gestión de calidad, donde se establecen políticas y objetivos enfocados en la mejora de procesos y productos.

Como cualquier otro sistema de gestión, el SMS, puede ser certificado o aprobados por entidades externas o autoridades competentes, cuando este cumple con requisitos establecidos en normas o regulaciones específicas, como ISO (9100, 9110), EASA (Part 21, Part 145).

NOTA: Según la definición proporcionada por la Organización Internacional de Normalización (ISO), un sistema de gestión es "un conjunto de elementos y actividades relacionados y coordinados que interactúan, y que, estableciendo Políticas y Objetivos, dirigen y controlan la organización con el fin de lograr dichas metas".

guía

Sistema de Gestión de la Seguridad (SMS)

¿Para qué es necesario un SMS?

El SMS permite a la organización implementar una política de seguridad efectiva, establecer objetivos concretos y definir las actividades necesarias para asegurar su rol en la seguridad de la aviación. El SMS es una herramienta de negocio que permite a una organización orientar sus decisiones de cara a la seguridad. Por ello la implementación de un SMS conlleva, entre otros los siguientes beneficios:

- Mejora la seguridad de la Aviación reduciendo el riesgo de que sucedan accidentes e incidentes.
- Fomenta en la empresa el equilibrio entre la seguridad y los beneficios.
- Proporciona una mejor priorización de los riesgos de seguridad y la correspondiente asignación de los recursos de la empresa. Esto permite obtener resultados óptimos, incrementar la eficiencia y reducir los costes.
- Proporciona un mecanismo de toma de decisiones mejor informado, sistemático y enfocado a la seguridad.
- Refuerza la cultura corporativa, enfocándola en la seguridad.
- Más seguridad en las organizaciones, siempre significa mayor crecimiento económico.

¿Qué no es un SMS?

Sin embargo, hay que tener claro que un SMS no es:

- Simplemente otro requisito del regulador más, que debemos cumplir. Limitar el SMS a un mero cumplimiento "en papel" minimiza sus beneficios y destruye la cultura.
- No implica la autorregulación, o una desregulación: el SMS ni supera ni reemplaza ni limita la supervisión requerida, tanto interna como por parte del regulador.
- No reemplaza ninguno de los sistemas de gestión ya preexistentes en la organización, como el de Calidad, en de Riesgos de Negocio, el de Riesgos Laborales, etc., sino que se integra con ellos, construyendo el sistema a partir de los procesos ya existentes.
- El SMS no es cosa de una persona o departamento aislado, sino que es la responsabilidad de todos los que componemos la organización.
- Y, definitivamente, no es un gasto inútil: los beneficios que aporta para la organización justifican la inversión en recursos necesaria para poner en marcha el sistema y mantenerlo.

"El SMS es una herramienta de negocio que permite a una organización orientar sus decisiones de cara a la seguridad"

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio

C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24

info@tedae.org
www.tedae.org

02 Elementos de un Sistema de Gestión de la Seguridad

1. **Política de seguridad**
   - Definición clara de la seguridad: La organización debe establecer una política que defina su compromiso con la seguridad.
   - Compromiso de la alta dirección: La política debe contar con el respaldo de la dirección y debe ser comunicada a todos los niveles de la organización.
2. **Gestión de riesgos**
   - Identificación de riesgos: Identificar los peligros que puedan afectar la seguridad.
   - Evaluación de riesgos: Evaluar la probabilidad y el impacto de esos peligros.
   - Control y mitigación de riesgos: Implementar medidas para reducir los riesgos a niveles aceptables.
3. **Aseguramiento de la seguridad**
   - Monitoreo y medición: Evaluar el desempeño de las actividades de seguridad, a través de auditorías internas y controles.
   - Acciones correctivas: Implementar acciones para corregir las deficiencias o fallos de seguridad detectados.
   - Mejora continua: El SMS debe ser revisado periódicamente para identificar áreas de mejora.
   - Adaptación a cambios: El sistema debe ser flexible para ajustarse a cambios operacionales, regulatorios o tecnológicos.
4. **Promoción de la seguridad**
   - Capacitación y entrenamiento: Todo el personal debe recibir formación en seguridad.
   - Comunicación: Fomentar una cultura de seguridad mediante la comunicación constante de los principios y objetivos del SMS.

Documentación y registro

- Mantenimiento de registros: El sistema debe incluir una base de datos para registrar incidentes, riesgos, acciones de contención y auditorías.
- Procedimientos documentados: Todos los procesos deben estar documentados para asegurar su correcta implementación. Así mismo deben ser revisados y mantenidos al día.

Cada uno de estos componentes es esencial para crear un sistema que no solo gestione los riesgos de manera eficaz, sino que también fomente una cultura organizacional orientada a la seguridad.

03 Política de Seguridad, Objetivos, e Indicadores

La Política de Seguridad es un documento de alto nivel de la organización en la que se establece cómo es la filosofía y los principios de la organización en tanto a la seguridad de la operación.

La **Política de Seguridad** debe contener entonces:

- El compromiso y la responsabilidad de los gestores en la seguridad.
- Compromiso de la dirección en dedicar los recursos necesarios a la gestión de la seguridad.
- La responsabilidad de todos los participantes en el proceso productivo en la seguridad.
- El compromiso con la mejora continua en materia de seguridad.
- Concienciación de toda la organización con la seguridad.
- Animar y proteger (dentro de un entorno de "cultura justa") a reportar errores, omisiones, eventos, etc. utilizados para identificar peligros y realizar análisis de seguridad.

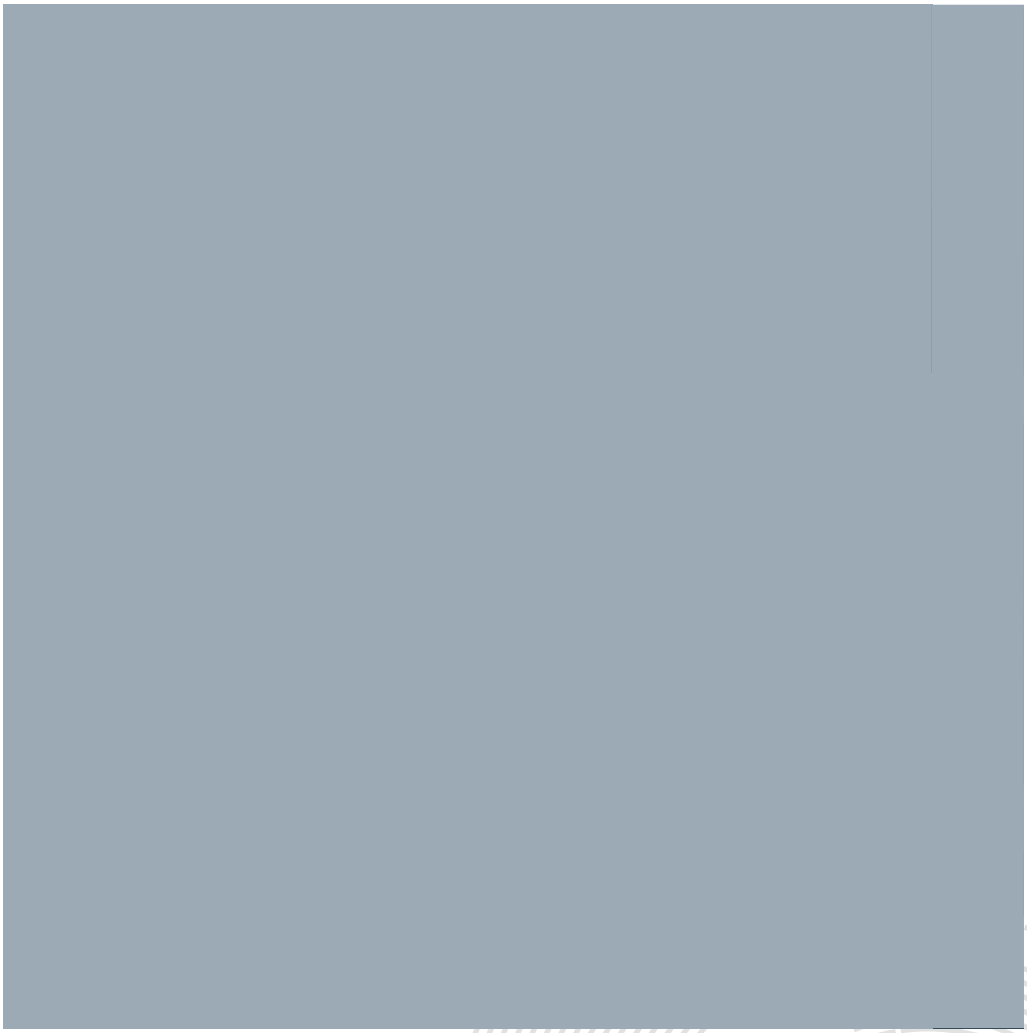
La Política de Seguridad se materializa en los objetivos de seguridad, que son, en definitiva, como la organización alcanza el nivel de seguridad deseado.

¿Cómo establecemos la política y los objetivos de seguridad?

Para definir de manera efectiva la política y los objetivos de seguridad, es fundamental adoptar un enfoque basado en datos y la experiencia previa de la organización. Esto se logra mediante un análisis de riesgos, el cual permite identificar los peligros potenciales y priorizar aquellos que han tenido mayor impacto o probabilidad de ocurrencia en el pasado.

Este proceso de priorización de riesgos se fundamenta en dos factores principales: la probabilidad y las consecuencias de los peligros identificados. Al evaluar ambos factores, la organización puede concentrar sus esfuerzos en evitar situaciones de riesgo que ya ha enfrentado o que presentan un alto grado de probabilidad de ocurrir.

El análisis de riesgos es clave para establecer tanto la política como los objetivos de seguridad, y debe estar alineado con los requisitos normativos y regulatorios aplicables. Esto asegura que los recursos y esfuerzos se dirijan de manera eficiente hacia la mitigación de los riesgos más significativos.



Ejemplo Política de Seguridad

Compromiso de la Dirección

La Dirección de la Organización [Nombre de la Empresa]. entiende la Seguridad como el principal emblema de la Organización, y así lo transmite a toda la Organización

La Organización reconoce la Seguridad como la principal prioridad organizativa, por delante de aspectos comerciales, operacionales, ambientales o sociales.

[Nombre de la Empresa], se compromete con la Seguridad, transmitiéndolo a todos los niveles de su organización y de aquellas organizaciones colaboradoras.

Es obligación de la dirección de esta Organización, y de los cargos intermedios, difundir y promover este compromiso con la Seguridad, y de proveer las herramientas necesarias para su gestión.

Responsabilidad individual y colectiva / concieciación

La Seguridad responsabilidad de todos y cada uno de los empleados, de su implicación y su trabajo en equipo. Para asegurarlo se requiere que todos los requisitos y métodos aplicables a cada puesto sean conocidos, entendidos e implantados

Cultura de Reporte

Todo empleado de [Nombre de la Empresa] tiene el compromiso y la obligación de notificar a través de los canales establecidos, cualquier situación que pudiera suponer un riesgo para la Seguridad.

Cultura Justa

Cualquier actividad relacionada con la notificación de riesgos y su análisis, tendrá el único fin de averiguar las causas del problema para evitar su recurrencia.

Nunca se tomarán medidas disciplinarias de aquellos errores involuntarios.

Compromiso con la mejora

La Organización trabajará en la búsqueda de las mejores prácticas de trabajo, enfocadas en mejorar los estándares de Seguridad, siendo esto una tarea a desarrollar por todos los empleados de la compañía,

Compromiso de proveer recursos

La dirección de [Nombre de la Empresa] proveerá los recursos necesarios, tanto humanos como financieros, para llevar a cabo todas las tareas asociadas con la seguridad.

Por todo esto, revisará esta Política de Seguridad de manera periódica para actualizar dicho compromiso y garantizar su aplicabilidad.

Gerente Responsable [Firma]

Es importante hacer hincapié en dos apartados de la política especialmente importantes:

- El establecimiento de la **responsabilidad individual y colectiva** en materia de seguridad, en la que todos los integrantes de la organización, independientemente de su participación, en mayor o menor medida, más directo o indirectamente, tienen su propia responsabilidad individual con respeto de las labores que realizan, pero, que a la vez, son corresponsables de las consecuencias de las que realizan todos los demás. Este aspecto, es fundamental para establecer una buena cultura de seguridad, en la que no sólo se reporten los errores/eventos propios, sino todos aquellos de los que seamos conscientes, aunque no participemos en ellos. Y mucho más importante, que no se permita el comportamiento inseguro por parte de ningún miembro de la organización.

- El establecimiento de la **política "no punitiva" o de "cultura justa"** como base de una cultura de seguridad positiva, basada en el reporte y en la mejora de la seguridad. Este tema es de especial interés y se comenta un poco más adelante.

El compromiso de la Dirección, su propio comportamiento con respecto a la seguridad, la asignación de recursos, y la promoción del reporte y de la Cultura Justa, son esenciales para la buena integración de la Política de Seguridad en la organización. No obstante, es responsabilidad de todo el personal adherirse a ella.

POLÍTICA → OBJETIVOS → SPIs

La Política de Seguridad indica el compromiso de la Dirección y que se trasladan en unos Objetivos, que establecen el nivel de seguridad que la organización quiere alcanzar y que serán medidos a través de unos indicadores (Safety Performance indicators o SPIs). Un ejemplo de objetivos son los siguientes:

1. Implementar la cultura de seguridad dentro de la Organización:
    a) Concienciando a los empleados de [organización] mediante el establecimiento y comunicación de las responsabilidades de seguridad operacional y formación al personal sobre la cultura de seguridad.
    b) Promoviendo el reporte voluntario de riesgos que puedan impacto en la seguridad operacional.
    c) Garantizando que los canales adecuados de reporte están disponibles y son conocidos, promocionando su uso de forma abierta y sin ningún tipo de consecuencia derivada.
2. Reducción de los eventos de seguridad (defectos, no-conformidades, escapes).
3. Minimizar el factor humano como causa en los eventos de seguridad.
4. Promocionar esta cultura de seguridad entre los suministradores.

Los objetivos de seguridad deben estar trazados al menos a un indicador. Estos indicadores deben de ser específicos para la organización y deben ayudar a medir la implementación de los objetivos. Y estos indicadores deben ser evaluados y monitorizados con el fin de identificar cómo la organización está alcanzando sus metas en materia de seguridad, a la vez que permitir tomar las acciones necesarias para revertir incumplimientos de estos. Esta actividad es parte de la mejora continua el sistema de seguridad, o aseguramiento de la seguridad se verá en un capítulo más adelante.

Los indicadores de seguridad además pueden ser reactivos (por ejemplo, número de eventos de seguridad) o proactivos (por ejemplo, nivel de cumplimiento del plan de formación). Estos últimos son los más interesantes, pues pueden alertar (umbrales) de la deriva hacia la inseguridad de la organización, pudiendo actuar (medidas de control) antes de que se vean reflejada la situación en indicadores reactivos.

Como ejemplo de Indicadores (SPIs) se encuentran los siguientes:

SPI	Descripción	Modo de cálculo	Objetivo	Frecuencia
SPI-1 (OBJ-5)	% nº de riesgos mitigados/nº riesgos reportados	Riesgos que tras implementación de acciones de mitigación reducen su riesgo a tolerable/ nº total de riesgos en proceso de reducción de riesgo	(80%)	trimestral
SPI-2 (OBJ-1, 2, 3)	% gente formada en el sistema SMS/ plantilla total:	Cantidad de personas que han recibido una formación concienciación/entre nº total de empleados.	50% (con referencia 3000 empleados)	anual
SPI-3 (OBJ – 3, 4)	Nº riesgos internos reportados/mes	Nº de riesgos reportados a mes vencido/cantidad de meses acumulados por año a mes vencido	1 reporte/mes Máximo: 12 reportes por año	trimestral
SPI-4 (OBJ - 6)	Nº de eventos con causa principal el factor humano/	Nº de eventos con causa principal el factor humano/eventos totales	50%	anual

Ejemplo de evaluación: KPI-3 mes junio: (1+1+3)/6=0.83

Reportes	Enero	Feb	Mar	Abr	May	Jun	Jul	Ago	Sept	Oct	Nov	Dic
Real	1	1	0	0	0	3	0					
Teórico	1	1	1	1	1	1	1	1	1	1	1	1

Consejos para elegir unos SPIs eficientes:

- SMART: Específicos (**S**pecific), measurable (**M**edibles), alcanzables (**A**chievable), realistas (**R**ealistic) y de duración limitada (**T**ime-bound)
- Adecuados a la complejidad de la organización.
- Alineados con los objetivos y con la política de seguridad
- Que permitan una mejora continua dentro de la organización

Personal clave en el SMS

Una vez una organización establece su Política de Seguridad, y a partir de ella, sus Objetivos de Seguridad, dos funciones nominadas adquieren un papel clave en el establecimiento, desarrollo y mejora del SMS:

- **Director/Gerente Responsable:** como la persona bajo la cual recae la responsabilidad última en materia de seguridad de toda la organización bajo su control y por ello debe contar con la capacidad necesaria para gestionar y asignar los recursos de esta. Por ello es responsable de:
  - Establecer y promover la Política de Seguridad, haciéndola de obligado cumplimiento para la organización.
  - Asegura la financiación y los recursos necesarios para llevar a cabo las tareas de seguridad.
  - Establecer y seguir los objetivos de seguridad, así como el establecimiento de las acciones de contención y su efectividad.
  - Garantizar la competencia de todo el personal de la organización en materia de seguridad
- **Responsable de seguridad:** dando soporte al director/Gerente responsable en materia de Seguridad, es el punto focal de la organización para el desarrollo, administración y mantenimiento de los procesos del SMS, asegurando su adecuado funcionamiento. Es, por tanto, responsable, además de:
  - Gestionar de manera eficiente el sistema de notificación de seguridad y de sucesos.
  - Gestionar y facilitar el inicio y seguimiento de las investigaciones de seguridad.
  - Facilitar la identificación de peligros y la evaluación y gestión de los riesgos correspondientes.
  - Controlar la implementación de las acciones de mitigación identificadas y su efectividad.
  - Proporcionar informes periódicos sobre el desempeño de la organización con respecto a la seguridad (obtener y analizar los indicadores de seguridad y su evolución).
  - Garantizar el mantenimiento de la documentación y registros del SMS.
  - Garantizar que exista y esté disponible la formación de seguridad y que esta cumpla los estándares aplicables.
  - Asesorar a la organización y en particular al Director/Gerente responsable en materia de seguridad.
  - Dar información de retorno sobre incidentes/problemas de seguridad a través de formación recurrente, boletines, u otros medios a la organización.

Por las funciones que desarrolla el Responsable de Seguridad debe tener capacidad de reporte directo con el Gerente Responsable, y debería ser un "senior manager" dentro de la organización para tener el grado de autoridad necesario para el ejercicio de sus funciones en materia de seguridad.

Del mismo modo, dependiendo de la complejidad de la organización, puede estar ayudado de un equipo de personas igualmente nominadas.

Por sus responsabilidades el Responsable de Seguridad debe, a parte de los correspondientes conocimientos técnicos y regulatorios, tener las siguientes competencias como deseables:

- La promoción de una cultura de seguridad positiva.
- Habilidades interpersonales, de influencia y liderazgo.
- Habilidades de comunicación oral y escrita.

- Gestión de datos, habilidades analíticas y de resolución de problemas.
- Integridad profesional.

CULTURA JUSTA

El mayor impedimento para prevención de errores en la industria es **"que castigamos a la gente por cometer errores"**.

Esta frase, resume lo que es, en esencia, la Cultura Justa, sobre todo aplicado a los sistemas de gestión de la seguridad aeronáutica.

Se entiende que las personas, a pesar de su formación, experiencia, habilidades y buena voluntad, pueden encontrarse en situaciones donde se producen resultados indeseables debido a los límites del rendimiento humano combinados con influencias sistémicas no deseadas e impredecibles. Por tanto, la responsabilidad individual debe focalizarse en determinar si las acciones, omisiones o decisiones tomadas, son acordes con la experiencia y el entrenamiento, y nunca en el resultado del evento.

Todo mecanismo que, de **manera preventiva**, pretenda evitar una situación de riesgo operacional, causada por un error o fallo humano, como el Sistema de Seguridad, depende, en una gran mayoría de los casos, de que las personas que lo hayan cometido o detectado **informen** del mismo, de modo que puedan ser **gestionadas** sus consecuencias.

Y es evidente que si, como consecuencia de esta comunicación, las personas son castigadas, antes o después, la reacción a dicho castigo provocará que los errores y omisiones no se informen, pudiendo poner en peligro la seguridad de las operaciones, perdiéndose la oportunidad de gestionar las consecuencias y aprender de ellos para evitarlos en el futuro.

Cultura Justa, implica que, con el objetivo de gestionar las consecuencias de los errores e infracciones (análisis de seguridad) y la mejora (evitar que sucedan el futuro), no se castigará por los errores o infracciones cometidas en el ejercicio normal de nuestras funciones y de acuerdo con nuestro conocimiento y capacidades. **Todo el personal tiene responsabilidad en la Seguridad.**

Pero es importante destacar que Cultura Justa no es un "paraguas" en el que esconderse ante cualquier situación: están expresamente **excluidos** los actos ***deliberados o significativamente negligentes*** realizados por individuos o grupos de ellos ("comportamiento inaceptable").

Implementar una Cultura Justa va mucho más allá del **compromiso** por parte de los organismos gestores y en particular del Gerente Responsable y que estará incluida en la **Política de Seguridad**, así como en los procedimientos que gobiernan la operación, sino que debe desarrollarse en varios aspectos clave:

Primero, establecer métodos de información que protejan a las personas que informan de estos errores o infracciones. Estos, se materializan en un ***Sistema de Reporte Voluntario*** (típicamente un buzón) donde recoger estos informes. El carácter debe ser confidencial, para asegurar la protección del informante, y no anónimo, con el fin de proporcionar retorno de las acciones e investigaciones que dicho reporte genere, así como poder aclarar o concretar puntos específicos del informe con la persona informante.

Segundo, se debe generar una cultura en la empresa que facilite la realización de estos informes, y estos fluyan de manera natural. Aspectos clave para tener en cuenta son:

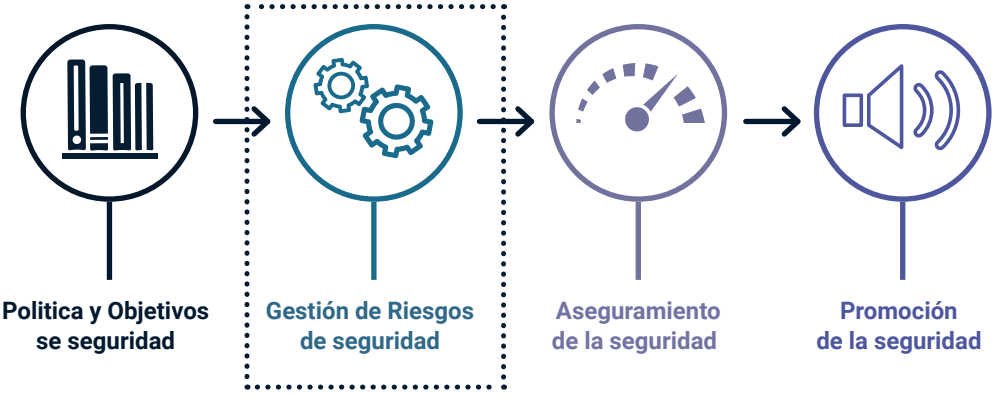
- **Fomentar y promocionar** activamente la notificación de errores y eventos, a todos los niveles de la organización, pero, especialmente, los gestores intermedios, los cuales tienen un papel relevante alentando a sus equipos a notificar estas situaciones.
- **Proteger y gestionar** la información suministrada por la persona informante, incluyendo a las posibles personas incluidas en la misma, siendo usada de manera efectiva para la gestión de los riesgos de seguridad y el aprendizaje y mejora continua.
- **Transmitir** a todos los miembros del equipo la importancia capital de la seguridad, de la responsabilidad individual (y colectiva) en la seguridad, que debe ser entendida y aceptada por todos, de estar vigilante ante situaciones que entrañen

un peligro para la seguridad, que los eventos puedan reportarse de manera libre, completa e inmediata, y que, de manera clara y evidente se reconozca y recompense el buen desempeño en seguridad y el reporte de los eventos.

- **Participación** de todo el equipo en las actividades mejora y grupos de análisis de causa raíz como 5Ws, 8Ds, Maintenance Error Decision Aid (MEDA) abiertos a la participación de todos los actores implicados en el evento estudiado, son clave para fomentar la Cultura Justa. Nota: se recomienda el método MEDA para la evaluación del factor humano en el mantenimiento.
- **Búsqueda** real de la causa raíz de los eventos, más allá de los propios errores o infracciones cometidas, fomentando de manera continua, la autocrítica relacionada con los procedimientos y métodos utilizados (efectividad del sistema de gestión) y en los factores contribuyentes que han llevado a dicha situación.
- Realizar **formación** que incluya los principios de la Cultura Justa, incluyendo todos los niveles de la organización (no sólo los operativos), haciendo toda la documentación interna relacionada accesible para todos.
- Dar **soporte** por parte de las organizaciones cuando su personal está sujeto a procedimientos externos, cuando estos reportan o están involucrados en una incidencia, reforzando la mutua confianza necesaria para asegurar una Cultura Justa efectiva.
- **Revisar** de manera regular la madurez de la Cultura Justa en la organización, comparándola con la percepción que de la misma tienen los miembros de esta (encuestas de seguridad).

Por último, y no menos importante que lo anterior, cada Organización debe crear un compendio de "reglas internas" convenientemente documentadas (y, eventualmente, acordadas con los representantes de los miembros de la Organización) que definan de manera clara el proceso y los actores implicados en la determinación de los "comportamientos inaceptables" que son motivo de exclusión de la protección que proporciona la Cultura Justa.

04 Gestión de riesgos



La Gestión de los Riesgos es una herramienta sistemática que sirve para la toma de decisiones (asignación de recursos, establecimiento de estrategia y acciones mitigadoras) por medio de la evaluación de las consecuencias que los riesgos identificados podrían tener, con respecto a la seguridad operacional. La Gestión de Riesgos tiene como objetivo:

- **MAXIMIZAR** la probabilidad de ocurrencia y efectos de eventos positivos (oportunidades).
- **MINIMIZAR** la probabilidad y efectos de eventos negativos (amenazas).

Definición de peligro: Acción, actividad que tenga un potencial de causar un daño o una consecuencia no deseada (riesgo). Son inherentes a cualquier actividad, inevitable pero gestionable.

Definición de riesgo: son las consecuencias (pueden ser varias), no deseadas (dañinas para la seguridad de la operación) que pueden ser ocasionadas por un determinado peligro.

La gestión de riesgos conlleva los siguientes pasos:

- Identificación de peligro / Registro del Riesgo
- Evaluación de Riesgos
- Estrategias de evaluación. Matriz de riesgos. Decisión gerencial.
- Establecimiento de acciones.
- Re-evaluación del riesgo tras implantación de acciones.

Peligro versus Riesgo: Para entender la relación entre peligro y riesgo, veamos un ejemplo: vamos a apretar una tuerca con una llave de vaso. Al ir a realizar la tarea, me encuentro que la llave está desgastada, pudiendo no apretarse adecuadamente la tuerca.

¿cuál es el peligro en este caso? ¿apretar i**nadecuadamente** la tuerca?

Considerando la definición de **peligr**o, en este caso, la acción peligrosa es el hecho de **apretar la tuerca**. Esta es la acción presente, e inevitable, porque la voy a realizar, y que potencialmente puede tener consecuencias.

Por otro lado. El **riesgo** es **hacerlo inadecuadamente**, como consecuencia del daño en la llave; esta acción es la que tiene consecuencias.

Identificación de peligro

La identificación de peligros permite identificar "problemas de seguridad" o "amenazas" (a las que se hace referencia como peligro).

Las fuentes de información de peligros que tiene habitualmente una organización identificada, para actividades de fabricación o mantenimiento, pueden ser:

- FOD (daños por objetos extraños).
- Cualquier trabajo realizado no de acuerdo con los datos aprobados (producto no conforme o sospechoso/fraudulento)
- Cualquier desviación de una herramienta detectada durante la calibración.
- Escapes de Calidad
- Avisos de Calidad de proveedores
- Incumplimientos relacionados con certificados o aprobaciones de productos.
- Notificaciones de alertas de las Autoridades
- Análisis de accidentes aéreos previos
- Decisiones organizacionales inherentes a la actividad

¿Podríamos tener un producto no conforme y seguro? y ¿podríamos tener un producto conforme y no seguro? La respuesta a ambas preguntas es que sí, aunque la segunda es la más interesante, puesto que pone de relieve que la seguridad operacional (Seguridad) va más allá de la conformidad del producto (Calidad), aunque, por supuesto no están desligadas, sino todo lo contrario. (ver. Seguridad vs Calidad.)

Para tenerlo más claro, veamos unos ejemplos:

- **Mantenibilidad:** En diseño, es posible tener un equipo que cumpla perfectamente la especificación (producto Conforme) y sin embargo a la hora de su instalación o desinstalación, comprometa otras piezas o cause problemas de factor humano, como incomodidad o posturas forzadas, etc. que al final cause daños o errores/omisiones que puedan provocar accidentes.
- **Defectos cosméticos:** En fabricación, un daño leve provocado por el propio proceso o el manejo de la una pieza hace que esta esté fuera de especificación haciendo la pieza no conforme, pero si son en partes no funcionales, por ejemplo, pueden considerarse simplemente cosméticos, y, por tanto, no afectar a la seguridad.

- **Procedimentales:** en mantenimiento, por ejemplo, se pueden establecer procedimientos para validar utillajes alternativos. Cumplir con estos procedimientos significa tener un producto conforme. Un fallo en la definición de los requisitos (por ejemplo, demasiado ligeros) podría comprometer la seguridad del producto afectado por dicho utillaje, y sin embargo, ser conforme (Calidad).

Evaluación de riesgos (probabilidad y severidad)

Una vez identificados los peligros y evaluados sus correspondientes riesgos asociados, es preciso realizar una evaluación de los riesgos, en tanto a la severidad de las posibles consecuencias de los riesgos, como la probabilidad de que se den estas consecuencias. Veámoslo en detalle:

a) Severidad de riesgos

El primer paso para la cuantificación del riesgo es determinar la severidad de la consecuencia del peligro si su potencial perjuicio se materializa durante la operación. Esto se conoce como evaluación de la severidad de riesgos de seguridad operacional.

La severidad de riesgos de seguridad operacional se define como los posibles efectos de una consecuencia, tomando como referencia la situación más probable y creíble, es decir, que no se exagera al expresar las condiciones extremas anticipadas. Esta evaluación se realizará en base a la experiencia de la organización y a juicio de los expertos involucrados.

Una forma de evaluar a severidad de los posibles efectos de una consecuencia es utilizando una tabla de severidad de los riesgos de seguridad operacional. En la figura adjunta se presenta una tabla típica de severidad de riesgos de seguridad operacional, que comprende cinco categorías para indicar el nivel de severidad de la consecuencia o evento, el significado de cada categoría y la asignación de un valor a cada categoría.Esto se conoce como evaluación de la probabilidad del riesgo de seguridad operacional.

SEVERIDAD DEL EVENTO

DEFINICIÓN CUALITATIVA	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. • Incidente grave • Lesiones a las persona	C
Leve	• Molestias • Limitaciones operacionales • Uso de procedimientos de emergencia • Incidente leve	D
Insignificante	• Pocas consecuencias	E

Nota: esta tabla es un ejemplo y cada organización deberá adaptarla a su complejidad y realidad operativa.

b) Probabilidad del riesgo de seguridad

Una vez identificada la severidad de las consecuencias hay que evaluar con que probabilidad se pueden producir.

Esto se conoce como evaluación de la probabilidad del riesgo de seguridad operacional.

La probabilidad del riesgo de seguridad operacional se define como la posibilidad de que una consecuencia en cuestión pueda ocurrir.

Al evaluar la probabilidad de la consecuencia (o evento), es esencial referirse a los datos históricos y toda la información disponible para asignar la probabilidad más acertada. Esta probabilidad debe ser asignada a cada una de las consecuencias (o eventos).

A modo de ejemplo se incluye en la figura adjunta una tabla típica de probabilidad de los riesgos de seguridad operacional, en este caso, con una matriz de cinco puntos. La tabla abarca cinco categorías para indicar la probabilidad de ocurrencia de una consecuencia o evento, el significado de cada categoría y una asignación de valor a cada categoría.

PROBABILIDAD DEL EVENTO

DEFINICIÓN CUALITATIVA	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 muy poco probable que ocurra (no se sabe que haya ocurrido	1

Nota: esta tabla es un ejemplo y cada organización deberá adaptarla a su complejidad y realidad operativa.

Para que la evaluación del riesgo, en tanto en cuanto a la severidad y la tolerabilidad sea lo más ajustada posible, dada la escasa información disponible, y salvo en casos especialmente simples, se requiere, normalmente, de la participación de varias personas, todas ellas con conocimientos y/o experiencias relevantes para el caso analizado, que pongan en común los diferentes aspectos del análisis, pruebas o experimentos realizados y lleguen a un acuerdo acerca de la severidad y tolerabilidad del riesgo.

Este grupo, se denomina Grupo de Acción de Seguridad (Safety Action Group, SAG, en inglés).

Estrategias de evaluación. Matriz de riesgos. Decisión gerencial.

La combinación alfanumérica de la probabilidad y la severidad constituye el riesgo de seguridad operacional de la consecuencia del peligro que se considera en la matriz de evaluación de riesgos.

MATRIZ DE EVALUACIÓN DE RIESGOS

PROBABILIDAD DEL RIESGO		SEVERIDAD DEL RIESGO				
		Catastrófico A	Peligroso B	Grave 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: esta tabla es un ejemplo y cada organización deberá adaptarla a su complejidad y realidad operativa.

Con esta combinación obtenemos el Indice de Riesgo de Seguridad Operacional, 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.

Gestión del Riesgo	Índice de Riesgo de Seguridad Operacional	Criterio de Tolerabilidad
Intolerable	5A, 5B, 5C, 4A, 4B	Intolerables
Tolerable	5D, 5E,4C, 4D, 4E,3B,3C,3D, 2A, 2B, 2C, 1A	Tolerable en base a mitigación de riesgos
Aceptable	3E, 2D, 2E, 1B, 1C, 1D, 1E	Aceptable

a) Establecimiento de acciones

En base al criterio de tolerabilidad se deben tomar las siguientes acciones:

PROBABILIDAD DEL EVENTO

CRITERIO TOLERABILIDAD	Acciones	Estrategía
Inaceptable	Se deben de implantar de inmediato acciones de contención urgentes. Además, el riesgo debe ser eliminado o reducido, hasta alcanzar niveles tolerables o aceptables, mediante un plan de reducción del riesgo	Eliminación
Aceptable en base a mitigación de riesgos	El riesgo debe ser reducido. Se deben implementar acciones mitigadoras a través un plan de reducción del riesgo	Mitigación
Tolerable	Nivel de riesgo tolerable para convivir con él	Aceptación

La decisión del criterio de tolerabiliad así como las acciones requeridas deben ser aceptados por la dirección de la organización asignando los recursos necesarios para la implementación de las mismas, en el denominado Comité de Seguridad (de Producto), SRB en sus siglas en inglés (Safety Review Board), dirigido por el Gerente Responsable, y con participación de los responsables de las distintas áreas de la organización con capacidad de decisión y de asignación de recursos.

b) Re-evaluación del riesgo tras implantación de acciones.

Una vez ejecutadas las acciones, se debe actualizar el Índice de Riesgo de seguridad Operacional (re-evaluación del riesgo). En caso de que el nivel de riesgo no haya disminuido significa que las acciones no han sido eficaces o que no se han orientado adecuadamente. Por lo tanto, se deberán definir acciones adicionales y se comenzará de nuevo el proceso. (Definición de acciones, implantación y re-evaluación).

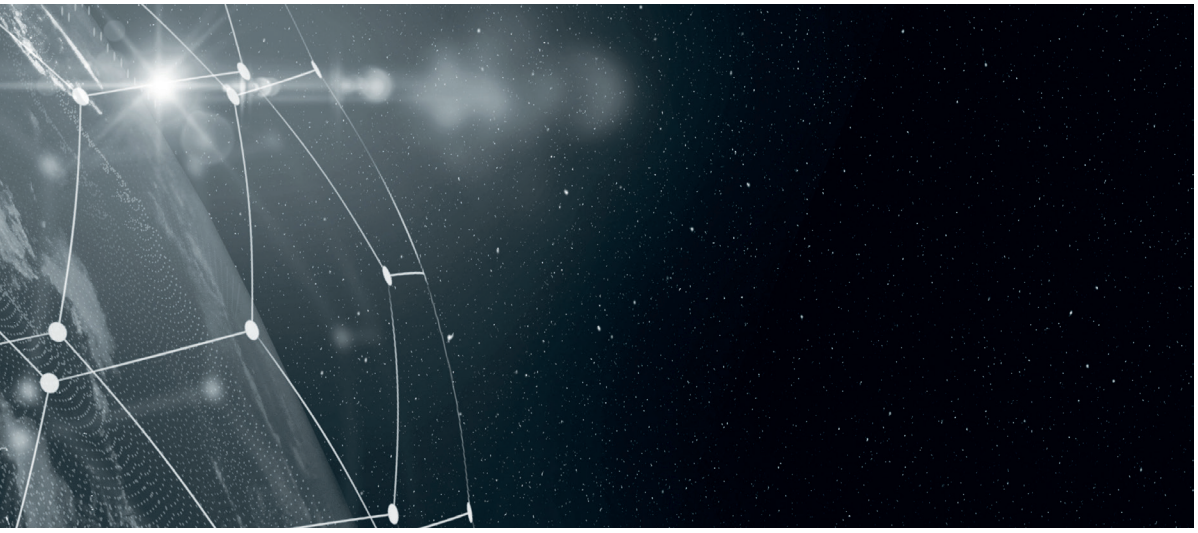
"La implementación de una mitigación puede conllevar nuevos riesgos"

Es importante destacar que se debe realizar un seguimiento de la efectividad de las acciones mitigadoras ejecutadas, así como una reevaluación del riesgo a lo largo del tiempo, si es que esas acciones no eliminan de modo completo el mismo.

"Los riesgos mitigados pueden variar su tolerabilidad con el tiempo," entre los párrafos"

Los riesgos mitigados, pueden tender la tendencia a incrementar su probabilidad (y en ocasiones su severidad) como consecuencia de la normal degradación de la efectividad de las acciones a lo largo del tiempo como consecuencia del propio factor humano, pero también de otros factores organizacionales y de cultura de la organización. Es en estos casos en los que, si el riesgo alcanzase de nuevo una situación no tolerable, nuevas acciones de mitigación deberán ser implementadas para volver a la situación tolerable.

Un ejemplo de esto, son las acciones mitigadoras basadas en la comunicación y la formación: en el momento puntual de ser ejecutadas tienen una alta eficacia, pero si no se renuevan (repiten) su efecto se va perdiendo (olvidando) hasta desaparecer totalmente al cabo de unos meses o años, en cuyo caso el riesgo vuelve a ser el mismo.



Este seguimiento de los riegos debe ser realizado como parte integrante del proceso de gestión de riesgos.

Por último, es importante considerar que las acciones de mitigación identificadas para mitigar un determinado riesgo pueden, en determinadas circunstancias hacer aparecer otros riesgos no considerados. Es preciso que, a la hora de determinar las acciones contenedoras, esta posibilidad sea tenida en cuenta para evitar situaciones de riesgo no identificadas.

Un ejemplo de este caso podría ser tener que diseñar un utillaje especial para realizar una inspección requerida para mitigar un riesgo en un equipo en operación. El citado utillaje puede provocar daños en otras áreas por si mismo o por su manejo que pueden crear riesgos nuevos.

Documentación del Sistema

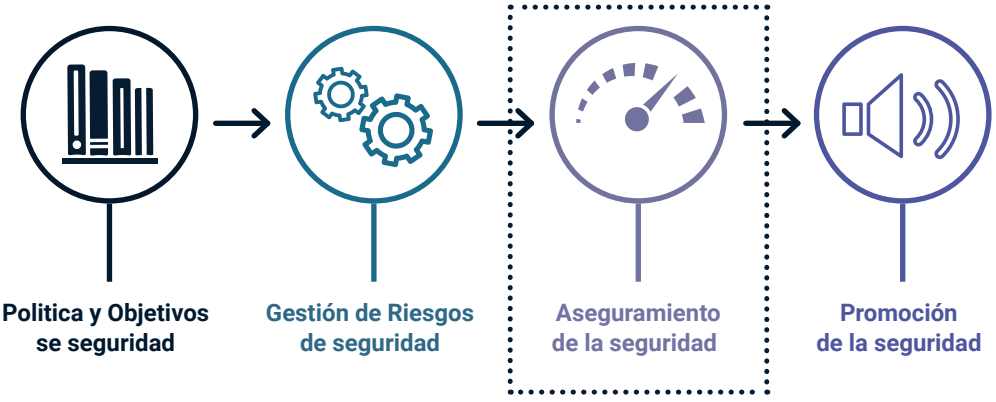
Tanto los peligros identificados, como los análisis realizados, como las acciones de mitigación puestas en marcha y su efectividad deben quedar documentados mediante una "base de datos" de seguridad operacional que permita el almacenamiento de la anteriormente citada información, como la revisión de los peligros y sus riesgos a lo largo del tiempo, y por tanto, la evolución de las acciones mitigadoras correspondientes.

Dicha "base de datos" puede adoptar diversas formas, dependiendo de la complejidad de la organización y su actividad, y debe contener tanto los peligros (y sus riesgos asociados) correspondientes a los eventos detectados, como aquellos correspondientes a la propia actividad de la organización (procedimientos, cultura, etc.).

La forma más simple, que puede tener esta "base de datos" corresponde con una lista que detalla todos esos riesgos, en particular los organizacionales. Dicha lista de peligros (o Hazard log) debe ser revisado de manera periódica para incluir nuevos peligros (y sus correspondientes riesgos), la evolución de los anteriormente identificados (cambios en probabilidad) y de las diferentes acciones de mitigación puestas en marcha.

Esta revisión debe ser realizada por el comité de alto nivel dirigido por el Gerente/Director Responsable denominado Comité de Seguridad (de Producto) (SRB),

05 Aseguramiento de la Seguridad



Definición de Aseguramiento de la Seguridad: Procesos dentro del SMS que funcionan sistemáticamente para garantizar el rendimiento y la efectividad de los controles de riesgo de seguridad y que la organización cumpla o supere sus objetivos de seguridad a través de la recolección, análisis y evaluación de información. (NAS9927)

El Aseguramiento de la Seguridad (SA, por sus siglas en inglés) se fundamenta en las siguientes actividades esenciales:

- **Monitoreo y medición del desempeño de seguridad**
- **Gestión del cambio.**
- **Mejora continua del SMS**

El SA se logra mediante la vigilancia constante de las actividades del Sistema de Gestión de Seguridad (SMS). Por lo tanto, el SA requiere la recopilación, análisis y monitoreo de datos generados por estas actividades para evaluar el desempeño de seguridad de la organización. Es especialmente importante la conexión entre SA y la Gestión de Riesgos de Seguridad (SRM), ya que esta relación permite medir la efectividad de las acciones correctivas o de las barreras preventivas establecidas.

Además, como parte de los requisitos regulatorios, la organización debe poseer un certificado de gestión de la calidad. Un sistema de gestión de calidad robusto puede fortalecer tanto el SMS como el SA. Este certificado abarca procedimientos de auditoría interna y externa, los cuales son cruciales para garantizar la conformidad y la mejora continua. Es esencial definir claramente las interfaces entre las auditorías y los procesos clave del SMS para asegurar una integración efectiva y una supervisión exhaustiva.

Para implementar efectivamente el SA, la organización debe:

1. **Monitorear y Medir el Desempeño de Seguridad:** Realizar un seguimiento constante de los indicadores de seguridad y analizar los datos para identificar tendencias, áreas de mejora y posibles riesgos.
2. **Gestionar el Cambio:** Evaluar y gestionar cualquier cambio en el entorno operativo que pueda afectar la seguridad, asegurando

que las modificaciones no introduzcan nuevos riesgos o comprometan las medidas de seguridad existentes.

3. **Fomentar la Mejora Continua del SMS:** Implementar acciones de mejora basadas en los resultados de las evaluaciones y auditorías, asegurando que el SMS evolucione y se adapte a las nuevas circunstancias y desafíos.

La vigilancia efectiva de estas actividades y la integración de los datos obtenidos en el proceso de SRM son fundamentales para mantener un alto nivel de seguridad operativa. Las auditorías internas y externas juegan un papel clave en este proceso, proporcionando una evaluación independiente del desempeño del SMS y del SA, y asegurando que las mejoras necesarias se implementen de manera oportuna y eficaz.

La organización debe garantizar que todas estas actividades estén alineadas con los objetivos de seguridad y calidad, y que se comuniquen adecuadamente a todos los niveles de la organización. La colaboración y el compromiso de todos los miembros del equipo son esenciales para el éxito del Aseguramiento de la Seguridad y la gestión efectiva de los riesgos.

Monitoreo y medición del desempeño de seguridad

El propósito del SMS de una organización es mantener los riesgos de seguridad operativa en un nivel aceptable o mejor. Esto implica implementar políticas y procedimientos que garanticen la identificación, evaluación y mitigación de riesgos. El proceso de Gestión de Riesgos de Seguridad no debe ser de circuito abierto; por lo tanto, el proceso de Aseguramiento de la Seguridad debe incluir mecanismos para monitorear continuamente el desempeño del SMS, tanto en su funcionalidad operativa como en la efectividad de los controles de riesgo implementados (seguridad del producto). Esto asegura que cualquier desviación o falla en los controles sea detectada y corregida oportunamente.

La organización debe llevar a cabo evaluaciones regulares sobre el desempeño del SMS en comparación con los objetivos de seguridad establecidos. Esto incluye la revisión y análisis de datos de desempeño, informes de auditoría interna y externa, y la retroalimentación de empleados y partes interesadas. Se espera que la organización desarrolle y mantenga indicadores de desempeño relacionados con la seguridad, tales como tasas de incidentes, cumplimiento de normativas, y resultados de auditorías, que sean apropiados y relevantes para su operación.

La organización debe identificar y asignar a la(s) persona(s) o equipo(s) adecuado(s) para monitorear el desempeño de seguridad, asegurando que tengan la experiencia y perspectiva necesarias para abordar la complejidad, alcance y tamaño de la organización. Esto puede incluir la formación de un comité de seguridad, la designación de oficiales de seguridad dedicados y la colaboración con expertos externos si es necesario.

El desempeño de seguridad de la organización debe ser revisado periódicamente por los ejecutivos responsables. Estas revisiones deben ser detalladas y basarse en informes precisos y actualizados, con el fin de tomar decisiones informadas y proactivas. Además, estas revisiones deben llevarse a cabo de manera recurrente, ya sea trimestral, semestral o anual, según lo requieran las políticas internas y las normativas del sector, para garantizar la mejora continua y el cumplimiento de los estándares de seguridad.

Entre otros ejemplos de indicadores de desempeño podemos encontrar:

- Número de reportes de seguridad realizados: este indicador tiene varias facetas, de las cuales su evolución a lo largo del tiempo, frente a su valor absoluto, es el mejor indicador de desempeño. Niveles muy bajos de informes pueden indicar una baja concienciación por parte de la or-

ganización o un inadecuado fomento de la cultura de reporte (por ejemplo, por canales inadecuados o inexistentes). Niveles altos y crecientes con el tiempo, pueden indicar una cierta degradación del desempeño en la seguridad.

- Acciones de control identificadas en las revisiones de seguridad ejecutadas durante la incorporación y desarrollo de nuevas tecnologías, implementación de nuevos procesos y en situaciones de cambio estructural en las operaciones. Este aspecto es especialmente significativo en lo concerniente a la gestión del cambio, al estar orientadas hacia los riesgos de seguridad inducidos por los propios cambios.

- Resultados de las encuestas de seguridad: en este caso, al realizarse a un relativamente elevado número de personas en la organización, el nivel de seguridad percibido, y en particular su evolución entre diferentes encuestas realizadas es un indicador claro del desempeño en seguridad.

- Monitorizado de las actividades del día a día, identificado la cantidad y extensión de los problemas encontrados. Un incremento en los problemas detectados puede indicar una degradación en la seguridad de la propia organización.

La monitorización de los indicadores de desempeño se realiza en el seno de Comité de Seguridad (SRB) anteriormente descrito.

Gestión del cambio

Las organizaciones viven en permanente cambio, entre los que se incluyen:

- Modificaciones o incorporación de nuevos centros productivos (nueva localización, transferencias de alcance a otro centro ya existente), instalaciones, equipos (máquinas), utillajes y materiales usados en los procesos productivos.

- Nuevas capacidades técnicas y tecnologías incorporadas al proceso productivo.
- Modificación del alcance de los trabajos realizados (nuevas capacitaciones, ampliación de las existentes o cese de estas).
- Cambios en el personal, tanto en número como en fluctuación o rotación, y en especial en el personal clave de la organización.
- Grandes incrementos de personal o de carga de trabajo (elevado desequilibrio entre carga y capacidad).
- Modificación en la estructura organizacional.
- Adición o modificación de los procesos, sistemas, procedimientos y regulaciones aplicables.
- Modificaciones en la cadena de suministro con la incorporación de nuevos subcontratistas o la modificación de su alcance.

Todos estos cambios, en principio **independientemente de su magnitud,** esto es, sean pequeños o grandes, pueden tener un cierto impacto en la seguridad de los productos y de la organización, pero también, y este es un aspecto clave, en factores humanos, pudiendo generar riesgos relacionados con las capacidades y limitaciones humanas.

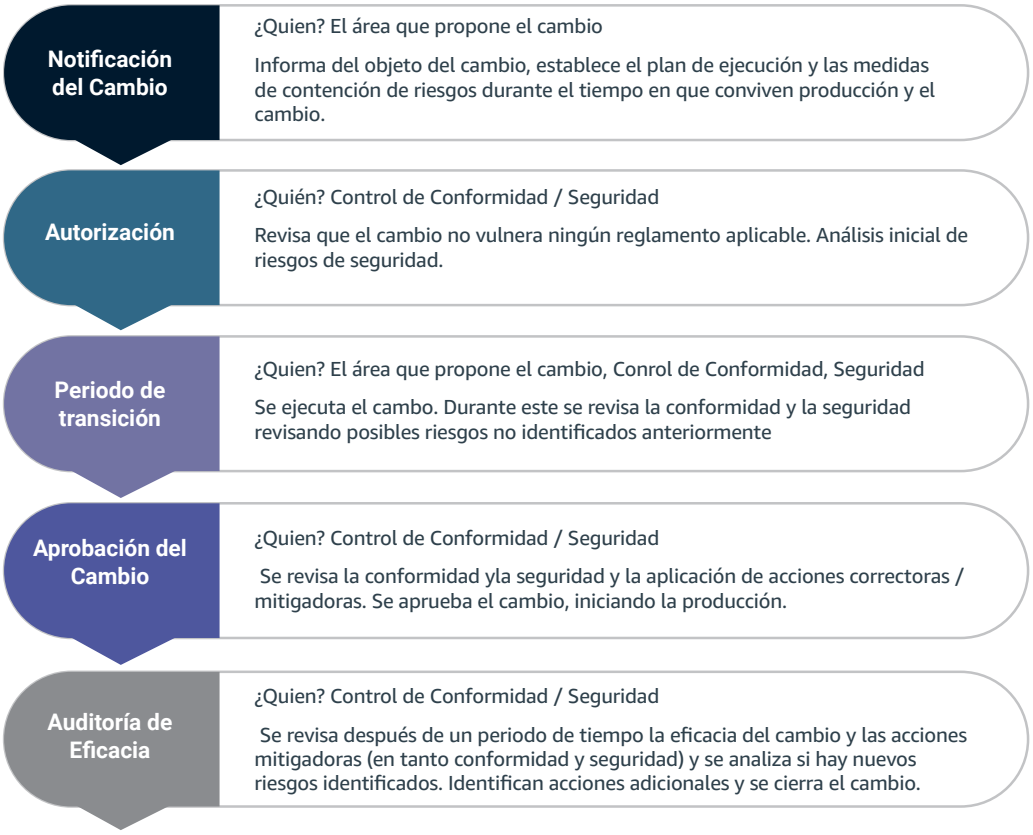
El objetivo de aseguramiento de la seguridad es asegurar que los resultados deseados de un cambio se logren sin comprometer el desempeño de seguridad. Para ello, se debe desarrollar un plan de aseguramiento junto con la estrategia de análisis de seguridad para mitigar los riesgos. Esto implica comprender el desempeño de seguridad de referencia y establecer un conjunto inicial de indicadores para medir el impacto del cambio. Posteriormente, se monitorea y verifica la implementación del cambio y su impacto final en el desempeño de seguridad del sistema, supervisando las mitigaciones de riesgo asociadas con cambios sustanciales en el SMS, evaluando el impacto del cambio en los controles de riesgo de seguridad existentes y asegurando que cualquier desviación se aborde adecuadamente.

Para esta situación de cambio continuo no genere riesgos para la seguridad no gestionados, que creen modificaciones significativas en el entorno operativo, ya sean planeadas o no planeadas, auto-inducidas o resultantes de influencias externas, las organizaciones deben establecer mecanismos que permitan, de una manera sistemática controlar el proceso del cambio, en sus diferentes fases: puesta en marcha, periodo de transición durante la ejecución, implantación y verificación de la implantación, de modo que se satisfagan todos los requisitos que sean aplicables, incluyendo aspectos financieros, de gestión de riesgos laborales, etc., pero sobre todo, los requisitos derivados de las regulaciones aplicables a través del área de Control de Conformidad y que se identifiquen los posibles riesgos de seguridad, y estos sean adecuadamente analizados y mitigados en los casos necesarios, a través del área de Seguridad de Producto. Para ello, es fundamental disponer de una descripción clara de la organización para determinar el alcance de la aplicabilidad del SMS y los cambios potenciales que podrían afectarlo. Si el cambio que se está implementando tiene un impacto en el sistema organizacional, la descripción del sistema debe actualizarse para reflejar dicho cambio. Esto asegura que todos los aspectos del sistema estén alineados con los cambios y que las medidas de seguridad se mantengan robustas y efectivas.

Este proceso de Gestión de Cambio necesariamente aunará la acción de los diferentes sistemas de gestión existentes de la organización (Gestión de Riesgos Laborares, Gestión Financiera, Gestión de industrialización/instalaciones, Calidad / Control de Conformidad y Seguridad de producto) con el objetivo de realizar los cambios de una manera ordenada, conforme con las regulaciones aplicables (incluidas las no aeronáuticas) y que no induzca nuevos

riesgos en la seguridad de producto, ni empeore la situación de los ya existentes en la organización, considerando como un factor trascendente la influencia en el factor humano del propio cambio.

Como ejemplo de procedimiento se puede tener el siguiente flujograma:



Los puntos clave de este flujograma de proceso son:

- **Autorización:** la revisión del cambio antes de ejecutarlo identifica posibles cambios que no son aceptables por ser no conformes con las regulaciones aplicables. En este momento se debe realizar un primer análisis de riesgos de seguridad de acuerdo a los procedimientos establecidos en la organización.
- **Periodo de transición**; muchos cambios requieren ser realizados mientras la producción continúa, coincidiendo tanto físicamente como en partes del proceso. Esta situación puede generar múltiples riesgos para la seguridad de la operación. La clave está en estudiar el proceso, analizar los posibles riesgos e implementar durante el proceso cuantas acciones sean requeridas para que la implementación del cambio no

comprometa la seguridad del resto de productos en proceso.

- **Aprobación del cambio:** tras implementar de manera completa y conforme el cambio, y tener mitigados los riesgos identificados, el cambio es aprobado y liberado para ser ejecutado.

- **Auditoría de eficacia:** se requiere, en determinados casos, que se verifique que la implementación del cambio ha sido eficaz, en particular en caso de procedimientos, nuevas capacidades, etc. En esta auditoría, se revisa de nuevo la conformidad del cambio, los riesgos de seguridad previamente identificados y sus acciones de contención y se analiza la existencia de nuevos riesgos o no conformidades, implementándose las correspondientes acciones. Tras la ejecución e implementación de dichas acciones, se cierra definitivamente el cambio. Mejora continua del SMS

Mejora continua del SMS

La mejora continua del SMS es un proceso gradual y constante enfocado en incrementar la efectividad y eficiencia de una organización para cumplir con su política y objetivos de seguridad.

Este proceso debe basarse en planes de acción derivados de la monitorización y medición del desempeño de seguridad. Es fundamental que la organización considere los resultados de estas mediciones al definir las acciones de mejora continua para el SMS.

A partir de los datos de seguridad recopilados, la organización debe asegurar lo siguiente:

1. Análisis de Datos a Nivel Organizacional: Se debe realizar un análisis exhaustivo de los datos para establecer un plan de acción, involucrando a los interesados responsables de implementar las acciones. Este plan debe abordar las causas raíz de fallas o malfunciones en el sistema donde el desempeño de seguridad no ha alcanzado el nivel esperado.
2. Implementación de Acciones de Mejora: Las acciones de mejora identificadas deben ser implementadas de manera efectiva. Esto incluye la aplicación de correcciones y la adopción de nuevas prácticas para prevenir la recurrencia de problemas.
3. Consideración de Mejores Prácticas y Lecciones Aprendidas: Es esencial incorporar las mejores prácticas y lecciones aprendidas para fortalecer el SMS. Estas mejores prácticas deben difundirse en toda la organización mediante actividades de promoción de la seguridad, garantizando que todo el personal esté informado y comprometido con la mejora continua.

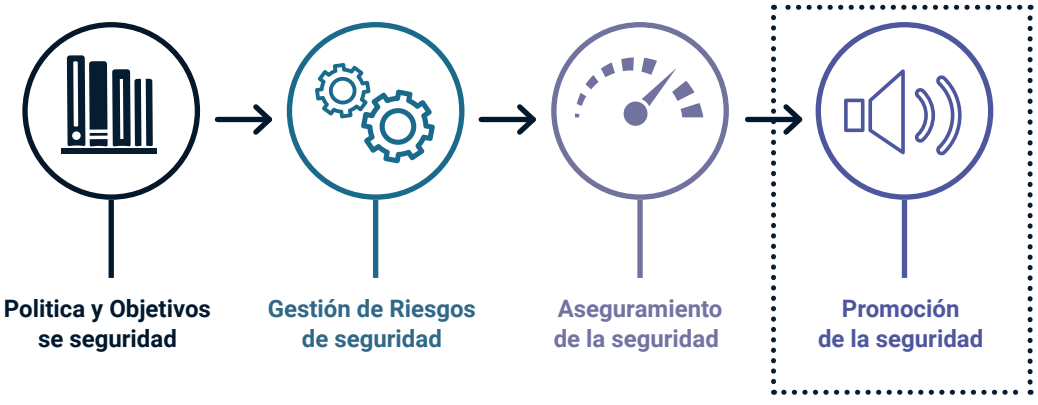
En el contexto de la mejora continua, se deben organizar revisiones periódicas del SMS con miembros de la dirección. La frecuencia y el formato de estas revisiones deben ser proporcionales al nivel de riesgos y la complejidad de la organización. Los resultados de estas revisiones deben ser utilizados como insumos para el proceso de Gestión de Riesgos de Seguridad, asegurando que las decisiones y acciones se basen en datos actualizados y análisis precisos.

La mejora continua del SMS no solo implica la corrección de fallas, sino también la proactividad en la identificación y mitigación de riesgos potenciales, la optimización de procesos y la adaptación a nuevas normativas y estándares de seguridad. Esto asegura que la organización no solo mantenga, sino que mejore su nivel de seguridad operativa de manera sostenida.

Y como parte de la mejora continua del sistema, están las auditorías realizadas sobre el Sistema de Seguridad por parte de la función Calidad/Control de Conformidad, en las que se determina el correcto funcionamiento del mismo, así como la identificación de posibles acciones de mejora que redunden en la eficacia del sistema y su evolución en respuesta a nuevos desafíos.

06 Promoción de la seguridad en un sistema SMS

De los cuatro componentes que forman los fundamentos de un sistema SMS: vamos a describir en este apartado el componente de: **Promoción de Seguridad SMS**



La Promoción de la Seguridad se define como las actividades que apoyan la implementación del SMS en una organización y se basa en tres pilares: l**a formación, el intercambio de conocimientos y la comunicación.**

Para promover la seguridad como valor fundamental de la empresa, los empleados deben comprender el sistema de gestión de la seguridad, aprender de la experiencia compartida y desarrollar la conciencia de los peligros. La dirección también debe ser capaz de explicar por qué se adoptan determinadas medidas con el fin de fomentar de forma coherente un entorno para la notificación abierta de los problemas de seguridad.

Los esfuerzos de seguridad no pueden tener éxito si la implementación de las políticas se realiza por mandato o estrictamente pensando en una puesta mecánica de las mismas. Por ello es fundamental que la organización promueva la seguridad mediante: Formación y Comunicación.

Formación

El promover la seguridad predispone tanto al comportamiento, con respecto a la seguridad, individual como de la organización.

Es recomendable la implementación a nivel organización de un programa, procedimiento o instrucción de seguridad SMS que asegure que el personal esté adecuadamente instruido y competente para realizar las funciones para las cuales fue designado.

Para cada empleado de la organización, incluido el personal directivo el programa de instrucción de seguridad debería adecuarse específicamente conforme a:

- Su nivel de responsabilidad;
- Su participación en el SMS
- Impacto en los productos o servicios de la organización
- A sus funciones específicas.

La organización deberá establecer la forma de evaluar la efectividad de los programas de formación en el SMS, posiblemente mediante indicadores (SPIs), encuestas o revisiones periódicas.

Intercambio de conocimientos

A modo de referencia se adjunta un ejemplo de actividades que deberían especificarse para promocionar la seguridad SMS acorde a tres niveles de cualquier organización.

El intercambio de conocimientos entre los tres niveles organizativos en materia de seguridad, debe ser clave para la correcta elaboración de los procedimientos, política, análisis de riesgos en material de seguridad asociados. Para ello es fundamental que la organización cuente con los canales de comunicación adecuados.

Personal Operativo

1. Política de Seguridad de la organización
2. Sistemas de Gestión de la organización, incluyendo fundamentos y descripción del SMS:
   - Definición de peligro, consecuencias y riesgos.
   - Proceso de gestión de riesgos.
   - Roles y responsabilidades
   - Sistema de reporte de seguridad.

1. Procesos y procedimientos específicos de la organización de acuerdo a sus funciones.
2. Capacitación técnica específica de acuerdo a sus funciones

Jefes y Supervisores

3. Proceso de seguridad.
4. Análisis de datos de seguridad
5. Identificación de riesgos
6. Evaluación y mitigación de riesgo
7. Gestión de cambio

1. Procesos y procedimientos específicos de la organización de acuerdo a sus funciones.
2. Capacitación de acuerdo a sus funciones

Directivos

8. Estándares de sguridad de la organización y las regulaciones
9. Asignación de recursos
10. Promoción y comunicación eficaz
11. Asesoramiento de la seguirdad
12. Establecimiento de niveles aceptables de seguridad

Comunicación

La organización desarrollará y mantendrá los medios formales para la comunicación de seguridad operacional que:

- Asegure que todo el personal tiene conocimiento del SMS.
- Comunica información sobre los riesgos y peligros para la seguridad.
- Explica las razones porque se toman acciones de mitigación.
- Explica porque los procedimientos de seguridad han sido incorporados o cambiados en caso necesario o ante la actualización de nuevos riesgos.
- Evolución de los indicadores establecidos para los objetivos.

Los medios de comunicación pueden incluir:

- Políticas y procedimientos de seguridad.
- Circulares de noticias.
- Boletines.
- Portal.

La comunicación de seguridad es un pilar esencial para el desarrollo y el mantenimiento de un SMS.

07 Relación Calidad y Seguridad

Durante muchos años, en el entorno normativo europeo (EASA), no existía diferencia entre la función Calidad y la de asegurar la seguridad de los productos y servicios entregados por las organizaciones de Diseño, Producción y Mantenimiento. De hecho, el Responsable de Calidad era, de facto, el responsable también de Seguridad Operacional. Esta situación era, del mismo modo compatible con el entorno EN9100/9110.

Esta situación hacía que tanto las funciones de calidad de producto, control de conformidad y seguridad, aunque pudieran estar en diferentes áreas, y personas, la responsabilidad estaba centralizada en una única persona nominada y, por tanto, reconocida por el regulador.

Sin embargo, con la última edición de la regulación, y con ella, la introducción del Sistema de Gestión, formado por una parte por la novedosa función Seguridad y por otro la función de control de conformidad, cada una de ellas, con su correspondientes personal nominado, introduce una situación en la que, parte de las funciones de Calidad, que antes existían en la regulación EASA y que aún existen en regulaciones EN9100/9110 y militares como PECAL, deben relacionarse de una manera muy estrecha con la función Seguridad, mientras que la función cumplimiento debe permanecer independiente del resto de las funciones del sistema.

La clave de la coordinación entre estas dos áreas está en el trabajo conjunto, dado que ambas funciones son totalmente complementarias. Si, por un lado, la función Calidad (de producto) tradicional se centraba en los eventos sucedidos, por ejemplo escapes de calidad, pero también eventos de proceso interno (no conformidad, discrepancias de verificación, etc.), corregir las deficiencias, el análisis de la causa raíz de los sucesos y la mejora, implantando acciones correctoras y para evitar recurrencias, la función Seguridad, se pregunta por las consecuen-

cias de estos eventos tanto en el pasado, porque pudieron suceder antes de detectar el evento, como de la posibilidad de que el sistema permita que suceda en el futuro en otros productos por la propia debilidad del mismo.

De este modo, la función Seguridad, aunque ya esbozaba en la función Calidad, implica una visión más amplia de los eventos expandiendo la implantación de acciones de contención a todos los ámbitos de la organización y, no sólo, a las áreas afectadas.

En resumen, la mayor diferencia entre la Función Seguridad y la de Calidad de Producto está en el enfoque proactivo (evitar los sucesos/eventos que pueden afectar a la seguridad de la operación) de la función seguridad, frente a un enfoque más reactivo (corregir los sucesos/eventos ya acontecidos) de la función Calidad de Producto.

Sin embargo, la función Seguridad no puede existir a parte de la función Calidad (de producto) dado que esta última identifica y trata de manera sistemática los eventos que suceden y alimentan de información (ejemplo: metodologías de análisis de causa raíz, identificación y seguimiento de planes de acción, definición de indicadores, etc.), mostrando las debilidades del sistema a la función Seguridad. Sin la función Calidad, la información que llega a Seguridad es incompleta, así como la generación de acciones de mitigación, su seguimiento y la evaluación de su efectividad.

La forma en que estas dos áreas han de coexistir en una organización depende de la propia organización y su complejidad. En todo caso, compartir la información junto con la participación de Seguridad en las investigaciones de eventos, es fundamental para una buena implementación del sistema de gestión.

Lo más importante es que Seguridad no reemplaza ninguno de los sistemas de gestión de la organización preexistentes, como Calidad de Producto, a parte de otros (Gestión de Riesgos Laborales, Seguridad Industrial, Continuidad de Negocio, Financiero, etc.), sino que trabaja en unión con ellos para mejorar la seguridad de la operación.

info@tedae.org
www.tedae.org

TEDAE
Defense, Security, Aeronautics and Space

Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio

C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24