Guía de soporte para su implementación y utilización

Gestión de la Seguridad de la información

(ISMS) en el ámbito aeronáutico (Part-IS)

2026

TEDAE
Defensa, Seguridad, Aeronáutica y Espacio

GRUPO DE TRABAJO

- Francisco Javier Sierra Domínguez. TEMAI INGENIEROS
- Jesús Bussión Fernández. TEMAI INGENIEROS
- Melisa Formento Pellegrini. TEMAI INGENIEROS
- David Guzmán Vegas. ITP AERO
- Roberto Jesús García García. THALES GROUP
- Mitxel Fuentes Larrañaga. AERNNOVA AEROSPACE
- Ramón Ortiz González. RHEINMETALL EXPAL MUNITIONS
- Sergio Pingarrón. CONSULTOR INDEPENDIENTE

AVISO LEGAL

La presente guía tiene carácter meramente informativo y orientativo, y no constituye en ningún caso una interpretación oficial ni vinculante de la normativa aplicable. Su contenido se basa en un análisis general de los requisitos establecidos en los Reglamentos Delegado (UE) 2022/1645 y de Ejecución (UE) 2023/203, relativos a la implantación de sistemas de gestión de la seguridad de la información (ISMS) en el ámbito de la seguridad aérea.

Esta guía no sustituye la obligación de las organizaciones de conocer, interpretar y aplicar directamente la normativa vigente, ni reemplaza el asesoramiento legal o regulatorio especializado. La responsabilidad de cumplimiento recae exclusivamente en cada organización, en función de su contexto, alcance y actividades específicas.

Asimismo, el contenido aquí recogido puede estar sujeto a cambios derivados de futuras actualizaciones normativas, interpretaciones de las autoridades competentes o evolución de las mejores prácticas en materia de seguridad de la información.

Los autores no asumen responsabilidad alguna por el uso que pueda hacerse de esta guía ni por posibles errores u omisiones en su contenido.

índice

01 ¿Qué es un sistema de seguridad de la información ISMS?

Un Sistema de Gestión de la Seguridad de la Información (SGSI o ISMS, por sus siglas en inglés) es un conjunto de elementos, políticas y procedimientos diseñado para proteger la información sensible de una organización, asegurando su autenticidad, confidencialidad, integridad y disponibilidad de las redes y sistemas de información. Sirve para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información con impacto potencial en la seguridad de la aviación. (Safety Vs Security)

¿Por qué es necesario un ISMS?

- Ayuda a las organizaciones a identificar y mitigar riesgos, como ataques cibernéticos, errores humanos o desastres naturales, que podrían comprometer la información con posibles repercusiones en la seguridad de la aviación.
- Debe tener capacidad de responder y recuperarse de incidentes asociados a la seguridad de la información.
- Facilita a las organizaciones a cumplir con las regulaciones y leyes que le apliquen para desempeñar su actividad.
- Permite a las organizaciones gestionar los riesgos de seguridad de manera proactiva, identificando vulnerabilidades y estableciendo controles para mitigarlos.
- Genera confianza hacia dirección y todas las partes interesadas de la organización (autoridad, clientes y proveedores), asegurando que los activos están debidamente protegidos frente a amenazas de forma continua.

Esta guía es un acercamiento a la normativa Part-IS para la implantación de un sistema de gestión de seguridad de la información (ISMS) que aborde los riesgos de seguridad de la información y su impacto en la seguridad aérea basándose en un enfoque de mejora continua. Los requisitos están descritos en los Reglamentos de delegación 2022/1645 y de ejecución 2023/203. Estos reglamentos en su artículo 2 indican sus respectivos ámbitos de aplicación.

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

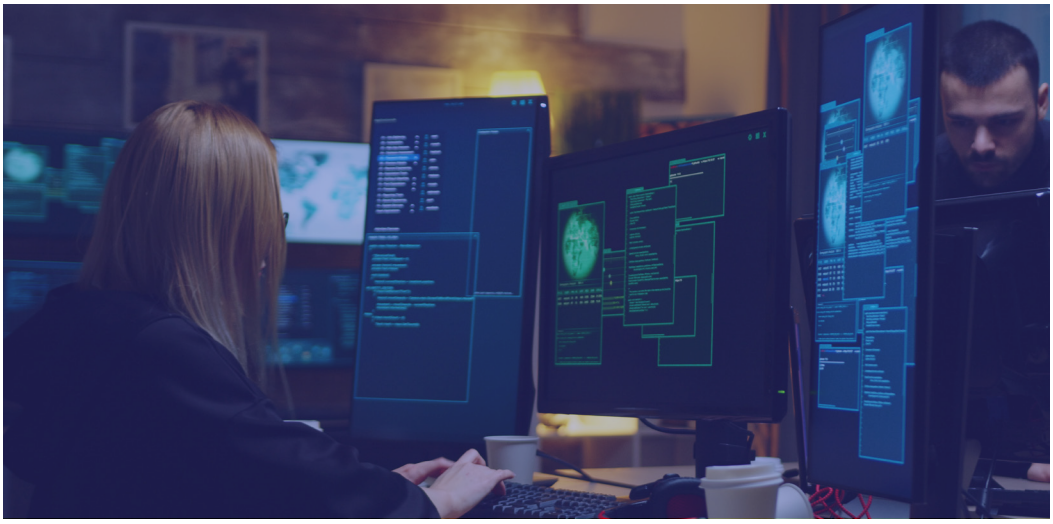
02 Estándares de Referencia

Aunque EASA no reconoce actualmente ninguna norma internacional relacionada con la seguridad de la información como la ISO 27001 u otras normas similares, sí que reconoce que la certificación en alguna de estas normas facilita el cumplimiento con la regulación descrita en la Part-IS, con los correspondientes matices y adaptaciones necesarias.

Las diferencias clave en la implementación de ISMS por parte de la ISO 27001 y los requisitos de la Part-IS son los siguientes:

- Orientación del ISMS a los riesgos de seguridad de la información que tengan potencial impacto en la seguridad de la aviación: los requisitos de la ISO 27001 no tienen por qué tener en cuenta esta orientación, ni los mismos objetivos. De este modo
  - La política de seguridad de la información,
  - el alcance del ISMS,
  - los análisis de riesgos de seguridad, y su orientación a las consecuencias sobre la seguridad de la aviación.
  - los planes de acción, deben ser alineados con este requisito.
- Vinculación entre ISMS y el resto de los sistemas de gestión: en la ISO 27001 el ISMS puede estar aislado de los otros sistemas de gestión de la compañía. La orientación a la seguridad de la aviación requiere que ISMS esté vinculado y relacionado con los otros sistemas de gestión de la compañía y en particular con el SMS.
- Autoridad competente (AESA, EASA): la supervisión de la autoridad no existe en la ISO 27001, siendo requerido por la Part-IS aprobación de procesos y procedimientos, requisitos de acceso a organizaciones contratadas, proporcionarles la documentación de gobernanza (Manual), así como de eventos, vulnerabilidades, análisis y medidas de seguridad de la información que afecten a la seguridad de la aviación (reporte de condiciones inseguras).
- Participación y responsabilidad del Gerente Responsable de la Organización en el ISMS: el Gerente Responsable como máxima autoridad, con capacidad de decisión a la vez que, de asignación de recursos orientados a la seguridad de la aviación, debe tener un papel clave en el ISMS (rol no contemplado en la ISO 27001), a la hora de estar informado del plan

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



de tratamiento de riesgos (ante un evento), hallazgos de auditorías, etc. A lo largo de esta guía, el término "Gerente Responsable" se utiliza para referirse al gestor responsable o, en el caso de las organizaciones de diseño, al responsable de la organización de diseño.

- Función de "compliance monitoring": aunque existe dentro de la ISO 27001 el proceso de auditorías de sistema, la verificación del cumplimiento regulatorio no está explícitamente incluido, siendo un requisito específico de la Part-IS, siendo posible cubrirlo con el realizado como consecuencia de otros requisitos, como es la propia regulación de aeronavegabilidad aplicable (PARTE 21, PARTE 145, CAMO).

- Interfaces con otras organizaciones: en la Part-IS requieren considerar la mutua exposición a los riesgos de seguridad de la información y, por tanto, la obligación de informar sobre los riesgos compartidos. Ampliación de las organizaciones consideradas en los interfaces. Introducción del concepto de "Cadenas funcionales" frente la propia protección. Estos requisitos, son más específicos en lo tocante a supervisión y comunicación en el caso de organizaciones contratadas.

- Exención y Derogación: La posibilidad de exención y derogación en casos específicos, que es totalmente independiente de la ISO 27001.

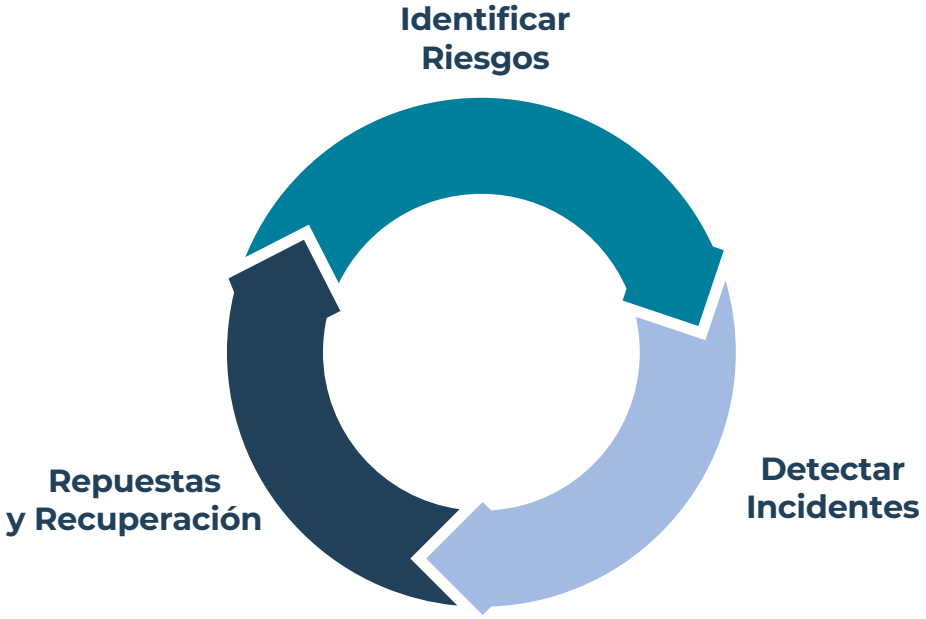
Se recomienda revisar en detalle el anexo IV "Part-IS requirements mapping to ISO/IEC 27001:2022 clauses and controls, and considerations on differences" de Easy Access Rules for Information Security ed. Dic. 2025 disponible en la página oficial web de EASA https://www.easa.europa.eu

EUROCAE ha publicado el informe ER-040 que ofrece orientación para la implementación de un sistema de gestión de la seguridad de la información que complementa el actual Sistema de Gestión de la Seguridad. Responde a la necesidad de soluciones de seguridad de la información coherentes en toda la cadena de suministro. Este informe tiene como objetivo establecer las mejores prácticas para la seguridad de la aviación, garantizando la coherencia y niveles mínimos de seguridad de la información en toda la cadena de suministro, y fomentando un entendimiento común para facilitar las auditorías a todas las partes interesadas. Este documento complementa y proporciona orientación adicional en apoyo de los Medios Aceptables de Cumplimiento (AMC) y los Materiales de Orientación (GM) de la Part-IS de la Agencia Europea de Seguridad Aérea (EASA).

03 Elementos de Un sistema de gestión de Seguridad de la información

El sistema de gestión de la seguridad tiene el objetivo de dotar a la organización de la capacidad de:

1. Identificar y gestionar los posibles riesgos de seguridad de la información que tengan efecto en la seguridad de la aviación
2. Detectar posibles incidentes de seguridad de la información que sufra la organización.
3. Responder a dichos incidentes y recuperarse de los mismos.



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

Para ello, la organización debe desarrollar un sistema, que esté integrado en el resto de los sistemas de la organización, alineado con estos, y que aproveche los procesos de gestión de riesgos existentes (como el Sistema de Gestión de la Seguridad, SMS) y los controles ya establecidos.

Como cualquier otro Sistema de Gestión, el ISMS se compone de cuatro pilares:

1. Política y Objetivos de Seguridad:

a. Compromiso y liderazgo de la Dirección en materia de seguridad de la información, mediante la toma de decisiones y asignación de los recursos necesarios, así como para desarrollar una cultura de seguridad positiva.

b. Establecimiento de los objetivos de la organización en materia de seguridad de la información.

2. Gestión de los Riesgos de Seguridad:

a. Identificación de los riesgos de seguridad de la información que pudieran tener efecto en la seguridad de la aviación.

b. Evaluación y clasificación de estos en base a la severidad de las consecuencias para la seguridad de la aviación, y la probabilidad de ocurrencia de la situación que dé lugar al riesgo.

c. Tratamiento de los riesgos, mediante la incorporación de medidas o controles de seguridad de la información (planes de tratamiento del riesgo).

3. Aseguramiento de la Seguridad

a. Supervisión continua de la eficacia de las medidas de seguridad de la información que puedan afectar a la seguridad de la aviación, mediante controles operacionales, indicadores y revisiones periódicas.

b. Verificación del cumplimiento de los requisitos regulatorios aplicables, incluyendo inspecciones, auditorías y pruebas de seguridad conforme a la normativa de aviación civil.

c. Detección, notificación y gestión de incidentes de seguridad de la información con impacto potencial en la seguridad de la aviación, garantizando la coordinación con las autoridades competentes cuando proceda.

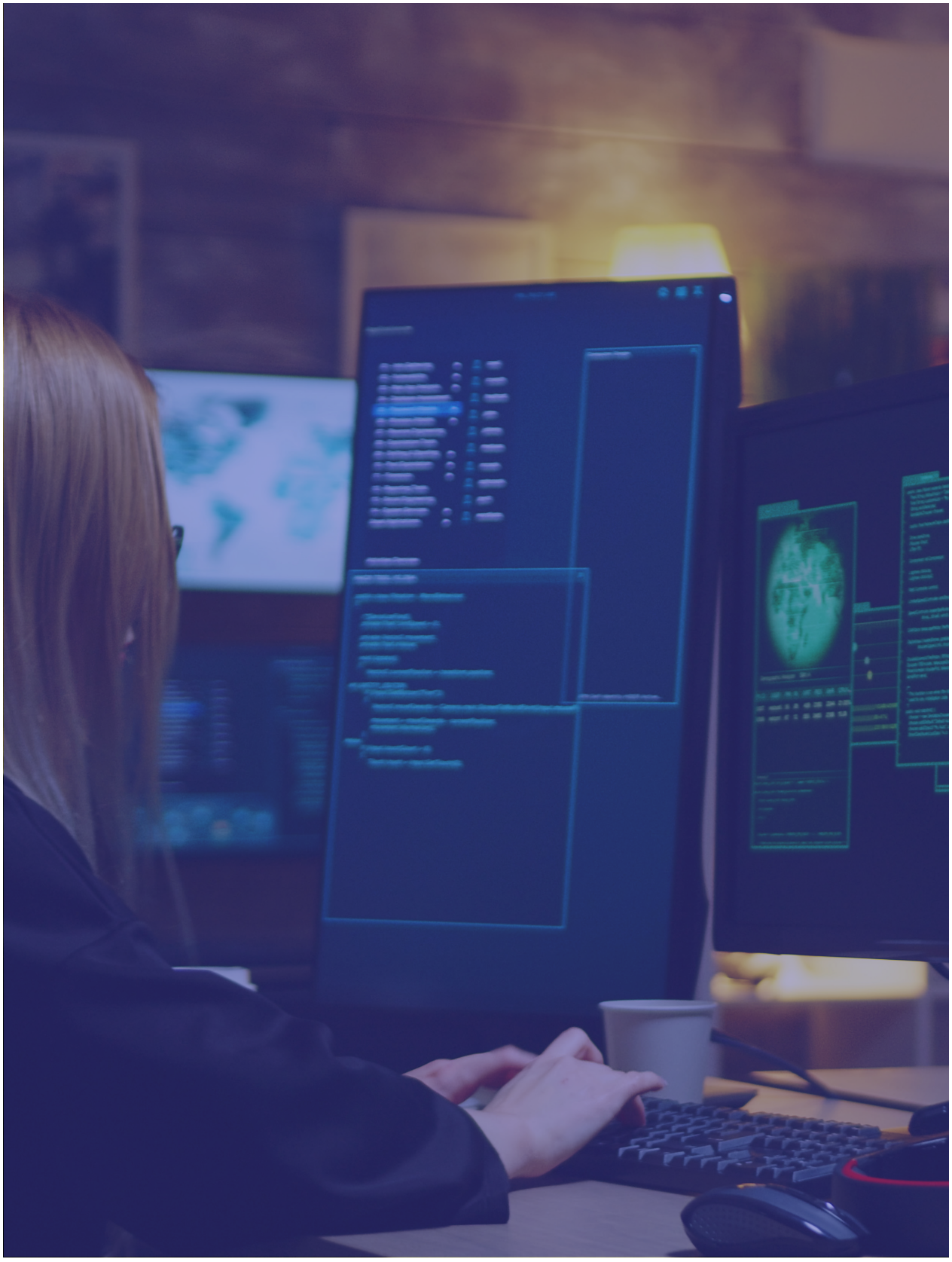
d. Evaluación periódica de la eficacia de los controles implementados, incluyendo su capacidad para prevenir, detectar y responder a actos de interferencia ilícita.

e. Implementación de acciones correctivas y de mejora continua derivadas de auditorías, incidentes o evaluaciones de seguridad.

4. Promoción de la Seguridad

a. Capacitación y entrenamiento: la instrucción y la educación sobre competencias técnicas, alienta una cultura de seguridad positiva, que contribuye a alcanzar los objetivos de seguridad.

b. Comunicación y distribución de la información: deben existir procesos y procedimientos que faciliten la comunicación eficaz a través de todos los niveles organizativos, mediante mecanismos abiertos y constructivos. Esta comunicación debe integrar también a las Autoridades competentes y las organizaciones con las que tenemos interfaces.



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

Junto con ellos, debe establecerse:

- los mecanismos de gobernanza del sistema, mediante la edición del Manual del Sistema de Seguridad de la información, así como los necesarios procedimientos que rijan las actividades encuadradas en dicho manual.

- mecanismos para el registro y documentación de escenarios de amenaza, riesgos, análisis de los riesgos, planes de tratamientos de los riesgos, etc.

Para una correcta implementación del sistema de acuerdo a la reglamentación de EASA, hay que considerar 13 aspectos clave para lograr los objetivos antes indicados:

1. Establecimiento de una Política en materia de seguridad: determina los principios generales de la organización con respecto a los riesgos relacionados con la seguridad de la información con respecto a la seguridad de la aviación.

2. Identifique y revise los riesgos de seguridad de la información.

3. Defina y aplique medidas de tratamiento de riesgos.

4. Implemente un esquema de informes internos conforme.

5. Detecte eventos de seguridad, identifique incidentes que afecten a la seguridad de la aviación, y responda y se recupere de ellos.

6. Aplique las medidas notificadas por las autoridades en respuesta a incidentes de seguridad o vulnerabilidades.

7. Aborde las observaciones reportadas por la autoridad competente.

8. Implemente un esquema de informes externos para que la autoridad competente tome medidas.

9. Cumpla con los requisitos al externalizar actividades.

10. Cumpla con los requisitos de personal.

11. Adhiera a los mandatos de mantenimiento de registros.

12. Monitorice el cumplimiento regulatorio, proporcionando retroalimentación para acciones correctivas.

13. Proteja la confidencialidad de la información sensible recibida.

Junto con estos aspectos, la organización debe implementar un proceso de mejora continua para cumplir consistentemente con los objetivos antes citados.

Todos los procesos y roles clave deben ser documentados, siendo actualizados con los requisitos aplicables.

Los procesos de la organización deben estar alineados con la complejidad de sus actividades y evaluación de riesgos, integrándose con los sistemas de gestión existentes si es posible.

Con la debida documentación y aprobación, la organización puede estar exenta de algunos requisitos si demuestra que no hay riesgos significativos de seguridad que impacten en la seguridad de la aviación, sujeto a revisión continua por parte de las autoridades.

Manual del ISMS

Con el objeto de documentar la gobernanza del sistema, la organización debe proporcionar un manual de gestión de seguridad de la información y documentos relacionados, a la autoridad competente.

Debe ser entregado y aprobado por la autoridad competente, tanto la versión inicial como sus actualizaciones y enmiendas, las cuales deben seguir un procedimiento establecido y documentado.

La organización puede integrarlo con otros manuales de gestión, con referencias cruzadas claras a los requisitos de la regulación aplicable de seguridad de la información (Part-IS).

04 Política de Seguridad de la información – Objetivos e Indicadores

Política de Seguridad

Uno de los pilares fundamentales de la implementación del Sistema de Seguridad de la Información de acuerdo con la Part-IS es la Política de la Seguridad de la Información.

La definición de la política se debe realizar de acuerdo con los siguientes aspectos: gobernanza, gestión del riesgo y cumplimiento regulatorio. Estos aspectos son básicos en el desarrollo de un sistema de seguridad de la información, basado por ejemplo en la ISO 27001, pero para adaptarse a la Part-IS debe alinearse con los objetivos de Seguridad de la Aviación previamente descritos en el Sistema de Gestión de la Seguridad (SGS).

La perspectiva de gobernanza implica proporcionar dirección y liderazgo para lograr los objetivos generales de la entidad, lo que incluye:

- Liderazgo y compromiso de la alta dirección, asegurando su estrecha participación y una implementación del ISMS de “arriba hacia abajo”, siendo una de las responsabilidades esenciales de todos los gestores de una Organización.
- Alineación y consistencia de los objetivos de seguridad y protección de la información con los objetivos de seguridad de la aviación, junto con otros objetivos de la empresa (como los comerciales, de continuidad de negocio, etc.), monitorizados a través de revisiones gerenciales.
- Estableciendo los principios y objetivos a alcanzar, medidas de rendimiento, y los roles, responsabilidades, competencias, en particular del personal clave, y dotar de los recursos necesarios para un ISMS efectivo.
- Promoviendo la política, dentro de la Organización, para todo el personal de manera periódica o ante cambios, mediante sesiones de formación y/o concienciación.
- Comprometiéndose con una comunicación efectiva de la política de seguridad de la información, adaptada a las partes interesadas internas y externas.
- Fomentar la “cultura justa” y la notificación de vulnerabilidades, sucesos sospechosos, anómalos y/o incidentes de seguridad de la información.

La perspectiva de gestión de riesgo se centra en un aspecto clave de un ISMS en el contexto de la seguridad de la aviación de acuerdo con la regulación. Forma una base para la toma de decisiones transparentes y la priorización de controles y opciones de tratamiento de riesgos, así como la asignación de recursos. Además, incluye la evaluación, tratamiento y monitorizado de los riesgos de seguridad de la información para apoyar la gestión de riesgos de seguridad de la aviación para procesos e informaciones clave. Tiene en cuenta los requisitos de protección, la exposición al riesgo, la actitud hacia los riesgos, los criterios de aceptación de riesgos, los métodos y los estándares de la industria.

La perspectiva de cumplimiento aborda la adherencia a los requisitos regulatorios, legales y contractuales. Esto incluye:

- Cumplimiento con la legislación aplicable, las normas pertinentes y las mejores prácticas.
- Adherencia a las propias políticas y estándares de la entidad, así como la aplicación de los requisitos del ISMS en todos los procesos de la Organización.

La política de seguridad de la información debe ser revisada de manera periódica, o como consecuencia de cambios significativos en la regulación aplicables, tecnológicos o del propio negocio de la Organización.

Ejemplo de Política de Seguridad de la Información

Propósito

La presente política establece el compromiso de la Organización [Nombre de la Empresa] con la protección de la información crítica para la seguridad operacional, de acuerdo con los requisitos de la Part-IS y otras normativas nacionales e internacionales aplicables

Objetivo

La Organización [Nombre de la empresa] considera de vital importancia la protección de los activos de información, tanto los propios como los de nuestros clientes y proveedores, para lo que se ha establecido un Sistema de Gestión de la Seguridad de la Información (ISMS) que salvaguarda la Confidencialidad, la Integridad, la Disponibilidad y la Trazabilidad de la información tratada en la Organización, adoptando una metodología formal para la identificación, evaluación (análisis) y tratamiento de riesgos que se revisarán periódicamente y se actualizarán ante cambios tecnológicos, normativos o de negocio

Alcance

Esta política aplica a todos los empleados, contratistas, sistemas, procesos y activos que intervienen en la gestión de información relacionada con la actividad de la organización

Compromiso

La Dirección de la Organización [Nombre de la Empresa] se compromete firmemente con la Seguridad de la Información proporcionando los recursos y medios que se necesiten para el desarrollo e implantación de cuantas medidas sean necesarias para la gestión proactiva y sistemática del ISMS así como su operación

Roles/ Res-posabilidades

Para ello se designa un Responsable de Seguridad de la Información (RSI), encargado de coordinar la implementación ISMS, y se establece un Comité de Seguridad de la Información, responsable de la revisión del ISMS y sus controles, demostrando su compromiso con la mejora continua.

Para conseguir un ISMS eficaz, es fundamental la participación e implicación de todas las personas que componen la Organización, mediante el cumplimiento de esta política, y, garantizado por la dirección, participando en actividades de formación y concienciación adecuadas a su actividad, que permita conocer y cumplir esta política y los requisitos de seguridad.

Reporte

La Organización [Nombre de la Empresa] establecerá canales seguros para la comunicación interna y externa de información sensible, así como garantizará la coordinación con autoridades nacionales y europeas en materia de seguridad de la información.

Cultura Justa

La Organización alienta a todas las personas que la componen a informar de cualquier evento/situación que afecte a la seguridad de la información en un contexto de "cultura justa" en el que no se tome acción alguna contra las personas que reporten dichos eventos, excepto en el caso de negligencia grave, violaciones intencionales o actos destructivos,

Revisión

Esta política será revisada al menos una vez al año o cuando se produzcan cambios significativos en el entorno normativo, tecnológico o de negocio.

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

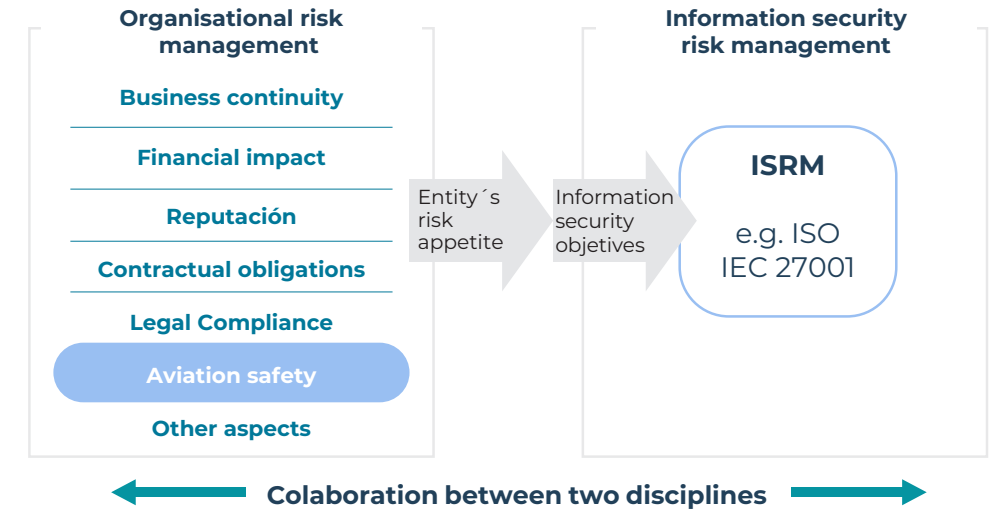
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24

info@tedae.org
www.tedae.org

Objetivos de Seguridad

Como cualquier sistema de gestión, el ISMS debe tener un conjunto de objetivos e indicadores que respondan a los compromisos que la Dirección de la Organización ha descrito en la correspondiente Política de Seguridad de la Información.

Dichos objetivos deben responder a los requisitos aplicables a la seguridad de la información, que garanticen la continuidad del negocio, el impacto financiero, requisitos legales y contractuales y aspectos reputacionales, tal y como, por ejemplo, la implementación del ISMS de acuerdo con la ISO 27001 requiere, pero, en el contexto de la implementación de la Part-IS, además, deben estar alineados, o incluirlos, los objetivos de Seguridad de la Aviación explicitados en el SMS, y que por tanto, tienen influencia en los elementos del ISMS.



Estos objetivos deben ser:

- Coherentes y alineados con la política de seguridad de la información.
- Considerar los requisitos de seguridad de la información aplicables derivados de los objetivos generales de la organización (en particular incluyendo los de seguridad de la aviación), y los resultados de la evaluación y el tratamiento de riesgos (que, a su vez, apoya la implementación de los objetivos estratégicos y la política de la seguridad de la información).
- Ser revisados periódicamente para asegurar que están actualizados y siguen siendo adecuados.
- Específicos, medibles si es factible, mediante KPIs, alcanzables, realistas y oportunos.
- Alineados con todas las personas afectadas.

Los siguientes KPIs, pueden servir de ejemplos para el ISMS en aplicación de la Part-IS:

- Porcentaje del personal con la formación de seguridad de la información completada.
- Número de hallazgos de Seguridad de la Información en auditorías.
- Número de análisis de riesgos de Seguridad de la aviación consecuencia de riesgos de seguridad de la información.

05 Evaluación y tratamiento de los Riesgos de seguridad de la información

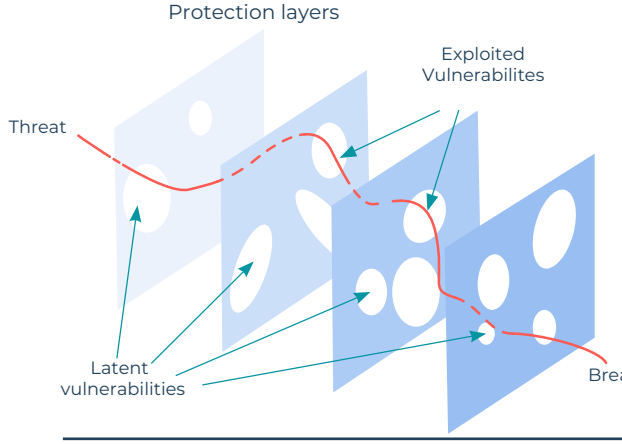
La organización debe identificar y revisar los riesgos de seguridad de la información.

Para ello necesita realizar las siguientes tareas:

1. Identificar todos los elementos que puedan estar expuestos a un riesgo de seguridad de la información. Esta identificación incluye las propias actividades, instalaciones, recursos, servicios operados, proporcionados, recibidos o mantenidos por la organización, equipos y sistemas y datos usados en los procesos anteriores.
2. Identificar todos los riesgos para la seguridad de la información que pudieran sufrir los interfaces que la organización tenga establecidos con otras organizaciones.

Estos riesgos conllevan lo que se denomina "Escenario de Amenaza" ("Threat Scenario") que responde a:

- Las posibles formas en las que en una organización podría materializarse una amenaza.
- La descripción de un ataque dirigido contra uno de los elementos identificados anteriormente.



clases de vulnerabilidades:

1) Las explotadas, en las que la violación en la seguridad de la información existe desde que el evento produce daños.
2) Las latentes, debilidades del sistema que podrían ser aprovechadas para dar lugar a un fallo o violación de la política de seguridad de la información.

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

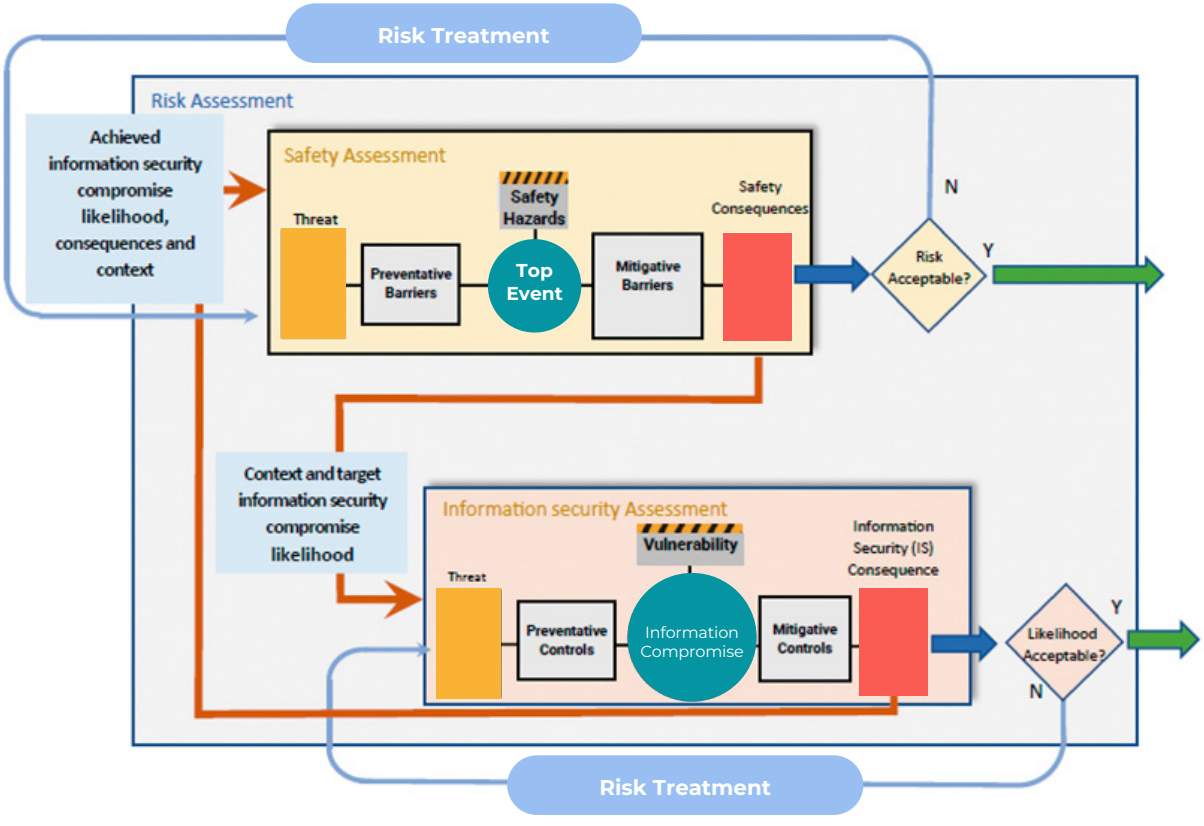
Es muy importante que la organización analice y determine el alcance ("scope") y los límites ("boundaries") del sistema ISMS. Para ello debe desarrollar un claro e integral conocimiento de sus propias actividades en la aviación, los procesos y sistemas de información asociados, así como los flujos de datos e intercambios de información relevante, los cuales definen el alcance y los límites de la evaluación de riesgos de seguridad de la información.

Este conocimiento debe estar debidamente documentado, estableciendo qué recursos, dependencias relacionadas con la informática, redes y servicios contratados, puedan afectar a la seguridad de la información, protección de servicios, capacidades y funciones de la propia organización.

Ejemplos de elementos a tener en cuenta:

- Entradas y salidas operacionales relevantes a las funciones, servicios y capacidades de la organización: transferencia electrónica de pedidos, comunicación electrónica de datos relevantes de fabricación, diseño o mantenimiento, etc.
- Activos relevantes usados en la actividad de la organización: ERP, Software de gestión de ciclo de vida (PLM), Software de MRO.
- Entornos operativos: oficina, áreas de acceso público, salas con control de acceso, etc.
- Los métodos, procesos y recursos usados para gestionar, operar o mantener los recursos identificados: servicios de mantenimiento informático, etc.

Por otro lado, la organización debe identificar aquellos riesgos de la seguridad de la información que pudieran tener impacto en la seguridad de la aviación.



Como se puede observar del gráfico anterior, ante un riesgo de seguridad de la información identificado, las posibles consecuencias deben considerarse como posibles amenazas para la seguridad de la aviación (SMS), ser analizados y tratados.

El riesgo identificado y así analizado, debe ser actualizado y revisado en caso de:

a. Hay cambios en los elementos sujetos a los riesgos de seguridad.

b. Hay cambios en los interfaces entre la organización y otras, así como cambios en los riesgos comunicados por las organizaciones con las que se tienen interfaces.

c. Haya cambios en la información o conocimiento usado para la identificación, análisis y clasificación de los riesgos de seguridad de la información.

d. Las lecciones aprendidas de los análisis de los incidentes de seguridad.

Nivel de Riesgo

A cada uno de ellos, elemento o interfaz antes indicado, deberá asignarles un nivel de riesgo, establecido de acuerdo con una clasificación decidida por la propia organización,

1. en la que se tendrá en cuenta la posibilidad de que se dé el escenario del suceso,

2. así como su impacto en la seguridad.

A la hora de establecer la clasificación, este debe realizarse con rigor y disciplina, documentado el proceso y su robustez, teniendo en cuenta:

- Su reproductibilidad, obteniendo los mismos resultados ante similares entradas,

- Su repetibilidad a lo largo del tiempo, de modo que dichos resultados puedan ser comparados con otros para determinar los cambios,

- La recopilación de datos que sean válidos y pertinentes para el caso, en particular, aquella información que permite la determinación de las consecuencias para la seguridad de la aviación, así como los que permiten establecer la potencial ocurrencia del "escenario de amenaza" correspondiente.

- Un refinamiento iterativo a lo largo del tiempo de los escenarios, a medida que los datos de entrada están disponibles, que permitan reducir las incertidumbres (amenazas, vulnerabilidades, efectividad de los controles existentes y dependencias de entidades externas).

Basado en dicha clasificación, la organización deberá establecer en qué casos el riesgo identificado es aceptable o requiere la implementación de acciones mitigadoras o de contención.

Siguiendo la anterior metodología de análisis, se recomienda que la potencial ocurrencia de un escenario sea englobada en una de las siguientes categorías:

- **Alta posibilidad de suceso:** el escenario es probable que ocurra; el ataque relacionado es posible y amenazas similares han ocurrido muchas veces en el pasado.

- **Potencial medio de suceso:** el escenario es improbable que ocurra; el ataque relacionado es posible y amenazas similares pudieran haber sucedido en el pasado.

- **Bajo potencial de suceso:** el escenario es muy improbable que ocurra; el ataque relacionado es teóricamente posible, pero no se conoce que haya ocurrido en el pasado.

Cada organización, si lo necesita, puede definir categorías adicionales para categorizar sus riesgos.

La evaluación de la potencial ocurrencia de un suceso se puede basar en los siguientes aspectos:

- **Protección:** medidas que evitan el acceso a los recursos comprometidos, el grado en que estas medidas evitan el ataque/acceso desde los recursos comprometidos, el grado en que dichas medidas pueden fallar, métodos de identificación del posible ataque.

- **Reducción de la exposición:** condiciones de acceso externo de usuarios y atacantes, limitaciones en la funcionalidad de acceso externo, gestión de vulnerabilidades, reducción de la severidad de ataques exitosos.

- **Intento de ataque:** capacidad de los atacantes determinados por sus recursos o conocimiento requerido para el mismo.

Con respecto a las consecuencias, la organización debe asociar la correspondiente severidad de las consecuencias de acuerdo con una clasificación como la que sigue:

- **Alta severidad:** aquellos escenarios, inmediatos o diferidos, que pueden causar o contribuir a una situación insegura para la operación de la aeronave, o lo que es lo mismo, que puedan producir la muerte o daños graves a las personas, que la aeronave sufra daños o fallo estructural, o que la aeronave se pierda o sea totalmente inaccesible.

- **Severidad moderada:** aquellos escenarios, inmediatos o diferidos, que pueden causar o contribuir a un incidente (cualquier situación que no sea un accidente), asociado con la operación de la aeronave, y que afecte o pueda afectar a la seguridad de la operación.

- **Baja severidad:** aquellos escenarios, inmediatos o diferidos, que causan o contribuyen a consecuencias con despreciable efecto en seguridad.

Cada organización, si lo necesita, puede definir categorías adicionales para categorizar sus riesgos.

Criterio de Aceptabilidad: matriz de aceptabilidad de riesgos de seguridad

Con la evaluación de la severidad y la potencial ocurrencia de un suceso/escenario, la organización debe clasificar los riesgos en una de las siguientes categorías:

- Riesgos inaceptables.
- Riesgos condicionalmente aceptables.
- Riesgos aceptables.

Estableciendo la matriz de aceptabilidad:

ICA Annex 13>	Negligible effect	Incident	Accicent
Threat scenario-potencial of cocurrence	Low safety consequences	Moderate safety consequences	High safety consequences
High	Conditionally acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally acceptable	Not acceptable
Low	Acceptable	Acceptable	Conditionally acceptable*

* La potencial de ocurrencia del suceso debe ser revisada periódicamente y monitorizada para asegurar que permanece baja, y si el riesgo se materializa, este es detectado y abordado a tiempo.

Esta matriz se debe ajustar a las diferentes clasificaciones identificadas por la organización y aceptada por el Gerente Responsable de la organización.

NOTA: Los criterios de aceptación condicional de riesgos deben tener en cuenta cuánto tiempo se espera que exista un riesgo, o pueden incluir requisitos para el tratamiento futuro para reducir el riesgo a un nivel aceptable dentro de un período de tiempo definido, así como su gestión a lo largo del tiempo. **Para poder definir estos criterios es requerido un alto nivel de madurez de la organización en la gestión de riesgos de seguridad de la información.**

Tratamiento de los riesgos de Seguridad

Una vez evaluados los riesgos para la seguridad y establecido su grado de aceptabilidad, la organización debe desarrollar medidas para gestionar los riesgos identificados como **inaceptables.**

Dichas medidas, o controles de seguridad de la información, deben estar orientadas a dotar a la organización de:

- Control sobre las circunstancias que contribuyen a que un determinado escenario de amenaza se materialice.
- Reducir las consecuencias sobre la seguridad de la aviación asociadas a la materialización de los escenarios de amenaza,
- Evitar los riesgos.

> **“ES REQUERIDO UN ALTO NIVEL DE MADUREZ DE LA ORGANIZACIÓN EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN”**

Es fundamental asegurar que las medidas adoptadas no generen nuevos riesgos potenciales para la seguridad de la aviación.

Los tratamientos de los riesgos deben considerar las medidas, métodos y recursos utilizados a lo largo del ciclo de vida de cada recurso, para:

- Gestionar la reducción del riesgo,
- Monitorizar y mantener cada recurso.
- Actualizar y cumplimentar actividades de gestión de configuración.
- Gestionar la cadena de suministro.
- Gestionar los servicios contratados y los proveedores de servicios.

Y deben ser revisadas (al igual que los análisis de riesgos) de manera regular o condicional, para identificar si siguen siendo efectivas o requieren adaptaciones.

Los resultados del análisis de riesgos, así como la clasificación de los escenarios de amenaza y las medidas adoptadas deben ser informadas a:

- El Gerente Responsable (“Accountable Manager”), o la persona o grupo de personas designados por estos para asegurar que la organización cumple con los requisitos de la regulación.
- Aquellas organizaciones con las que se tiene interfaz, en caso de que el riesgo sea compartido.

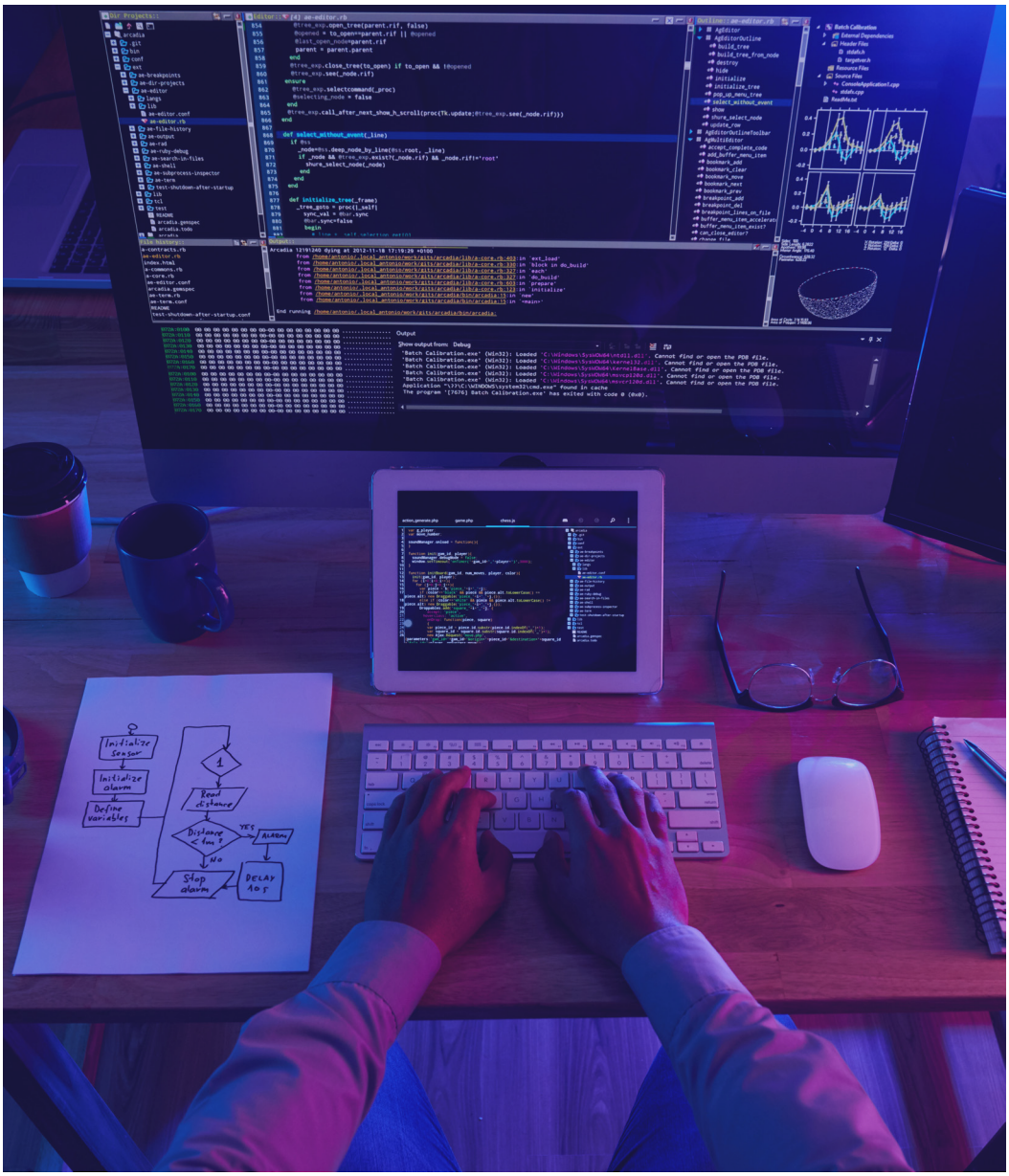
El resultado debe materializarse en un plan de tratamiento del riesgo que incluya una priorización de los riesgos, los objetivos y medios necesarios para obtener un nivel de riesgo aceptable, así como un plan de hitos (“timeline”) en el que las medidas deben ser implementadas, acordado con los responsables de la implantación y aprobados por el Gerente Responsable (“Accountable Manager”), o la persona o grupo de personas designados. Este plan se puede usar como medio de comunicación

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

con la Autoridad Competente, así como con las organizaciones con las que se tiene interfaces, para demostrar el tratamiento efectivo de los riesgos inaceptables, y cómo los riesgos compartidos son controlados.

Cualquier retraso en la implementación del plan, debe ser registrado en el caso de que los riesgos puedan causar una situación insegura, caso que debe ser comunicado a la Autoridad Competente (tras su actualización) y aceptado por el Gerente Responsable ("Accountable Manager"), o la persona o grupo de personas designados. Esta situación puede requerir la implementación o disponibilidad de controles de compensación o medidas reactivas, que permitan la detección y reacción a tiempo en caso de que el riesgo se materialice.

Los tratamientos de los riesgos deben ser registrados y documentados, por ejemplo, en un registro de riesgos, incluso aunque se hayan evitado completamente



06 Incidentes de seguridad de la información. Detección, Respuesta, Recuperación

Debemos establecer un enfoque sistemático para detectar, responder y recuperarse de incidentes de seguridad de la información, alineado con los requisitos de Part-IS. .

1. Detección de Incidentes

- Establecer mecanismos de monitorización continua de los sistemas críticos.
- Configurar alertas tempranas y reglas de correlación (SIEM, IDS/IPS, antivirus, etc.).
- Capacitar al personal para la identificación temprana de eventos sospechosos.

Buenas prácticas:

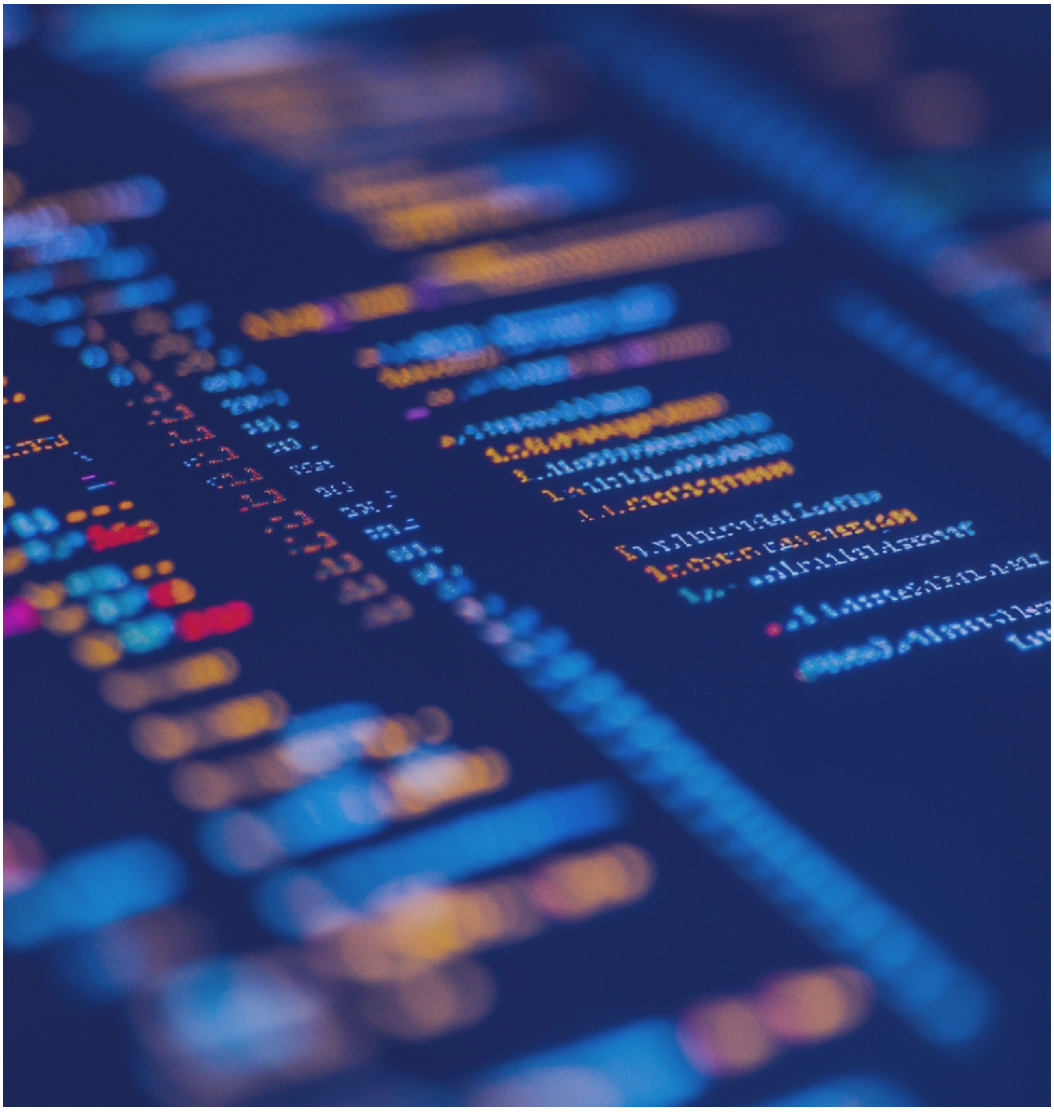
- Implementar herramientas orientadas a la detección de incidentes.
- Definir qué constituye un "incidente" (violaciones de confidencialidad, integridad, disponibilidad y autenticidad).
- Mecanismos de comunicación internos y externos.
- Crear un registro centralizado de eventos e incidentes.

2. Respuesta a Incidentes

- Establecer un procedimiento de gestión de incidentes (clasificación, priorización, escalado).
- Formar un equipo de respuesta a incidentes (IRT/CSIRT) interno o externalizado.
- Mantener canales de comunicación internos y externos (incluyendo autoridades regulatorias si aplica).
- Disponer de un plan de contención y mitigación.

Buenas prácticas:

- Usar herramientas de ticketing para el ciclo de vida del incidente.
- Ejecutar simulacros y ejercicios de respuesta periódicamente.
- Documentar todas las acciones tomadas durante la respuesta.



3. Recuperación tras el Incidente

- Activar los planes de continuidad y recuperación establecidos en el ISMS.
- Restaurar los sistemas afectados a un estado seguro y funcional.
- Evaluar el impacto y aplicar medidas de mejora.

Buenas prácticas:

- Realizar análisis post mortem e identificar y documentar lecciones aprendidas.
- Actualizar controles, reglas de detección y documentación.
- Verificar la integridad de las copias de seguridad antes de la restauración.

07 Registros internos y externos (Informes)

Se deben establecer mecanismos formales para la creación, mantenimiento y comunicación de registros relacionados con la gestión de incidentes de seguridad de la información. Estos registros aseguran la trazabilidad de las acciones, el cumplimiento normativo y la mejora continua.

1. Registros Internos

- Eventos e incidentes de seguridad (detección, respuesta, impacto, resolución).
- Tiempos de actuación (detección, contención, recuperación).
- Decisiones tomadas, responsables y acciones ejecutadas.
- Cambios aplicados a la configuración o controles de seguridad tras un incidente.
- Revisión y aprobación de planes de mejora tras incidentes.

Requisitos:

Los registros deben ser auditables, protegidos contra alteración y almacenados por el tiempo que indique la política corporativa o la regulación.

El acceso debe ser restringido a personal debidamente autorizado.

2. Informes Externos

Obligaciones:

Notificar a la autoridad competente en los plazos requeridos, cuando el incidente:

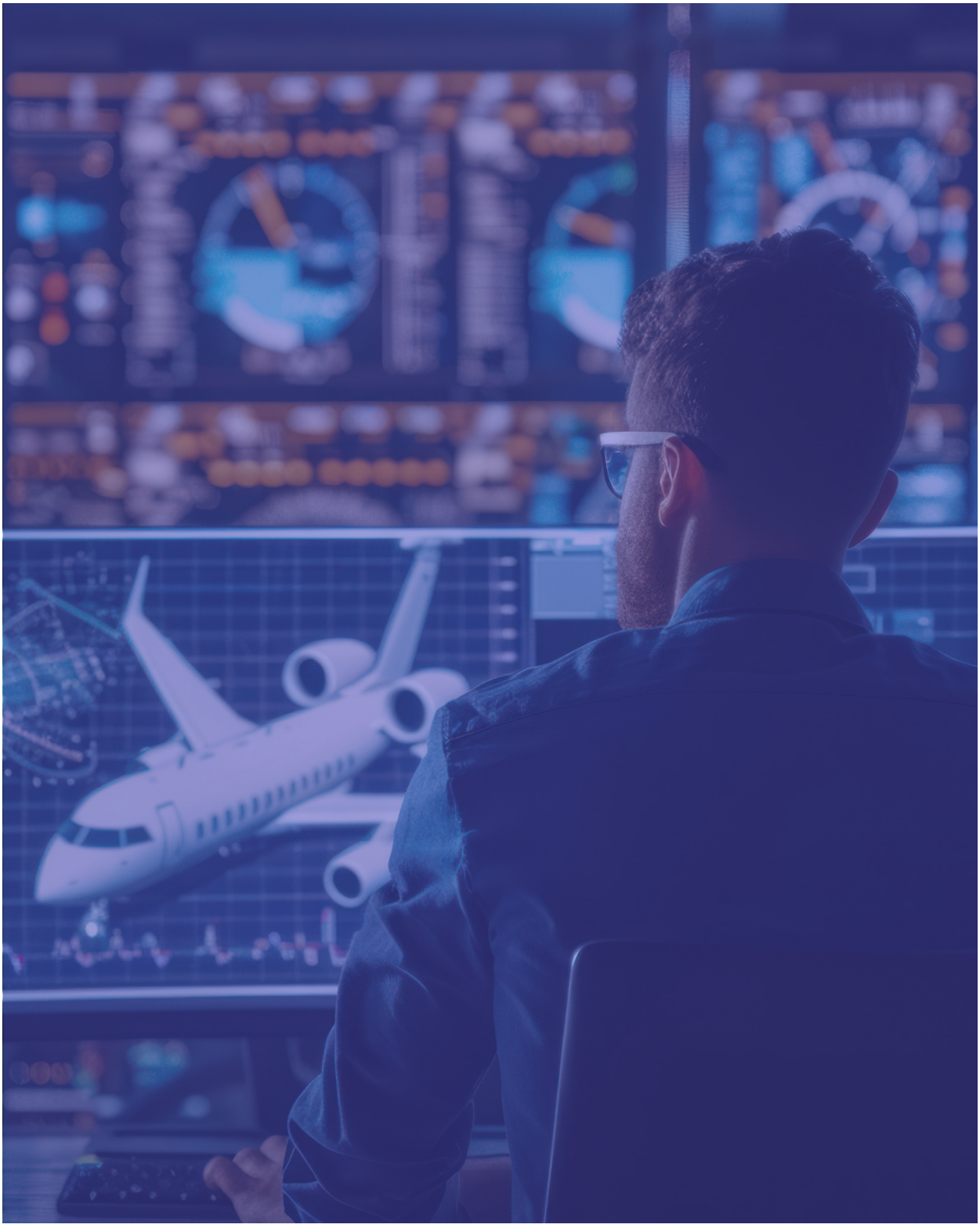
- Impacte servicios esenciales.
- Suponga una amenaza significativa para la seguridad o continuidad operativa.

Informar a socios, clientes o proveedores afectados según acuerdos contractuales o cláusulas de seguridad.

Buenas prácticas:

- Tener modelos de informe predefinidos (fichas, plantillas PDF)
- Establecer un canal formal de comunicación con la autoridad
- Conservar copia de todos los informes enviados

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



08 Comunicación con la autoridad

La organización establece un proceso formal para la comunicación con la autoridad competente en materia de seguridad de la aviación, garantizando la notificación oportuna de incidentes de seguridad de la información que puedan afectar a la seguridad de la aviación, conforme a los requisitos regulatorios aplicables.

1. Principios Clave

- **Notificación inmediata** de incidentes críticos que puedan comprometer la seguridad de la aviación o facilitar actos de interferencia ilícita.
- **Confidencialidad, integridad, autenticidad y trazabilidad de la información comunicada**, garantizadas mediante el uso de canales seguros, mecanismos de identificación del emisor y el registro completo de las comunicaciones.
- **Coordinación con el Sistema de Gestión de Seguridad Operacional (SMS),** asegurando la integración con los procesos de reporte de seguridad de la aviación.
- **Cumplimiento normativo**, garantizando la adecuación a los requisitos de la autoridad competente y marcos regulatorios aplicables.

2. Roles y Responsabilidades

Las siguientes funciones participan en el proceso de comunicación:

Responsable del ISMS

- Garantiza la activación del procedimiento de notificación.
- Supervisa la correcta clasificación del incidente.
- Asegura la conformidad con los requisitos regulatorios aplicables.

Coordinador de Respuesta a Incidentes

- Lidera la ejecución del plan de respuesta.
- Coordina la recopilación de información técnica.
- Prepara el reporte para la autoridad competente.

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

Equipo de Seguridad / Comité de Gestión de Incidentes

- Evalúa el impacto del incidente en la seguridad de la aviación.
- Determina la criticidad del evento.
- Aprueba la comunicación externa.
- Garantiza la trazabilidad del proceso.

Punto de Contacto con la Autoridad Competente

- Actúa como enlace oficial con la autoridad.
- Gestiona el envío de notificaciones.
- Garantiza el cumplimiento de plazos y formatos requeridos.

Las funciones descritas podrán ser asumidas por una o varias personas en función del tamaño, estructura y recursos de la organización, siempre que se garantice la adecuada segregación de funciones cuando sea necesario, así como el cumplimiento efectivo de todas las responsabilidades definidas.

3. Flujo de Notificación

El flujo de notificación de eventos de seguridad de la información incluye las siguientes fases:

1. Detección y clasificación del incidente.
2. Activación del procedimiento de respuesta a incidentes.
3. Evaluación del impacto en la seguridad de la aviación.
4. Notificación a la autoridad competente.
5. Seguimiento y actualización de la información.
6. Registro, cierre y lecciones aprendidas.

Tras estas fases, el proceso de comunicación habrá sido completado.

4. Canales y Plazos

Algunos de los canales habituales, entre otros, incluyen los siguientes:

- Correo electrónico, preferentemente cifrado.
- Plataformas seguras habilitadas por la autoridad competente.
- Comunicación telefónica en caso de incidentes críticos.

Se deben considerar los distintos plazos según la criticidad de la comunicación:

- Inmediato: incidentes críticos con impacto en la seguridad de la aviación.
- ≤ 24 horas: incidentes significativos.
- ≤ 72 horas: envío de informe detallado o final.

5. Contenido Mínimo del Reporte

El reporte requerido por el regulador debería contener:

- Identificación del incidente (fecha, hora, sistemas afectados).
- Descripción del incidente y contexto.
- Evaluación del impacto en la seguridad de la aviación.
- Medidas de mitigación aplicadas.
- Estado actual del incidente.
- Información de contacto para seguimiento.

09 Contratación de actividades de Gestión de seguridad de la información

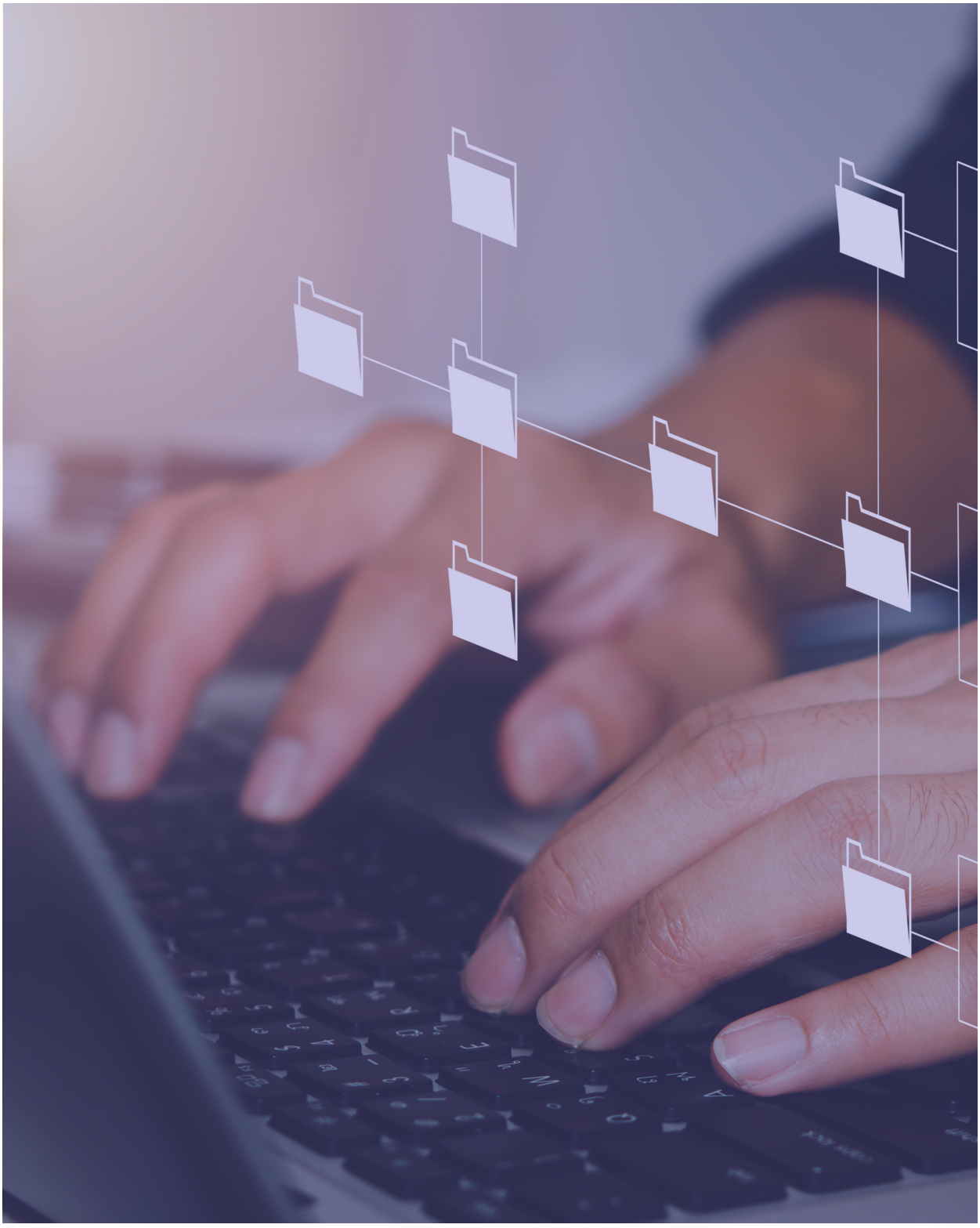
Cuando se contraten externamente actividades directamente relacionadas con el ISMS (auditoría interna, consultoría para la evaluación de riesgos, etc.), estas tienen que cumplir los requisitos y estar bajo la supervisión de la organización.

La autoridad podrá requerir tener acceso a esta organización externa para comprobar que cumple los requisitos exigidos.

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

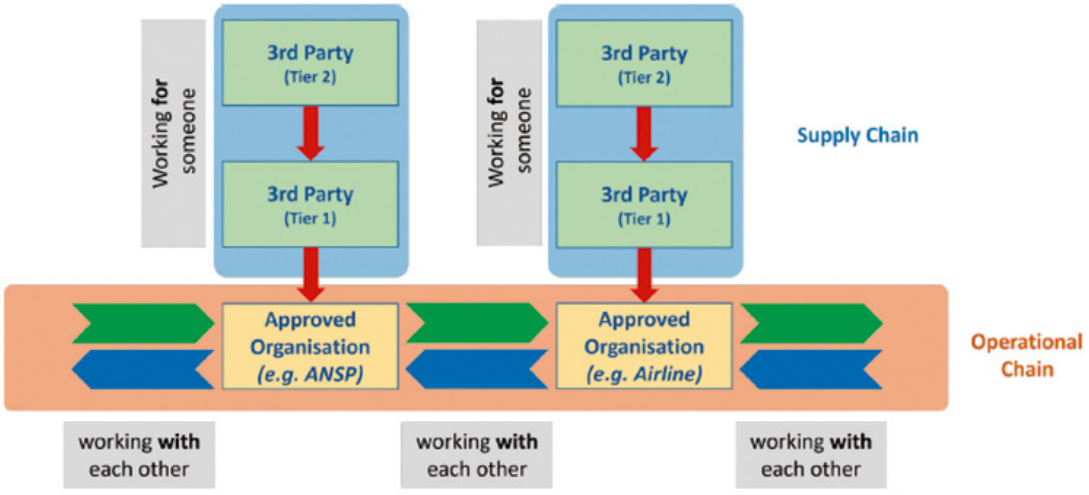


10 Cadena de suministro

¿Qué tienen que cumplir al trabajar con ellos?

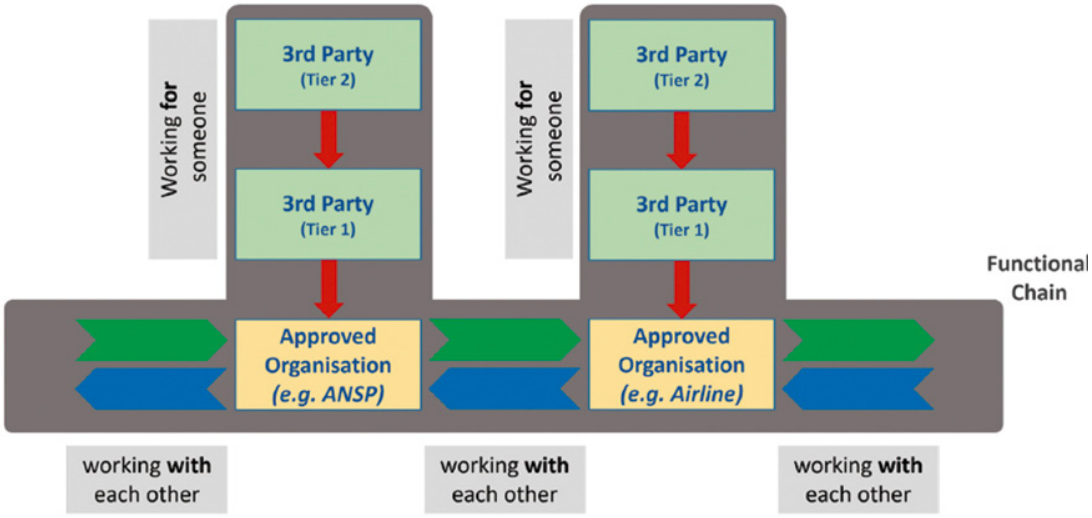
La cadena de suministro juega un papel fundamental en el ISMS requerido por la Part-IS.

Los ISMS basados en el cumplimiento de la ISO 27001, ponen el acento en las interfaces y dependencias entre las actividades realizadas por la organización y las que realizan otras organizaciones, como los proveedores de la cadena de suministro, de modo que se pone el foco en el uso que la organización hace de los productos o servicios del proveedor, analizando los riesgos y vulnerabilidades desde la perspectiva de la propia organización, y los interfaces con sus propios clientes ("cadena operativa"). Los miembros de esta "cadena operativa" son todos aquellos que están aprobados por la correspondiente autoridad de aviación civil, incluyendo a esta misma en dicha cadena.



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

Por otra parte, se define el concepto de "cadena funcional" en el que se integra la cadena de suministro dentro de la "cadena operacional". En este caso, lo que se busca es asegurar que los interfaces entre las diferentes organizaciones (tengan la correspondiente aprobación o no) están adecuadamente protegidas de modo que se prevenga la transferencia de riesgos no deseados, así como minimizar la exposición global a los ataques, mientras que cada organización gestiona sus propios riesgos de manera efectiva. Protegiendo dichos interfaces y manteniendo una potente gestión de riesgos interno, los riesgos de seguridad globales son minimizados



Se espera que tanto los receptores de la información, también llamados consumidores, y los generadores de esta, o proveedores, colaboren para asegurar que la confidencialidad, integridad y disponibilidad de la información está dentro de los límites aceptables para todos los consumidores. Esto implica que puede ser necesario compartir la información de los análisis de riesgos de seguridad de la información y colaborar en los interfaces identificados, proporcionado información de retorno sobre eventos o riesgos que la siguiente organización en la cadena pueda no gestionarlos adecuadamente.

Por tanto, las organizaciones que se interrelacionan (tiene interfaces entre ellas) deben compartir información entre ellas (de manera bilateral) acerca de la potencial exposición a riesgos de seguridad de la información. El propósito de este intercambio de información es establecer un mapa de los servicios que dichas organizaciones prestan, incluyendo todos los flujos de datos e información entre las organizaciones para:

a. Ilustrar, por ejemplo, mediante un diagrama funcional, la lista de las rutas lógicas como físicas que conectan las diferentes partes implicadas.

b. Identificar claramente todos los activos (es decir, hardware, software, red y recursos informáticos) que se utilizarán en el intercambio de información y datos entre las organizaciones.

c. Identificar todas las funciones, actividades y procesos, incluyendo la correspondiente información y datos, que se crearán, transmitirán, procesarán, recibirán y almacenarán, y asociarlos con la parte responsable que proporciona o realiza dichas funciones, actividades y procesos;

d. Determinar, para estas rutas o cadenas funcionales, el papel de cada parte interconectada como productor, procesador, distribuidor o consumidor de la información o los datos involucrados;

e. Determinar si una parte interconectada actúa como originador o receptor de un flujo a través de dicha ruta.

Existen para la regulación dos tipos o categorías de organizaciones interconectadas:

1. La organización interconectada está sujeta a la regulación de la Part-IS: en este caso, y dado que ambas organizaciones deben tener sus propio ISMS de acuerdo a lo regulado en la Part-IS, cada entidad:

   a. Es responsable de identificar los interfaces que su propia organización tiene con otras organizaciones y que pueden ser causa de mutua exposición a riesgos de seguridad de la información. El intercambio de información de riesgos puede ser beneficiosa para poder realizar análisis de seguridad más precisos.

   b. Es responsable ("accountable") de la adecuada gestión de los riesgos de seguridad dentro del alcance de su propio ISMS.

2. En cualquier otro caso, la organización es responsable ("accountable") de la adecuada gestión de los riesgos de seguridad que pueden aparecer como consecuencia de su exposición a la entidad con la que interactúa (o tiene interfaz). En el caso de que dichos riesgos deban ser tratados, la organización siempre tiene la opción de incorporar medidas de mitigación y controles, dentro de su propio alcance. En el caso de que el interfaz sea con un suministrador, la organización puede decidir gestionar estos riesgos mediante cláusulas contractuales y requerir al suministrador medidas de mitigación y controles en su organización.

Ejemplos de interfaces entre organizaciones:

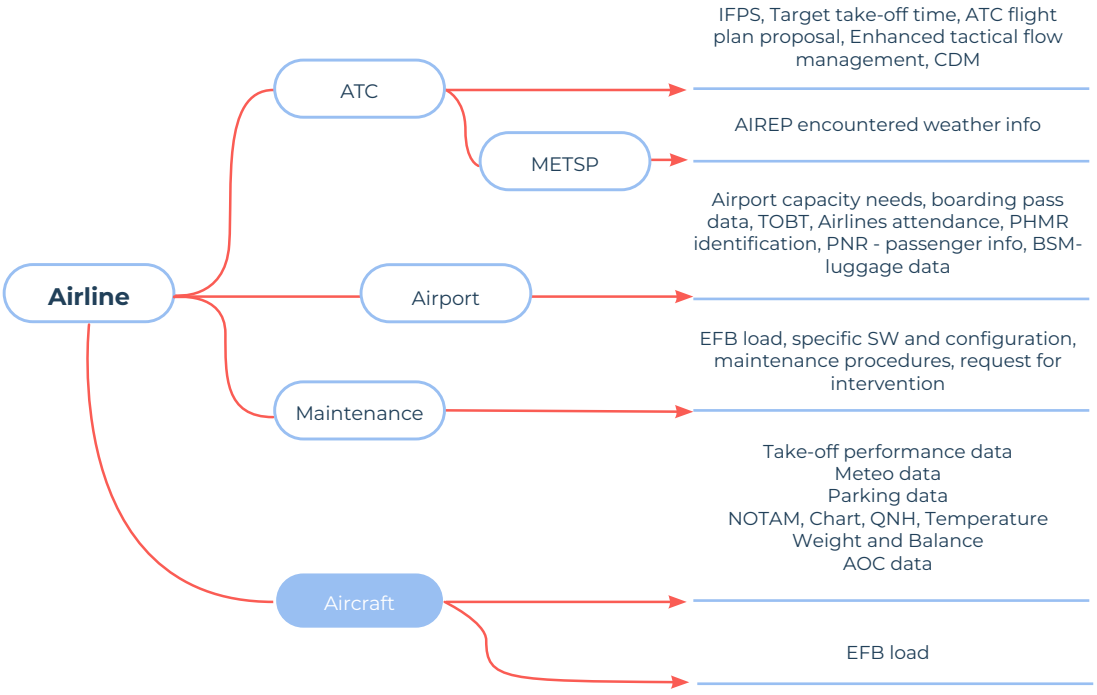


Figure 2: Interfaces of an airline operator with other organisations

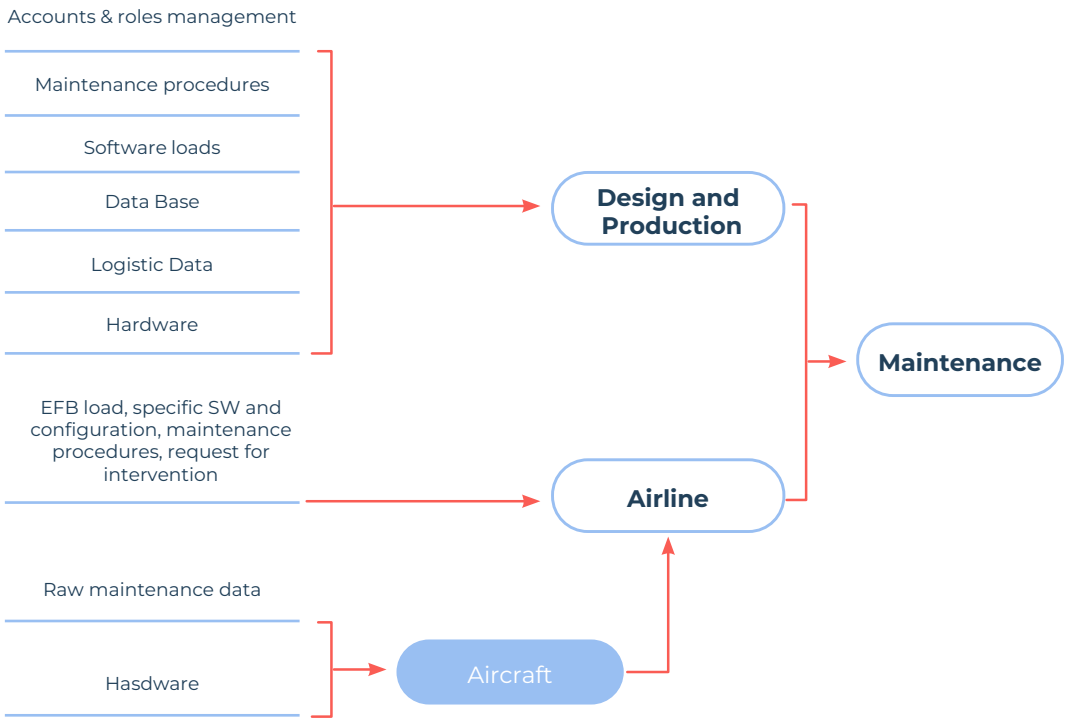


Figure 3: Interfaces of other organisations with a maintenance service providence

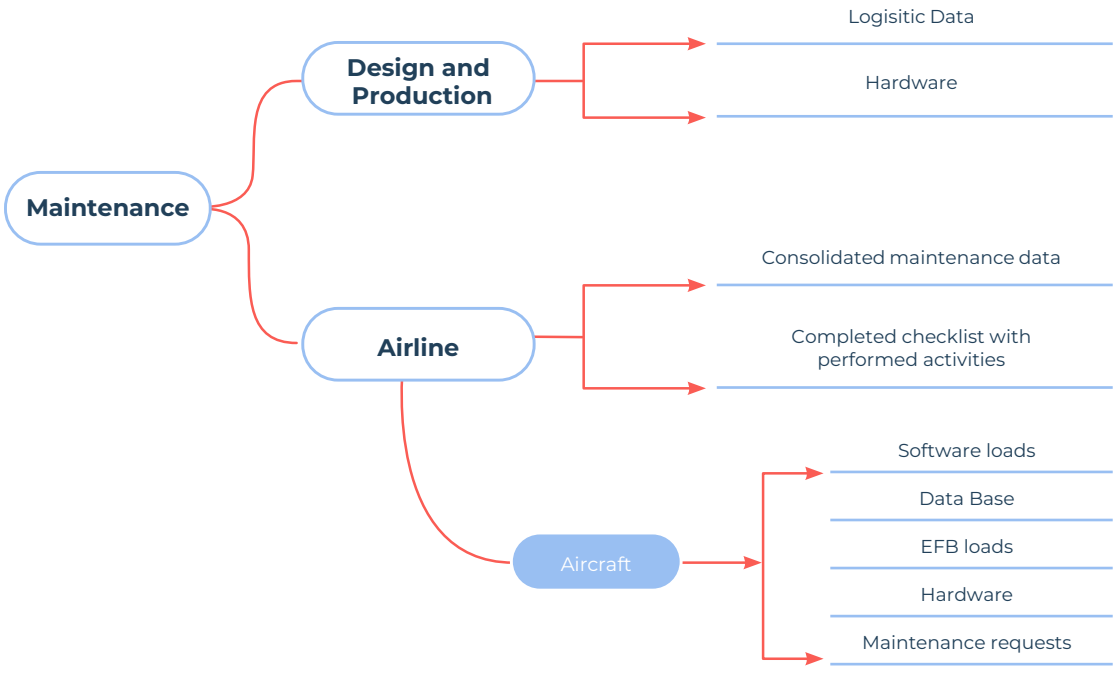


Figure 4: Interfaces of a maintenance service provoder with other organisations

11 Requisitos de Personal. Estructura organizativa

El gestor responsable nombrará a una persona o grupo de personas que velarán por que la organización cumpla los requisitos, y definirá el alcance de su autoridad. En los procedimientos deberá determinarse quién sustituye a una persona determinada en caso de ausencia prolongada de esta.

Si la organización comparte estructuras organizativas, políticas, procesos y procedimientos de seguridad de la información con otras organizaciones o con áreas de su propia organización que no formen parte de la aprobación o declaración, el gestor responsable podrá delegar sus actividades en una persona responsable común.

Entre sus funciones están:

- Garantizar la activación del procedimiento de notificación y supervisa la conformidad con la normativa.
- Liderar la ejecución del plan de respuesta y coordina la recopilación de información técnica.
- Actuar como enlace oficial con la autoridad competente y asegura el cumplimiento de plazos y formatos.
- Evaluar el impacto del incidente en la seguridad operacional y aprobación de la correspondiente comunicación externa.

Competencias necesarias:

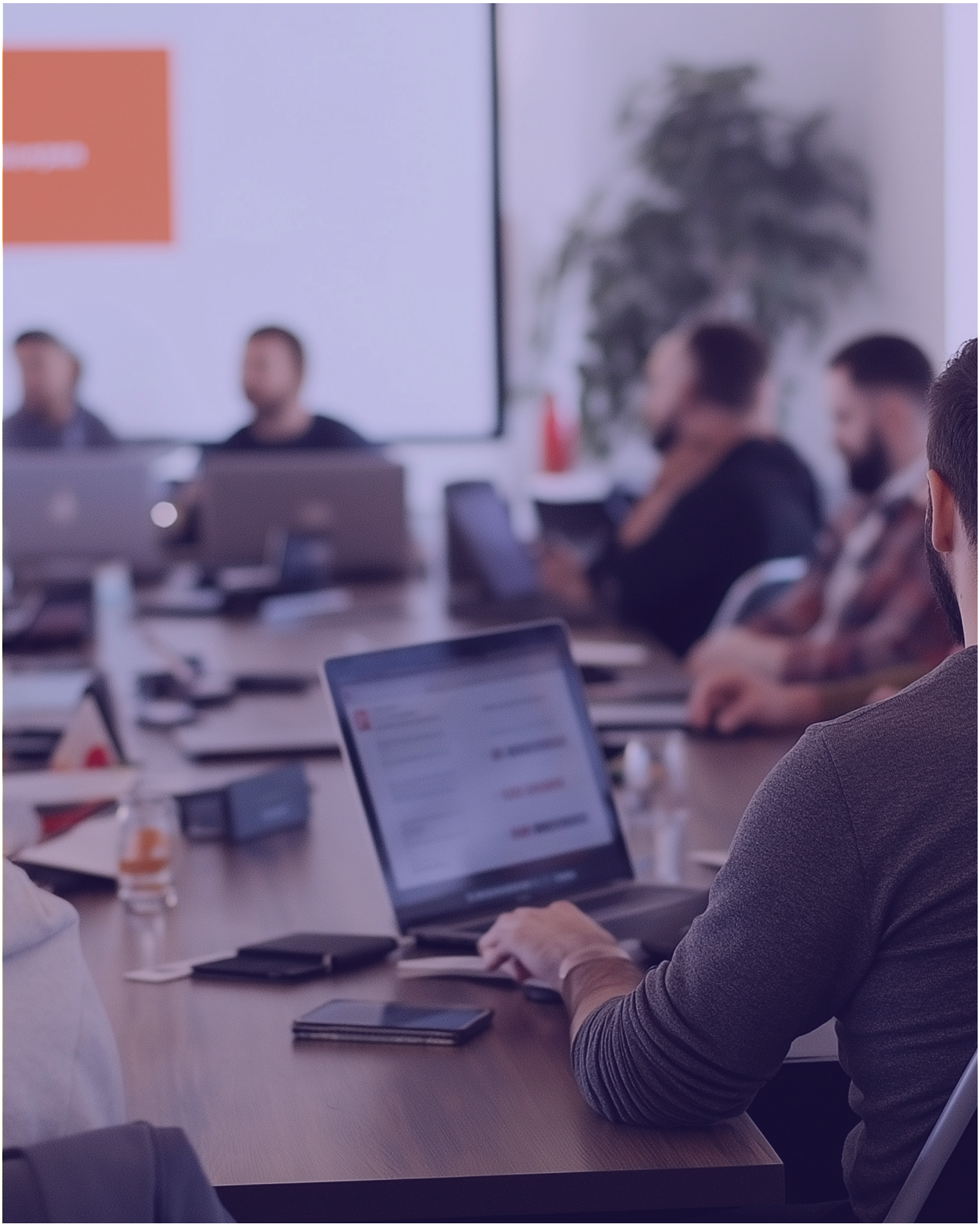
- conocimiento en seguridad de la información aplicada al entorno aeronáutico.
- Formación específica en normativa Part-IS y gestión de riesgos.
- Conciencia sobre la relación entre ciberseguridad e impacto en la seguridad operacional.

El personal implicado en el ISMS debe participar en programas de formación y concienciación periódicos que incluyan actualización sobre amenazas emergentes, procedimientos internos, obligaciones regulatorias y simulacros de respuesta a incidentes.

Las funciones críticas deben desempeñarse con independencia respecto a las áreas supervisadas, garantizando trazabilidad y responsabilidad en todas las acciones relacionadas con la seguridad de la información.

La organización debe mantener registros actualizados sobre cualificación, formación y experiencia del personal que participa en el ISMS, para demostrar conformidad ante auditorías y autoridades competentes.

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



12 Promoción de la seguridad de la información

Las compañías tienen que llevar a cabo acciones de promoción siguiendo un plan de concienciación que incluya, sesiones formativas e informativas, con los aspectos más relevantes de la seguridad de la información, esto es:

- Promoción de la política de seguridad
- Definición de los riesgos y oportunidades
- Acciones preventivas y de mitigación del riesgo
- Acciones correctivas en casos de incidentes

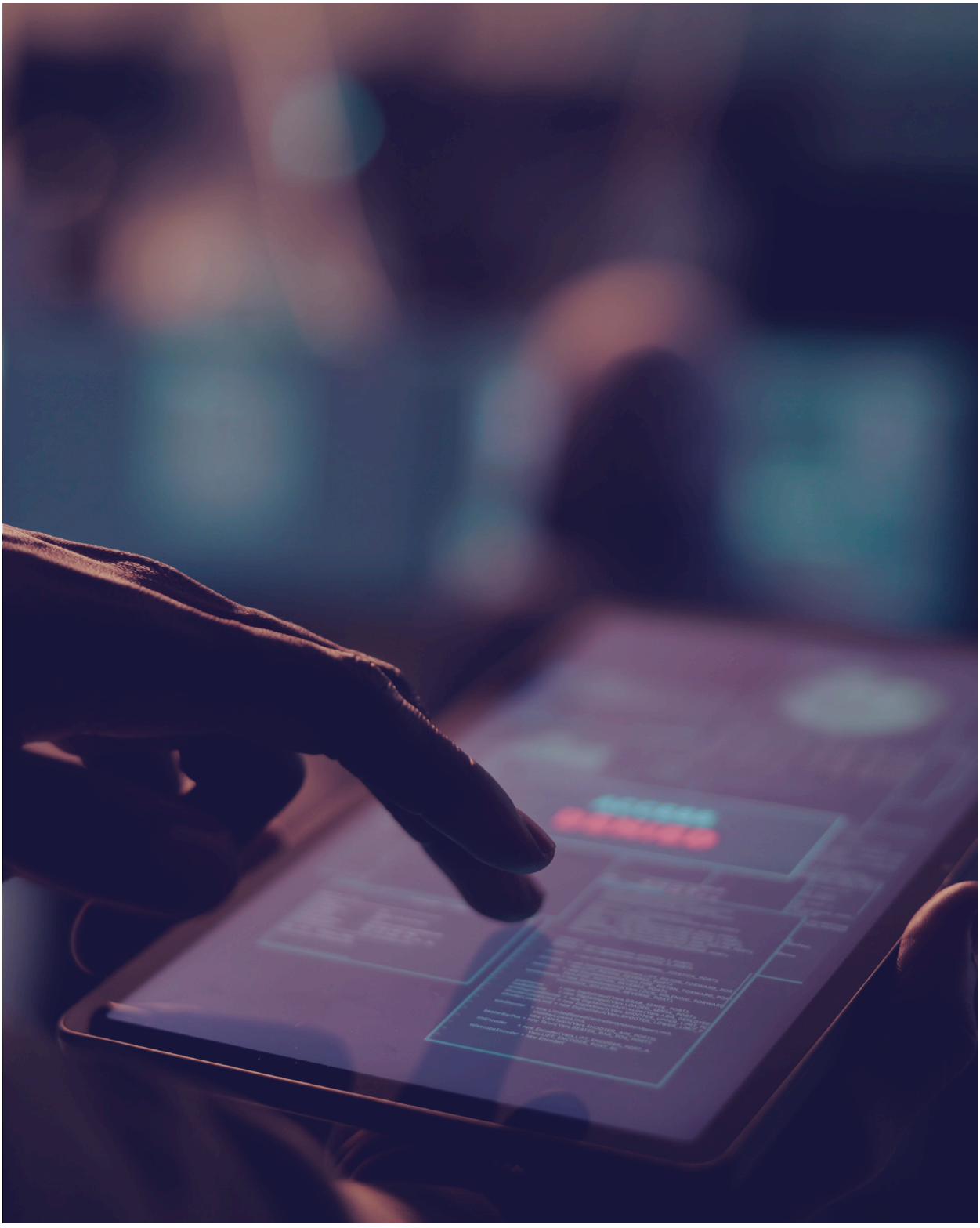
Este plan se debe realizar con una periodicidad como mínimo anual, para refrescar los conocimientos e incorporar a todos los integrantes de la compañía que se incorporen a lo largo del año.

Se debe medir periódicamente el estado de concienciación de la organización, para lo cual se pueden definir indicadores o métricas basados en encuestas, resultados de las formaciones, con umbrales de mínimo número de participantes, o resultados esperados de encuestas o test, permita hacer un seguimiento de la promoción.

Adicionalmente, se debe establecer una cultura de seguridad mediante charlas o conferencias periódicas desde las direcciones de los departamentos o áreas de negocio.

Establecer un sistema de alertas y de reportes a la seguridad, con varios niveles de criticidad para anticiparse a los incidentes y mitigar su impacto.

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



13 Aseguramiento, gestión de cambios y mejora continua

El aseguramiento de la Seguridad de la Información consiste en procesos dentro del ISMS que funcionan sistemáticamente para garantizar el rendimiento y la efectividad de los controles de riesgo de seguridad de la información, y que la organización cumpla o supere sus objetivos de seguridad a través de la recolección, análisis y evaluación de información, dentro del ámbito de seguridad de la información.

El Aseguramiento de la Seguridad de la información se fundamenta en las siguientes actividades esenciales:

- Seguimiento y medición del desempeño de seguridad de la información
- Mejora continua del ISMS
- Gestión del cambio.

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

Para una implementación efectiva la organización debe:

1. Monitorizar y medir el Desempeño de Seguridad de la información: Realizar un seguimiento constante de los indicadores de seguridad y analizar los datos para identificar tendencias, áreas de mejora y posibles riesgos.

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

3. Gestionar el Cambio: Evaluar y gestionar cualquier cambio en el entorno operativo del ISMS que pueda afectar la seguridad de la aviación, asegurando que las modificaciones no introduzcan nuevos riesgos o comprometan las medidas de seguridad existentes.

La vigilancia efectiva de estas actividades y la integración de los datos obtenidos en el proceso de ISRM 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, asegurando que las mejoras necesarias se implementen de manera oportuna y eficaz.

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

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 de la información y la gestión efectiva de los riesgos.

Seguimiento y medición del desempeño de seguridad de la información

El propósito del ISMS de una organización es mantener los riesgos de seguridad de la información 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 de la información no debe ser de circuito abierto; por lo tanto, el proceso de Aseguramiento de la Seguridad debe incluir mecanismos para monitorizar continuamente el desempeño del ISMS, tanto en su funcionalidad operativa como en la efectividad de los controles de riesgo implementados. Esto asegura que cualquier desviación o fallo en los controles sea detectada y corregida oportunamente.

La organización debe llevar a cabo evaluaciones regulares sobre el desempeño del ISMS 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 nominar a la(s) persona(s) o equipo(s) adecuado(s) para realizar el seguimiento del 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 organización 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.

El seguimiento de los indicadores de desempeño se realiza en el seno de Comité de Seguridad de la información anteriormente descrito.

Gestión del cambio

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

- Cambios tecnológicos, infraestructura, hardware, software, sistemas de comunicación o cualquier otro que afecte al ISMS que afecte a la seguridad de la aviación.
- 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 realiza el seguimiento, se 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 ISMS, evaluando el impacto del cambio en los controles de riesgo de seguridad existentes y asegurando que cualquier desviación se aborde adecuadamente.

Para que esta situación de cambio continuo no genere riesgos para la seguridad no gestionados, que creen modificaciones significativas en el entorno de la seguridad de la información, ya sean planeadas o no planeadas, autoinducidas 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 im-

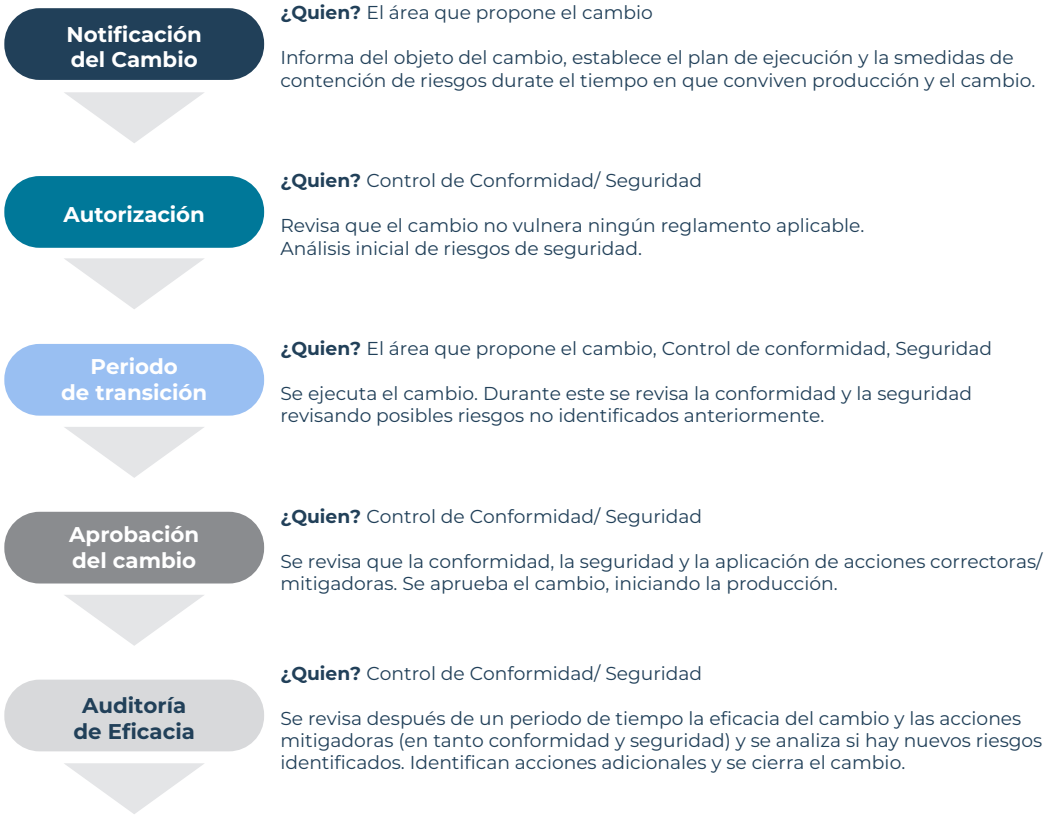
Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio
C/ Velázquez, 31 / 3º izda.
28001 Madrid
T. 91 700 17 24
info@tedae.org
www.tedae.org

plantación, 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 ISMS 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 la información) 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 con 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.

Ejemplos de cambios que pueden impactar el ISMS

(a) Cambios en el alcance, interfaces o políticas
(Referencia: "The organisation expands its business functions...")

- Expansión de funciones empresariales o integración de otra empresa.
- No conformidades que indiquen un alcance incorrecto.
- Modificación de la política u objetivos de seguridad con impacto potencial en la seguridad aérea.
- Cambios en interfaces debido a actividades externalizadas o internalizadas.

(b) Cambios en responsabilidades y estructura organizativa

- Delegación de responsabilidades del accountable manager.
- Contratación de actividades de gestión de seguridad de la información (IS.I.OR.235).

(c) Cambios en la metodología de gestión de riesgos

- Cambios en la clasificación de probabilidad o impacto.
- Cambios en la metodología de tratamiento del riesgo.
- Integración de la gestión de riesgos de seguridad de la información en otros sistemas de gestión.

(d) Cambios en la gestión de eventos de seguridad

- Externalización de la gestión de eventos.
- Cambios en el proceso de notificación y escalado.
- Cambios en la política de mitigación de vulnerabilidades.
- Cambios en el procedimiento de recuperación ante incidentes.

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

Ejemplos de cambios que NO impactan el ISMS
(Referencia: "Not all operational changes related to information security...")

- Campañas de concienciación tras un evento detectado.
- Actualización de programas de formación.
- Sustitución de herramientas de cifrado.
- Reestructuraciones internas sin cambios en responsabilidades del ISMS.
- Actualización de controles preventivos (p. ej., configuración de un firewall).

Mejora continua del ISMS

La mejora continua del Sistema de Gestión de la Seguridad de la Información (ISMS) es un proceso gradual y constante, cuyo objetivo es incrementar la efectividad y eficiencia de la organización para garantizar el cumplimiento de la política y los objetivos de seguridad. Para ello, la organización debe evaluar periódicamente la efectividad y madurez del ISMS mediante indicadores de rendimiento, ya sea en intervalos definidos o tras la ocurrencia de incidentes.

Si se detectan deficiencias, es imprescindible adoptar medidas correctivas y reevaluar los elementos afectados para asegurar la eliminación de las causas raíz y la mejora de los procesos. Este ciclo de mejora debe fundamentarse en planes de acción derivados de la monitorización y medición del desempeño de seguridad, utilizando los resultados de estas mediciones para definir las acciones a implementar.

A partir de los datos de seguridad recopilados, la organización debe realizar un análisis exhaustivo a nivel organizacional para establecer planes de acción que involucren a los responsables de implementar las mejoras. Dichos planes deben abordar las causas raíz de fallos o mal funcionamiento del sistema, donde el desempeño de seguridad no haya alcanzado el nivel esperado. Las acciones de mejora identificadas deben ser implementadas de forma efectiva, incluyendo la aplicación de correcciones inmediatas y la adopción de nuevas prácticas para prevenir la recurrencia de problemas.

Es esencial incorporar las mejores prácticas y lecciones aprendidas, difundiendo estas entre todo el personal mediante actividades de promoción de la seguridad, para fortalecer el ISMS y garantizar el compromiso de la organización con la mejora continua. Además, se deben organizar revisiones periódicas del ISMS con miembros de la dirección, cuya frecuencia y formato serán proporcionales al nivel de riesgos y la complejidad de la organización. Los resultados de estas revisiones deben servir como datos de entrada para el proceso de Gestión de Riesgos de Seguridad, asegurando que las decisiones y acciones se basen en datos actualizados y análisis precisos.

El proceso de mejora continua debe identificar oportunidades de mejora, evaluarlas en términos de coste-beneficio y posibles efectos no deseados, proponerlas a la dirección, planificar e implementar las acciones, y finalmente evaluar la efectividad de las medidas adoptadas y verificar la eliminación de las causas raíz. La dirección debe revisar periódicamente los resultados de este proceso, lo que permite no solo corregir fallos sino también anticipar y mitigar riesgos potenciales, optimizar procesos y adaptarse a nuevas normativas y estándares de seguridad.

Para la evaluación de la efectividad del ISMS, la organización debe definir quién monitoriza y toma decisiones, cuándo se realizan las evaluaciones, qué métodos de medición y análisis se emplean. Es necesario recopilar métricas y analizar tendencias, gestionando las deficiencias mediante correcciones inmediatas, acciones correctivas basadas en análisis de causa raíz, verificación de efectividad, y documentación y reporte a la dirección. Las auditorías internas realizadas por la función de Calidad/ Control de Conformidad contribuyen a determinar el correcto funcionamiento del sistema y a identificar posibles acciones de mejora que redunden en la eficacia del ISMS y su evolución ante nuevos desafíos.

14 Relación entre SMS – ISMS – Calidad. Sistemas integrados de Gestión

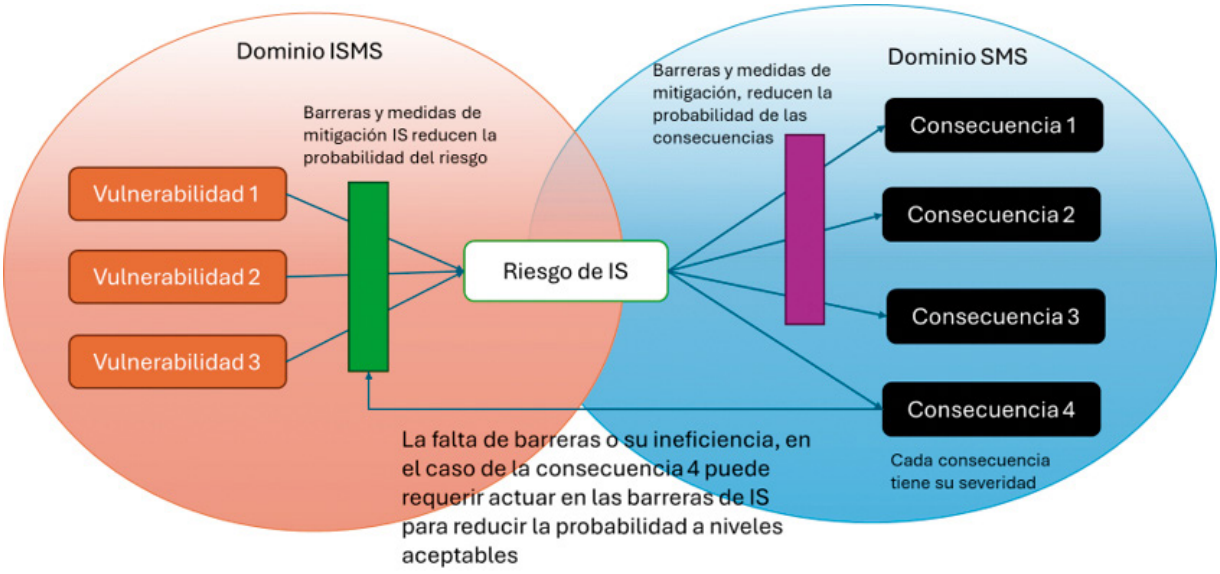
En anteriores guías de TEDAE se abordó la implementación del sistema de seguridad y su relación con los sistemas de calidad preexistentes en las organizaciones, observándose la necesidad de una colaboración estrecha, en la que ambos sistemas, con sus diferentes enfoques, proactivo en el caso de los sistemas de seguridad, identificando los posibles riesgos y sus consecuencias, pudiendo, mediante acciones contenedoras, evitar dichas consecuencias o minimizarlas; por otro lado el sistema de calidad, con su enfoque más reactivo, afronta las situaciones existentes actualmente, evitando con sus acciones posibles recurrencias.

De este modo, el sistema de gestión de la seguridad de la información, ISMS, como evolución de otros sistemas de protección de la información, como la implementación de la norma ISO 27001 así como otras normativas y regulaciones, viene a integrarse con el sistema de gestión de Seguridad y de Calidad preexistentes. Esta integración es necesaria puesto que en el contexto del ISMS, los posibles riesgos para la seguridad de la información deben analizarse en tanto a su posible efecto en la seguridad de la aviación, y no en el mero sentido de proteger el dato.

Este enfoque específico hace que ISMS y SMS (y con el QMS) deben colaborar de manera muy estrecha y en sentido bidireccional, dado que la identificación de los posibles riesgos de seguridad de la información, p. ej. un ciberataque, puede tener un correspondiente riesgo inherente en la seguridad de la aviación, p. ej. la corrupción (cambio) de una cota crítica de fabricación puede hacer insegura una pieza sin ser por ello percibido (supuestamente correcto en la base de datos de diseño)[1]. Este último riesgo, existen posibles barreras implementadas por SMS y QMS, pero tienen que contar con las barreras implementadas por ISMS al propio evento. Y este análisis puede indicar la necesidad de revisar ambas barreras, por lo que es necesario el retorno por parte del análisis generado por SMS.

Esta orientación es clave, porque puede darse la situación en la que una organización puede requerir un sistema de protección de la información, a nivel corporativo, y sin embargo no tener ningún riesgo por ello para la seguridad de la aviación, pudiendo no ser necesario implementar ISMS, tal y como establece la propia regulación. P. ej. una organización que repara un componente simple, con operaciones y maquinaria manual, y documentación simple y en papel, puede ser “inmune” a posibles ciberataques (no requiere ISMS), mientras que sus departamentos de facturas y personal sí, requiriendo un sistema de protección de la información.

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



La integración de todos estos sistemas supone un gran reto para las organizaciones dado que:

- Los sistemas de seguridad de la información y los de seguridad y calidad por regla general "hablan distintos idiomas"; el entendimiento de los recursos, sistemas y relaciones, así como los riesgos percibidos, debe hacerse común para poder evaluar de manera adecuada los riesgos para la seguridad de la aviación provocados por los riesgos de seguridad de la información. En particular, dos aspectos son fundamentales:
  - Los riesgos de Seguridad de Información suelen clasificarse en función del efecto en el negocio, descartando riesgos cuyo efecto puede ser menor en este sentido. Sin embargo, sin un análisis profundo, esos riesgos no pueden descartarse a priori en lo tocante a la seguridad de la aviación.
  - Los eventos de seguridad de la información, pueden gestionarse internamente (aplicación de ISO 27001 por ejemplo) de modo que se solucionen sin por ello analizar su implicación en la seguridad de la aviación.
- Es preciso establecer de manera clara las responsabilidades entre los diferentes sistemas, para evitar problemas de comunicación entre los distintos sistemas que puedan provocar análisis de seguridad incompletos o simplemente inexistentes.
- Es también necesario, como se dijo antes, las acciones de contención de todos los sistemas, para tener una eficiente contención de los riesgos de seguridad de la aviación.
- Es necesario alinear los requisitos y acciones de contención relacionados con la cadena de suministro, en particular en sistemas de seguridad de la información orientados fundamentalmente a la propia protección, excluyendo o minimizando las conexiones presentes en la cadena de suministro.

[1] Un caso paradigmático es un intercambio de materiales entre elementos en el plano de diseño, como por ejemplo el material de unos tornillos. Se pueden fabricar de manera totalmente correcta según ese diseño erróneo y no detectarse, y sin embargo ser completamente inseguro, al no corresponder la dureza/resistencia en los puntos correspondientes.

- Otro aspecto clave es la gestión de cambio, siendo un requisito que los cambios en los elementos gestionados por seguridad de la información sean revisados por el correspondiente cumplimiento regulatorio (QMS) y de seguridad de producto, y viceversa, para los cambios gestionados por SMS+QMS que deben ser analizados por ISMS. (Ej. Cambios en las medidas de seguridad de un software de producción requieren analizar si pueden existir riesgos para la seguridad de la aviación. La incorporación de una nueva máquina conectada requiere ser analizada por ISMS).

- Por último, es necesario alinear también los sistemas de reporte voluntario, y los procesos formativos.

El desarrollo de esta integración entre ISMS y SMS+QMS permite, por tanto, una mejor evaluación de los riesgos, incorporando aspectos de seguridad de la información a la decisión de aplicación de los recursos necesarios para contener las posibles consecuencias de los citados riesgos. Esto redunda en un uso más eficiente de los recursos disponibles orientando a la organización en la seguridad de la aviación.

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

Gestión de la Seguridad de la información

(ISMS) en el ámbito aeronáutico (Part-IS)

TEDAE
Defensa, Seguridad, Aeronáutica y Espacio

info@tedae.org
www.tedae.org

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

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