Sistema de Gestión de la Seguridad de la Información (ISMS)

Jesús Bussión *– Responsable ISMS – TEMAI*

Francisco Sierra *– Responsable IT – TEMAI*

Miembros del Grupo de Trabajo

David Guzmán

ITP AERO

Roberto Jesús García

THALES

Ramón Ortiz

Rheinmetall

AERnnova

Mitxel Fuentes

AERnnova

Sergio Pingarrón

Independiente

Melisa Formento

TEMAI

Francisco Sierra

TEMAI

Jesús Bussión

TEMAI

¿Para qué existe este Grupo de Trabajo?

Objetivo y alcance

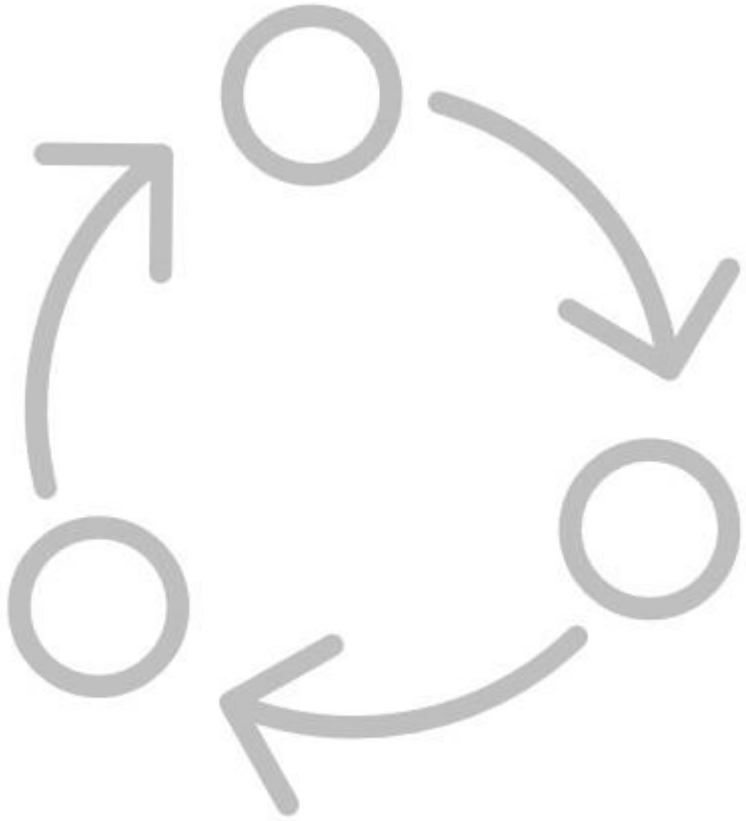
Objetivo del Grupo

Realizar una Guía de Implementación del Sistema de Gestión de la Seguridad de la Información (ISMS), que sirva para entender:

- Porqué es necesario un ISMS
- Qué debe incluir
- Cómo se relaciona con otros Sistemas de Gestión

Alcance

Según los requisitos 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.



Grupo de Trabajo

Grupo de Trabajo

Desde la constitución del Grupo de trabajo el 18 de Marzo de 2025, se han seguido los siguientes pasos:

Se han realizado 10 reuniones de las cuales dos fueron presenciales de jornada completa en las Instalaciones de ITP AERO y TEMAI.

Dando por finalizada la Guía el 10 de abril de 2026,

Guía de gestión de la seguridad de la información (ISMS) en el ámbito aeronáutico (Part-IS)

índice

índice

1. ¿QUÉ ES UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN ISMS?
2. ESTÁNDARES DE REFERENCIA
3. ELEMENTOS DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – OBJETIVOS E INDICADORES
5. EVALUACIÓN Y TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.
6. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. DETECCIÓN – RESPUESTA – RECUPERACIÓN
7. REGISTROS INTERNOS Y EXTERNOS (INFORMES)
8. COMUNICACIÓN CON LA AUTORIDAD
9. CONTRATACIÓN DE ACTIVIDADES DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
10. CADENA DE SUMINISTRO
11. REQUISITOS DE PERSONAL ESTRUCTURA ORGANIZATIVA
12. PROMOCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
13. ASEGURAMIENTO, GESTIÓN DE CAMBIOS Y MEJORA CONTINUA
14. RELACIÓN ENTRE SMS – ISMS – CALIDAD. SISTEMAS INTEGRADOS DE GESTIÓN

¿Por qué un sistema de seguridad de la información ISMS?

De proteger los datos comerciales de la empresa, a salvaguardar de manera efectiva la vida humana y la continuidad de las operaciones aéreas.

Los 4 Pilares del ISMS

1. Política

Compromiso absoluto de la Dirección y creación de una cultura justa de reporte proactivo.

2. Riesgos

Identificación de escenarios de amenaza que afecten potencialmente a la seguridad aérea.

3. Aseguramiento

Monitoreo continuo de KPIs, auditorías frecuentes y gestión efectiva de la resiliencia.

4. Promoción

Formación integral, simulacros anuales y distribución ágil de alertas de seguridad.

Sistemas de Referencia

La certificación en ISO 27001 facilita el cumplimiento con la regulación descrita en la Part-IS, con los correspondientes matices y adaptaciones necesarias.

Criterio Clave	Norma ISO 27001 (Negocio)	Regulación Part-IS (Aeronáutico)
Orientación Principal	Protección del negocio y privacidad	Impacto directo en la seguridad aérea (Safety)
Rol de la Dirección	Patrocinador corporativo	Gerente Responsable (Nominado por la dirección)
Supervisión Regulatoria	No obligatoria (Auditor privado)	Aprobación estricta de Autoridades (AESA/EASA)
Foco en Proveedores	Gestión básica de contratos	Exposición mutua y "Cadena Funcional" integrada

Evaluación y tratamiento de los Riesgos

Debemos identificar y revisar los riesgos de seguridad de la información.

Matriz de Riesgos

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	**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*

Incidentes de seguridad de la información

1. Detección

Uso de herramientas SIEM/IDS, antivirus, y alertas activas las 24 horas del día.

2. Respuesta

Activación del plan de contención de incidentes liderado por equipos especializados (CSIRT).

3. Reporte

Notificación estricta a la autoridad reguladora (AESA/EASA) en menos de 24 horas si es crítico.

4. Aprendizaje

Análisis post-mortem detallado para ajustar defensas, actualizar procesos y robustecer controles.

La Cadena de Suministro
Cadena Funcional

En el espacio aéreo nadie vuela solo de forma aislada. La ciberseguridad ya no consiste únicamente en blindar tu servidor local.
Part-IS introduce la "Cadena Funcional": un modelo integrado de corresponsabilidad donde aerolíneas, aeropuertos, talleres de mantenimiento y fabricantes cooperan de manera estrecha.
Se exige identificar todos los flujos de datos y activos involucrados en la transmisión de información aeronáutica.

Gobernanza y Liderazgo

El Gerente Responsable

La máxima autoridad de la organización (Gerente Responsable) debe tener un papel clave en el ISMS.
Es la persona que lidera la gobernanza, autoriza y prioriza los recursos necesarios, autoriza los planes de tratamiento de riesgos.

Nombra al Responsable del Sistema de Seguridad de la información

Relación Calidad y Seguridad
SMS + ISMS + Calidad

La seguridad de la información no puede estar en una isla separada de las operaciones y la calidad corporativa.
Un error informático o ciberataque silencioso que altere las bases de datos de diseño o de fabricación (sin ser detectado por controles tradicionales) puede resultar catastrófico en vuelo. Los riesgos de software son, hoy en día, riesgos de seguridad física.

Muchas Gracias por su Atención