MINISTERIO
DE TRANSPORTES
Y MOVILIDAD SOSTENIBLE

AESA AGENCIA ESTATAL
DE SEGURIDAD AÉREA

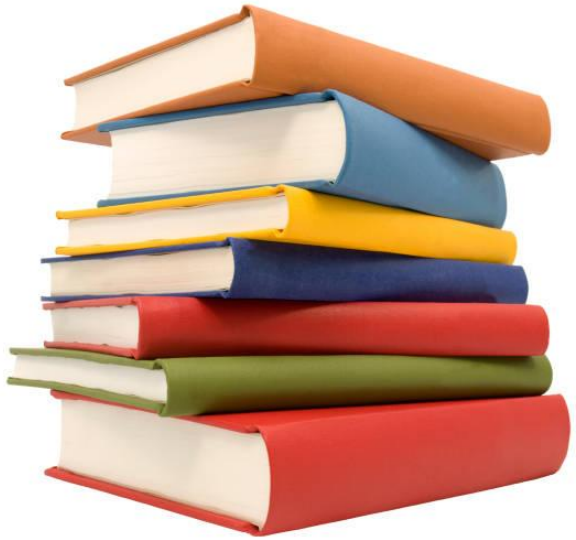
# WEBINAR Organizaciones de Aeronavegabilidad

*Parte IS*

Francisco GUERRERO y Alberto ORGAZ

06-NOV-2025

## Índice:



# 1. DOCUMENTACIÓN DISPONIBLE
# Parte-IS

# EASA

- **Easy Access Rules on Information Security:** Easy Access Rules on Information Security
- **Part-IS oversight approach:** https://www.easa.europa.eu/community/topics/part-oversight-approach-guidelines
- Implementation guidelines for Part-IS* - IS.I/D.OR.200 (e)
- **Application of the European Cybersecurity Skills to Aviation**

**Otros documentos:**

- **Guidelines ISO/IEC 27001 vs PART-IS**
- **FAQ Information Security (Part-IS)**

# Autoridades nacionales:

- **GM-INFO Information Security**

Federal Office of Civil Aviation Switzerland

- **CAP1223: Framework for an Aviation Security Management System (SeMS)**

UK Civil Aviation Authority

# EUROCONTROL

- **https://www.eurocontrol.int/cybersecurity**

- CYBERG - GM contractual VM req. V1.0
  (requerimentos de IT para ATC y ANSP)

# AESA – Seguridad Aérea

## Organizaciones Parte 145 y CAMO: Guías de Usuario – Sistema de Gestión

Organizaciones

Mantenimiento nacional

Organizaciones Parte 145

Organizaciones de formación de Mantenimiento (Parte 147)

Organización de gestión de la aeronavegabilidad (CAMO)

Organizaciones de aeronavegabilidad combinada (CAO)

Última modificación: Jueves, 2 Octubre 2025

### Organizaciones Parte 145

Procedimiento para la emisión y modificación de la aprobación como Organización de Mantenimiento según la Parte 145.

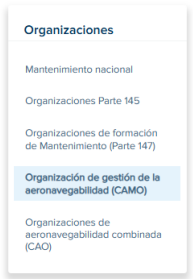
**Qué persigue**

Este proceso contempla la emisión inicial y la modificación de la aprobación como Organización de Mantenimiento conforme a la Parte 145 (Anexo II al Reglamento (UE) 1321/2014).

- Lista de Organizaciones de mantenimiento Parte 145 **(Actualizado octubre 2025)**

**Documentación**

- AC-MTO-P01-GU01 Guía de Información Usuario **(Actualizado septiembre 2025)**
- AC-MTO-P01-DT01 Guía de Evaluación MOE **(Actualizado septiembre 2025)**
- AC-MTO-P01-DT02 Guía de Formación de Tarea **(Actualizado noviembre 2022)**
- AC-MTO-P01-DT03 Guía de Certificadores de Componentes **(Actualizado septiembre 2025)**
- AC-MTO-P01-DT04 Guía de Aceptación de Personal **(Actualizado septiembre 2025)**
- AC-MTO-P01-DT05 Guía de Experiencia 6-24 Meses Certificadores **(Actualizado noviembre 2022)**
- AC-MTO-P01-DT06 Guía de Herramientas Alternativas **(Actualizado noviembre 2022)**
- Guías de Usuario - Sistema de Gestión



Organizaciones

Mantenimiento nacional

Organizaciones Parte 145

Organizaciones de formación de Mantenimiento (Parte 147)

Organización de gestión de la aeronavegabilidad (CAMO)

Organizaciones de aeronavegabilidad combinada (CAO)

Última modificación: Martes, 14 Octubre 2025

### Organización de gestión de la aeronavegabilidad (CAMO)

**Organizaciones de Gestión del Mantenimiento de Aeronavegabilidad (CAMO Parte CAMO)**

- Lista de Organizaciones de Gestión del Mantenimiento de la Aeronavegabilidad (CAMO Parte CAMO) **(Actualizado octubre 2025)**

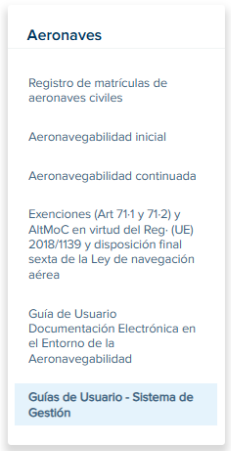
**Qué persigue**

Este proceso contempla la emisión inicial y la modificación de la aprobación como Organización del Mantenimiento de la Aeronavegabilidad (CAMO) de acuerdo a los requisitos aplicables de los anexos I (Parte M), Va (Parte T), Vb (Parte ML) y Vc (Parte CAMO) del Reglamento (UE) 1321/2014.

**Documentación**

- AC-CAMO-P01-GU01 Ed.02 Guía de información CAMO (Actualizado febrero 2025)
- AC-CAMO-P01-DT01 Ed.01 Guía de Evaluación del CAME (Actualizado octubre 2024)
- AC-CAMO-P01-DT02 Ed.01 Guía de aceptación de personal (Actualizado octubre 2024)
- Guías de Usuario - Sistema de Gestión





Aeronaves

Registro de matrículas de aeronaves civiles

Aeronavegabilidad inicial

Aeronavegabilidad continuada

Exenciones (Art 71·1 y 71·2) y AltMoC en virtud del Reg· (UE) 2018/1139 y disposición final sexta de la Ley de navegación aérea

Guía de Usuario Documentación Electrónica en el Entorno de la Aeronavegabilidad

Guías de Usuario - Sistema de Gestión

Última modificación: Viernes, 17 Octubre 2025

### Guías de Usuario - Sistema de Gestión

- **Qué persigue**

Se pone a disposición de las organizaciones las guías del Manual del Sistema de Gestión y Evaluación de Cargos Responsables relativos al Sistema de Gestión.

Estas guías aplican a:

- compañías aéreas **con licencia** concedida con arreglo al Reglamento (CE) n.º 1008/2008 (Licencia de Explotación).
- operadores aéreos de transporte aéreo comercial que **no tengan concedida una Licencia de Explotación**.
- organizaciones de Gestión del Mantenimiento de la Aeronavegabilidad (**CAMO**) con aprobación según el Anexo Vc (Parte CAMO) del Reglamento (UE) n.º 1321/2014.
- organizaciones de Mantenimiento (**145**) con aprobación según el Anexo II (Parte 145) del Reglamento (UE) n.º 1321/2014.
- organizaciones de Producción (**POA**) con aprobación según el Anexo I (Parte 21) del Reglamento (UE) n.º 748/2012.

- **Documentación**
  - DSA-SG-P01-GU01 Guía del Manual del Sistema de Gestión **(julio 2025)**
  - DSA-SG-P01-GU02 Guía de evaluación de cargos responsables **(julio 2025)**
  - DSA-SG-P01-GU03 Guía de Sistemas de Gestión entre AOC y CAMO con contrato **(diciembre 2024)**
  - DSA-SG-P01-GU04 Guía del Manual del Sistema de Gestión de Seguridad de la Información **(julio 2025)**

# AESA – Seguridad Aérea

Organizaciones Parte 145 y CAMO: Guías de Usuario – Sistema de Gestión


DSA-SG-P01-GU02 Guía de evaluación de cargos responsables **(julio 2025)**

DR
PERSONA RESPONSABLE COMÚN (CRP)
RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN (RSI)
RESPONSABLE CONTROL CONFORMIDAD
PERSONAL DE LA ORGANIZACIÓN CON ACCESO A SISTEMAS E INFORMACIÓN CRÍTICOS


DSA-SG-P01-GU04 Guía del Manual del Sistema de Gestión de Seguridad de la Información **(julio 2025)**

PROCEDIMIENTO DEROGACIONES
RESUMEN PARA INCLUIR EN EL MANUAL DEL SISTEMA DE GESTIÓN EL CONTENIDO DEL MANUAL DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN.
ESTRUCTURA DEL MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MSGSI)

# AESA – Seguridad Aérea

## GENERAL. SEGURIDAD DE LA INFORMACIÓN. ÁMBITO SAFETY.


# 2. ALCANCE PARTE IS

## BASE DE REGULACIÓN

# Parte IS

## RE (UE) 2023/203.

Reglamento (EU) 2023/203
De 27 de octubre de 2023

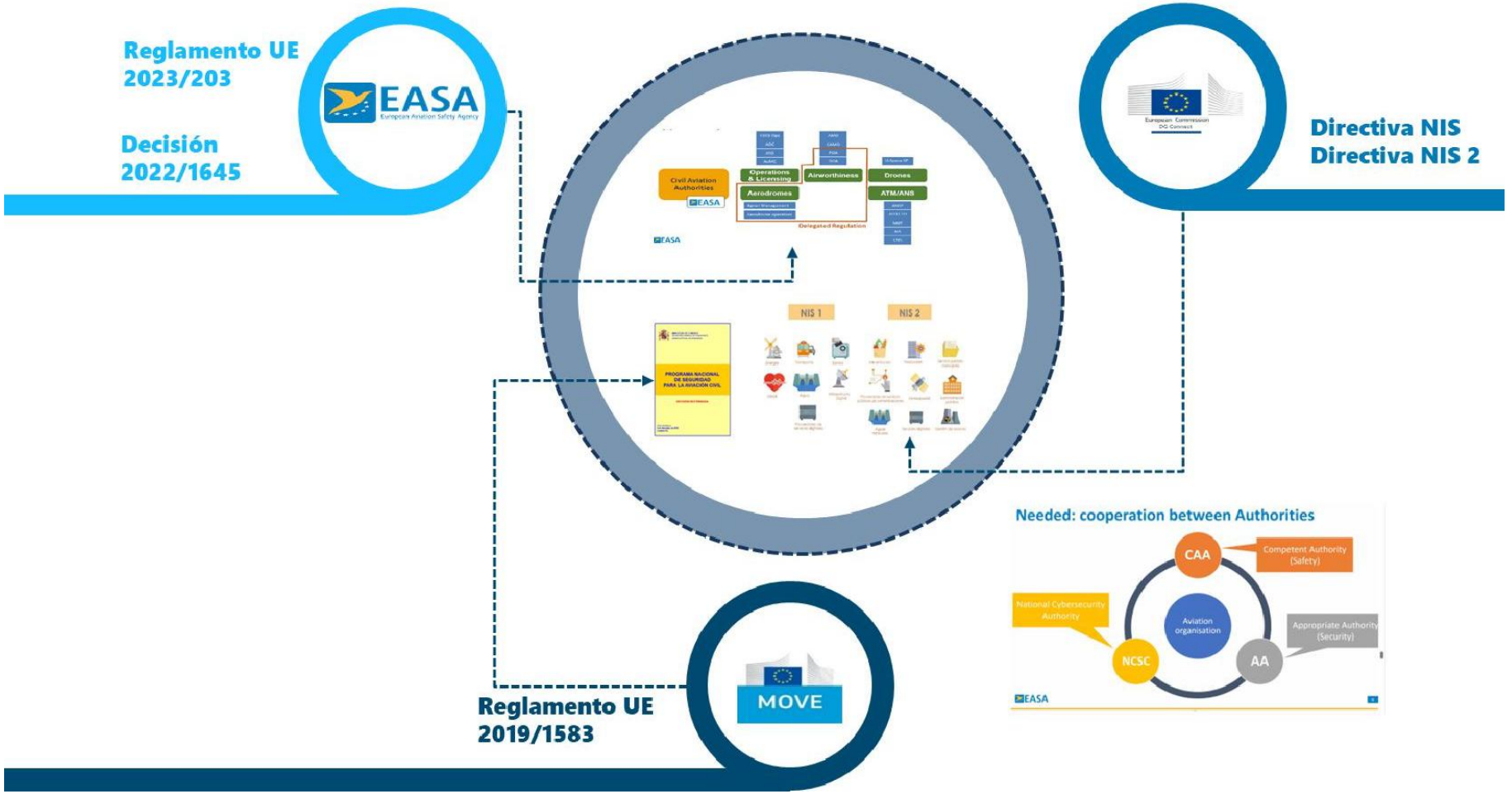
Aplicable a partir del 22 de febrero de 2026

**PARTE IS.AR**: Requisitos aplicables a las autoridades

**PARTE IS.I.OR**: Requisitos aplicables a las organizaciones

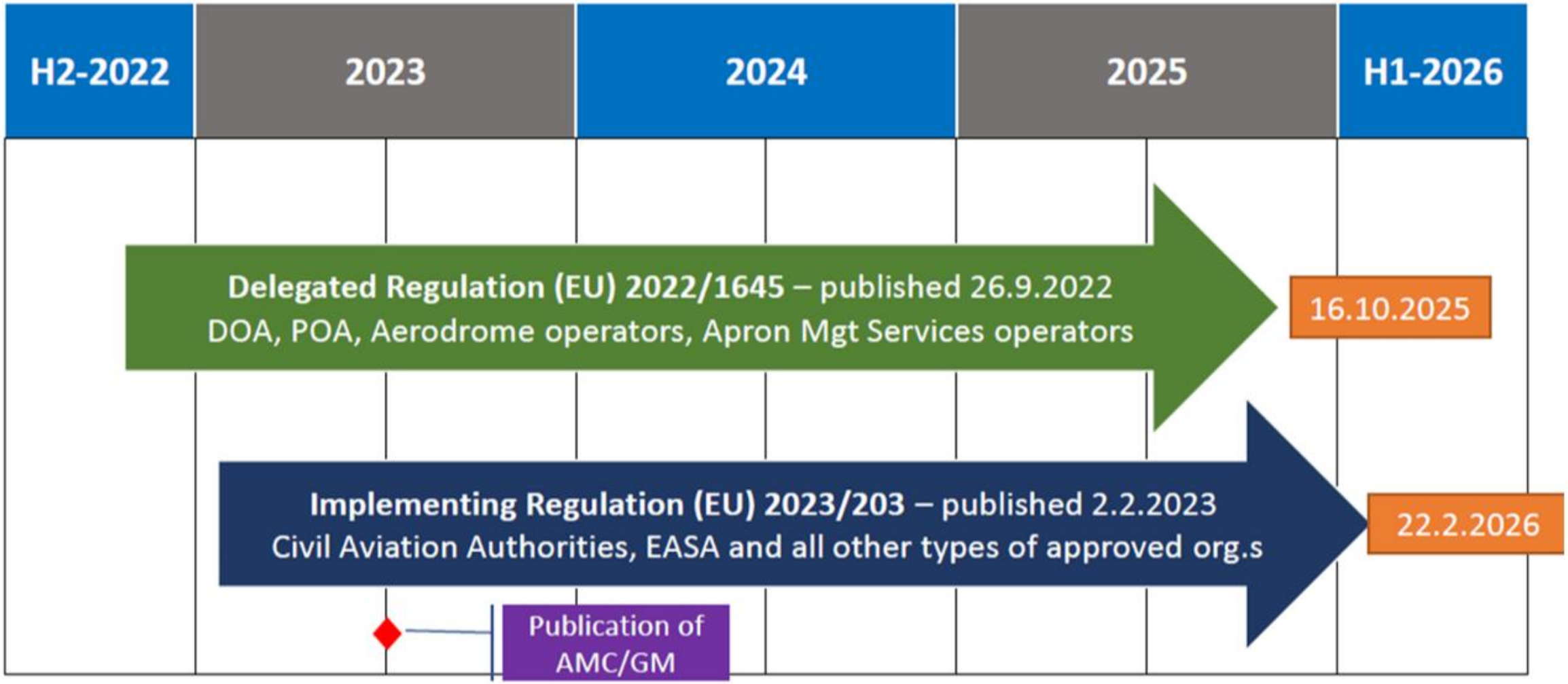
- **IS.I.OR.100**: Ámbito de aplicación
- **IS.I.OR.200**: Sistema de Gestión de Seguridad de la Información (SGSI)
- **IS.I.OR.205**: Evaluación de riesgos
- **IS.I.OR.210**: Tratamiento de riesgos
- **IS.I.OR.215**: Sistema interno de notificación
- **IS.I.OR.220**: Incidentes, detección respuesta y recuperación
- **IS.I.OR.225**: Respuesta a incidencias notificadas por la autoridad
- **IS.I.OR.230**: Sistema externo de notificación
- **IS.I.OR.235**: Contratación de actividades de gestión
- **IS.I.OR.240**: Requisitos relativos al personal
- **IS.I.OR.245**: Conservación de registros
- **IS.I.OR.250**: Manual de Gestión de Seguridad de la Información (MGSI)
- **IS.I.OR.255**: Cambios en el SGSI
- **IS.I.OR.260**: Mejora continua

## Marco regulatorio europeo en materia de ciberseguridad aplicable a aviación civil




IS en el Programa Nacional de Seguridad.

## Desarrollo normativo




## EASY ACCESS RULES Part-IS

Un único documento para facilitar la lectura reglamentaria de los reglamentos y sus AMC y GM relacionados

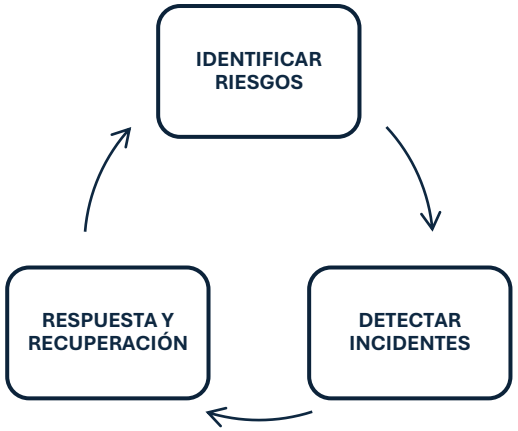
**RE (UE) 1321/2014.** → **RE (UE) 2023/203. 22.02.2026**

## Los reglamentos (UE) 2023/203 & 2022/1645

**ARTÍCULOS**

Artículo 1: Objeto

a) Detectar y gestionar riesgos
b) Detectar incidentes
c) Responder y recuperarse de los incidentes




Artículo 2: Ámbito de aplicación

Excepciones…

[…]

Artículo 16: Entrada en vigor

Aplicable a partir del 22 de febrero de 2026

# Correlación punto normativo – descripción

| ORGANISATION | Description |
|---|---|
| IS.I.OR.100 | Scope |
| IS.I.OR.200 | Information security management system (ISMS) |
| IS.I.OR.205 | Information security risk assessment |
| IS.I.OR.210 | Information security risk treatment |
| IS.I.OR.215 | Information security internal reporting scheme |
| IS.I.OR.220 | Information security incidents — detection, response, and recovery |
| IS.I.OR.225 | Response to findings notified by the competent authority |
| IS.I.OR.230 | Information security external reporting scheme |
| IS.I.OR.235 | Contracting of information security management activities |
| IS.I.OR.240 | Personnel requirements |
| IS.I.OR.245 | Record-keeping |
| IS.I.OR.250 | Information security management manual (ISMM) |
| IS.I.OR.255 | Changes to the information security management system |
| IS.I.OR.260 | Continuous improvement |

# 2. ALCANCE PARTE IS

## ISO27001 Y PART-IS

**ISO/IEC 27001:** Estándar internacional para la seguridad de la información publicado en 2005 por ISO (International Standatization Organization) y IEC (International Electrotechnical Organization).

Asociación de organizaciones de normalización nacionales de 167 países desde 1947.

Desarrolla estándares internacionales voluntarios, como ISO 9001 (sistema de gestión de la calidad).


ISO 27002 son los controles para tratar los riesgos de la IS.

## **Guidelines ISO/IEC 27001 vs PART-IS:** Delta para 46 sub-puntos normativos Part-IS

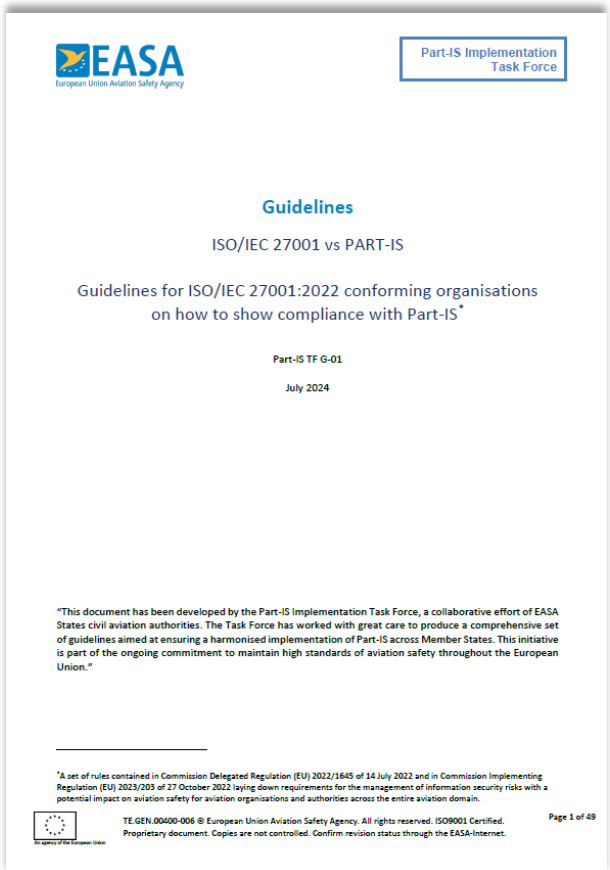
**Requirement**

**ISO/IEC 27001 mapping**

**Part-IS particularity**

**Guidance for Part-IS implementation**

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM



EASA
European Union Aviation Safety Agency

Part-IS Implementation Task Force

Guidelines

ISO/IEC 27001 vs PART-IS

Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS*

Part-IS TF G-01

July 2024

"This document has been developed by the Part-IS Implementation Task Force, a collaborative effort of EASA States civil aviation authorities. The Task Force has worked with great care to produce a comprehensive set of guidelines aimed at ensuring a harmonised implementation of Part-IS across Member States. This initiative is part of the ongoing commitment to maintain high standards of aviation safety throughout the European Union."

*A set of rules contained in Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 and in Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down requirements for the management of information security risks with a potential impact on aviation safety for aviation organisations and authorities across the entire aviation domain.

TE.GEN.00400-006 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified.
Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet.

Page 1 of 49

**A.5 Controles organizacionales**

**A.6 Controles personales**

**A.7 Controles físicos**

**A.8 Controles tecnológicos**

Relación entre controles ISO27001 y puntos Part-IS.

| Control | Part-IS |
|---|---|
| A.5.1 Políticas para la seguridad de la información | • IS.D.OR.200(a)(1)<br>• IS.D.OR.200(b)<br>• IS.D.OR.260<br>• IS.D.OR.200(c)<br>• IS.D.OR.260(a)<br>• IS.D.OR.260(b)<br>• IS.D.OR.240(a)(2)<br>• IS.D.OR.240(a)(3) |
| A.5.2 Roles y responsabilidades en la seguridad de la información | • IS.D.OR.200(c)<br>• IS.D.OR.240(f)<br>• IS.D.OR.240(a)(1)<br>• IS.D.OR.240(b)<br>• IS.D.OR.240(c)<br>• IS.D.OR.240(d) |
| A.5.4 Responsabilidades de gestión | • IS.D.OR.240(a)(2)<br>• IS.D.OR.240(a)(3)<br>• IS.D.OR.240(b)<br>• IS.D.OR.240(c)<br>• IS.D.OR.240(d) |

# 2. ALCANCE PARTE IS
## EXCEPCIONES

# Excepciones al cumplimiento del reglamento:

**DELEGATED REGULATION (EU) 2023/203**

***Artículo 2 – Ámbito de aplicación***

1. El presente Reglamento se aplica a las organizaciones siguientes: *[…]*

***a) 145*** *e*xcepto aquellas que participen exclusivamente en el mantenimiento de aeronaves de conformidad con el anexo V ter (parte ML)

***b) CAMO*** *e*xcepto aquellas que participen exclusivamente en la gestión del mantenimiento de la aeronavegabilidad de aeronaves de conformidad con el anexo V ter (parte ML)

**ML.1**

(a) In accordance with paragraph 2 of Article 3, this Annex (Part-ML) applies to the following other than complex motor-powered aircraft not listed in the air operator certificate of an air carrier licensed in accordance with Regulation (EC) No 1008/2008:

(1) aeroplanes of 2 730 kg maximum take-off mass (MTOM) or less;

(2) rotorcraft of 1 200 kg MTOM or less, certified for a maximum of up to 4 occupants;

(3) other ELA2 aircraft.

# 2. ALCANCE PARTE IS
## DEROGACIÓN

# AMC1 IS.I.OR.200(e) Information security management system (ISMS)

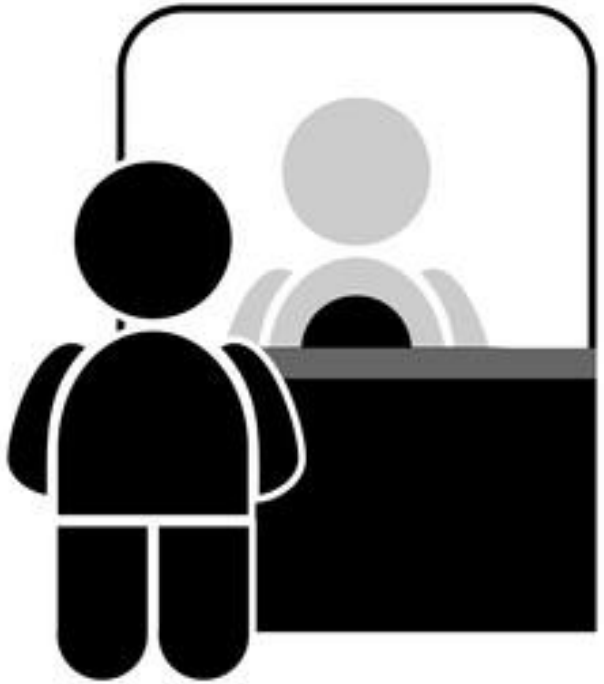
**DEROGATION**

Organisations should follow the directions provided in AMC1 IS.I.OR.205(a) and AMC1 IS.I.OR.205(b) to perform a documented information security risk assessment to seek the approval by the competent authority of a derogation under point IS.I.OR.200(e). In order to justify the grounds for a derogation, the risk assessment is expected to provide explanations for the exclusion of all elements from the scope of the ISMS. It is up to the authority to determine whether this assessment is deemed satisfactory for a derogation to be granted.

Organisations that would like to have the risk assessment performed by a third party should consider the requirements of IS.I.OR.235 and the related AMC.

# Derogaciones por **no** afectación a la seguridad:

-Se deben solicitar a AESA (Formato común AIRW)
-Formato único para varias aprobaciones
-Recepción solicitud única
-Formato de resolución Positiva o Negativa



**Nota:** el Gerente Responsable de la organización debe demostrar un conocimiento del proceso de derogación y de los términos en los que se otorga la derogación.

Formato de derogación:

INFORMACIÓN SENSIBLE

MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

**SOLICITUD DE DEROGACIÓN**

*ATENCIÓN: Antes de cumplimentar este formato, consulte las Instrucciones de la página 5.*

| A | DATOS DE LA ORGANIZACIÓN | | | |
|---|---|---|---|---|
| A.1 | Nombre: | | A.2 NIF | |
| A.3 | Dirección: | | | |
| A.4 | Teléfono: | | | |
| A.5 | Email: | | | |

| B | APROBACIONES/DECLARACIONES AFECTADAS |
|---|---|
| B.1 | ☐ Certificado de Operador Aéreo (AOC) |
| B.2 | ☐ Declaración de Operaciones Aéreas Especializadas (SPO) |
| B.3 | ☐ Declaración de Operaciones Aéreas No Comerciales con Aeronaves Complejas (NCC) |
| B.4 | ☐ Organización de Mantenimiento (Parte 145) |
| B.5 | ☐ Organización de Gestión del Mantenimiento de la Aeronavegabilidad (Parte CAMO) |
| B.6 | ☐ Organización de Producción (POA) |

Debe incluir:

-Memoria de la Organización mencionando el ISMS

-Evaluación del riesgo que justifique la no afectación

- Debe ir firmada por el Gerente Responsable
- Se debe enviar un único formato (para varias aprobaciones) por “Solicitud general”

Derogaciones por **no** afectación (diagrama de flujo):

**Solicitud general** → **Recepción de Solicitud** → **Evaluación de Solicitud** → **Resolución Estimatoria**

Incluye el formato común de solicitud de derogación.

Si estos documentos son correctos:

- Firmada por el DR
- Manual (MOE, CAME…)
- Estudio evaluación de riesgos (puede estar hecho por 3ª parte)

Se abre expediente de modificación
Recepción de solicitud única

Acorde a su propio SMS.
No afecta a la seguridad aérea

Se abre actuación de modificación.
Gestión de Discrepancias e Informe Técnico.

Si cumple los criterios

**Res. Desestimatoria**

Si **NO** cumple los criterios

Según doc.: *Implementation guidelines for Part-IS* - IS.D.OR.200 (e)*

**Criterios para evaluar la solicitud de derogación:**

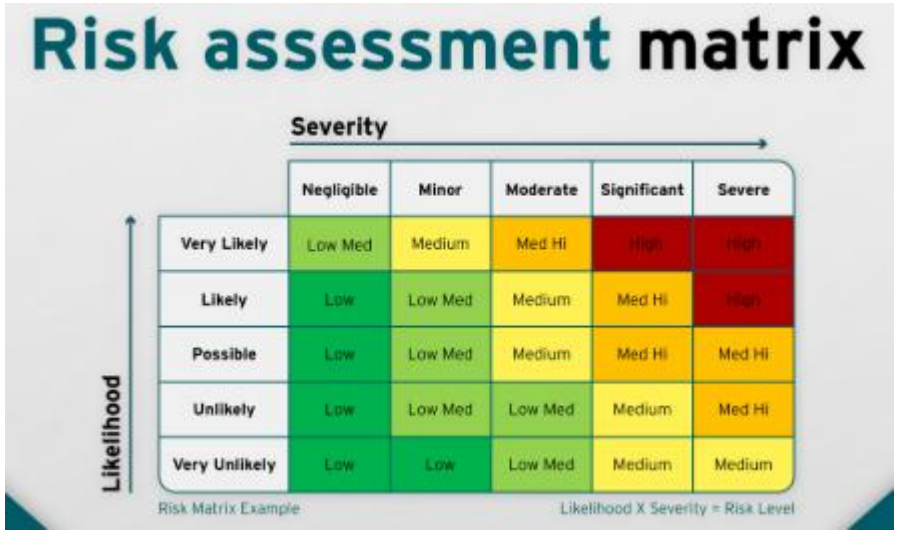

- Posición de la Organización en la cadena funcional de la aviación
- Nivel de contribución a las consecuencias para la seguridad operacional
- Servicios que provee (y recibe) la Organización incluyendo sus interfaces
- Procesos establecidos para proveer y recibir esos servicios

En cuanto a evidencias, se tendrán en cuenta:

1. Ámbito de trabajo
2. Tamaño y complejidad de la Organización
3. Impacto potencial en la seguridad causado por incidentes de Seguridad de la información
4. Criticidad de la Organización para el panorama de la aviación civil dentro del Estado miembro
5. Actividades transfronterizas de la organización, si corresponde
6. Madurez del Sistema de Gestión de la Seguridad de la Organización

Evaluación del riesgo (Risk Assessment): ¿Qué se espera?

La metodología del estudio de evaluación del riesgo debe realizarse según el SMS ya existente en la Organización.




La evaluación de riesgos de acuerdo a Part IS puede ser externalizada: IS.I.OR.235

**Los puntos no derogables son:**

IS.I.OR.200 (a) (13) Proteger la confidencialidad de la información recibida de (y enviada a) otras Organizaciones.

IS.I.OR.205 Evaluación de Riesgos de la Seguridad. Si hay cambios pueden anular las condiciones de Derogación.

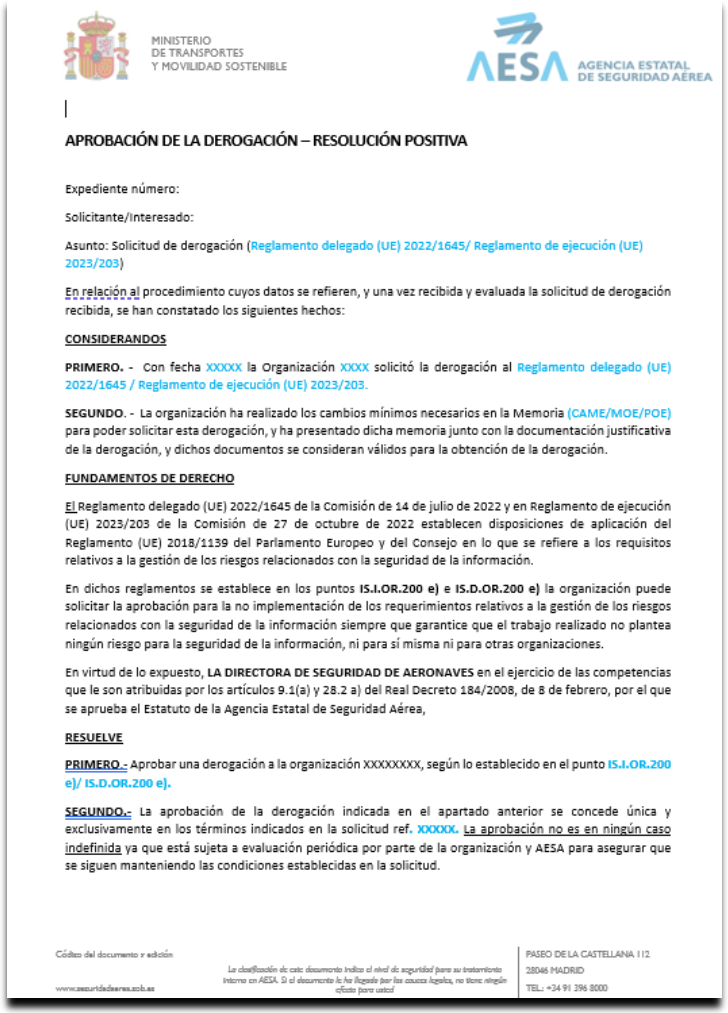
IS.I.OR.240 Requerimientos adicionales de personal. El DR debe tener conocimientos básicos de Part-IS.

| | | |
|---|---|---|
| IS.OR.200 (a) (13) | Protect confidentiality of information received from other organisations | This requirement should not be limited to only protect the received information. When transmitting information with confidential nature, the organisation needs to have secure means in place as well. |
| IS.OR.205 | Information security risk assessment | At least IS.I.OR205 (d) should still be applicable. Business environment can and will change over time. |
| IS.OR.240 | Additional personnel requirements | At least IS.I.OR.240 (3) should still be applicable. Someone needs to have an understanding of the rule. |

**Nota:** el Director Responsable de la organización debe demostrar un conocimiento del proceso de derogación y de los términos en los que se otorga la derogación.

**Resoluciones:**

## Positiva



MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

**APROBACIÓN DE LA DEROGACIÓN – RESOLUCIÓN POSITIVA**

Expediente número:

Solicitante/Interesado:

Asunto: Solicitud de derogación (Reglamento delegado (UE) 2022/1645/ Reglamento de ejecución (UE) 2023/203)

En relación al procedimiento cuyos datos se refieren, y una vez recibida y evaluada la solicitud de derogación recibida, se han constatado los siguientes hechos:

**CONSIDERANDOS**

**PRIMERO.** - Con fecha XXXXX la Organización XXXX solicitó la derogación al Reglamento delegado (UE) 2022/1645 / Reglamento de ejecución (UE) 2023/203.

**SEGUNDO.** - La organización ha realizado los cambios mínimos necesarios en la Memoria (CAME/MOE/POE) para poder solicitar esta derogación, y ha presentado dicha memoria junto con la documentación justificativa de la derogación, y dichos documentos se consideran válidos para la obtención de la derogación.

**FUNDAMENTOS DE DERECHO**

El Reglamento delegado (UE) 2022/1645 de la Comisión de 14 de julio de 2022 y en Reglamento de ejecución (UE) 2023/203 de la Comisión de 27 de octubre de 2022 establecen disposiciones de aplicación del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos relativos a la gestión de los riesgos relacionados con la seguridad de la información.

En dichos reglamentos se establece en los puntos **IS.I.OR.200 e)** e **IS.D.OR.200 e)** la organización puede solicitar la aprobación para la no implementación de los requerimientos relativos a la gestión de los riesgos relacionados con la seguridad de la información siempre que garantice que el trabajo realizado no plantea ningún riesgo para la seguridad de la información, ni para sí misma ni para otras organizaciones.

En virtud de lo expuesto, **LA DIRECTORA DE SEGURIDAD DE AERONAVES** en el ejercicio de las competencias que le son atribuidas por los artículos 9.1(a) y 28.2 a) del Real Decreto 184/2008, de 8 de febrero, por el que se aprueba el Estatuto de la Agencia Estatal de Seguridad Aérea,

**RESUELVE**

**PRIMERO.-** Aprobar una derogación a la organización XXXXXXXX, según lo establecido en el punto **IS.I.OR.200 e)/ IS.D.OR.200 e).**

**SEGUNDO.-** La aprobación de la derogación indicada en el apartado anterior se concede única y exclusivamente en los términos indicados en la solicitud ref. **XXXXX.** La aprobación no es en ningún caso indefinida ya que está sujeta a evaluación periódica por parte de la organización y AESA para asegurar que se siguen manteniendo las condiciones establecidas en la solicitud.

Código del documento y edición

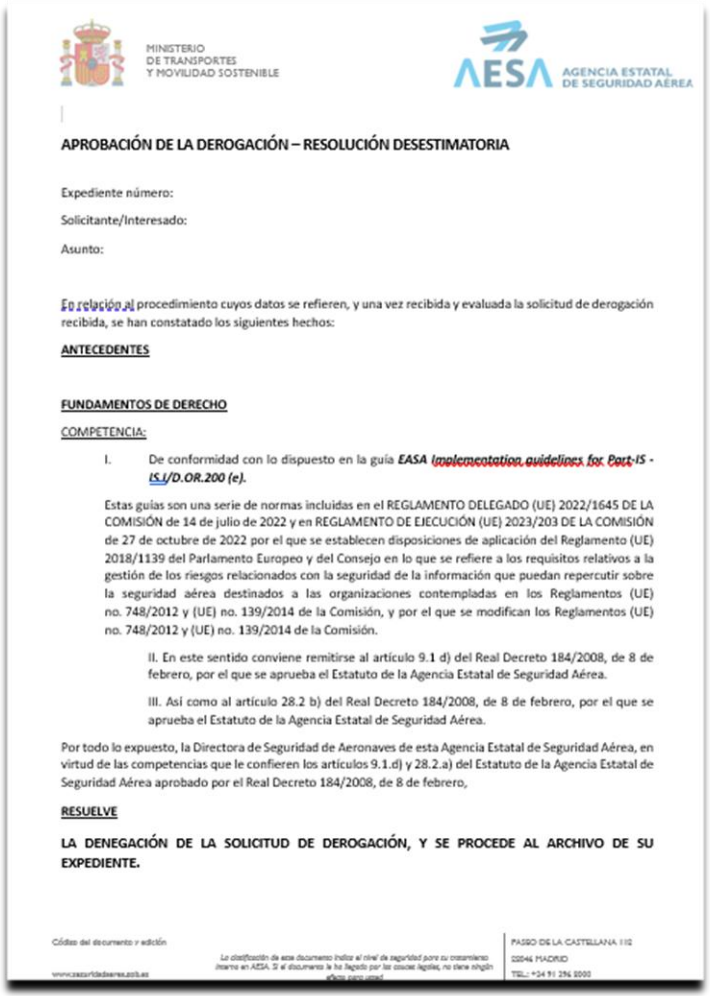
La clasificación de este documento indica el nivel de seguridad para su tratamiento interno en AESA. Si el documento le ha llegado por las causas legales, no tiene ningún efecto para usted

www.seguridadaerea.gob.es

PASEO DE LA CASTELLANA 112
28046 MADRID
TEL.: +34 91 396 8000

Se emite junto a la Aprobación del Manual.

## Desestimatoria



MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

**APROBACIÓN DE LA DEROGACIÓN – RESOLUCIÓN DESESTIMATORIA**

Expediente número:

Solicitante/Interesado:

Asunto:

En relación al procedimiento cuyos datos se refieren, y una vez recibida y evaluada la solicitud de derogación recibida, se han constatado los siguientes hechos:

**ANTECEDENTES**

**FUNDAMENTOS DE DERECHO**

COMPETENCIA:

I. De conformidad con lo dispuesto en la guía ***EASA Implementation guidelines for Part-IS - IS.I/D.OR.200 (e).***

Estas guías son una serie de normas incluidas en el REGLAMENTO DELEGADO (UE) 2022/1645 DE LA COMISIÓN de 14 de julio de 2022 y en REGLAMENTO DE EJECUCIÓN (UE) 2023/203 DE LA COMISIÓN de 27 de octubre de 2022 por el que se establecen disposiciones de aplicación del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos relativos a la gestión de los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea destinados a las organizaciones contempladas en los Reglamentos (UE) no. 748/2012 y (UE) no. 139/2014 de la Comisión, y por el que se modifican los Reglamentos (UE) no. 748/2012 y (UE) no. 139/2014 de la Comisión.

II. En este sentido conviene remitirse al artículo 9.1 d) del Real Decreto 184/2008, de 8 de febrero, por el que se aprueba el Estatuto de la Agencia Estatal de Seguridad Aérea.

III. Así como al artículo 28.2 b) del Real Decreto 184/2008, de 8 de febrero, por el que se aprueba el Estatuto de la Agencia Estatal de Seguridad Aérea.

Por todo lo expuesto, la Directora de Seguridad de Aeronaves de esta Agencia Estatal de Seguridad Aérea, en virtud de las competencias que le confieren los artículos 9.1.d) y 28.2.a) del Estatuto de la Agencia Estatal de Seguridad Aérea aprobado por el Real Decreto 184/2008, de 8 de febrero,

**RESUELVE**

**LA DENEGACIÓN DE LA SOLICITUD DE DEROGACIÓN, Y SE PROCEDE AL ARCHIVO DE SU EXPEDIENTE.**

## EVALUACIÓN CASO A CASO

En términos generales, podrían ser potencialmente derogables en aeronavegabilidad continuada las siguientes organizaciones:

- Utilizan exclusivamente un soporte físico como papel, CD, etc.; tanto para la gestión de datos como para almacenamiento de registros.
- Organizaciones 145 de determinados componentes no turbina (no aviónica) o que se dediquen exclusivamente a NDTs.
- Organizaciones CAMO y 145 que gestionen o mantengan **aeronaves distintas de las aeronaves motopropulsadas complejas** y que **no** estén incluidos en un **AOC** que cumple con Reg. 1008/2008.

"complex motor-powered aircraft" means:

(i) an aeroplane

— with a maximum certificated take-off mass exceeding 5 700 kg, or

— certificated for a maximum passenger seating configuration of more than nineteen, or

— certificated for operation with a minimum crew of at least two pilots, or

— equipped with (a) turbojet engine(s) or more than one turboprop engine, or

(ii) a helicopter certificated:

— for a maximum take-off mass exceeding 3 175 kg, or

— for a maximum passenger seating configuration of more than nine, or

— for operation with a minimum crew of at least two pilots, or

(iii) a tilt rotor aircraft.

Ejemplos de baremación del riesgo:

- Organización 145 dedicada en exclusiva a pintura de aeronaves, sin intercambio de datos aeronáuticos y equipos no conectados a internet => Riesgo bajo => Probabilidad de derogación alta.

- Organización CAMO que utiliza software en local, CDs, etc. => Riesgo medio (puestos de trabajo conectados/aislados y otras condiciones) => Probabilidad de derogación media.

- Organización 145 que realiza mantenimiento en base de aeronaves comerciales => Sistemas integrados OnLine (AMOS, ERP, etc.) => Riesgo alto => Probabilidad de derogación nula.

## Excepción

***Article 2 – Scope***

No tienen que cumplir la parte-IS las organizaciones dedicadas a aeronaves parte ML.

## Derogación

***IS.D.OR.200(e) - ISMS***

Organizaciones con poco riesgo de Seguridad de la Inf.

- Debe solicitarse y aprobarse por AESA (evaluación caso a caso)
- Presentar evaluación de riesgos
- Cumplir ciertos puntos normativos:
  IS.I.OR.200(a)(13)
  IS.I.OR.205
  IS.I.OR.240

# 3. FASE DE IMPLEMENTACIÓN
# Parte-IS

## Derogación

***IS.D.OR.200(e) - ISMS***

Antes de la fecha de efectividad del Reglamento:

Aprobada / Desestimada

22/02/2026

## Aprobación


**Step 1: Initial ISMS implementation ("Present" and "Suitable")**

Organisations should:

- Implement an ISMS at the "Present and Suitable" level by the applicability date of the relevant Part-IS regulation (i.e., 16 October 2025 for organisations covered by Delegated Rule (EU) 2022/1645, and 22 February 2026 for organisations covered by Implementing Regulation (EU) 2023/203, and perform, by that date, a Compliance Monitoring activity to ensure that the organisation meets those requirements.
- Start operating such ISMS immediately after the applicability date.

Aprobación en 4 fases:

P – **Present**

S – **Suitable**

O – Operational

E – Effective

## Operational & Effective

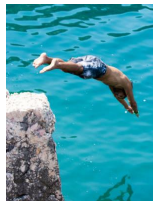
Requiere un "rodaje"

Integrado en la supervisión continuada (PVC)

Auditorías previsiblemente a partir de 2º semestre 2026

# 4. MANUAL ISMS Y APROBACIÓN
# Parte-IS

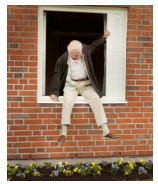
# Flujograma Procedimiento



Vía Solicitud de Cambio

**Organizaciones 145/CAMO**

Vía Solicitud de Derogación



**Solicitud Modificación**

Nueva solicitud modificación

**Solicitud Derogación**

Guía del Manual ISMS

Solicitud Común

Guidelines - Part-IS derogation - IS.I.OR_.200 (e)

Solicitud de Derogación

**Resolución Positiva de la modificación**

**Resolución Positiva del Manual**

**Res. Desestimatoria**

**Resolución Estimatoria**

**Resolución Positiva del Manual**

## IS.D.OR.200 (d) PROPOCIONALIDAD DE PROCEDIMIENTOS, PROCESOS, ROLES Y RESPONSABILIDADES

# COMPLEJIDAD ORGANIZACIÓN

RIESGOS ORGANIZACIÓN

EXPOSICIÓN DE RIESGOS A OTRA ORGANIZACIÓN

### SEGURIDAD DE LA INFORMACIÓN

**CADENA DE SUMINISTROS**

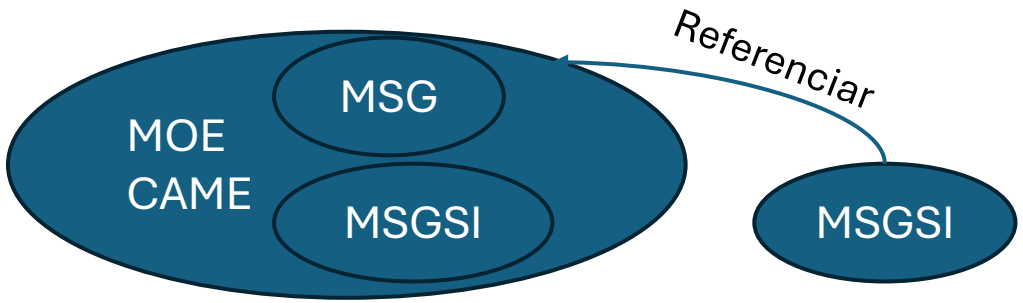
**ESTRUCTURA ORGANIZACIONAL**

**COMPLEJIDAD DE LOS SISTEMAS TECNOLÓGICOS DE COMUNICACIÓN E INFORMACIÓN Y DE LOS DATOS Y CONEXIÓN CON ORGANIZACIONES**

# SGSI. Implementación Present & Suitable.

**APROBACIÓN INICIAL MANUAL MSGSI**

MISMO CONCEPTO APROBACIÓN SISTEMA DE GESTIÓN




**APROBACIÓN DEL MANUAL MSGSI**

**PROCEDIMIENTO DE CAMBIOS – CAME/MOE/MSGSI**

**APROBACIÓN MOE/CAME**

## PRESENT AND SUITABLE

# SGSI. Implementación Present & Suitable

| Part-IS requirement | Description | Relevance (High /Background) | |
|---|---|---|---|
| | | ISMS Foundation | ISMS Operation |
| IS.I/D.OR.100 | Scope definition | High | Background |
| IS.I/D.OR.200 | Information security management system | High | Background |
| IS.I/D.OR.205 | Information security risk assessment | High | Background |
| IS.I/D.OR.210 | Information security risk treatment | High | Background |
| IS.I/D.OR.215 | Information security internal reporting scheme | Background | High |
| IS.I/D.OR.220 | Information security incidents — detection, response, and recovery | Background | High |
| IS.I/D.OR.225 | Response to findings notified by the competent authority | Background | High |
| IS.I/D.OR.230 | Information security external reporting scheme | Background | High |
| IS.I/D.OR.235 | Contracting of information security management activities | Background | High |
| IS.I/D.OR.240 | Personnel requirements | High | Background |
| IS.I/D.OR.245 | Record-keeping | Background | High |
| IS.I/D.OR.250 | Information security management manual | High | Background |
| IS.I/D.OR.255 | Changes to the ISMS | High | Background |
| IS.I/D.OR.260 | Continuous improvement | Background | High |

**Implementation levels (PSOE)**

**PRESENT**

**SUITABLE**

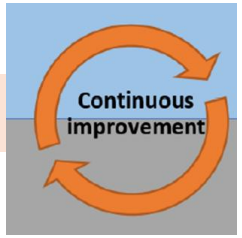
**ISMS Foundation**

**OPERATING**

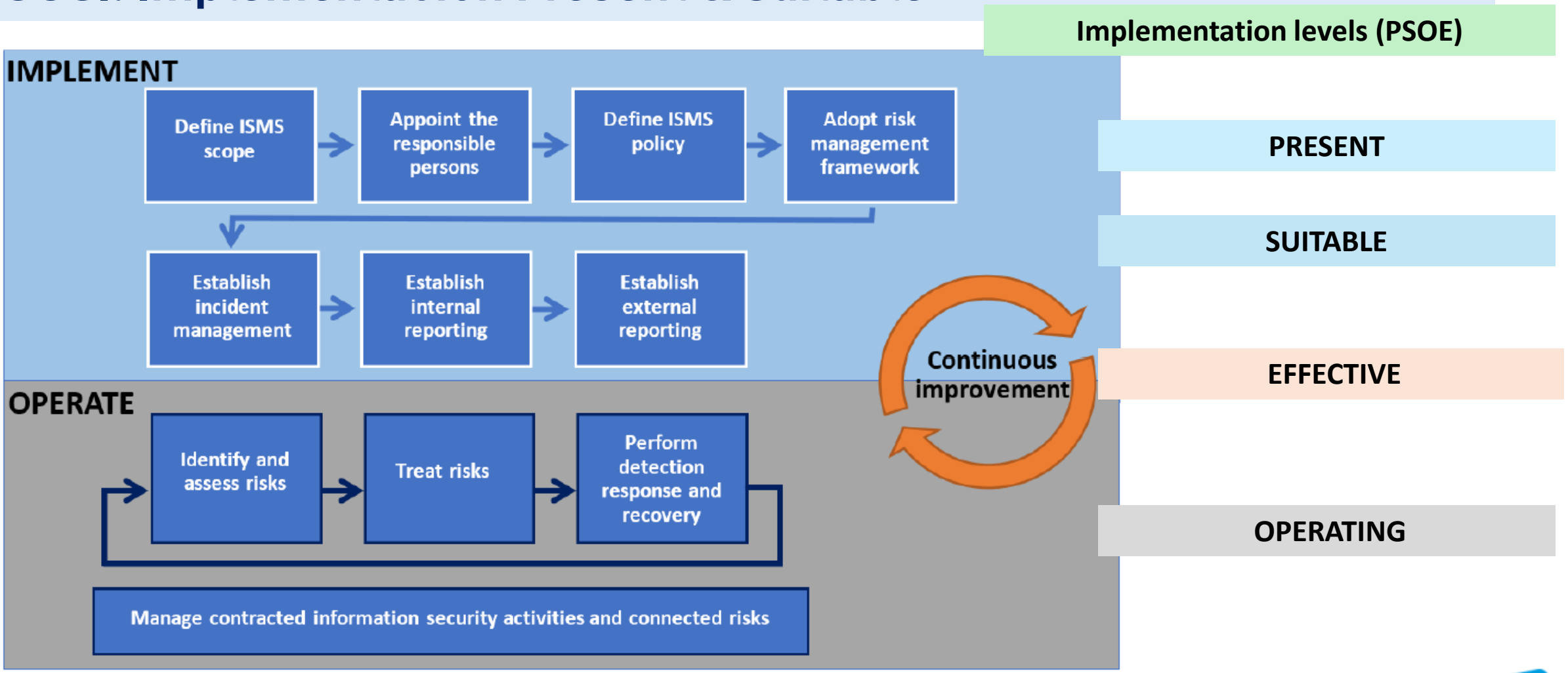
**ISMS Operation**

**Modelo de madurez:**
**Determinación de requisitos cumplidos y …**

**EFFECTIVE**



# SGSI. Implementación Present & Suitable



## El reglamento (UE) 2023/203

### IS.I.OR.250: Manual de Gestión de Seguridad de la Información (MGSI)

**MGSI**

- Declaración firmada por gestor responsable
- Identidad, funciones, potestades, obligaciones y responsabilidades del personal
- Política de seguridad de la información
- Planificación de disponibilidad del personal
- Organigrama que muestre las cadenas de obligaciones y responsabilidades
- Descripción del sistema interno de notificación

- Procedimientos que especifiquen la forma en la que la organización cumple con el reglamento
- Procedimiento de control de las organizaciones contratadas
- Procedimiento de modificación del MGSI
- Detalles de los medios alternativos de cumplimiento aprobados (si los hubiese)

**Resolución Positiva del Manual**


Deberá estar aprobado antes del 22 de febrero 2026.

# MANUAL ISMS – ALCANCE

**ACTIVIDADES / INTERFACES**

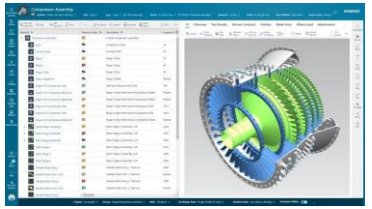
**PROCESOS / PROCEDIMIENTOS**

**SISTEMAS DE SOPORTE**

**Ejemplos de sistemas de información específicos:**

- ERP(*) de fabricación (SAP, ENOVIA…)
- Software de Gestión de Ciclo de Vida de Producto PLM (Teamcenter)
- Software de MRO (AMOS)

**AMC1 IS.D.OR.200(a)(1) Information security management system (ISMS)**




**GUÍA INTERNA PARA LA DEFINICIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISMS) EN ORGANIZACIONES EASA PART-IS**


# ASPECTOS CLAVE PARA EL ISMS

1. DEFINICIÓN DEL ALCANCE DE SEGURIDAD DE LA INFORMACIÓN
2. POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN
3. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
4. DETECCIÓN, RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES
5. CONTRATACIÓN ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN
6. GESTIÓN DEL CAMBIO DE SEGURIDAD DE LA INFORMACIÓN
7. PROMOCIÓN SEGURIDAD DE LA INFORMACIÓN
8. CONTROL DE CONFORMIDAD DE SEGURIDAD DE LA INFORMACIÓN

# MANUAL ISMS – POLÍTICA Y OBJETIVOS

IS.I.OR.200(a)(1)

IS.I.OR.200(c)(d)

IS.I.OR.250(a)(1), (a)(4), (a)(9)

| PROCESO | POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES |
|---|---|
| **1. Política y Objetivos de Seguridad** | Política de Seguridad de la Información |
| | Política de Cultura Justa |
| | Programa o Plan de Seguridad de la Organización |
| | Sistema de Notificación de sucesos/eventos |
| | Organigrama de la organización |
| | Procedimiento de rendición de cuentas y funciones del DR/CRP y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización e incluyendo la identidad y la fiabilidad del personal que tenga acceso a los sistemas de información y a los datos. |
| | Plan de respuesta ante Emergencias |
| | Procedimiento para gestionar la documentación y registro del sistema de gestión de seguridad de la información. |

# MANUAL ISMS – GESTIÓN DE RIESGOS

***JUSTIFICAR EXCLUSIONES***

**Alcance MSGI ---**

**Elementos**

Actividades, instalaciones, recursos y servicios
Equipos, sistemas, datos, información

**Interfaces**

Proveedores de servicios, cadena de suministro y otros

Sujetas a PARTE IS – Intercambio mutuo

NO Sujetas a PARTE IS – Contrato para mitigación y control

**ACTIVOS RELEVANTES SAFETY**

- PERSONAS
- FÍSICO
- INFORMACIÓN

**EXPOSICIÓN MUTUA DE RIESGOS INTERFACES**

DOCUMENTACIÓN DE REFERENCIA

**PROCESO DOCUMENTADO PARA IDENTIFICACIÓN DEL ALCANCE**

COMPARTIR RIESGOS

# MANUAL ISMS – GESTIÓN DE RIESGOS

FUNCIONES
SERVICIOS
CAPACIDADES

**INPUTS Y OUTPUTS OPERACIONALES**

Internos o externos.
Dependencias. Servicios contratados o gestionados.

Crear, procesar, transmitir, almacenar o recibir.

**ACTIVOS**

Hardware, software, redes, recursos.

Métodos
Procesos
Recursos internos o contratados

**GESTIÓN OPERACIÓN MANTENIMIENTO**

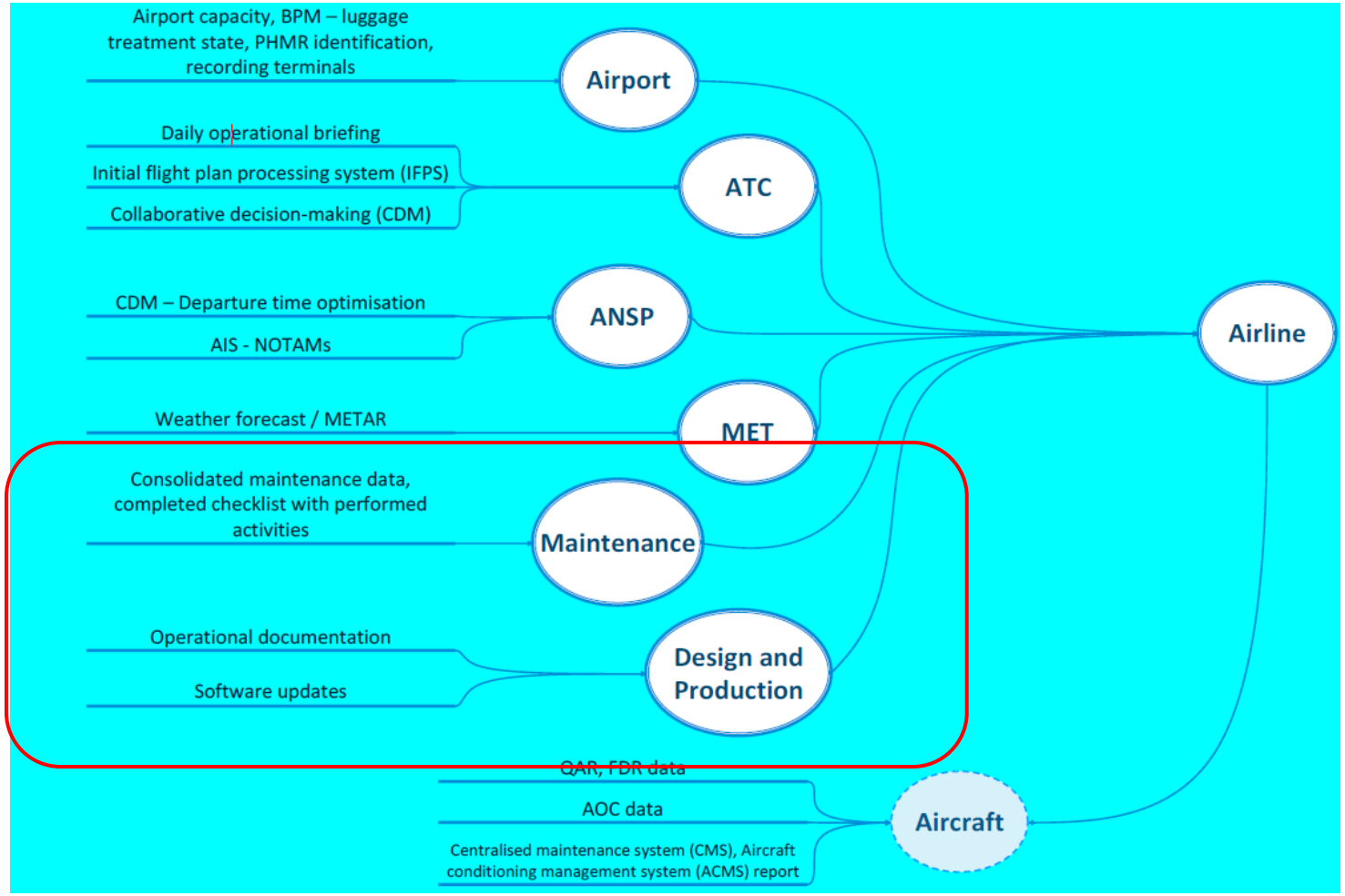
**ENTORNO OPERATIVO LOCALIZACIÓN**

Oficinas, áreas de acceso público, áreas de acceso controlado

# MANUAL ISMS – GESTIÓN DE RIESGOS

INTERFACES

Organizaciones de mantenimiento y producción con un operador aéreo



# MANUAL ISMS – GESTIÓN DE RIESGOS IS

IS.I.OR.200(a)(2)
IS.I.OR.205(a)(b)
IS.I.OR.210

**THREAT SCENARIO**

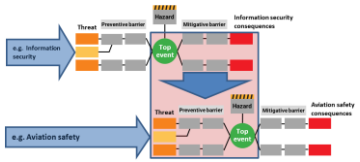
**OBJETIVO PARTE IS → LISTA DE ESCENARIO DE AMENAZAS**

- Posibles formas en que podría materializarse una amenaza.
- Describe un ataque dirigido a los activos definidos en el alcance.

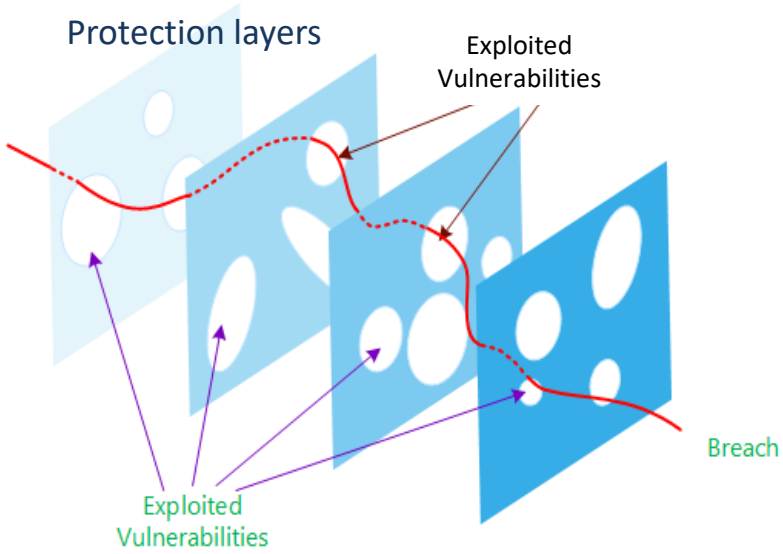
## IDENTIFICACIÓN

- Fuente de amenaza del ataque
- Vector de ataque y un camino a través de la organización hasta el activo;
- Controles de seguridad de la información que mitigarían el ataque.
- Consecuencias del ataque.

## OTROS MÉTODOS: BOW TIE ANÁLISIS



**CATÁLOGOS:**
ARINC 811 – Att. 3 – Tables 3-7 and 3-8
ENISA threat taxonomy.




violación de la seguridad de la información que existe desde el momento en que una entidad, circunstancia, acción o hecho puede ocasionar daños;

**Latent vulnerabilities**

defecto o debilidad presente en un activo o un sistema, en los procedimientos, en el diseño, en la aplicación o en las medidas de seguridad de la información que podría aprovecharse y dar lugar a un fallo o una violación de la política de seguridad de la información.

# MANUAL ISMS – GESTIÓN DE RIESGOS IS

**DETERMINAR NIVELES DE RIESGOS**

**THREAT SCENARIO**

**OCURRENCIA** **SEVERIDAD**

**ASOCIACIÓN DE RIESGOS A ELEMENTOS O INTERFACES**

**ACEPTABILIDAD Y TRATAMIENTO**

**METODOLOGÍA DOCUMENTADA**
- REPRODUCIBILIDAD
- REPETITIBIDAD
- RECOPILACIÓN DE INPUTS
- ITERATIVIDAD

**PERIODICIDAD REVISIÓN**

**CASO**


ESTANDARES EVALUACIÓN DE RIESGOS
CRITERIO DE ACEPTACIÓN
ELEMENTOS PARA ESTABLECER PROBABILIDAD
COMPARABILIDAD EVALUACIONES DE RIESGO

ADAPTADO A LA ORGANIZACIÓN

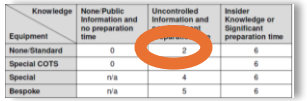
# MANUAL ISMS – GESTIÓN DE RIESGOS IS

EUROCAE ED-203A

PROBABILIDAD

## MEDIOS DE PROTECCIÓN

Denegación de accesos
Accesos a medidas de seguridad
Mecanismos de fallo
Reconocimiento de ataques



| Equipment \ Knowledge | None/Public Information and no preparation time | Uncontrolled Information and | Insider Knowledge or Significant preparation time |
|---|---|---|---|
| None/Standard | 0 | 2 | 6 |
| Special COTS | 0 | | 6 |
| Special | n/a | 4 | 6 |
| Bespoke | n/a | 5 | 6 |

## VENTANA DE EXPOSICIÓN

Acceso desde conexiones externas
Gestión de vulnerabilidades
Medidas de reducción de severidad tras ataques
…

| Effect | Description |
|---|---|
| 0 | The attack can be carried out at any time. |
| | The attack can be carried out during regular cruise flight. |
| 2 | The attack vector is available while the aircraft is on the ground. |
| | Maximum effectiveness for mandatory operational procedures limiting the window of opportunity. |
| 6 | The attack vector is only available in a restricted time phase, e.g. on the ground in maintenance mode. |
| 8 | The attack can only be carried out during a very restricted time slot independent from the flight phase (e.g. during system reboot). |

## INTENTOS DE ATAQUE

Capacidad y experiencia del atacante
CERTS/ISACS…

| Expertise / Equipment | Layman | Proficient | Expert | Multiple Expert |
|---|---|---|---|---|
| None/Standard | | 4 | 6 | 10 |
| Special COTS | 4 | 4 | 6 | 10 |
| Special | | 6 | 8 | 12 |
| Bespoke | n/a | n/a | 10 | 12 |

| points | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| effectiveness | None | | | | | | | Basic | | | | | | Moderate | | | | | | High | | | | | | Very High | | | | | |
| level of threat | Very High | | | | | | | High | | | | | | Moderate | | | | | | Low | | | | | | Very Low | | | | | |

EUROCAE ED-201A

SEVERIDAD

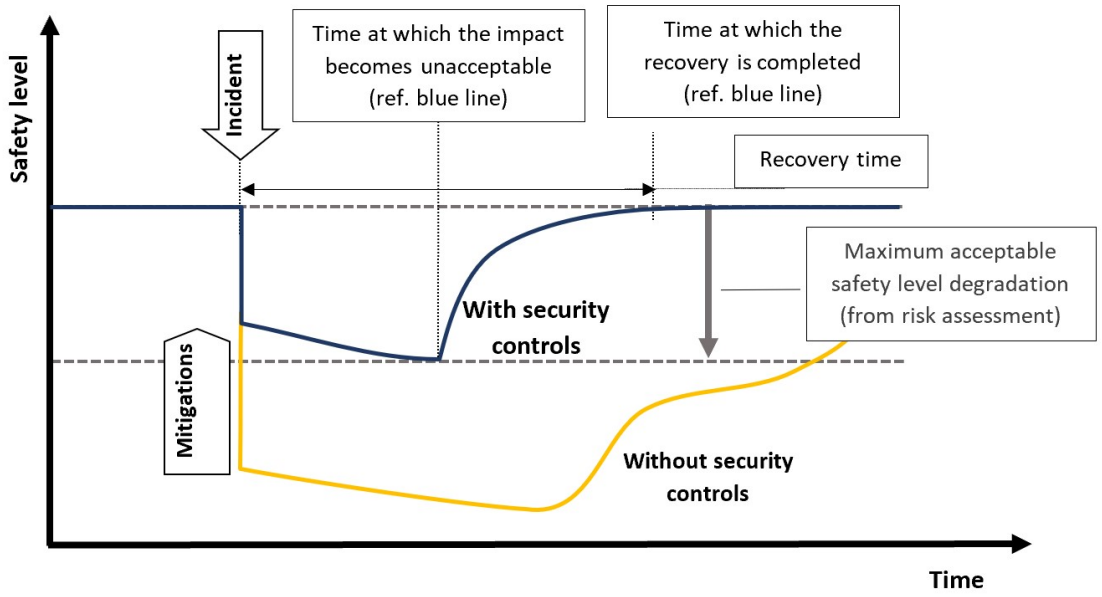
| ICAO Annex 13 > | Negligible effect | Incident | Accident |
|---|---|---|---|
| Threat scenario — potential of occurrence | **Low safety consequences** | **Moderate safety consequences** | **High safety consequences** |
| **High** | Conditionally acceptable | **Not acceptable** | **Not acceptable** |
| **Medium** | Acceptable | Conditionally acceptable | **Not acceptable** |
| **Low** | Acceptable | Acceptable | Conditionally acceptable* |

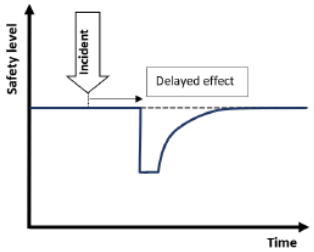
Criterio aceptación del riesgo
Cuanto tiempo va a existir el riesgo
Tratamiento
DR/CRP

# MANUAL ISMS – DETECCIÓN, RESPUESTA Y RECUPERACIÓN

**Incidente:** todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información

IS.I.OR.220



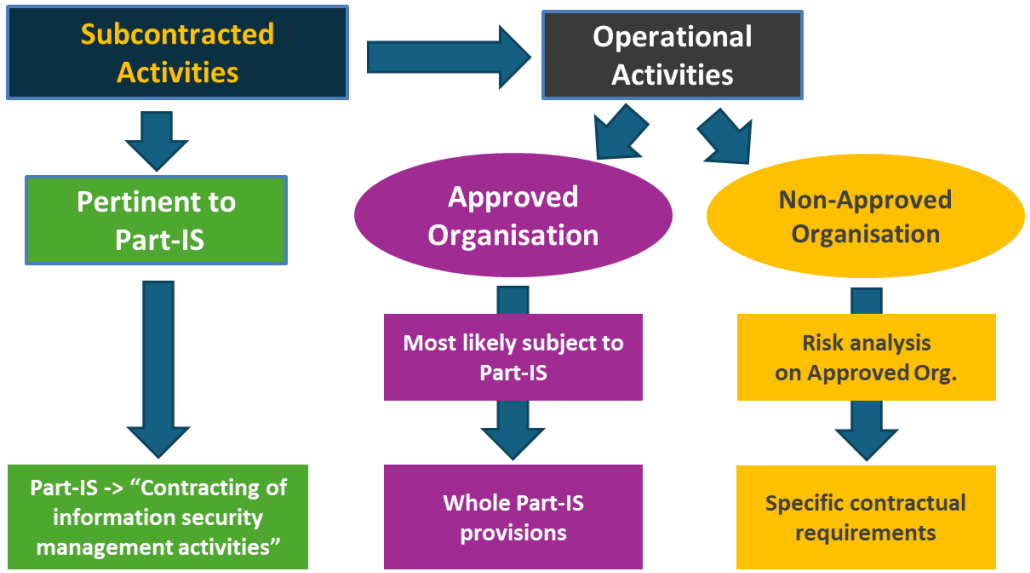




1 Preparar | 2 Detectar | 3 Responder | 4 Recuperar

Enfoque sistemático y bien definido para gestionar y mitigar el impacto de un incidente de ciberseguridad.

# MANUAL ISMS – CONTRATACIÓN ACTIVIDADES IS

IS.I.OR.235




## SUPERVISIÓN

- Requisitos de las actividades contratadas.
  - Definición y acuerdo sobre el alcance de las actividades.
  - Definición de los roles y responsabilidades de las partes (es decir, organización contratante y organización contratada).
  - Definición y revisión de los KPI.
  - Reacción ante desviaciones de las obligaciones contractuales.
  - Realización de auditorías de cumplimiento, de acuerdo con el alcance y los objetivos predefinidos, con el fin de evaluar las actividades operativas y de aseguramiento asociadas.
  - Provisión de retroalimentación sobre el resultado de las auditorías de cumplimiento tanto dentro de la organización como a la organización contratada, y respuesta a los hallazgos.

## GESTIÓN DE RIESGOS

## ACCESO

# MANUAL ISMS – GESTIÓN DEL CAMBIO IS

IS.I.200 (b)&(c)
IS.I.OR.255
IS.I.OR.250(a)(9)
IS.I.OR.250(c)
IS.I.OR.260

## CAMBIOS

- Procedimiento desarrollado por la organización y aprobado por la autoridad.

- Procedimiento de cambios que requieren aprobación de la autoridad.
  - nivel inaceptable de riesgo
  - impacto en el SGSI

# MANUAL ISMS – PROMOCIÓN IS

IS.I.OR.200 (a)(10)
IS.I.OR.240 (g)
AMC1 IS.I.OR.200 (a)(1); (h)

## Instrucción y educación

***COMPETENCIA DEL PERSONAL***

- **EVALUAR ROLES** — Los roles laborales y las tareas asociadas.
- **DEFINIR GAP** — Conocimientos, habilidades y capacidades requeridos
- **PROGRAMA DE CAPACITACIÓN** — Alcance, contenido, frecuencia, métodos
  Revisión programa ante nuevas amenazas

# MANUAL ISMS – CONTROL DE CONFORMIDAD

**Función de control de conformidad y Programa de auditorías (Resp. Control Conf.)**

## IS.I.OR.200 (a) (12)

- CONTROL Y CUMPLIMIENTO DEL SGI Y ADECUACIÓN DE PROCEDIMIENTOS INCLUIDOS PROCESOS AUDITORÍAS Y GESTIÓN DE RIESGOS.
- PLAN DE AUDITORÍAS INTERNAS.
- INDEPENDENCIA.
- REPORTAR DISCREPANCIAS A DR/CRP PARA ASEGURAR IMPLEMENTACIÓN DE ACCIONES.

## IS.I.OR.240 (c)(h)

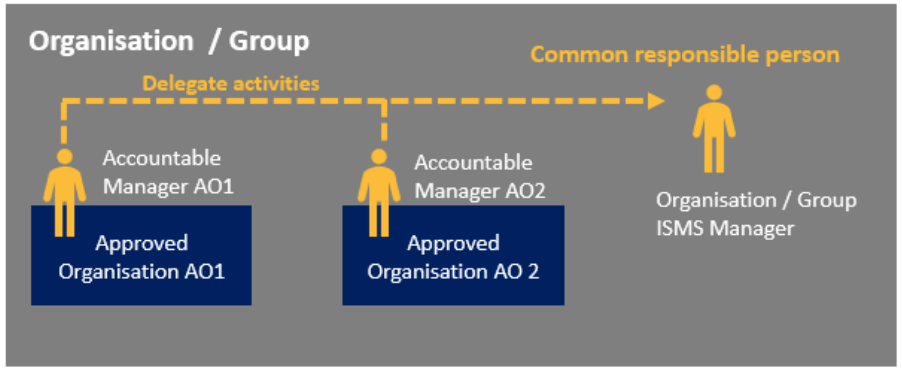
- DESIGNADO POR DR, ORGANIGRAMA, TABLA DE ROLES Y RESPONSABILIDADES
- PUEDE SER EL RCC CAMO, RCC 145 O RCC IS REPORTANDO A RCC CAMO, RCC 145
- LA ORGANIZACIÓN DEBE ASGURAR QUE CONOCE SUS RESPONSABILIDADES EN FUNCIÓN DE ROLES Y TAREAS.

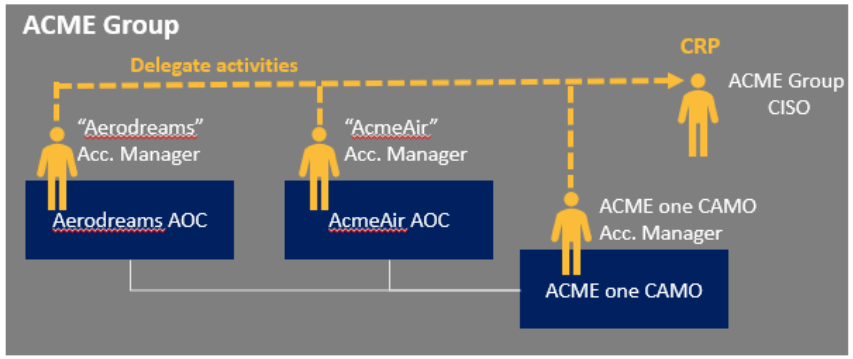
IS.I.OR.200(a)(12)
IS.I.OR.240 (c)(h)(i)
IS.I.OR.200(c)(d)
IS.I.OR.250(a)(9)
IS.I.OR.200 (a)(7)
IS.I.OR.225
IS.I.OR.250(a)(9)
IS.I.OR.200 (a)(6)
IS.I.OR.220 (b) (c)
IS.I.OR.250(a)(9)(10)

# 5. DUDAS Y PREGUNTAS
# Parte-IS

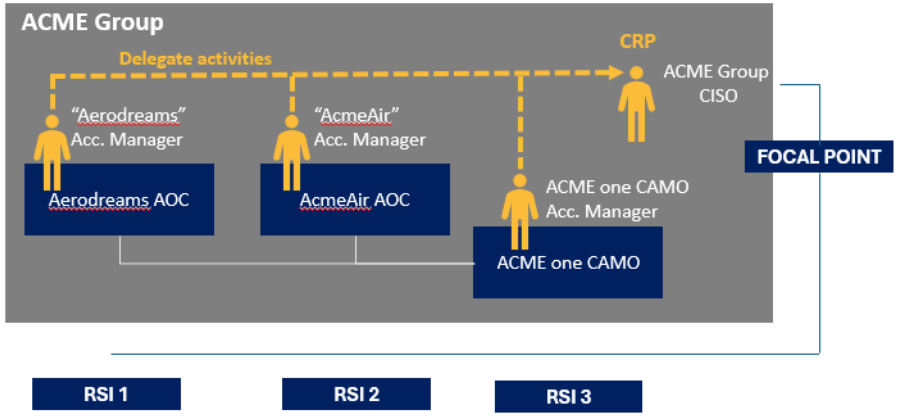
**Fórmula para hacer combinar roles que se solicitan en el ISMS y recursos disponibles.**

- PERSONA RESPONSABLE COMÚN.




- RSI.




RCC

- PUEDE SER EL RCC CAMO, RCC POA, RCC 145
- RCC IS REPORTANDO A RCC CAMO, RCC POA, RCC 145

**Alcance de las auditorías externas. Es decir, según indica EASA, en este primer paso, el SGSI debe estar presente y ser adecuado, para posteriormente entrar en operación y ser eficaz.**
**Según esto:**

**1- ¿Se tendrá en cuenta que el nivel de madurez del SGSI puede estar en su estado inicial con planes de acción y mejoras?**

SGSI Present and Suitable

Auditoría previa de la organización
Operar el SGSI desde el 22 febrero 2026
MSGI / Procedimiento de cambios / Evaluación de riesgos inicial

La organización debe estar en posición de operar el SGSI y, por tanto, se necesitaría conocer caso a caso sobre cómo afectan dichos planes de acción y mejoras.

Existen elementos Present and Suitable que se evaluarán una vez obtenida la aprobación inicial en fase de supervisión.

**2- En la auditoría se seguirá la guía de Easa (Part IS implementation task force) para evaluar los elementos que se indican? O se añadirán más por parte del auditor.**
Documentación EASA.
Documentación AESA.
Normativa.

**¿Cuándo está previsto adaptar el Sistema de Notificación de Sucesos de AESA (SNS) para reportar suceso relacionados con la parte IS. En la actualidad, una vulnerabilidad en la organización, por ejemplo, no tiene cabida en el actual formato de SNS**

**Dudas de cómo notificar un suceso relacionado con la parte IS en el actual SNS.**

Sobre la posibilidad de notificación de sucesos relacionados con la parte IS, la taxonomía específica está ahora mismo bajo desarrollo por parte del Data Quality and Taxonomy Working Group y la versión reducida preliminar se espera en la próxima actualización del sistema prevista proximamente.

Actualmente, se pueden notificar sucesos con parte IS al SNS que tengan afección en la seguridad operacional como se ha podido siempre a través del buzón de notificación como se indica en: Notifica un suceso | AESA-Agencia Estatal de Seguridad Aérea – MTMS. Teniendo en cuenta que actualmente:

- El registro por parte del SNS de dicho suceso está limitado por la taxonomía actual disponible.
- La taxonomía no es una limitación para el notificante.
- Esta situación es la misma para todas las autoridades europeas hasta que se implemente esa nueva taxonomía que ofrece más campos de registro de datos específicos IS.

# 5. DUDAS Y PREGUNTAS

# Gracias por su atención

www.seguridadaerea.gob.es