Agencia Estatal
de Seguridad Aérea

Guía para la elaboración del Manual de Gestión de la Seguridad de la Información (IS.I.OR.250. Part-IS) en el ámbito de Navegación Aérea

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE
AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

REGISTRO DE EDICIONES		
EDICIÓN	**Fecha de APLICABILIDAD**	**MOTIVO DE LA EDICIÓN DEL DOCUMENTO**
Ed. 01	Desde publicación	Creación de la guía

REFERENCIAS	
CÓDIGO	**TÍTULO**
N/A	FIRST EASY ACCESS RULES FOR INFORMATION SECURITY (REGULATIONS (EU) 2023/203 AND 2022/1645)
Part-IS TF G-03	PART-IS OVERSIGHT APPROACH GUIDELINES FOR COMPETENT AUTHORITIES FOR THE CONDUCT OFOVERSIGHT ACTIVITIES OF ORGANISATIONS IMPLEMENTING PART-IS

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
AESA	AGENCIA ESTATAL DE SEGURIDAD AÉREA
AMC	MEDIO ACEPTABLE DE CUMPLIMIENTO
ATM/ANS	GESTIÓN DE TRÁFICO AÉREO/SISTEMAS DE NAVEGACIÓN AÉREA
CCN	CENTRO CRIPTOLÓGICO NACIONAL
CE	COMISIÓN EUROPEA
CEO	DIRECTOR EJECUTIVO
DLP	PREVENCIÓN DE PÉRDIDA DE DATOS
DNA	DIRECCIÓN DE NAVEGACIÓN AÉREA
EASA	AGENCIA EUROPEA DE SEGURIDAD AÉREA
ED	EUROCAE DOCUMENT
EDR	DETECCIÓN Y RESPUESTA DE ENDPOINTS
ENS	ESQUEMA NACIONAL DE SEGURIDAD
EUROCAE	ORGANIZACIÓN EUROPEA PARA EL EQUIPAMIENTO DE LA AVIACIÓN CIVIL
GM	MATERIAL GUÍA
GSI	GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
INCIBE	INSTITUTO NACIONAL DE CIBERSEGURIDAD
ISO/IEC	ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN / COMISIÓN ELECTROTÉCNICA INTERNACIONAL
KPI	INDICADOR CLAVE DE DESEMPEÑO
MGSI/ISMM	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
NIS2	DIRECTIVA SOBRE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN
NIST	INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA
SGSI/ISMS	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
SIEM	GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
SOC	CENTRO DE OPERACIONES DE SEGURIDAD
U-SPACE	ESPACIO DE GESTIÓN DEL TRÁFICO DE AERONAVES NO TRIPULADAS
UE	UNIÓN EUROPEA

ÍNDICE

1 OBJETO

Esta Guía tiene por objeto orientar a las organizaciones del **ámbito de navegación aérea** incluidas en el alcance del Reglamento de Ejecución (UE) 2023/203 Anexo II (a partir de ahora REG PART-IS) sobre el contenido mínimo, pautas y buenas prácticas a considerar en la elaboración del **Manual de Gestión de seguridad de la Información** (MGSI o ISMM por sus siglas en inglés). Todo ello para facilitar el cumplimiento del requisito **IS.I.OR.250**[1] del **REG PART-IS**, sin perjuicio del cumplimiento con otra normativa de seguridad de la información que sea de aplicación.

2 ALCANCE

La presente Guía va dirigida a las siguientes organizaciones:

- los proveedores de servicios ATM/ANS sujetos al anexo III del Reglamento de Ejecución (UE) 2017/373.
- las organizaciones de formación de controladores de tránsito aéreo sujetos a lo dispuesto en el reglamento (UE) 2015/340.
- proveedores de servicios de U-Space y proveedores de servicios de información común sujetos al Reglamento de Ejecución (UE) 2021/664.

Quedan fuera del alcance de esta guía aquellas organizaciones que, estando incluidas en los puntos anteriores, demuestren, conforme al punto **IS.I.OR.200 (e)**, que sus actividades, instalaciones y recursos, así como los servicios que gestionan, prestan, reciben y mantienen, no plantean ningún riesgo relacionado con la seguridad de la información que pueda repercutir en la seguridad aérea, ni para ella misma ni para otras organizaciones

[1] A lo largo de esta guía se utilizará el siguiente código de colores (azul, naranja o verde), respectivamente, para las indicaciones, en función de la clasificación que tengan en la normativa (requisito, medio aceptable de cumplimiento AMC o material guía GM):

Requisito normativo

Medio aceptable de cumplimiento AMC

Material guía GM

3 NORMATIVA APLICABLE

El requisito reglamentario al que se refiere este material guía es el siguiente:

IS.I.OR.250 Manual de gestión de seguridad de la información (MGSI)

a) La organización pondrá a disposición de la autoridad competente un manual de gestión de la seguridad de la información (MGSI) y, en su caso, cualquier manual y procedimiento asociado referenciado que contenga:

1) una declaración firmada por el director responsable en la que se confirme que la organización trabajará en todo momento de conformidad con el presente anexo y con el MGSI; si el director responsable no es el director ejecutivo (consejero delegado) de la organización, este deberá refrendar la declaración;

2) el título, el nombre, las funciones, las obligaciones, las responsabilidades y las potestades de la persona o personas definidas en el punto IS.I.OR.240, letras b) y c);

3) el título, el nombre, las funciones, las obligaciones, las responsabilidades y las potestades de la persona responsable común definida en el punto IS.I.OR.240, letra d), si procede;

4) la política de seguridad de la información de la organización a que se refiere el punto IS.I.OR.200, letra a), punto 1);

5) una descripción general del número y las categorías del personal y del sistema en vigor para planificar la disponibilidad de personal, como requiere el punto IS.I.OR.240;

6) el título, el nombre, las funciones, las obligaciones, las responsabilidades y las potestades de las personas clave responsables de la aplicación del punto IS.I.OR.200, incluida la persona o personas responsables de la función de control del cumplimiento a que se refiere el punto IS.I.OR.200, letra a), punto 12);

7) un organigrama que muestre las cadenas de obligaciones y responsabilidades asociadas de las personas a que se refieren los puntos 2) y 6);

8) la descripción del sistema interno de notificación a que se refiere el punto IS.I.OR.215;

9) los procedimientos que especifiquen la forma en que la organización garantiza el cumplimiento de la presente parte, y en particular:

i) la documentación mencionada en el punto IS.I.OR.200, letra c);

ii) los procedimientos que definen cómo controla la organización las actividades contratadas a que se refiere el punto IS.I.OR.200, letra a), punto 9);

iii) el procedimiento de modificación del MGSI a que se refiere la letra c);

10) los detalles de los medios alternativos de cumplimiento aprobados.

b) La autoridad competente aprobará la edición inicial del MGSI y conservará una copia. El MGSI se modificará según sea necesario para seguir constituyendo una descripción actualizada del SGSI de la organización. Se entregará a la autoridad competente una copia de las modificaciones introducidas en el MGSI.

c) Las modificaciones del MGSI se gestionarán mediante un procedimiento establecido por la organización. Las modificaciones que no estén incluidas en el ámbito de este procedimiento, así como las modificaciones relacionadas con los cambios a que se refiere el punto IS.I.OR.255, letra b), serán aprobadas por la autoridad competente.

d) La organización podrá integrar el MGSI con otras guías o manuales de gestión que posea, siempre que exista una referencia cruzada clara que indique qué partes de la guía o manual de gestión corresponden a los diferentes requisitos que figuran en el presente anexo.

GM1 IS.I.OR.250(a) INFORMATION SECURITY MANAGEMENT MANUAL (ISMM)

ED Decision 2023/009/R

The organisation may choose to document some of the information required under point IS.I.OR.250(a) in separate documents (e.g. procedures). In this case, it should ensure that the manual contains adequate references to any document kept separately. Any such documents are then to be considered an integral part of the organisation's information security management system manual.

In the event where an entity holds multiple authorisations or declarations, the ISMM may apply to one or more organisations at a time based on a common ISMS. This ISMM should include at least an approval document of each organisation and should formally be approved by each organisation's accountable manager or responsible person. A common responsible person may be appointed as per IS.I.OR.240(d) and the guidelines of GM1 IS.I.OR.240(e).

To ensure that all parties involved can fulfil their responsibilities, all manuals, procedures, and communication between them are advised to be, at least, in one common language, e.g. English. Those parties involved include the competent authorities with which that common language should be agreed upon.

4 MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Antes de indicar el contenido mínimo que debe incluir, se debe introducir el concepto de MGSI.

Un MGSI es un documento o conjunto de documentos que establece las **directrices, políticas, procedimientos y controles** necesarios para proteger la información requerida para la prestación de los servicios de una organización. Su objetivo principal es asegurar la confidencialidad, la integridad, la autenticidad y la disponibilidad de la información.

Es una herramienta clave para que una organización **implemente, mantenga y mejore de manera continua su sistema de gestión de seguridad de la información (SGSI**), ayudando a prevenir, detectar, y responder ante las amenazas que puedan comprometer la seguridad de la información, y restablecer las operaciones ante su materialización.

5 CONTENIDO DEL MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El MGSI debe seguir una estructura clara y detallada, teniendo en cuenta las particularidades y **necesidades específicas de la organización**, los **riesgos a los que está expuesta** y la **normativa de aplicación.**

El MGSI debe reflejar fielmente la forma en la que la entidad cumple con todos los requisitos establecidos en el REG PART-IS, mediante la inclusión en el propio documento o haciendo referencia en el mismo a todas las normas, procedimientos y procesos que se siguen por parte de la organización.

El **alcance del MGSI** deberá comprender todos los equipos, sistemas, información y datos requeridos para la prestación de todos los servicios que pudieran estar expuestos a riesgos de seguridad de la información, de acuerdo a como se establece en **IS.I.OR.205 (a)(2)**.

El texto del recuadro sombreado en gris que aparece a continuación, y el de todos los recuadros siguientes, procede de la guía de EASA "Part-IS oversight approach - Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS" Part-IS TF G-03 March 2025.

El MGSI deberá definir el alcance del SGSI, p. ej., los servicios, sistemas, activos, procesos, interfaces y perímetro, con las justificaciones adecuadas del resultado y las exclusiones que se hayan

Adicionalmente, la Guía interna para la definición del alcance del sistema de gestión de seguridad de la información (ISMS) en organizaciones EASA PART-IS, SEC-CB-GU01 desarrollada por AESA, proporciona un marco metodológico y sistemático para la definición y documentación del **alcance del Sistema de Gestión de Seguridad de la Información (ISMS)**, conforme al **AMC1 IS.AR.200(a)(1)**. Aunque está orientada a su uso por parte del personal auditor puede servir de ayuda a las organizaciones para determinar el alcance de su SGSI.

A continuación, se detalla el contenido mínimo que debe formar parte del MGSI o estar referenciado en el mismo**.**

5.1 Declaración responsable

Tal y como se indica en el punto **IS.I.OR.250 (a)(1)** la organización debe disponer de una declaración responsable en la que se comprometa a trabajar en todo momento de conformidad con los requisitos del REG PART-IS y de acuerdo a lo establecido en el MGSI.

Esta declaración responsable representa el compromiso formal de la alta dirección con la seguridad de la información en la organización, lo que es esencial para asegurar el cumplimiento y la protección de los activos de información y por lo tanto debe ir firmada por el **director responsable** de la entidad.

A modo de ejemplo:

> ***Declaración de Cumplimiento con el Manual de Gestión de seguridad de la Información (MGSI)***
>
> *Yo, [Nombre del Director Responsable], en calidad de [Cargo], declaro que el Sistema de Gestión de la Seguridad de la Información (SGSI) implementado en [Nombre de la organización] cumple con los requisitos establecidos en el Reglamento de Ejecución (UE) 2023/203 (PART-IS).*
>
> *Esta declaración se emite en base a la documentación contenida en el Manual de Gestión de la Seguridad de la Información (MGSI), que incluye:*
>
> - *El alcance del SGSI, incluyendo servicios, sistemas, activos, procesos, interfaces y perímetro.*
> - *La estructura organizativa y responsabilidades asignadas.*
> - *La política de seguridad de la información aprobada por la dirección.*
> - *La evaluación de riesgos y el tratamiento correspondiente.*
> - *Los procedimientos de notificación interna y externa.*
> - *Las medidas de control y supervisión implementadas.*
> - *La evidencia documental de cumplimiento y mejora continua.*
>
> *Esta declaración se firma en [Ciudad], a [Fecha].*
>
> *Firma:*
>
> *[Nombre del Director Responsable]*
> *[Cargo]*
> *[Organización]*

La declaración responsable podrá formar parte del MGSI, de la política de seguridad de la información o bien estar incluida en un documento aparte. En los dos últimos casos, el Manual debe contener una referencia clara al documento en el que se encuentra la declaración responsable.

Si el **director responsable** no es el **director ejecutivo (CEO)** de la organización, entonces el CEO deberá refrendar dicha declaración.

5.2 Organización de la seguridad de la información

El mantenimiento y gestión de seguridad de la información (en adelante GSI) requiere la identificación y definición de las diferentes actividades y responsabilidades en materia de GSI.

Definir los **roles y responsabilidades** en el **MGSI** es fundamental para establecer claramente quién es responsable de cada aspecto de la seguridad de la información dentro de la organización.

Al asignar responsabilidades específicas, se asegura que todas las tareas relacionadas con la seguridad de la información, como el control de acceso, la gestión de riesgos, la respuesta ante incidentes y el cumplimiento de políticas, sean realizadas por personas capacitadas y con la autoridad necesaria.

5.2.1 Identificación de roles y responsabilidades

Para dar cumplimiento al punto **IS.I.OR.250 (a)(2)**, **(3)** y **(6)** la organización deberá identificar los principales **roles y responsabilidades en la organización de la seguridad.**

La organización deberá evidenciar que el **director responsable** de la misma designado de conformidad con el Reglamento (UE) 2015/340, y los Reglamentos de Ejecución (UE) 2017/373 y (UE) 2021/664, según el tipo de organización afectada, tiene autoridad corporativa para garantizar que todas las actividades exigidas por el **REG PART-IS** puedan financiarse y llevarse a cabo (**IS.I.OR.240 (a)**).

La organización deberá actualizar la estructura para reflejar el SGSI (por ejemplo, nombramiento de un responsable de seguridad de la información, estructura de reporte).

El **director responsable** deberá:

- Garantizar que se dispone de todos los recursos necesarios para cumplir los requisitos del presente Reglamento.
- Establecer y promover la política de seguridad de la información a que se refiere el punto **IS.I.OR.200 (a)(1)**.
- Demostrar un conocimiento básico del REG PART-IS.

Dentro de la organización de seguridad debe identificarse (título, nombre, funciones, obligaciones, responsabilidades y potestades) la persona o grupo de personas responsables de (**IS.I.OR.200 (a)(10)**):

- Velar por el **cumplimiento de los requisitos reglamentarios** en materia de seguridad de la información. Este puesto deberá tener acceso directo al **director responsable** de la organización **(IS.I.OR.240 (b))**. Dicha persona o grupo de personas nombradas por el **director responsable** tendrán los conocimientos, la formación y la experiencia adecuados para ejercer sus responsabilidades. En los procedimientos deberá determinarse quién sustituye a esta persona o grupo de personas en caso de ausencia prolongada de esta (**AMC1 IS.I.OR.240(b)**).
- Gestionar la **función de control del cumplimiento** (**IS.I.OR.240 (c)**) de acuerdo a los requisitos recogidos en el punto **IS.I.OR.200 (a)(12)**.
- Crear, implantar y mantener el **SGSI** definido en el punto **IS.I.OR.200**. 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 director responsable podrá delegar sus actividades en una **persona responsable común** (**IS.I.OR.240 (d)**).

  En tal caso, se establecerán **medidas de coordinación** entre el director responsable de la organización y la persona responsable común para garantizar una **integración adecuada de la GSI en la organización.**

El **director responsable** o la **persona responsable común** tendrá autoridad corporativa para establecer y mantener las estructuras organizativas, políticas, procesos y procedimientos necesarios para aplicar el SGSI en la organización (**IS.I.OR.240 (e)**).

5.2.2 Procesos relacionados con la disponibilidad, capacitación y responsabilidades del personal

La organización contará con procesos que garanticen que (**IS.I.OR.250 (a)(9)(i)**):

- Dispone de personal suficiente para llevar a cabo las actividades de seguridad de la información (**IS.I.OR.240 (f)**).
- Dicho personal tiene la competencia necesaria para llevar a cabo sus tareas **IS.I.OR.240 (g)**. La organización deberá evidenciar que el personal que realiza funciones en materia de seguridad de la información dispone de los **conocimientos, formación y experiencia** adecuados para ejercer sus funciones y responsabilidades.

La organización deberá desarrollar un marco de competencias y un proceso de evaluación. Se deberá evaluar la competencia del personal actual.

- El personal reconozca las responsabilidades asociadas a las funciones y tareas que tiene asignadas **IS.I.OR.240 (h)**. La organización deberá informar al personal relacionado con los sistemas de información sobre sus deberes, obligaciones y responsabilidades en materia de seguridad.

  De acuerdo al **AMC1 IS.I.OR.240(h)**, la organización debe asegurarse de que todo el personal que desempeñe actividades relacionadas con el REG PART-IS reconozca de forma trazable y verificable las responsabilidades asociadas a su rol.

  Para los titulares de puesto de alta responsabilidad como; el Director responsable(**IS.I.OR.240 (a)** o Persona responsable común (common responsible person (CRP) **IS.I.OR.250 (a)(3))** o Responsable Part-IS (CISO) (**IS.I.OR.240 (b)**), se deberá contar con una evidencia ad-hoc que documente de forma clara y verificable la asunción de estas responsabilidades, análogamente a como se realiza en el Reglamento (UE) 2017/373. Se podrá disponer de una **designación formal (nombramiento) que incluya las responsabilidades firmada** o bien, se podría incorporar en un **documento o manual** (acompañado de un organigrama que recoja las líneas de responsabilidad y que permita identificar claramente quien de ellos ocupa cada puesto) **firmado por todos los responsables que ostenten los nombramientos**.

La organización velará por que se establezca adecuadamente la identidad y la fiabilidad del personal que tenga acceso a los sistemas de información y a los datos sujetos a los requisitos del REG PART-IS (**IS.I.OR.240 (i)**).

La organización deberá disponer de un marco/política para abordar los diferentes niveles de fiabilidad de la plantilla. Se deberá evaluar la fiabilidad del personal actual.

De acuerdo con el **AMC1 IS.I.OR.240(i)**, la organización debe establecer un proceso documentado que garantice que la identidad y la fiabilidad del personal con acceso a los sistemas de información y a los datos sujetos a los requisitos del REG PART-IS se establecen adecuadamente.

Atendiendo, al **GM1 IS.I.OR.240(i)** se podría esperar del proceso documentado:

- **Que establezca criterios para identificar al personal** con acceso a sistemas de información y datos regulados por el REG PART-IS cuya fiabilidad deba ser garantizada.
- Que requiera, al menos, las siguientes evaluaciones para garantizar la fiabilidad del personal:

  Antes del inicio del empleo:

  - Verificación documental de la identidad.
  - Comprobación de antecedentes penales conforme a la legislación nacional o de origen.
  - Verificación de la formación académica, experiencia laboral previa y periodos de inactividad.
  - Evaluación de cualquier otra información o inteligencia relevante para la idoneidad del candidato. Puede considerarse el análisis de fuentes públicas (como redes sociales), siempre dentro de los límites legales aplicables.

  Durante el empleo:

  - Seguimiento del compromiso y la conducta del empleado.
  - Aplicación de criterios más estrictos para roles críticos como personal con acceso a sistemas de información y datos, con una alta gravedad de las consecuencias para la seguridad, o que aplica medidas de seguridad, deben aplicarse criterios más estrictos, en función del nivel de riesgo asociado a los activos que gestionan.

Las organizaciones sujetas al Reglamento (UE) 2015/1998 y al PNS, que exige la superación satisfactoria de verificaciones de antecedentes para el personal en determinados roles, así como un mecanismo para la revisión continua de dichas verificaciones, puede considerar adecuado emplear para el PART-IS, el proceso y los criterios definidos para esos otros marcos normativos.

Criterios y requisitos similares, deberían exigirse a las activades contratadas.

5.2.3 Descripción de la organización y organigrama de seguridad de la información

La definición de **roles y responsabilidades** en el **MGSI** está estrechamente ligada a la existencia de un **organigrama** (**IS.I.OR.250 (a)(7)**), ya que este último proporciona una representación visual clara de la estructura jerárquica y funcional de la organización. El organigrama permitirá identificar de manera inmediata **las obligaciones y responsabilidades** de los roles identificados en el apartado 5.2.1.

La organización deberá establecer un vínculo entre las funciones de seguridad operacional y de seguridad de la información.

La organización deberá realizar una descripción general del número y las categorías del personal y del sistema en vigor para planificar la disponibilidad de personal (**IS.I.OR.250 (a)(5)**).

5.3 Política de seguridad de la información

La organización establecerá una **política en materia de seguridad de la información** (IS.I.OR.250 (a)(4)) que determine los principios generales de la organización con respecto a las posibles repercusiones de los riesgos relacionados con la seguridad de la información que puedan tener impacto en la seguridad aérea (AMC1 IS.I.OR.200(a)(1)):

- Que defina y documente el alcance del SGSI, determinando las actividades, procesos y sistemas de apoyo, e identificando aquellos que puedan tener un impacto en la seguridad aérea.
- Que esté aprobada por el **director responsable y sea revisada** a intervalos planificados o cuando ocurran cambios significativos[2].

La **política** deberá incluir, como mínimo, los siguientes **aspectos con un impacto potencial en la seguridad aérea**:

- **Compromiso de cumplimiento** de la legislación aplicable, y de consideración de las normas pertinentes y las mejores prácticas.
- Establecimiento de **objetivos** e **indicadores de rendimiento** para la GSI.
- Definición de los **principios generales**, **actividades** y **procesos** para que la organización proteja adecuadamente los sistemas y datos de las tecnologías de la información y la comunicación.
- Compromiso de aplicación de los requisitos del SGSI en los procesos de la organización.
- Compromiso de mejora continua hacia niveles más altos de madurez del proceso de seguridad de la información (IS.I.OR.260).
- Compromiso de cumplimiento de los requisitos aplicables en materia de seguridad de la información y su gestión proactiva y sistemática, así como de provisión de los recursos adecuados para su aplicación y funcionamiento.
- Asignación de la seguridad de la información como una de las responsabilidades esenciales de todos los directivos.
- Compromiso de promoción de la política de seguridad de la información a través de sesiones de formación o concienciación dentro de la organización a todo el personal de forma periódica o tras modificaciones a dicha política.
- Fomento de la aplicación de una «cultura justa» y la notificación de vulnerabilidades, sucesos sospechosos/anómalos y/o incidentes de seguridad de la información.

[2] Nota: Un cambio significativo es una alteración o modificación notable que tiene un impacto significativo en las operaciones de la organización, como un cambio estructural dentro de la organización debido a reorganizaciones, un cambio en los procesos empresariales (por ejemplo, trabajo desde casa, uso de dispositivos personales), una evolución tecnológica (por ejemplo, recursos informáticos distribuidos, inteligencia artificial/aprendizaje automático) o una evolución en el panorama de las amenazas ((AMC1 IS.I.OR.200(a)(1)).

- Compromiso de comunicación de la política de seguridad de la información a todas las partes pertinentes, según proceda.

- La Política debe establecer claramente el propósito garantizando que el concepto de seguridad de la aviación forma parte integral de la misma.
- Debe definir los objetivos de seguridad de la información.
- Debe ser adecuada a la complejidad de la organización.
- Debe establecer unos criterios para su revisión.
- Debe hacer referencia al sistema de clasificación de la información de la organización.

En la auditoría se verificará que está a disposición de todo el personal/contratados y se debe comunicar adecuadamente.

5.4 Incidentes de seguridad de la información

5.4.1 Sistema Interno de Notificación

La organización debe establecer un sistema **interno** de notificación (**IS.I.OR.200 (a)(4)**) conforme a lo indicado en el punto **IS.I.OR.215**, que permita la recopilación y evaluación de los eventos de seguridad de la información.

5.4.2 Sistema Externo de Notificación

La organización deberá aplicar un sistema **externo** de notificación (**IS.I.OR.200 (a)(8)**) de conformidad con el punto **IS.I.OR.230** a fin de que la autoridad competente pueda adoptar las medidas adecuadas.

La organización deberá disponer de procedimientos para:

- La notificación de sucesos dentro de la organización y por parte de terceros. Dichos procedimientos deben ser informados al personal y a las partes externas.
- La evaluación de los sucesos para decidir cuáles deben considerarse incidentes o vulnerabilidades. Se deben definir responsabilidades a la hora de realizar esta actividad.
- La determinación de qué incidentes y vulnerabilidades deben notificarse a través del sistema de notificación externa.
- La notificación externa (incluidas todas las etapas de la notificación, el análisis de la causa raíz, el seguimiento, etc.).

En la auditoría se verificará que el personal implicado en el tratamiento de informes internos y externos está debidamente identificado, formado y autorizado.

5.4.3 Detección, Respuesta y Recuperación

La organización debe definir las medidas necesarias (IS.I.OR.200 (a)(5)) para detectar eventos de seguridad de la información, conforme al IS.I.OR.220, **determinar cuáles de ellos se consideran incidentes** con posibles repercusiones sobre la seguridad aérea —salvo lo permitido en el punto IS.I.OR.205 (e)— y establecer el mecanismo que permita responder a dichos incidentes de seguridad de la información y recuperarse de ellos.

Para ello deberá disponer de procedimientos para garantizar:

- La detección de incidentes relacionados con la seguridad de la información, incluidos mecanismos de vigilancia de posibles amenazas.
- La respuesta en tiempo a los incidentes detectados (por ejemplo, medidas iniciales de contención).
- La recuperación de los incidentes y el retorno al nivel de seguridad adecuado después de un incidente.

En la auditoría se verificará la adecuación de las medidas de respuesta y recuperación implantadas.

Evento de seguridad de la información: un suceso detectado en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o un fallo de los controles de seguridad de la información, o una situación desconocida hasta ese momento que puede tener importancia para la seguridad de la información [Artículo 3.2 Reglamento (UE) 2023/203].

5.5 Gestión de riesgos

Tal y como se recoge en el requisito IS.I.OR.205, el análisis y gestión de riesgos será parte esencial del sistema de gestión de seguridad y, por tanto, del MGSI. La aplicación e implantación de las medidas de seguridad debe realizarse valorando y asumiendo un nivel de riesgo conocido, consiguiendo de esta forma un nivel de protección aceptable en proporción a los daños que pudieran producirse.

La organización deberá documentar (IS.I.OR.250 (a)(9)(i)), al menos:

- La identificación de entre todos sus elementos, cuáles pueden estar expuestos a riesgos relacionados con la seguridad de la información (IS.I.OR.205 (a)).
- La identificación de las interfaces que tiene con otras organizaciones y que podrían dar lugar a la exposición mutua a riesgos de seguridad de la información (IS.I.OR.205 (b)).
- La identificación de los riesgos para la seguridad de la información que puedan tener un impacto potencial en la seguridad aérea (IS.I.OR.205 (c)). La metodología utilizada para la evaluación de los riesgos (AMC1 IS.D.OR.205(a)), incluyendo la cadena de suministro (AMC1 IS.I.OR.205(b)).

El proceso para la gestión de los riesgos, incluyendo la identificación, evaluación (IS.I.OR.200 (a)(2)) y tratamiento (IS.I.OR.210) de estos (AMC1 IS.I.OR.205(c)).

Proceso que asegure la monitorización y revisión periódica del análisis de riesgos (AMC1 IS.I.OR.205(d)) en las siguientes situaciones:

- un cambio en los elementos sujetos a riesgos de seguridad de la información;
- un cambio en las interfaces entre la organización y otras organizaciones, o en los riesgos comunicados por las otras organizaciones;
- un cambio en la información o conocimientos utilizados para la identificación, análisis y clasificación de riesgos;
- hay lecciones aprendidas del análisis de incidentes de seguridad de la información.

La organización deberá establecer un proceso formal para la gestión de riesgos de seguridad de la información. Este proceso debe incluir las Identificación de riesgos, su evaluación y su tratamiento. Como parte del proceso deberá:

- Realizar un inventario de activos (procesos, software, hardware).
- Definir claramente los criterios de aceptabilidad del riesgo y las responsabilidades.
- Definir cómo gestionará los riesgos relacionados con los contratistas/proveedores operacionales (que no sean actividades contratadas).
- Realizar la evaluación inicial de riesgos (por ejemplo, riesgos importantes y escenarios de amenazas relacionados tanto internos como en las interfaces).

En la auditoría se verificará que la organización:

- Ha incluido en el inventario los activos aplicables.
- Ha establecido un proceso formal para la gestión de riesgos de seguridad de la información.

5.6 Procedimientos del SGSI

El MGSI debe incluir o bien referenciar los **procesos y procedimientos** mediante los cuales la organización garantiza una correcta implantación del SGSI (IS.I.OR.250 (a)(9)(i)), así como el proceso que permite la modificación de dicha documentación (IS.I.OR.200 (c), IS.I.OR.255).

- Adicionalmente a los mencionados en los apartados precedentes la organización documentará todos los procesos, procedimientos, funciones y responsabilidades clave necesarios para**:**
  - aplicar las medidas notificadas por la autoridad competente como reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea (IS.I.OR.200 (a)(6)).
  - tomar las medidas adecuadas, de conformidad con el punto IS.I.OR.225, para abordar las incidencias notificadas por la autoridad competente (IS.I.OR.200 (a)(7)).

- cumplir los requisitos del punto **IS.I.OR.235** cuando contrata alguna parte de las actividades mencionadas en el punto **IS.I.OR.200** a otras organizaciones (**IS.I.OR.200(a)(9)**).

> La organización deberá:
>
> - Definir qué actividades de GSI se contratan, en su caso, a terceros.
> - Establecer los contratos adecuados.
> - Disponer de procedimientos que definan cómo realiza la supervisión de las actividades de GSI contratadas y cómo gestiona los riesgos asociados.
> - Garantizar el acceso adecuado de la Autoridad Competente a las partes contratadas incluyendo un requisito a tal efecto en los contratos correspondientes.

- cumplir los requisitos de conservación de registros (**IS.I.OR.200 (a)(11)**) establecidos en el punto **IS.I.OR.245**.

> La organización deberá definir qué registros se conservan, el periodo de conservación y formato de los mismos, así como el nivel de protección adecuada (p. ej., contra daños, alteración, robo, acceso no autorizado, etc.)

- **supervisar el cumplimiento** de los requisitos del REG PART-IS por parte de la organización y proporcionar información sobre las deficiencias al **director responsable**, a fin de garantizar la aplicación efectiva de las medidas correctoras (**IS.I.OR.200 (a)(12)**).
- proteger, sin perjuicio de los requisitos de notificación de incidentes aplicables, la confidencialidad de cualquier información que la organización pueda haber recibido de otras organizaciones, en función de su nivel de sensibilidad (**IS.I.OR.200 (a)(13)**).

Los procesos y procedimientos se adaptarán a la naturaleza y complejidad de las actividades de cada organización.

5.7 Medios alternativos de cumplimiento aprobados

El MGSI deberá recoger los medios alternativos de cumplimiento **(IS.I.OR.250 (a)(10)) aprobados por la autoridad** competente para satisfacer los requisitos de la normativa PART-IS, si los hubiera.

En caso de que la organización considere que existen unos medios alternativos de cumplimiento deberá **presentarlos a la autoridad competente** de acuerdo con los procedimientos establecidos.

6 ELABORACIÓN, ACTUALIZACIÓN Y DISTRIBUCIÓN DEL MANUAL

6.1 Elaboración y actualización

La organización elaborará el MGSI siguiendo las indicaciones realizadas en la presente guía. Asimismo, deberá cumplir con los plazos establecidos para la entrega del MGSI a la autoridad competente con objeto de que ésta pueda realizar la aprobación del mismo **(IS.I.OR.250 (b))** y la notificación de posibles cambios.

El MGSI se modificará según sea necesario para que siga siendo una descripción actualizada del SGSI de la organización. Se facilitará a la autoridad competente una copia de cualquier modificación del MGSI.

Dichas modificaciones se gestionarán mediante un procedimiento establecido por la organización **(IS.I.OR.250 (c)).** Se considera que el procedimiento para modificaciones del MGSI al que se refiere el apartado c) del IS.I.OR.250, puede ser propio el procedimiento de gestión de cambios en el SGSI del IS.I.OR.255. Aquellas modificaciones que no estén incluidas en el ámbito de dicho procedimiento deberán ser aprobadas previamente por la autoridad competente.

6.2 Distribución interna

La organización deberá establecer un procedimiento para identificar las partes del MGSI, y de los procedimientos asociados, que deben ser compartidas con el personal (en función de las responsabilidades del mismo) teniendo en cuenta el principio de necesidad de conocer.

Se describirá la forma en la que se distribuyen al personal las partes del MGSI identificadas.

Finalmente, el procedimiento deberá asegurar que el personal es conocedor de las partes del MGSI que le afectan.

6.3 Distribución a otras partes interesadas

La organización deberá identificar si el MGSI o alguna de sus partes debe ser compartida con otras organizaciones, que puedan verse impactadas por dichos cambios.

6.4 Distribución a la autoridad

6.4.1 Comunicación inicial para aprobación

La organización deberá compartir el MGSI de acuerdo con los requisitos establecidos por la autoridad competente (AESA) y el procedimiento de aprobación establecido por ésta (IS.I.OR.250(a)).

6.4.2 Comunicación de actualizaciones en el MGSI

Las actualizaciones al MGSI deberán ser notificadas a AESA (**IS.I.OR.250(b)**) de acuerdo con; el procedimiento establecido por la organización para modificaciones al MGSI (**IS.I.OR.250 (c))** o, con el procedimiento de gestión de cambios de la organización establecido conforme al requisito **IS.I.OR.255**.

7 INTEGRACIÓN DEL MANUAL CON EL SISTEMA DE GESTIÓN

La organización podrá integrar el MGSI con otras memorias o manuales de gestión que posea (**IS.IOR.250 (d)**), siempre que exista una clara referencia cruzada que indique qué partes de la memoria o manual de gestión corresponden a los diferentes requisitos contenidos en el REG PART-IS. Estos documentos deben considerarse parte integrante del MGSI de la organización **GM1 IS.I.OR.250(a)**.

8 RELACIÓN CON OTROS MARCOS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En el caso de que la organización disponga de una certificación de seguridad de la información (p. ej., ISO 27001:2022 o Esquema Nacional de Seguridad) en vigor, ello no implica que cumple automáticamente los requisitos del REG PART-IS. No obstante, podrá adaptarlo y ampliarlo al ámbito y contexto del **REG PART-IS** incluyendo la seguridad aérea en la gestión de riesgos de la organización, con el nivel de aceptación del riesgo pertinente (**GM1 IS.D.OR.200**). Por lo tanto, es necesario determinar cuidadosamente el alcance del SGSI relacionado con los riesgos de seguridad de la aviación, ya que podría diferir del relacionado con los demás riesgos organizativos.

Se debe tener en cuenta que el REG PART-IS contempla la equivalencia en el cumplimiento de los requisitos de seguridad de la información incluidos en la Directiva NIS2.

> ***Artículo 2 Part-IS***
>
> *4. El presente Reglamento se entiende sin perjuicio de los requisitos en materia de seguridad de la información y ciberseguridad establecidos en el punto 1.7 del anexo del Reglamento de Ejecución (UE) 2015/1998 y en el artículo 14 de la Directiva (UE) 2016/1148*
>
> ***Artículo 5 Part-IS***
>
> ***1.** Si una organización de las contempladas en el artículo 2, apartado 1, cumple requisitos de seguridad establecidos en el artículo 14 de la Directiva (UE) 2016/1148 que sean equivalentes a los requisitos establecidos en el presente Reglamento, se considerará que el cumplimiento de aquellos requisitos de seguridad constituye un cumplimiento de los requisitos establecidos en el presente Reglamento.*

4. La Comisión, previa consulta a la Agencia y al Grupo de cooperación a que se refiere el artículo 11 de la Directiva (UE) 2016/1148, podrá emitir directrices para la evaluación de la equivalencia de los requisitos establecidos en el presente Reglamento y en la Directiva (UE) 2016/1148.

En los anteriores puntos donde dice Directiva (UE) 2016/1148 debe entenderse Directiva (UE) 2022/2555 (NIS2) por ser la que está actualmente en vigor.

9 MEJORA CONTINUA

El MGSI deberá establecer el proceso de mejora continua conforme a lo indicado en el **IS.I.OR.260**, de forma que se pueda medir la madurez del sistema y se establezcan medidas para la mejora hasta alcanzar el nivel de madurez óptimo.

Para ello se deberán establecer Indicadores de madurez (tomar como referencia los definidos por el ENS y guías del CCN).

10 ASPECTOS DE PROPORCIONALIDAD PARA LA IMPLEMENTACIÓN DE PART-IS EN RELACIÓN CON LA COMPLEJIDAD ORGANIZACIONAL Y LA RELEVANCIA DE LA SEGURIDAD

Como se indica en **GM1 IS.I.OR.200(d)** al implantar el REG PART-IS, la organización debe considerar principalmente:

- Los riesgos que puede generar a otras organizaciones.
- Su propia exposición al riesgo.

También debe tener en cuenta:

- las necesidades y objetivos de la organización,
- los requisitos de seguridad de la información,
- sus propios procesos,
- el tamaño, la complejidad y la estructura de la organización.

Es clave que las organizaciones ajusten sus recursos para cumplir con los requisitos de seguridad y protegerse eficazmente frente a riesgos relevantes.

La **guía de EASA Part-IS oversight approach Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS Part-IS TF G-03, March 2025** proporciona ciertas pautas para las autoridades a la hora de evaluar la complejidad de las organizaciones.

Dado que no existe una distinción clara entre organizaciones complejas y no complejas, la evaluación de la complejidad debe hacerse considerando distintos elementos por separado. Cada uno de estos elementos puede influir en cómo se aplica proporcionalmente el SGSI:

- ✓ **ROL DE LA ORGANIZACIÓN EN LA CADENA FUNCIONAL** y número/importancia de las partes interesadas con las que interactúa.

El rol de la organización en la cadena funcional puede influir en la profundidad del análisis de riesgos que se realice. De esta manera, se pueden considerar los dos casos siguientes, con los métodos que se pueden seguir, en función de los posibles riesgos que pueden plantear dicho rol y la interacción de la organización con otras organizaciones:

1. **Su rol e interfaces no plantean un riesgo de condiciones inseguras:**
    - **Evaluación de Riesgos Simplificada** que priorice los riesgos en función de su impacto potencial en la seguridad. La evaluación se centra en áreas de alto impacto y aplica evaluaciones más detalladas solo si es necesario.
    - **Priorización del Tratamiento de Riesgos** dirigida a abordar los riesgos de alto impacto con medidas rentables económicamente. Se pueden utilizar controles rentables que reduzcan los riesgos a niveles aceptables, aprovechando procesos existentes, controles físicos o tecnología.
2. **Su rol e interfaces pueden crear un riesgo de condiciones inseguras:**
    - **Evaluaciones de Riesgos Detalladas** más profundas y, a menudo, más frecuentes.

✓ **COMPLEJIDAD DE LA ESTRUCTURA ORGANIZATIVA, incluyendo número de empleados, departamentos y niveles jerárquicos.**

Cuanto más compleja es una organización (por su tamaño, jerarquía o procesos), mayor es la necesidad de coordinación interna y de intercambio de información. De esta manera, se pueden considerar los casos siguientes, con los métodos que se pueden seguir, en función del número de empleados, niveles jerárquicos y procesos:

1. **Número limitado de empleados, pocos niveles jerárquicos y procesos sencillos:**
    - **Documentación Simplificada**: realizar documentos claros, breves y fáciles de usar, adaptados a equipos pequeños. Se pueden usar plantillas y macros para facilitar su elaboración.
    - **Enfoque en Políticas Clave**: se priorizan temas críticos como compromiso de la dirección, control de accesos y respuesta a incidentes.
    - **Programas de Capacitación Específicos**: adaptados a los roles y riesgos concretos de la organización.
    - **Cultura de Seguridad**: se promueve mediante sesiones breves y campañas regulares de concienciación.
    - **Externalización**: se recurre a proveedores especializados cuando no se dispone de experiencia interna.
    - **Colaboración con Pares**: se intercambia información con organizaciones similares para mejorar la comprensión del entorno de seguridad.

- **Informes Simplificados a la Gestión**: se presentan métricas clave a la alta dirección para demostrar la eficacia del SGSI y asegurar su apoyo continuo.
- **Auditorías Regulares pero Escaladas**: se realizan auditorías internas periódicas, ajustadas al tamaño y complejidad de la organización, enfocadas en áreas críticas.
- **Proceso de Revisión Ágil del SGSI**: se revisa regularmente para adaptarlo a nuevas necesidades y amenazas.

2. **Gran número de empleados, niveles jerárquicos y procesos e interfaces interconectados:**

- **Comités de Gobernanza de Seguridad de la Información**: supervisan el SGSI y aseguran su alineación con los objetivos de seguridad. Deben incluir representantes de dirección, TI, legal y áreas clave.
- **Métricas e Informes**: se implementan indicadores clave (KPI) y reportes periódicos a la alta dirección para garantizar apoyo y recursos.
- **Políticas y Procedimientos Detallados**: se requiere un conjunto amplio de políticas y procedimientos que cubran distintas áreas como seguridad en la nube, gestión de terceros y de dispositivos móviles.
- **Armonización de Políticas**: alineadas en toda la organización, bajo un modelo de gobernanza centralizado.
- **Evaluaciones de Riesgos Cruzadas**: se analizan riesgos en múltiples departamentos, ubicaciones y tecnologías.
- **Agregación y Correlación de Riesgos**: se correlacionan los resultados para detectar problemas sistémicos y escalar riesgos a nivel organizacional.
- **Capacitación Basada en Roles**: programas adaptados a cada función (TI, ejecutivos, usuarios).
- **Campañas Continuas de Concienciación sobre Seguridad**: se utilizan métodos variados (phishing simulado, talleres, e-learning) para mantener la concienciación activa.
- **Gestión de Riesgos de la Cadena de Suministro**: se evalúan y monitorizan los riesgos de proveedores, integrando requisitos de seguridad en los contratos.
- **Auditorías de Terceros**: se realizan auditorías periódicas a los proveedores para verificar el cumplimiento de los objetivos de seguridad**.**
- **Centro de Operaciones de Seguridad (SOC) Dedicado**: Centro operativo 24/7 para monitorizar y dar respuesta a incidentes.
- **Planes de Respuesta a Incidentes**: documentos detallados que cubren escenarios diversos y coordinación interdepartamental.
- **Ejercicios de Simulación de Crisis**: ejercicios regulares para probar la efectividad de los planes.
- **Auditorías Internas y Externas**: evaluaciones regulares para verificar cumplimiento y detectar mejoras.

- **Programas de Mejora Continua**: el SGSI se actualiza basándose en auditorías, análisis post-incidente y cambios en amenazas.

✓ **COMPLEJIDAD DE LOS SISTEMAS TIC Y DE LOS DATOS UTILIZADOS, así como su conexión con terceros.**

La complejidad de los sistemas TIC, los datos utilizados y su conexión con terceros determina el grado de personalización necesario para gestionar riesgos y responder a incidentes.

1. **Organización con uso de pocas herramientas TIC y utilización de productos estándar en una arquitectura básica y comercial:**

   - **Aprovechamiento de los Controles de ISO/IEC 27001**: se usan como lista de verificación para cubrir áreas críticas sin diseñar controles desde cero, alineando con Part-IS.
   - **Gestión Simplificada de Incidentes**: proceso sencillo para identificar, notificar y responder rápidamente, integrando aprendizajes al SGSI.
   - **Herramientas Automatizadas**: se emplean para monitorizar y gestionar incidentes, reduciendo esfuerzo manual y manteniendo el cumplimiento.
   - **Registros Esenciales**: solo se conservan los registros necesarios para demostrar cumplimiento y efectividad, evitando documentación innecesaria.
   - **Uso de Soluciones Digitales**: se utilizan para facilitar la gestión, acceso y seguridad de los documentos y registros.

2. **Organización con uso de varias y diversas herramientas TIC, entre las cuales se encuentran soluciones y arquitecturas a medida:**

   - **Integración de Herramientas de Seguridad Avanzadas**: se integran tecnologías de seguridad como la Gestión de Información y Eventos de Seguridad (SIEM), la Prevención de Pérdida de Datos (DLP) y los sistemas de Detección y Respuesta de Endpoints (EDR) para gestionar eficazmente la detección y respuesta ante incidentes en entornos complejos.
   - **Inteligencia de Amenazas Automatizada**: se usan plataformas que permiten detectar y responder en tiempo real a amenazas en múltiples frentes.
   - **Documentación Detallada**: se documentan de forma extensa los procesos del SGSI, evaluaciones de riesgos, incidentes y cumplimiento.
   - **Retención de Registros**: los registros y datos se almacenan de forma segura y accesible durante largos periodos, garantizando trazabilidad y cumplimiento.

11 REFERENCIAS

1. 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) n. o 1321/2014, (UE) n. o 965/2012, (UE) n. o 1178/2011 y (UE) 2015/340 de la Comisión y los Reglamentos de Ejecución (UE) 2017/373 y (UE) 2021/664 de la Comisión, así como a las autoridades competentes contempladas en los Reglamentos (UE) n. o 748/2012, (UE) n. o 1321/2014, (UE) n. o 965/2012, (UE) n. o 1178/2011, (UE) 2015/340 de la Comisión y en los Reglamentos de Ejecución (UE) 2017/373, (UE) n. o 139/2014 y (UE) 2021/664 de la Comisión, y por el que se modifican los Reglamentos (UE) n. o 1178/2011, (UE) n. o 748/2012, (UE) n. o 965/2012, (UE) n. o 139/2014, (UE) n. o 1321/2014 y (UE) 2015/340 de la Comisión y los Reglamentos de Ejecución (UE) 2017/373 y (UE) 2021/664 de la Comisión.
2. Easy Access Rules Part-IS (IR/DR + AMC/GM).
3. Reglamento de Ejecución (UE) 2017/373 de la Comisión de 1 de marzo de 2017 por el que se establecen requisitos comunes para los proveedores de servicios de gestión del tránsito aéreo/navegación aérea y otras funciones de la red de gestión del tránsito aéreo y su supervisión, por el que se derogan el Reglamento (CE) nº 482/2008 y los Reglamentos de Ejecución (UE) nº 1034/2011, (UE) nº 1035/2011 y (UE) 2016/1377, y por el que se modifica el Reglamento (UE) nº 677/2011.
4. Reglamento (UE) 2015/340 de la Comisión de 20 de febrero de 2015 o por el que se establecen requisitos técnicos y procedimientos administrativos relativos a las licencias y los certificados de los controladores de tránsito aéreo en virtud del Reglamento (CE) n o 216/2008 del Parlamento Europeo y del Consejo, se modifica el Reglamento de Ejecución (UE) n 923/2012 de la Comisión y se deroga el Reglamento (UE) n (Texto pertinente a efectos del EEE) LA COMISIÓN EUROPEA, Visto el Tratado de Funcionamiento de la Unión Europea, Visto el Reglamento (CE) nº 805/2011 de la Comisión.
5. Reglamento (UE) 376/2014 del Parlamento Europeo y del Consejo de 3 de abril de 2014 relativo a la notificación de sucesos en la aviación civil, que modifica el Reglamento (UE) n 996/2010 del Parlamento Europeo y del Consejo, y por el que se derogan la Directiva 2003/42/CE del Parlamento Europeo y del Consejo y los Reglamentos (CE) n o 1321/2007 y (CE) n o 1330/2007 de la Comisión.
6. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)
7. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
8. UNE-EN ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.
9. Guidelines Part-IS oversight approach | Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS. EASA.