Agencia Estatal
de Seguridad Aérea

Guía para la gestión de cambios en el Sistema de Gestión de la Seguridad de la Información (IS.I.OR.255. 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-01	ISO/IEC 27001 VS PART-IS GUIDELINES FOR ISO/IEC 27001:2022 CONFORMING ORGANISATIONS ON HOW TO SHOW COMPLIANCE WITH PART-IS (EASA)

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
ATCO	CONTROLADOR DE TRÁNSITO AÉREO
CISO	RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (CHIEF INFORMATION SECURITY OFFICER)
CRP	PERSONA RESPONSABLE COMÚN (COMMON RESPONSIBLE PERSON)
DNA	DIRECCIÓN DE NAVEGACIÓN AÉREA
EASA	AGENCIA EUROPEA DE SEGURIDAD AÉREA
GM	MATERIAL GUÍA
ISO/IEC	ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN / COMISIÓN ELECTROTÉCNICA INTERNACIONAL
MGSI/ISMM	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
SGSI/ISMS	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
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**, con indicaciones sobre ciertas pautas a la hora de gestionar los **cambios** que se realicen al **Sistema de Gestión de Seguridad de la Información (SGSI),** y la elaboración de un procedimiento para la gestión de dichos cambios, en aras de facilitar el cumplimiento del requisito recogido en el Reglamento de Ejecución (UE) 2023/203, conocido como Part-IS (a partir de ahora REG PART-IS), concretamente en el requisito **IS.I.OR.255**[1]. Dicho procedimiento forma parte del Manual de Gestión de Seguridad de la Información (MGSI), y de la documentación que permitirá a las organizaciones implementar el requisito **IS.I.OR.200** del mencionado REG PART-IS.

2. ALCANCE

La presente Guía va dirigida a las siguientes organizaciones del ámbito de la navegación aérea:

- 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 sujetas 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)** y el procedimiento establecido por la Dirección de Navegación Aérea de AESA (a partir de ahora AESA DNA), 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.

En relación a los proveedores ATM/ANS y U-Space, esta guía está dirigida únicamente a cambios en el sistema de gestión de seguridad de la información. Los cambios derivados de este sistema que tengan una afección al sistema funcional de los proveedores de servicios ATM/ANS y U-Space serán gestionados conforme a los procedimientos aprobados para tal fin.

---

[1] A lo largo de esta guía se utiliza 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

Con la publicación del *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*, Europa regula la gestión de los riesgos de la seguridad de la información que puedan tener impacto en la seguridad operacional del transporte aéreo.

Como parte de los requisitos que impone a las organizaciones afectadas, el requisito **IS.I.OR.255** regula la gestión de los cambios que se realicen al SGSI de dichas organizaciones, incluyendo la posibilidad de que éstas dispongan de un procedimiento al uso para la gestión de dichos cambios, que deberá estar aprobado por la autoridad competente, en este caso AESA:

IS.I.OR.255 Cambios en el sistema de gestión de la seguridad de la información

a) Los cambios en el SGSI podrán gestionarse y notificarse a la autoridad competente en un procedimiento elaborado por la organización. Este procedimiento deberá ser aprobado por la autoridad competente.

b) Por lo que respecta a los cambios en el SGSI no cubiertos por el procedimiento a que se refiere la letra a), la organización solicitará y obtendrá una aprobación expedida por la autoridad competente.

Por lo que se refiere a estos cambios:

1) *la solicitud deberá presentarse antes de que tenga lugar cualquiera de estos cambios, para que la autoridad competente pueda determinar si se sigue cumpliendo el presente Reglamento y, si fuera necesario, modificar el certificado de la organización y las correspondientes condiciones de aprobación que lleva adjuntas;*
2) *la organización pondrá a disposición de la autoridad competente toda la información que solicite para evaluar el cambio;*
3) *el cambio solo se aplicará tras la recepción de una aprobación formal por parte de la autoridad competente;*
4) *la organización operará bajo las condiciones prescritas por la autoridad competente durante la aplicación de dichos cambios.*

4. GESTIÓN DE CAMBIOS AL SGSI

Los cambios en el SGSI de los proveedores de servicios ATM/ANS, organizaciones de formación de controladores de tránsito aéreo, los proveedores de servicios de U-Space y proveedores de servicios de información común, serán tratados y gestionados de la siguiente manera:

La notificación y la gestión de cambios en el SGSI de la organización, se deberá definir en un procedimiento de acuerdo a lo indicado en el requisito **IS.I.OR.255** y su **AMC** asociado.

Dentro de los cambios al SGSI se identifican dos grupos:

1. Cambios que requieren aprobación por parte de AESA.
2. Cambios que NO requieren aprobación por parte de AESA.

4.1. Cambios que requieren aprobación por parte de AESA

Las organizaciones deberán disponer un procedimiento en el que se recoja de qué manera tienen que proceder con los cambios que requieren aprobación, de forma que se dé cumplimiento al **IS.I.OR.255(b)**.

IS.I.OR.255(b) Procedimiento de gestión de cambios al SGSI

b) Por lo que respecta a los cambios en el SGSI no cubiertos por el procedimiento a que se refiere la letra a), la organización solicitará y obtendrá una aprobación expedida por la autoridad competente.
Por lo que se refiere a estos cambios:
1) la solicitud deberá presentarse antes de que tenga lugar cualquiera de estos cambios, para que la autoridad competente pueda determinar si se sigue cumpliendo el presente Reglamento y, si fuera necesario, modificar el certificado de la organización y las correspondientes condiciones de aprobación que lleva adjuntas;
2) la organización pondrá a disposición de la autoridad competente toda la información que solicite para evaluar el cambio;
3) el cambio solo se aplicará tras la recepción de una aprobación formal por parte de la autoridad competente;
4) la organización operará bajo las condiciones prescritas por la autoridad competente durante la aplicación de dichos cambios.

4.1.1. *¿Qué cambios requieren aprobación previa?*

Por un lado, el AMC1 IS.I.OR.255, recoge que una vez establecido el procedimiento de gestión de cambios que no requieren aprobación previa, y aprobado por la autoridad, cualquier modificación que se realice sobre él, estará sujeta también a la aprobación por parte de la autoridad competente.

Por otro lado, tomando como referencia el GM2 IS.I.OR.255 y en base a la **criticidad** de los procesos del SGSI establecidos por el REG PART-IS, se han considerado los dos siguientes procesos que, en caso de sufrir modificaciones, estarán sometidos a aprobación previa por la autoridad:

- Proceso de gestión de riesgos.
- Proceso de gestión de incidentes y vulnerabilidades.

En el Anexo I se recoge la lista de los cambios en el SGSI que requieren de aprobación previa.

4.1.2. *Proceso de solicitud de aprobación de los cambios al SGSI*

Tal y como se recoge en el AMC1 IS.I.OR.255, cuando se solicite la aprobación previa de la autoridad competente para un cambio recogido en el punto 4.1.1, o un cambio no cubierto por el procedimiento aprobado (punto 4.2 de esta guía), o cuando no exista tal procedimiento aprobado (punto 4.1.2), la organización deberá proporcionar, al menos la siguiente información:

— la naturaleza y la finalidad del cambio;

— el plan de implantación del cambio;

— el plan de verificación del cambio;

— el potencial impacto en la seguridad aérea que pudiera introducir el cambio.

Igualmente, una desviación significativa del plan de implantación original durante el proceso de cambio es un evento que debe notificarse a la autoridad competente, ya que esta desviación puede requerir una reconsideración del impacto del cambio.

La dimensión de esos planes deberá ser proporcional a la entidad del cambio. Cuanto más complejo o mayor criticidad o impacto tenga el cambio, más complejos y detallados deberán ser los planes requeridos y viceversa, cambios simples precisarán de planes simples y sencillos.

Un plan de implantación debería recoger los elementos necesarios para que un cambio en el SGSI se acometa de forma segura y ordenada. Indicando qué hay que hacer (coordinar interna y externamente, formar, informar, actualizar herramientas, definir proceso de reversión, etc.), quiénes son los responsables de llevarlo a cabo (una única persona, un conjunto de personas, un responsable del cambio, etc.), cómo se va a hacer (definir un cronograma de implantación ya que de las distintas acciones unas pueden ser dependientes de otras).

Un plan de verificación debería ser parte de un plan de implantación, ya que la verificación debería recoger las acciones necesarias para chequear que las distintas etapas del proceso de implantación de un cambio se han realizado de forma completa y satisfactoria. El plan de verificación debería indicar cuáles son las acciones de verificación, quienes son sus responsables.

Todo esto deberá quedar recogido en el procedimiento para gestionar cambios que requieren aprobación previa.

Cuando la organización tenga intención de introducir cualquiera de los cambios cuya aprobación es requerida por AESA previa a su implantación, deberá presentar por registro electrónico la siguiente documentación:

- Solicitud de aprobación, de acuerdo con el formato establecido (y que contemple lo indicado en el **AMC1 IS.I.OR.255**), de cambios sujetos a aprobación.
- Documentación cuya aprobación se solicita, así como la información requerida en el **AMC1 IS.I.OR.255**. Adicionalmente, si los cambios en los procesos que requieren aprobación implican una modificación del MGSI para mantener la coherencia de contenidos, el MGSI también habrá de presentarse como documentación.

AESA realizará acuse de recibo de dicha solicitud en un plazo máximo de 10 días laborables desde la recepción de la misma.

La notificación de los cambios al SGSI que requieran aprobación se realizará con una antelación mínima de 30 días hábiles a la entrada en vigor de dicho cambio, salvo que la normativa nacional establezca un plazo distinto adicional.

Para la notificación se emplearán los procedimientos electrónicos existentes de notificación de cambios no funcionales.

4.2. Cambios que no requieren aprobación por parte de AESA

IS.I.OR.255(a) Procedimiento de gestión de cambios al SGSI

a) Los cambios en el SGSI podrán gestionarse y notificarse a la autoridad competente en un procedimiento elaborado por la organización. Este procedimiento deberá ser aprobado por la autoridad competente.

Las organizaciones pueden acogerse a la posibilidad que ofrece el requisito **IS.I.OR.255** del REG PART-IS de eximir a determinados cambios en su SGSI de la obligación de disponer de una aprobación específica por parte de la autoridad competente, siempre y cuando cumplan las siguientes condiciones:

- la organización debe disponer de un **procedimiento** para la gestión y notificación a la autoridad de los cambios al SGSI que no requieran aprobación previa,
- dicho procedimiento deberá estar **aprobado** por la autoridad.

Esta posibilidad permitiría facilitar el proceso de implantación de cambios. Sin embargo, los cambios no contemplados en dicho procedimiento sí requerirán de esa aprobación específica, conforme se detalla más arriba en el punto 4.1 de esta guía.

Para la elaboración del citado procedimiento la organización tendrá en cuenta, además, las siguientes consideraciones:

- **Criticidad de los cambios (AMC1 IS.I.OR.255):**

El hecho de que la organización disponga de un procedimiento para la gestión de los cambios al SGSI, no le exime de dar cumplimiento a las obligaciones que establecen los reglamentos de ejecución de la normativa europea que le sean de aplicación.

La organización deberá tener en cuenta en su procedimiento para la gestión de los cambios al SGSI, la criticidad de los mismos a la hora de establecer cómo va a realizar su gestión. En particular, aquellos cambios que puedan tener un impacto en el logro o mantenimiento del cumplimiento de las disposiciones del REG PART-IS, o que puedan conducir a un nivel de riesgo inaceptable conforme a lo establecido en los procedimientos de análisis de riesgos de la organización, deben ser objeto de un análisis detallado.

La organización, para gestionar estos cambios, deberá considerar en el procedimiento las acciones a realizar para: analizar el cumplimiento con la normativa vigente, el impacto a su sistema de seguridad de la información, así como la afección o interrelación con otros procesos/procedimientos internos; coordinar con todos los actores afectados y asegurar una implantación correcta. Para ello deberá indicar los roles y responsabilidad de los actores involucrados.

Por otro lado en relación con los planes de implantación y verificación, si bien, tal y como indica el AMC1 IS.I.OR.255 estos planes son necesarios para cambios que requieran aprobación, se aconseja disponer de ellos para todo tipo de cambio efectuado.

4.2.1. Notificación de cambios que no requieren aprobación por parte de AESA.

Independientemente de que un cambio al SGSI pueda estar cubierto por el procedimiento y no estar sujeto a aprobación por parte de la autoridad, deberá ser siempre convenientemente notificado GM1 IS.I.OR.255.

La notificación de los mismos no requiere el envío de documentación adjunta relativa al cambio; no obstante, se deberá completar el formulario de notificación de cambios al SGSI no sujetos a aprobación y adjuntar un listado de los cambios implantados.

Para la notificación se emplearán los procedimientos electrónicos existentes de notificación de cambios no funcionales.

Las notificaciones se harán mediante registro oficial, se debe presentar el formato de notificación establecido en la sede electrónica adjuntando adicionalmente el listado de los cambios notificados en formato Word o Excel, y con una **periodicidad bimestral**, con las siguientes excepciones:

- Las bases de cumplimiento con el PART-IS y sus evidencias, se notificarán con **CARÁCTER ANUAL.**

- Los cambios en los titulares de los siguientes puestos se notificarán con **CARÁCTER INMEDIATO**:
    - Director responsable (accountable manager **IS.I.OR.240 (a)**),
    - Persona responsable común, si aplica[2] (common responsible person (CRP) **IS.I.OR.250 (a)(3)**),
    - Responsable Part-IS (CISO) (**IS.I.OR.240 (b)**), y,
    - Gestor de monitorización del cumplimiento (Compliance monitoring manager **IS.I.OR.240 (c)**).
- Los cambios en la política identificada a continuación se notificarán con **CARÁCTER INMEDIATO**:
    - Política del SGSI (**IS.I.OR.200 (a)(1)**).

En el Anexo II se recoge la lista de los cambios en el SGSI que no requieren de aprobación previa.

4.3. Cambios no contemplados anteriormente

Adicionalmente, en el caso de que las organizaciones quieran implementar cambios al SGSI que, sin estar sujetos a aprobación, consideren que tienen la entidad suficiente como para involucrar a AESA en el proceso de implementación, deberán notificar dichos cambios con el objeto de obtener asesoramiento técnico al respecto, de manera que se garantice una implantación segura de los mismos.

Estos cambios serán notificados de la misma manera que los cambios que requieren aprobación previa (apartado 4.1.2) indicando que el objeto de la notificación es obtener asesoramiento técnico, y AESA (DNA) indicará los mecanismos apropiados para la implantación segura de los mismos.

Para analizar la entidad del cambio, se podrán tener en cuenta, entre otros, criterios como:

- Importancia para la prestación del servicio.
- Complejidad.
- Alcance (nº de dependencias y/o departamentos afectados, nº de personal afectado, etc.).
- Recursos necesarios.
- Simultaneidad con otros cambios.
- Tiempo de implantación estimado.

[2] Aplicable al caso en el que 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.

- Impacto en otras organizaciones y posible coordinación.
- Número de documentos/procesos afectados.
- Otros factores relevantes.

A tal efecto, la organización puede elaborar un cuestionario a modo de lista de comprobación ("checklist") en el que plantee una serie de preguntas cubriendo estos aspectos, u otros que considere aplicables, otorgando una puntuación a cada una de ellas, de forma que el resultado global pueda servir de orientación a la hora de decidir si ese cambio se considera como significativo.

Ejemplos de cambios relacionados con la seguridad de la información con posible impacto en el SGSI (GM2 IS.I.OR.255)

A modo de ejemplo, y de guía, a continuación, se citan algunos cambios que pueden tener un impacto en el SGSI, o que podrían conducir a un nivel de riesgo inaceptable y, por lo tanto, deben estar sujetos a escrutinio por parte de la autoridad competente:

(a) Cambios en el alcance del SGSI, interfaces o políticas relacionadas:

— Ampliación de las funciones empresariales de la organización e integración de otra empresa dentro de su estructura organizativa.

— Identificación por parte de la organización de no conformidades que indican un alcance incorrecto.

— Cambios en las interfaces de la organización resultantes, por ejemplo, de modificaciones en las actividades internas o externalizadas.

(b) Cambios en las responsabilidades y las obligaciones, así como en la estructura organizativa, que impliquen la aplicación y el control permanente del cumplimiento del REG PART-IS:

— El responsable ha delegado determinadas responsabilidades en una persona o un grupo de personas.

— La organización contrata actividades de gestión de la seguridad de la información conforme a IS.I.OR.235.

5. INTEGRACIÓN DEL PROCESO DE GESTIÓN DE CAMBIOS EN EL SGSI EN OTROS SISTEMAS DE GESTIÓN.

Tal y como sugiere el **IS.I.OR.200(d)** e **IS.I.OR.250(d)** la organización puede integrar el MGSI con otros sistemas de gestión. En este sentido, y para el caso de la gestión de cambios, si la organización ya dispone de un procedimiento de gestión y notificación de cambios conforme a lo establecido en los requisitos **ATM/ANS.OR.A.040**, **ATCO.OR.B.015** y **AMC12 Article 15(1)(e)**[3] de los reglamentos comunitarios correspondientes, la guía de EASA **"ISO/IEC 27001 vs PART-IS Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS"** recomienda que se amplíe dicho procedimiento para incluir los requisitos del REG PART-IS aplicables.

Aquellas organizaciones que ostenten distintos certificados y cuenten, por tanto, con distintos procedimientos de gestión de cambio, a la hora de realizar la notificación solo tendrán que hacerla una vez a través de uno de los procedimientos electrónicos de notificación.

Como orientación para las organizaciones que dispongan de un certificado ISO/IEC 27001:2022, esta guía también incluye la trazabilidad entre el requisito **IS.I.OR.255** del REG PART-IS y la norma ISO/IEC 27001:2022.

.

[3] Reglamento de Ejecución (UE) 2021/664.

ANEXO I. LISTADO DE CAMBIOS SUJETOS A APROBACIÓN

Área	Requisitos	Cambios en
Gestión del cambio	IS.I.OR.255	Procedimiento de gestión de cambios en el SGSI
Gestión de riesgos	IS.I.OR.205 IS.I.OR.210	Procesos de evaluación y tratamiento de los riesgos relacionados con la seguridad de la información
Gestión de incidentes	IS.I.OR.220	Procesos para la detección, respuesta y recuperación, ante incidentes relacionados con la seguridad de la información.

ANEXO II. LISTADO DE CAMBIOS SUJETOS A NOTIFICACIÓN QUE NO REQUIEREN APROBACIÓN

Área	Requisitos	Cambios en
Política	IS.I.OR.200(a)(1) IS.I.OR.250(a)(4)	Política de seguridad de la información
Notificación interna de incidentes	IS.I.OR.200(a)(4) IS.I.OR.215	Sistema interno de notificación de incidentes
Reacción inmediata	IS.I.OR.200(a)(6)	Proceso 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
Personal	IS.I.OR.250(a)(2), (3), (6))	Titulares de roles y responsabilidades clave en seguridad de la información: Director responsable (accountable manager) Persona responsable común (common responsible person (CRP) Responsable Part-IS (CISO) Gestor de monitorización del cumplimiento (Compliance monitoring
	IS.I.OR.250(a)(7)	Organigrama de seguridad de la información
	IS.I.OR.200(a)(10) IS.I.OR.240(f), (g), (h), (i);	Procesos sobre disponibilidad, capacitación y responsabilidades del personal

Área	Requisitos	Cambios en
Notificación externa de incidentes	IS.I.OR.200(a)(8) IS.I.OR.230	Sistema externo de notificación de incidentes
Actividades contratadas	IS.I.OR.200(a)(9) IS.I.OR.235	Procedimientos para actividades contratadas y gestión de riesgos asociados
Registros	IS.I.OR.200(a)(11) IS.I.OR.245	Procedimientos de conservación y protección de registros
Monitorización del cumplimiento	IS.I.OR.200(a)(12) IS.I.OR.225	Procedimiento de supervisión del cumplimiento y medidas correctoras
Confidencialidad	IS.I.OR.200(a)(13)	Procedimiento para proteger la confidencialidad de información recibida de otras organizaciones
Mejora continua	IS.I.OR.200(b) IS.I.OR.260	Procedimiento de mejora continua del SGSI
Distribución interna	AMC1 IS.I.OR.200(c)(f)(1)	Procedimiento de distribución interna del MGSI
Modificación del MGSI*	IS.I.OR.250(c)	Cambios en el MGSI no derivados de cambios en procesos que requieren aprobación previa

*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, en cuyo caso las modificaciones de este último sí requieren aprobación previa.