Agencia Estatal
de Seguridad Aérea

# Guía para la solicitud de exenciones al Reglamento (UE) 2023/203 (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 |

| FORMATOS | |
|---|---|
| **CÓDIGO del FORMATO** | **TÍTULO** |
| NA-ISEC-GU03-F01 | Formato de solicitud de exención |
| | |
| | |
| | |

| REFERENCIAS | |
|---|---|
| **CÓDIGO** | **TÍTULO** |
| N/A | FIRST EASY ACCESS RULES FOR INFORMATION SECURITY (REGULATIONS (EU) 2023/203 AND 2022/1645) |
| Part-IS TF G-02 | EASA IMPLEMENTATION GUIDELINES FOR PART-IS - IS.I/D.OR.200 (E) |

| 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 |
| DNA | DIRECCIÓN DE NAVEGACIÓN AÉREA |
| EASA | AGENCIA EUROPEA DE SEGURIDAD AÉREA |
| ED | EUROCAE DOCUMENT |
| EUROCAE | EUROPEAN ORGANIZATION FOR CIVIL AVIATION EQUIPMENT |
| GM | MATERIAL GUÍA |
| INCIBE | INSTITUTO NACIONAL DE CIBERSEGURIDAD |
| ISO/IEC | ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN / COMISIÓN ELECTROTÉCNICA INTERNACIONAL |
| NIST | INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA |
| 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 definir el proceso a seguir por las organizaciones para solicitar las exenciones recogidas 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.200 (e)** [1], facilitando así su evaluación y aprobación por parte de AESA.

Con este fin y tomando como referencia la **guía de EASA "Implementation guidelines for Part-IS* - IS.I/D.OR.200 (e)" Part-IS TF G-02 July 2024**, se proporciona orientación a las organizaciones, con indicaciones sobre ciertas pautas a la hora de solicitar dichas exenciones.

## 2. ÁMBITO DE APLICACIÓN

Esta guía es de aplicación a aquellas organizaciones en el ámbito de la navegación aérea (proveedores ATM/ANS, organizaciones de formación de controladores de tránsito aéreo y proveedores de servicios de U-Space y proveedores de servicios de información común) que, estando sujetas al cumplimiento del REG PART-IS, deseen presentar una solicitud de exención.

Para obtener la exención, la organización deberá demostrar que no está expuesta a ningún riesgo relacionado con la seguridad de la información que pueda repercutir en la seguridad aérea, ni para ella misma ni para otras organizaciones. Por ello, en principio, se considera que, en el ámbito de la navegación aérea, únicamente las organizaciones de formación inicial de controladores de tránsito aéreo sujetas a lo dispuesto en el reglamento (UE) 2015/340, pueden ser susceptibles de obtener dicha exención.

La solicitud de exención de las organizaciones bajo la supervisión de la Dirección de Navegación Aérea de AESA, deberá ser aprobada por ésta.

---

[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

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 el REG PART-IS impone a las organizaciones afectadas, el requisito **IS.I.OR.200 (e)** otorga a la autoridad competente la posibilidad de eximir a una organización del cumplimiento de determinados requisitos del reglamento, en el caso de que se cumplan determinadas condiciones:

> **IS.I.OR.200 Sistema de gestión de de la seguridad de la información (SGSI)**
> *e) Sin perjuicio de la obligación de cumplir los requisitos de información establecidos en el Reglamento (UE) nº 376/2014 y los requisitos establecidos en el punto IS.I.OR.200, letra a), punto 13), la autoridad competente podrá permitir que la organización no aplique los requisitos a que se refieren las letras a) a d) ni los requisitos relacionados que figuran en los puntos IS.I.OR.205 a IS.I.OR.260 si demuestra a satisfacción de dicha autoridad que sus actividades, instalaciones y recursos, así como los servicios que gestiona, presta, recibe y mantiene, 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. La aprobación se basará en una evaluación del riesgo relacionado con la seguridad de la información documentada y realizada por la organización o un tercero de conformidad con el punto IS.I.OR.205 y revisada y aprobada por su autoridad competente.*
> *El mantenimiento de la validez de dicha aprobación será revisado por la autoridad competente tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.*

## 4. EXENCIONES AL CUMPLIMIENTO DE REQUISITOS DEL PART-IS

Como ya se ha visto anteriormente, el requisito **IS.I.OR.200 (e)** del REG PART-IS ofrece la posibilidad de que la autoridad competente otorgue exenciones al cumplimiento de la mayoría de los requisitos del propio reglamento, siempre y cuando se cumplan determinadas condiciones.

Este requisito tiene asociado un **AMC** y un **GM**, aportando información, el primero de ellos sobre la evaluación de riesgos que la organización tiene que realizar para solicitar la aprobación de la exención, y el segundo sobre la condición que debe cumplir una organización para poder optar a solicitar dicha exención.

**AMC1 IS.I.OR.200(e) Sistema de gestión de la seguridad de la información (SGSI)**

***EXENCIÓN***

*Las organizaciones deben seguir las instrucciones proporcionadas en el **AMC1 IS.I.OR.205(a)** y **AMC1 IS.I.OR.205(b)** para realizar una evaluación documentada de los riesgos para la seguridad de la información con el fin de solicitar la aprobación por parte de la autoridad competente de una exención en virtud del punto **IS.I.OR.200(e)**. Para justificar los motivos de una exención, se espera que la evaluación de riesgos ofrezca explicaciones sobre la exclusión de todos los elementos del ámbito de aplicación del SGSI. Corresponde a la autoridad determinar si esta evaluación se considera satisfactoria para que se conceda una exención. Las organizaciones que deseen que un tercero realice la evaluación de riesgos deben tener en cuenta los requisitos de **IS.I.OR.235** y el AMC correspondiente.*

**GM1 IS.I.OR.200(e) Information security management system (ISMS)**

*Una organización que considere que no tiene ningún riesgo para la seguridad de la información con impacto potencial en la seguridad operacional de la aviación, tanto para sí misma como para otras organizaciones, puede solicitar una aprobación para una exención por parte de la autoridad competente siguiendo el procedimiento descrito en AMC1 IS.I.OR.200(e).*

*[…]*

Sin perjuicio de la obligación de cumplir los requisitos de reporte establecidos en el Reglamento (UE) n.º 376/2014 y los requisitos del punto **IS.I.OR.200(a)(13)**, la organización podrá obtener una aprobación para no aplicar los requisitos establecidos en **IS.I.OR.200(a)** a **(d)** y los requisitos pertinentes de los puntos **IS.I.OR.205** a **IS.I.OR.260** si evidencia que sus actividades, instalaciones y recursos, y los servicios que opera, proporciona, recibe y mantiene, no plantean un riesgo para la seguridad de la información con un impacto potencial en la seguridad aérea, ya sea para sí misma o para otra organización.

## 4.1. Proceso de solicitud de exenciones

Cuando la organización tenga intención de solicitar la exención al cumplimiento de los correspondientes requisitos del REG PART-IS, procederán del siguiente modo dependiendo de la situación:

- Las organizaciones que ya dispongan de certificado en vigor en su ámbito deberán realizar la solicitud a través del procedimiento electrónico de Solicitud General de la Sede Electrónica de AESA, aportando; solicitud de exención de acuerdo al formato **NA-ISEC-GU03-F01**, firmada por el director responsable y evaluación de riesgos de seguridad de la información.
- Las organizaciones que no cuenten con certificado, deberán realizar la solicitud en el marco del correspondiente proceso de certificación. Al cumplimentar el cuestionario de certificación indicarán en la celda del requisito correspondiente tal intención y aportarán la evaluación de riesgos de seguridad de la información como evidencia asociada.
- La modificación de exenciones previamente concedidas se tramitará a través del procedimiento electrónico de Solicitud General de la Sede Electrónica de AESA, aportando; solicitud de exención de acuerdo al formato **NA-ISEC-GU03-F01** en el que se indique a qué responde la modificación y evaluación de riesgos de seguridad de la información actualizada.

## 4.2. Consideraciones para realizar la evaluación de riesgos de seguridad de la información

La guía publicada por EASA contiene indicaciones para armonizar el proceso de solicitud y evaluación de exenciones por parte de las autoridades competentes en los diferentes estados miembros.

De la guía se pueden extraer una serie de consideraciones que deberían ser tenidas en cuenta por las organizaciones a la hora de presentar la solicitud de exención:

- La organización deberá utilizar la metodología de evaluación de riesgos ya establecida como parte obligatoria de su Sistema de Gestión de Seguridad, cuando le sea de aplicación, para abordar los riesgos para la seguridad de la información.
- En el caso de que no disponga de un Sistema de Gestión de Seguridad implantado, podrá realizar la evaluación de riesgos de seguridad de la información basándose en la metodología descrita en el apartado 4.2.1. o en una metodología reconocida (ej.: ISO/IEC 27005, ISO/IEC 31000, NIST SP 800-30). Las organizaciones también pueden considerar las orientaciones específicas para la aviación definidas en el capítulo sobre gestión de riesgos de la última versión de EUROCAE ED-201A y, según proceda para el entorno operativo específico, en los capítulos de EUROCAE ED-205A y EUROCAE ED-206.
- La metodología debe ser aplicada por personal que tenga conocimientos sobre su uso, debiendo contar también con personal experto en seguridad de la información (ciberseguridad), que pueda realizar una identificación y evaluación precisa de los riesgos, así como personal experto en seguridad operacional y en los servicios que la organización provee para valorar su repercusión o no sobre la seguridad aérea.
- Esta evaluación podrá ser realizada por una empresa externa con experiencia reconocible en la realización de evaluaciones de riesgos de seguridad de la información (ciberseguridad).
- La organización deberá especificar:
  - La Metodología utilizada para realizar la evaluación de riesgos para la seguridad de la información.
  - La lista de personas (tanto pertenecientes a la organización como externas a ella) y funciones implicadas en el proceso de evaluación de riesgos para la seguridad de la información.
- A la hora de realizar la evaluación de riesgos para la seguridad de la información se deberán considerar los siguientes aspectos:
  - Tamaño y complejidad de la organización.
  - Impacto potencial en la seguridad causado por incidentes de seguridad de la información, en los servicios que presta y recibe la organización, incluidas sus interfaces.
  - Procesos que la organización ha establecido para prestar y recibir los servicios.

- Posición de la organización dentro de la cadena funcional de la aviación y el consiguiente grado de criticidad de la organización dentro del ámbito de la aviación civil en el Estado miembro.
- Actividades transfronterizas de la organización, si procede.
- Madurez del sistema de gestión de la seguridad de la organización, si procede.
- Listado de sistemas digitales, flujos de datos y procesos.

- La evaluación de riesgos identificará los riesgos para la seguridad de la información que puedan tener un impacto potencial en la seguridad aérea.

### *4.2.1. Metodología para la evaluación de riesgos*

La evaluación de riesgos de seguridad de la información, tal como se describe en el requisito **IS.I.OR.205** y sus **AMC** y **GM** asociados, es un proceso sistemático y fundamental para que una organización identifique, analice y clasifique los riesgos con un potencial impacto en la seguridad operacional de la aviación.

No se exige un marco de seguridad de la información específico (como ISO o NIST), teniendo las organizaciones la flexibilidad de adaptar y personalizar los marcos existentes para satisfacer sus necesidades particulares, especialmente para integrar los aspectos de seguridad aérea.

El proceso debe ser riguroso y documentado, asegurando la reproducibilidad de los resultados y la comparabilidad entre evaluaciones. Es crucial que se revise y actualice periódicamente, teniendo en cuenta la criticidad de los activos y los niveles de riesgo residual.

A grandes rasgos, la metodología para realizar una evaluación de riesgos de seguridad de la información se puede describir a través de los siguientes pasos:

1. Definición del Alcance y Fronteras (**IS.I.OR.205(a)**)

- Identificar todos los elementos que están expuestos a riesgos relacionados con la seguridad de la información, incluyendo las actividades, instalaciones y recursos de la organización, así como los servicios que gestiona, presta, recibe o mantiene,

- Identificar los equipos, sistemas, datos e información que contribuyan al funcionamiento de los elementos anteriores.

- Documentar los flujos de datos, sistemas de información y servicios contratados que puedan afectar a la seguridad de la información y, por ende, a la seguridad operacional.

Para ello, se puede consultar el **AMC1 IS.I.OR.205(a)** y el material guía **GM1 IS.I.OR.205(a)**, que contiene ejemplos de elementos que pueden tenerse en cuenta para la identificación del alcance y fronteras.

2. Identificación de interfaces (**IS.I.OR.205(b)**)

- Identificar las interfaces con otras organizaciones (proveedores, clientes, socios) que puedan suponer una exposición mutua a riesgos de seguridad de la información.

- Documentar los flujos de información, activos compartidos y responsabilidades de cada parte.

3. Identificación y Clasificación de los Riesgos de Seguridad de la Información (**IS.I.OR.205(c)**)

- Identificar los riesgos de seguridad de la información que puedan tener un impacto potencial en la seguridad aérea. Como ejemplo de riesgo para las organizaciones de formación, conforme al **Example 5: Training system** del **Appendix I — Examples of threat scenarios with a potential harmful impact on safety,** el uso de sistemas de formación que contengan modelos funcionales, datos operativos y escenarios que reflejan el comportamiento del sistema real, podría facilitar la obtención de información técnica que permita diseñar ataques más eficaces contra el sistema operativo real.

- Para cada riesgo identificado:
  - Asociar el riesgo con el elemento o interfaz correspondiente.
  - Asignar un nivel de riesgo según una clasificación predefinida, teniendo en cuenta la probabilidad de ocurrencia y la severidad de sus consecuencias, identificando si tienen o no tienen repercusión sobre la seguridad aérea
  - Clasificar el riesgo en base a los criterios de aceptación del riesgo establecidos.

4. Documentación y Trazabilidad

- Mantener evidencia documentada del análisis, incluyendo:
  - Metodología utilizada.
  - Registro de riesgos (risk register).
  - Clasificación de riesgos
  - Justificación de aceptabilidad y no repercusión en la seguridad aérea

5. Conclusión

Para que la organización pueda optar a la exención, la evaluación de riesgos de seguridad de la información debe concluir que sus actividades, instalaciones y recursos, así como los servicios que gestiona, presta, recibe y mantiene, 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.

## 4.3. Obligaciones de la organización con exención aprobada

Una vez que AESA haya concedido la aprobación de una exención conforme al **IS.I.OR.200 (e)**, y en línea con la **guía de EASA,** la organización, de forma continuada, tendrá que:

- Cumplir con los requisitos de información contenidos en el Reglamento (UE) nº 376/2014 y con las disposiciones del REG PART-IS de cuyo cumplimiento no exime la exención otorgada **IS.I.OR.200 (a) (13)**.

- Monitorizar continuamente cualquier cambio en el alcance del trabajo, y de cualquier actividad, de la organización e identificar aquellos que puedan tener un impacto potencial en la información documentada que respalda la aprobación de la exención, y que podrían afectar a la vigencia de la aprobación (esta monitorización deberá realizarse por una persona o grupo de personas con los conocimientos necesarios de Part-IS, así como conocimiento suficiente para poder evaluar y controlar que las condiciones de la derogación se mantienen). Cuando se detecten tales cambios, la organización debe asegurarse de que se pongan en conocimiento de AESA sin demora y se notifiquen a través del procedimiento de solicitud general. Dicha notificación implicará el inicio de una revisión y posterior reevaluación de la validez de la exención previamente otorgada por AESA.

- Poder demostrar que el director responsable de la organización comprende el proceso de exención y los términos en los que se ha otorgado la misma.

- Implementar una protección básica contra los riesgos de seguridad de la información de acuerdo con las mejores prácticas de la industria.

- Consultar al Instituto Nacional de Ciberseguridad (INCIBE) para obtener orientación adicional en caso de necesidad.

## 4.4. Requisitos exentos de cumplimiento

Tal y como establece el requisito **IS.I.OR.200 (e)** del REG PART-IS, una vez que la autoridad autorice una exención solicitada por una organización, ésta le eximirá del cumplimiento de los requisitos a que se refieren los requisitos **IS.I.OR.200 (a)** a **(d)**, así como de los requisitos relacionados que figuran en los puntos **IS.I.OR.205** a **IS.I.OR.260** de dicho reglamento, sin perjuicio de la obligación de cumplir los requisitos de información establecidos en el Reglamento (UE) nº 376/2014 y los requisitos establecidos en **IS.I.OR.200 (a)(13)** relativo a la protección de la confidencialidad de la información recibida de otras organizaciones, en función de su nivel de sensibilidad.

La organización no estaría obligada, por tanto, a establecer un sistema de gestión de la seguridad de la información (SGSI), ni a elaborar un Manual de gestión de la seguridad de la información (MGSI), o establecer un sistema de notificación en materia de seguridad de la información, aplicar un proceso de mejora continua, etc.

Sin embargo, independientemente de la aprobación de la exención, la organización debe cumplir con el requisito **IS.I.OR.200 (a)(13)**. Como orientación para dar cumplimiento a dicho requisito, en la **guía de EASA** se recoge una lista de puntos a verificar por la autoridad competente que puede valer como pauta a la organización para garantizar el cumplimiento:

- Cuenta con medidas adecuadas para proteger la confidencialidad de la información en reposo y en tránsito. Este requisito no debe limitarse a proteger únicamente la información recibida. Cuando se transmite información de carácter confidencial, la organización debe disponer también de medios seguros.

- Ha establecido un esquema de clasificación de datos.

- Ha establecido medidas adecuadas de control de acceso para garantizar un principio de "necesidad de saber" eficaz.