Agencia Estatal
de Seguridad Aérea

GUÍA SOBRE LA SOLICITUD DE UNA DEROGACIÓN A LA APLICACIÓN DEL REGLAMENTO DE EJECUCIÓN (UE) 2023/203 PARA OPERADORES AÉREOS

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**
01	Desde publicación	Primera edición

REFERENCIAS	
CÓDIGO	**TÍTULO**
DSA-SG-P01-F11 Ed.01	RESOLUCIÓN APROBACIÓN DEROGACIÓN
DSA-SG-P01-F10 Ed.01	SOLICITUD DEROGACIÓN
LSA	LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS
LPAC	LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS
RIA	REAL DECRETO 98/2009, DE 6 DE FEBRERO, POR EL QUE SE APRUEBA EL REGLAMENTO DE INSPECCIÓN AERONÁUTICA Y MODIFICACIONES POSTERIORES
REAL DECRETO 203/2021	REAL DECRETO 203/2021, DE 30 DE MARZO, POR EL QUE SE APRUEBA EL REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS
BR	REGLAMENTO (UE) N.º 2018/1139 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 4 DE JULIO DE 2018, SOBRE NORMAS COMUNES EN EL ÁMBITO DE LA AVIACIÓN CIVIL Y POR EL QUE SE CREA UNA AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD AÉREA Y POR EL QUE SE MODIFICAN LOS REGLAMENTOS (CE) N.º 2111/2005, (CE) N.º 1008/2008, (UE) N.º 996/2010, (UE) N.º 376/2014 Y LAS DIRECTIVAS 2014/30/UE Y 2014/53/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y SE DEROGAN LOS REGLAMENTOS (CE) N.º 552/2004 Y (CE) N.º 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y EL REGLAMENTO (CEE) N.º 3922/91 DEL CONSEJO
REGLAMENTO (UE) 965/2012	REGLAMENTO (UE) NO 965/2012 DE LA COMISIÓN DE 5 DE OCTUBRE DE 2012 POR EL QUE SE ESTABLECEN REQUISITOS TÉCNICOS Y PROCEDIMIENTOS ADMINISTRATIVOS EN RELACIÓN CON LAS OPERACIONES AÉREAS
REGLAMENTO (UE) 2023/203	REGLAMENTO (UE) NO 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
Part-IS TF G-03	GUIDELINES FOR COMPETENT AUTHORITIES FOR THE CONDUCT OF OVERSIGHT ACTIVITIES OF ORGANISATIONS IMPLEMENTING PART-IS
Part-IS TF G-02	IMPLEMENTATION GUIDELINES FOR PART-IS - IS.I/D.OR.200 (E)
Part-IS TF G-01	GUIDELINES FOR ISO/IEC 27001:2022 CONFORMING ORGANISATIONS ON HOW TO SHOW COMPLIANCE WITH PART-IS

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
AESA	AGENCIA ESTATAL DE SEGURIDAD AÉREA
AOC	CERTIFICADO DE OPERADOR AÉREO (AIR OPERATOR CERTIFICATE)
DAEOA	DIVISIÓN DE APROBACIONES Y ESTANDARIZACIÓN DE OPERACIONES AÉREAS
DR	DIRECTOR RESPONSABLE
DSA	DIRECCIÓN/DIRECTOR DE SEGURIDAD DE AERONAVES
EASA	AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD AÉREA (EUROPEAN UNION AVIATION SAFETY AGENCY)
LSA	LEY DE SEGURIDAD AÉREA (LEY 21/2003)
MO	MANUAL DE OPERACIONES
MSG	MANUAL DEL SISTEMA DE GESTIÓN
PGIA	PROCEDIMIENTO GENERAL DE INSPECCIÓN AERONÁUTICA DE LA DSA DE AESA
PO	PRINCIPAL DE OPERACIONES
PVC	PLAN DE VIGILANCIA CONTINUADA
RS	RESPONSABLE DE SEGURIDAD
SIPA	SISTEMA INTEGRADO DE PROCESOS AERONÁUTICOS
SG	SISTEMA DE GESTIÓN (MANAGEMENT SYSTEM)
SGI	SISTEMA DE GESTIÓN DE LA INFORMACIÓN

ÍNDICE

1. INTRODUCCIÓN

La implementación del Reglamento de Ejecución (UE) 2023/203, de la Comisión, de 27 de octubre de 2022, añade nuevos requisitos en materia de ciberseguridad y seguridad operacional aplicable a los operadores obligados por la Subparte ORO del Reglamento 965/2012, a partir del 22 de febrero de 2026.

No obstante lo anterior, existen escenarios y/o condiciones en los que un operador aéreo puede obtener un alivio parcial (en adelante, derogación) al cumplimiento de estos nuevos requisitos.

Esta guía pretende proporcionar a las organizaciones afectadas información sobre este proceso de derogación de requisitos normativos.

2. OBJETO Y ALCANCE

El objeto de esta guía es describir el proceso de obtención de una derogación al cumplimiento de ciertos puntos normativos del Reglamento (UE) 2023/203, con potencial impacto en la seguridad operacional.

Este proceso incluye el tratamiento de los siguientes aspectos y documentos:

- Establecimiento de ciertos escenarios operativos susceptibles de obtener la derogación.
- Los requisitos que los operadores deben cumplir para obtener la derogación.
- Indicaciones para cumplimentar la solicitud de derogación y la documentación que los operadores deben aportar junto a la mencionada solicitud.
- El formato de solicitud de derogación.

La derogación podrá ser solicitada por aquellos operadores a los que les aplique el Reglamento 2023/203, que a su vez son aquellos operadores de avión o helicóptero a los que les aplica la Subparte ORO del Reglamento 965/2012:

- Operadores que realizan operaciones de transporte aéreo comercial (AOC),
- Operadores que realizan operaciones comerciales especializadas (SPO), u
- Operadores que realizar operaciones no comerciales con aeronave motopropulsada compleja (NCC).

3. DEROGACIÓN AL CUMPLIMIENTO DEL REGLAMENTO DE EJECUCIÓN (UE) 2023/203

AESA reconoce la posibilidad de que una organización obtenga una derogación, es decir, la aprobación para no aplicar ciertos requisitos de la Parte IS, de acuerdo con IS.I.OR.200(e). Para ello, AESA no sólo se basa en el reglamento, sino también en las directrices adicionales publicadas por EASA para la aplicación de excepciones, siempre que sean adecuadas y aplicables al entorno de la aviación civil española.

Sin perjuicio de la obligación de cumplir los requisitos de información establecidos en el Reglamento (UE) 376/2014 y los requisitos del punto IS.I.OR.200(a)(13), la aprobación de una derogación comprenderá la no aplicación de los requisitos establecidos en las letras (a) a (d) del requisito IS.I.OR.200 ,así como en los puntos IS.I.OR.205 a IS.I.OR.260, si se demuestra a satisfacción de AESA que las actividades, instalaciones y recursos, así como los servicios que presta, recibe y mantiene la organización, no plantean un riesgo para la seguridad de la información con un impacto potencial en la seguridad aérea, ni para sí misma ni para otra organización.

En cualquier caso, esta derogación estará basada en una Evaluación Documentada de los Riesgos para la Seguridad de la Información, que debe ser realizada por la organización o por un tercero de conformidad con el punto IS.I.OR.205, y revisada y aprobada por AESA.

Esta evaluación de riesgos puede llevarse a cabo y documentarse utilizando el procedimiento de evaluación de riesgos existente en la organización, o bien un procedimiento definido ad hoc para los riesgos de seguridad de la información con efecto en la seguridad operacional.

AESA ha establecido unos criterios y condiciones básicas para facilitar a la organización la obtención de una derogación a la Parte IS.

Es importante señalar que los criterios y condiciones básicas que se indican no constituyen por sí mismos la aprobación de una derogación. Cada solicitud de derogación se evaluará individualmente. En caso satisfactorio AESA aprobará la derogación a la Parte IS.

3.1. Organizaciones a las que no le aplica la Parte IS

Aun cuando el Reglamento 2023/203 define la aplicabilidad de la Parte IS en base al cumplimiento de la Subparte ORO del Reglamento 965/2012, en su artículo 2(c) determina la no aplicabilidad para las organizaciones que única y exclusivamente operen bajo alguno de los epígrafes siguientes:

- Operaciones con aeronaves ELA 2 conforme al artículo 182), punto (j) del Reglamento (UE) 748/2012.
- Operaciones con aviones de un solo motor propulsados por hélice, no clasificados como aeronaves complejas y con un MOPSC menor o igual a 5, despegando y aterrizando del mismo aeródromo o lugar de operación, en condiciones VFR y de día.
- Operaciones con helicópteros de un solo motor, no clasificados como aeronaves complejas y con un MOPSC menor o igual a 5, despegando y aterrizando del mismo aeródromo o lugar de operación, en condiciones VFR y de día.

Las condiciones anteriores pueden resumirse en el siguiente cuadro:

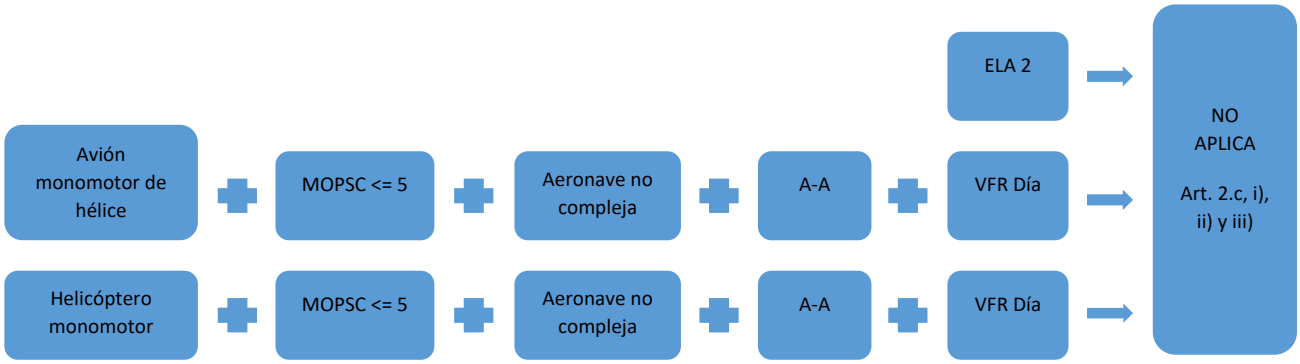


Figura 1: Operaciones excluidas de la aplicación del Reglamento de Ejecución (UE) 2023/203

3.2. Criterios y condiciones básicas para la evaluación positiva de una solicitud de derogación

Aun cuando cualquier organización puede solicitar una derogación en los términos de IS.I.OR.200 (e), se considera conveniente establecer un primer conjunto de características que las organizaciones deben reunir, con el objetivo de proporcionar una indicación de si la correspondiente solicitud tiene perspectivas de éxito, sobre la base de una Evaluación de Riesgos de Seguridad de la Información sin potencial impacto sobre la seguridad operacional.

Estas condiciones parten de ampliar las condiciones de no aplicabilidad del Art.2 (c) del Reglamento 2023/203, y se definen por áreas conforme al siguiente listado:

- **Tipo de aeronave/s.**
  - ✓ Aviones distintos de los motopropulsados complejos equipados con más de un motor de pistón.
  - ✓ Aviones motopropulsados complejos sólo porque su MCTOM es igual o superior a 5700 kg.
  - ✓ Aviones motopropulsados complejos de MCTOM igual o inferior a 5700 kg, equipados con motores turbohélice, que efectúen operaciones no comerciales, conforme al artículo 6, apartado 8 del Reglamento 965/2012.
  - ✓ Helicópteros distintos de los motopropulsados complejos equipados con más de un motor, desarrollados a partir de un modelo monomotor.
  - ✓ Helicópteros motopropulsados complejos con un nivel bajo de automatización.
- **Tipo de operación.**
  - ✓ Vuelos VFR, de día o de noche.
  - ✓ Vuelos con origen y destino el mismo aeródromo o lugar de operaciones (en delante vuelos A-A). Existen vuelos con origen o destino no coincidentes (en adelante vuelos A-B), que son marginales con respecto al total de las operaciones.

- ✓ Aeronaves con MOPSC igual o inferior 5 o en el caso de paracaidismo donde no se cuenta con asientos para los paracaidistas.

- **Características organizativas y de alcance de la operación realizada.**
  - ✓ Alcance de la operación reducido (por ejemplo, sólo operaciones comerciales especializadas).
  - ✓ Recursos humanos limitados: menos de 20 FTEs (empleados equivalentes a jornada completa) y con un número reducido de empleados expuestos a seguridad de la información.
  - ✓ Organización no crítica en la cadena funcional de la aviación civil española, con bajo impacto en términos de seguridad operacional.
  - ✓ No se cuenta con proveedores que deban cumplir con Parte IS.
  - ✓ La actividad transfronteriza no existe o es marginal.
  - ✓ El Sistema de Gestión de la Seguridad Operacional (SMS) del operador presenta un grado de madurez adecuado.

Las operaciones desarrolladas bajo estos criterios y condiciones, acompañadas de una Evaluación de Riesgos de Seguridad de la Información sin riesgos con consecuencias en la seguridad operacional, son situaciones que favorecen la resolución positiva, aunque no suponen por sí mismas la obtención de una derogación.

3.3. Evaluación Documentada de los Riesgos para la Seguridad de la Información

La realización de una Evaluación Documentada de Riesgos para la Seguridad de la Información es crucial para identificar riesgos de seguridad de la información con potencial impacto en la seguridad operacional.

Se recomienda que el primer paso de esta evaluación consista en seleccionar dentro de la organización un equipo multidisciplinar con personal proveniente de varias áreas como por ejemplo IT, operaciones vuelo, operaciones tierra, entrenamiento, mantenimiento, recursos humanos, gestión, etc.

Este equipo debe realizar una revisión completa de todos los sistemas de información y comunicación y de los datos asociados con vistas a identificar vulnerabilidades y amenazas potenciales. Se deberá por tanto documentar un registro de riesgos donde se categoricen los mismos en base a su probabilidad y ocurrencia. También deberá contarse con las barreras existentes y, en un último paso evaluador, las posibles mitigaciones que se consideren necesarias.

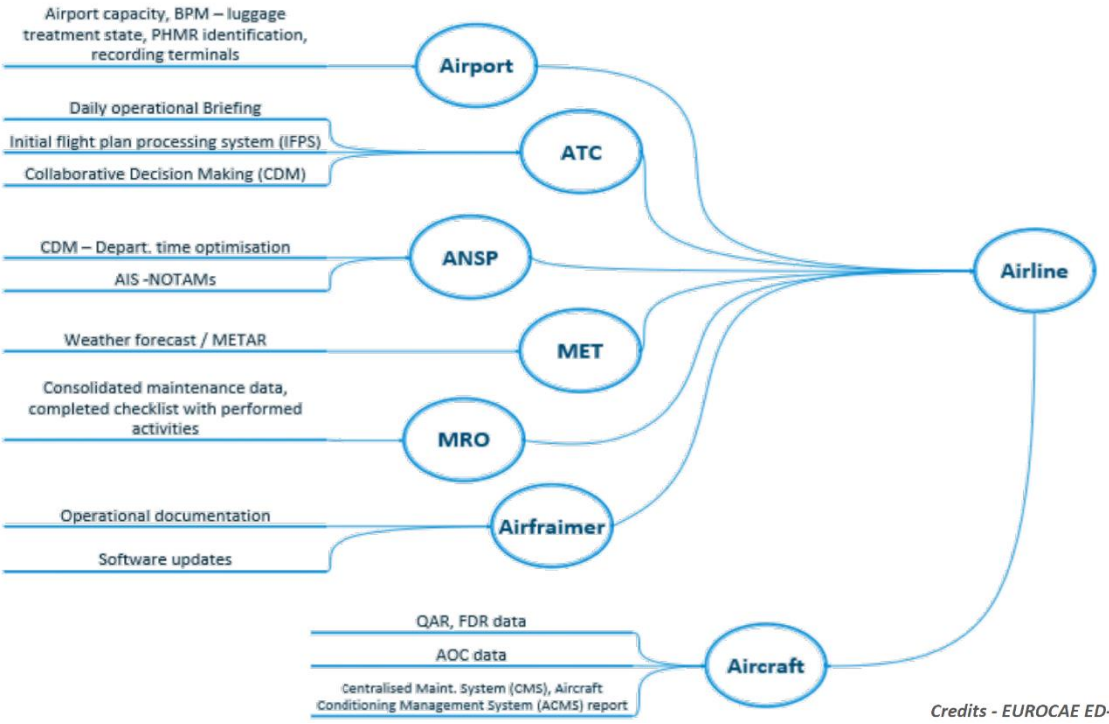
La organización debe, por tanto, identificar como primera acción todos los elementos que pueden estar expuestos a riesgos de seguridad de la información, incluyendo actividades, instalaciones y recursos, así como los servicios que opera, proporciona, recibe o mantiene.

Como acción siguiente deberá también identificar las interfaces con otras organizaciones, de las cuales pueden resultar exposiciones mutuas a riesgos de seguridad de la información que puedan incrementar los riesgos de seguridad operacional a los que se expongan tanto la propia organización como otras partes.

Se deberá también determinar una metodología de evaluación de riesgos y un criterio para determinar el nivel de aceptación o mitigación de cada uno de ellos. Como recomendación, se considera que lo más razonable es el uso de la misma metodología de evaluación de riesgos que la organización tenga implantada dentro de su Sistema de Gestión de la Seguridad Operacional, adaptándola a las particularidades de los Sistemas de Seguridad de la Información.

Así, los puntos más importantes a tener en cuenta dentro de la Evaluación Documentada de Riesgos para la Seguridad de la Información son:

1. Listar e identificar los diferentes elementos del sistema de información de la organización, con detalle de su naturaleza y función.
2. Listar e identificar las diferentes fronteras del sistema de información de la organización, es decir las diferentes interfaces con otras organizaciones o actividades. Como ejemplos tomados de EUROCAE ED-201A, se presentan las siguientes figuras.



Credits - EUROCAE ED-201A for data

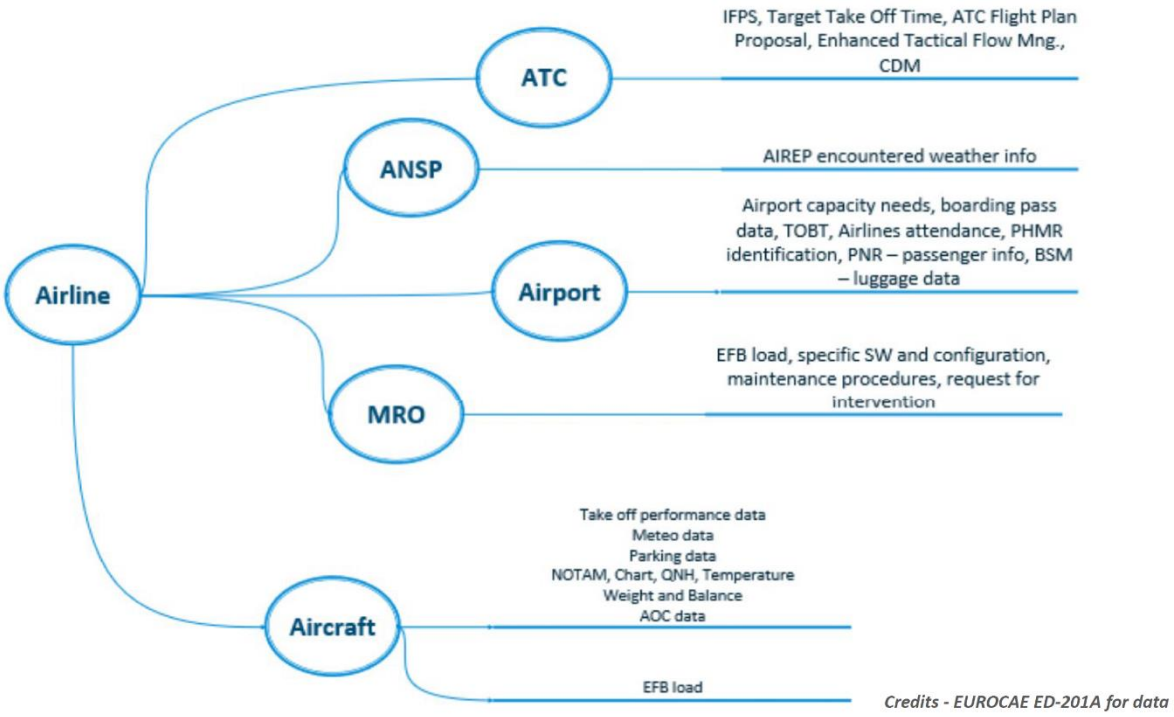


Figura 2: relaciones entre operador aéreo y otros actores de la operación

3. Identificar a continuación las diferentes amenazas presentes, caracterizando el escenario de la organización en los siguientes aspectos:
    - Fuentes de amenazas de seguridad de la información.
    - Vectores de ataque y camino a través de la organización hasta el activo amenazado.
    - Controles de seguridad de la información que podrían mitigar el ataque (posibles barreras).
    - Las consecuencias de que esa amenaza se materialice en un ataque, incluyendo los aspectos de seguridad operacional.
4. Cada riesgo deberá asociarse con los elementos relevantes de la organización ya descritos (interfaces con otras organizaciones, actividades, instalaciones, recursos, etc).
5. La organización asegurará que esta evaluación del riesgo se realiza desde el rigor y la disciplina, documentando el proceso.
6. Cada riesgo deberá ser aceptado o mitigado de acuerdo con el criterio que defina la organización y basándose en aquellos que tengan un potencial impacto en la seguridad operacional, es decir:
    - Se deberá asignar un nivel de riesgo conforme a la clasificación establecida por la organización.
    - Cada riesgo se deberá relacionar con su correspondiente elemento/categoría (interfaz con otra organización, área de la operación, etc).

Cuando se esté realizando la evaluación, los aspectos de ciberseguridad y de seguridad operacional deberán ser coordinados a través de un procedimiento o proceso que asegure el entendimiento entre ambos aspectos. Por ejemplo, esto puede hacerse a través de un diagrama "bow-tie" que resalte la conexión entre el control de los riesgos y el sistema de gestión subyacente.

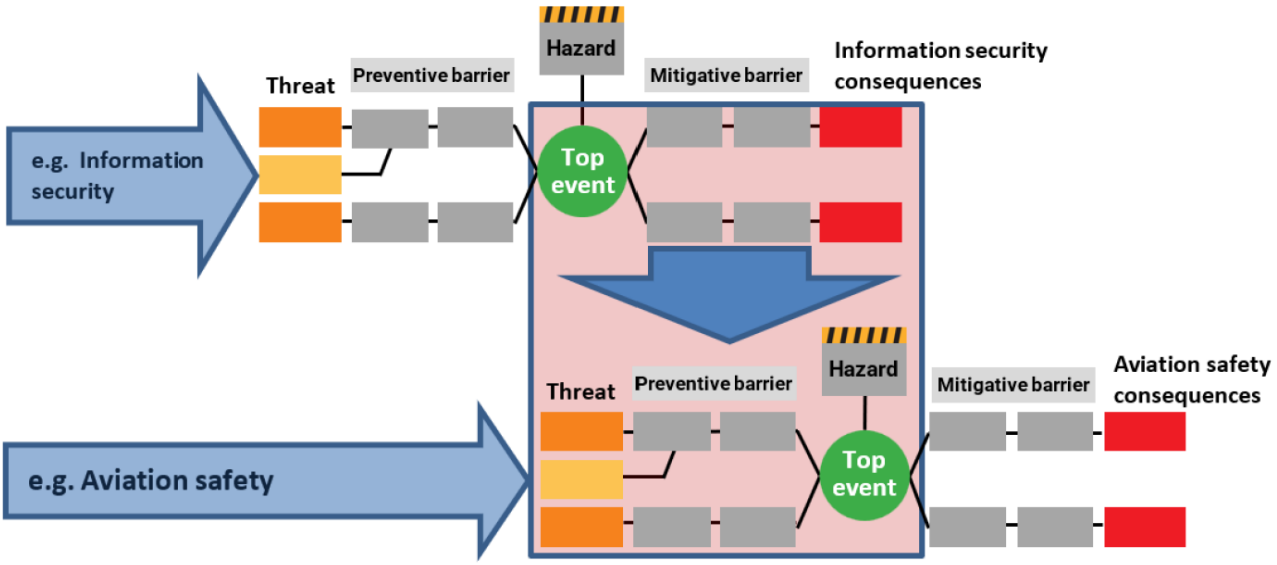


Figura 4: Propuesta de modelo de coordinación entre la evaluación de riesgos de seguridad de la información y la de riesgos de seguridad operacional

Es importante señalar que conforme a AMC1 IS.I.OR.200(e) y a IS.I.OR.235, si la organización considera la necesidad se podrán subcontratar como servicio externo la realización de esta evaluación de riesgos y/o las necesidades de personal cualificado detalladas en el apartado 3.6 de esta Guía.

Finalmente, se recomienda a las organizaciones el uso extensivo y el apoyo en el Reglamento 2023/203 y en las normativas y guías conexas incluyendo AMCs y GMs asociados, en concreto:

- IS.I.OR.200 Information security management system (ISMS).
- IS.I.OR.205 Information security risk assessment.
- IS.I.OR.210 Information security risk treatment.
- IS.I.OR.240 Personnel requirements.
- Appendix I – Examples of threat scenarios with a potential harmful impact on safety.
- EUROCAE ED-203A.
- EUROCAE ED-202A.

3.4. Personal de la organización relacionado con la Seguridad de la Información

Los requisitos de personal se definen conforme a IS.I.OR.240. Este punto normativo, una vez aprobada la derogación, es excluido parcialmente. La organización debe mantener, al menos, la capacidad de contar con un conocimiento básico en ciberseguridad.

Así, los requisitos de Vigilancia Continuada detallados en el punto 3.7 de esta guía refuerzan la necesidad de contar con una persona con conocimientos suficientes en ciberseguridad (o recurrir a una figura externa si fuera necesario), así como asegurar el conocimiento básico en la materia por parte del Director Responsable.

La persona con conocimientos suficientes en ciberseguridad deberá desarrollar su labor de monitorización en estrecha colaboración con el Responsable de Seguridad de la organización, pudiendo ser la misma persona.

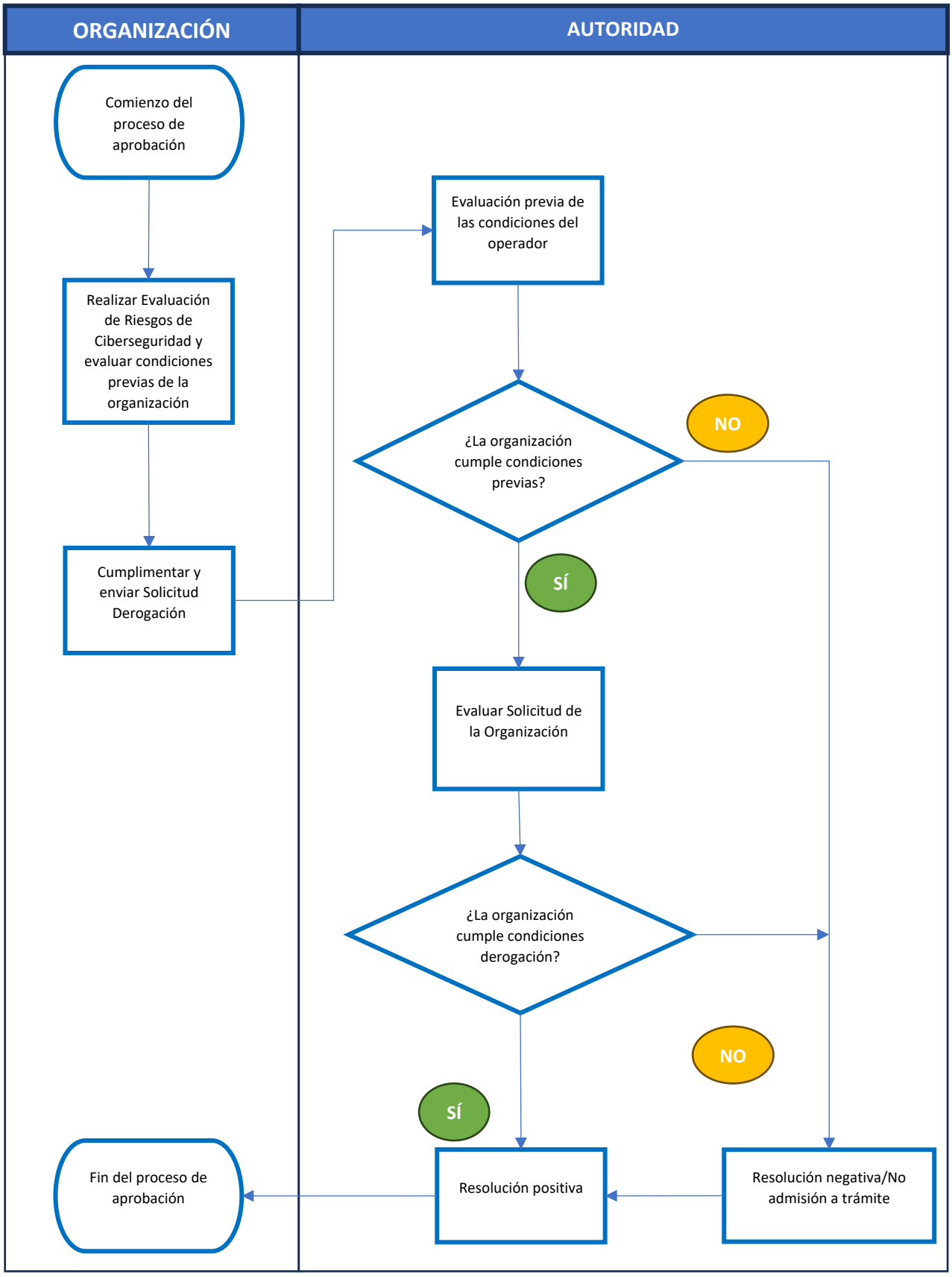
3.5. Resumen de requisitos Reglamento 2023/203 (Parte IS)

NOTA PASAR A TABLA EN EXCEL Y LUEGO COPIAR EN EL WORD PARA QUE NO SEA UNA IMAGEN

Requisitos del Reglamento verde: derogación total amarillo: derogación parcial **blanco**: no derogación	Contenido	Observaciones
IS.I.OR.200 (a)	Implementación de un ISMS	
IS.I.OR.200 (a) (1)	Política de Seguridad de la Información	
IS.I.OR.200 (a) (2)	Identificación y evaluación de los riesgos de seguridad de la información	
IS.I.OR.200 (a) (3)	Definición e implementación de medidas de mitigación	
IS.I.OR.200 (a) (4)	Esquema de reporte interno	
IS.I.OR.200 (a) (5)	Implementación de medidas para la detección de eventos e incidentes de seguridad de la información	
IS.I.OR.200 (a) (6)	Implementación de medidas para una reacción inmediata ante un incidente de seguridad de la información	
IS.I.OR.200 (a) (7)	Acciones requeridas ante hallazgos notificados por la Autoridad Competente	
IS.I.OR.200 (a) (8)	Implementación de un esquema de reporte externo	
IS.I.OR.200 (a) (9)	Mantener conformidad con los requisitos cuando se contratan servicios de gestión de seguridad de la información	Conforme a IS.I.OR.235
IS.I.OR.200 (a) (10)	Mantener conformidad con los requisitos de personal	
IS.I.OR.200 (a) (11)	Mantenimiento de registros	
IS.I.OR.200 (a) (12)	Control de la conformidad	
IS.I.OR.200 (a) (13)	Proteger la confidencialidad de la información compartida por otras organizaciones	Este requisito no debería limitarse a proteger la información recibida. Cuando se transmite información de naturaleza confidencial la organización debe contar con medios seguros para su manejo.

Requisitos del Reglamento verde: derogación total amarillo: derogación parcial **blanco**: no derogación	**Contenido**	**Observaciones**
IS.I.OR.200 (b)	Mejora continua	
IS.I.OR.200 (c)(d)	Documentación de procesos clave, procedimientos, roles y responsabilidades	
IS.I.OR.205	Evaluación de riesgos de seguridad de la información	Al menos IS.I.OR205 (d) debe ser aplicable. El entorno organizacional puede ser cambiante con el tiempo
IS.I.OR.210	Mitigación de riesgos de seguridad de la información	
IS.I.OR.215	Reporte interno de seguridad de la información	
IS.I.OR.220	Detección de incidentes de seguridad de la información. Medidas de respuesta y recuperación	
IS.I.OR.225	Obligaciones con respecto a los hallazgos notificados por la Autoridad	
IS.I.OR.230	Reporte de incidentes a la Autoridad Competente	
IS.I.OR.235	Gestión de riesgos de actividades contratadas	
IS.I.OR.240	Requisitos adicionales de personal	Al menos IS.I.OR.240 (3) debe ser aplicable. Alguien en la organización debe tener conocimiento de la norma
IS.I.OR.245	Conservación de registros de seguridad de la información	
IS.I.OR.250	Manual de Gestión de la Seguridad de la Información (ISMM)	
IS.I.OR.255	Aprobación de cambios	
IS.I.OR.260	Mejora continua	

3.6. Flujo de trabajo



3.7. Validez de la aprobación y vigilancia continuada

La derogación se otorgará con una duración ilimitada. Conservará su validez siempre y cuando se sigan cumpliendo con los criterios y condiciones por los que se otorgó y no se renuncie a ella o haya sido revocada.

La organización deberá monitorizar e informar a AESA de los cambios que puedan producirse en su Evaluación Documentada de los Riesgos para la Seguridad de la Información y/o en el alcance de sus operaciones.

El cumplimiento con los criterios y condiciones por los que se otorgaron la derogación serán revisados por AESA en el marco de los Planes de Vigilancia Continuada aplicables a la organización.

4. FORMATOS Y REGISTROS

- DSA-SG-P01-F11 Ed.01 Resolución aprobación derogación.
- DSA-SG-P01-F10 Ed.01 Solicitud derogación