Agencia Estatal
de Seguridad Aérea

Guía de aplicación
PARTE-IS

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 del documento

FORMATOS	
CÓDIGO del FORMATO	**TÍTULO**
FOR-ATO-DT02-F01	SOLICITUD DEROGACIÓN PART IS
FOR-ATO-DT02-F02	FORMULARIO DE ANÁLISIS DE RIESGOS

REFERENCIAS	
CÓDIGO	**TÍTULO**
REGLAMENTO (UE) 2018/1139	REGLAMENTO (UE) 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) Nº 2111/2005, (CE) Nº 1008/2008, (UE) Nº 996/2010, (CE) Nº 376/2014 Y LAS DIRECTIVAS 2014/30/UE Y 2014/53/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y SE DEROGAN LOS REGLAMENTOS (CE) Nº 552/2004 Y (CE) Nº 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y EL REGLAMENTO (CEE) Nº 3922/91 DEL CONSEJO.
REGLAMENTO (UE) Nº 1178/2011	REGLAMENTO (UE) Nº 1178/2011 DE LA COMISIÓN, DE 3 DE NOVIEMBRE DE 2011, POR EL QUE SE ESTABLECEN REQUISITOS TÉCNICOS Y PROCEDIMIENTOS ADMINISTRATIVOS RELACIONADOS CON EL PERSONAL DE VUELO DE LA AVIACIÓN CIVIL EN VIRTUD DEL REGLAMENTO (CE) NºO 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.
REGLAMENTOS (UE) N.º 2022/1645	REGLAMENTOS (UE) N.º 2022/1645 DE LA COMISIÓN DE 14 DE JULIO 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) 748/2012 Y (UE) 139/2014 DE LA COMISIÓN, Y POR EL QUE SE MODIFICAN LOS REGLAMENTOS (UE) 748/2012 Y (UE) 139/2014 DE LA COMISIÓN.
REGLAMENTO DE EJECUCIÓN (UE) 2023/203	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 REGLAMENTO (UE) 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 748/2012 (UE) 1178/2011, (UE) 2015/340 DE LA COMISIÓN Y EN LOS REGLAMENTOS DE EJECUCIÓN (UE) 2017/373, (UE) 139/2014 Y (UE) 2021/664 DE LA COMISIÓN, Y POR EL QUE SE MODIFICAN LOS REGLAMENTOS (UE) 1178/2011, (UE) 748/2012, (UE) 2015/340 DE LA COMISIÓN Y LOS REGLAMENTOS DE EJECUCIÓN (UE) 2017/373 Y (UE) 2021/664 DE LA COMISIÓN.
REGLAMENTO (UE) N.º 376/2014	REGLAMENTO (UE) N.º 376/2014 ESTABLECE NORMAS PARA LA NOTIFICACIÓN DE SUCESOS EN LA AVIACIÓN CIVIL, CON EL OBJETIVO DE MEJORAR LA SEGURIDAD AÉREA MEDIANTE LA RECOPILACIÓN Y ANÁLISIS DE INFORMACIÓN SOBRE INCIDENTES.

REFERENCIAS	
CÓDIGO	**TÍTULO**
REGLAMENTO DELEGADO (UE) 2022/1645	REGLAMENTO DELEGADO (UE) 2022/1645 DE LA COMISIÓN DE 14 DE JULIO 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 748/2012 Y (UE) N.O 139/2014 DE LA COMISIÓN, Y POR EL QUE SE MODIFICAN LOS REGLAMENTOS (UE) N.O 748/2012 Y (UE) N.O 139/2014 DE LA COMISIÓN.
REGLAMENTO (UE) 2016/1191	REGLAMENTO (UE) 2016/1191 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 6 DE JULIO DE 2016, POR EL QUE SE FACILITA LA LIBRE CIRCULACIÓN DE LOS CIUDADANOS SIMPLIFICANDO LOS REQUISITOS DE PRESENTACIÓN DE DETERMINADOS DOCUMENTOS PÚBLICOS EN LA UNIÓN EUROPEA Y POR EL QUE SE MODIFICA EL REGLAMENTO (UE) N.° 1024/2012.
REGLAMENTO (UE) NO 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 EN VIRTUD DEL REGLAMENTO (CE) NO 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.
LEY 39/2015	LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS.
LEY 21/2003	LEY 21/2003, DE SEGURIDAD AÉREA.
LEY ORGÁNICA 3/2018	LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.
REAL DECRETO 98/2009	REAL DECRETO 98/2009, DE 6 DE FEBRERO, POR EL QUE SE APRUEBA EL REGLAMENTO DE INSPECCIÓN AERONÁUTICA.

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
AESA	AGENCIA ESTATAL DE SEGURIDAD AÉREA
AMC	MEDIO ACEPTABLE DE CUMPLIMIENTO
ATO	ORGANIZACIÓN DE ENTRENAMIENTO APROBADO
CAMO	ORGANIZACIONES DE GESTIÓN DEL MANTENIMIENTO DE AERONAVEGABILIDAD
CRP	PERSONA RESPONSABLE COMÚN
CSIRT	EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA
DR	DIRECTOR RESPONSABLE
FFS	SIMULADOR DE VUELO
FNPT	ENTRENADOR DE PROCEDIMIENTOS DE VUELO Y NAVEGACIÓN
FSTD	DISPOSITIVO DE SIMULACIÓN DE VUELO PARA ENTRENAMIENTO
FTD	EQUIPO DE INSTRUCCIÓN DE VUELO
GM	MATERIAL DE GUÍA
IFR	REGLAS DEL VUELO INSTRUMENTAL
ISMS	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
IT	TECNOLOGÍA DE LA INFORMACIÓN (IT)
MOPSC	CONFIGURACIÓN MÁXIMA OPERATIVA DE ASIENTOS DE PASAJEROS
MSGSI	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
OT	TECNOLOGÍA OPERATIVA
POA	ORGANIZACIONES DE PRODUCCIÓN

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
RC	RESPONSABLE DE CALIDAD
RCC	RESPONSABLE DE CONTROL DEL CUMPLIMIENTO
RSI	RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN
SGSI	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
SOC	CENTROS DE OPERACIONES SEGURAS
TIC	TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN
UE	UNIÓN EUROPEA
VFR	REGLAS DE VUELO VISUAL

ÍNDICE

1. OBJETO Y ALCANCE 7

2. DEFINICIONES 8

3. APLICABILIDAD REGLAMENTO DE EJECUCIÓN (UE) 2023/203 DE LA COMISIÓN, DE 27 DE OCTUBRE DE 2022, PART-IS 8

3.1. Organizaciones a las que no le aplica la Parte IS 9

3.2. Organizaciones susceptibles de derogación 9

3.3. Organizaciones obligadas al cumplimiento 11

4. PROCEDIMIENTO DE DEROGACIONES A LA PARTE IS 11

4.1. Evaluación Documentada de los Riesgos para la Seguridad de la Información 12

4.2. Personal de la organización relacionado con la Seguridad de la Información 13

4.3. La derogación se otorgará con una duración ilimitada. 13

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 14

5.1. Implementación y mantenimiento del SGSI 14

5.2. Pilares de un sistema de gestión 15

5.2.1. Política y objetivos de seguridad 15
5.2.2. Gestión de riesgos de seguridad 16
5.2.3. Aseguramiento de la seguridad 16
5.2.4. Promoción de la seguridad 16

6. ESTRUCTURA DEL MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MSGSI) 17

6.1. Generalidades 17

6.2. Política y objetivos de seguridad 20

6.2.1. Naturaleza y complejidad. 20
6.2.2. Alcance 21
6.2.3. Compromiso de la dirección 21
6.2.4. Rendición de cuentas y responsabilidades de seguridad. Designación del personal clave 23
6.2.5. Documentación del SGSI 28

6.3. Gestión de riesgos de seguridad 28

6.3.1. Identificación de peligros 28
6.3.2. Evaluación y mitigación de riesgos de seguridad 29

6.4. Aseguramiento de la seguridad de la información 31

6.4.1. Observación y medición del rendimiento en materia de seguridad de la información 31
6.4.2. Gestión del cambio 33
6.4.3. Mejora continua del SGSI. Supervisión y revisión de la efectividad del sistema de gestión de seguridad de la información 33

6.5. Promoción de la seguridad 34

6.5.1. Instrucción y educación 34
6.5.2. Comunicación de la seguridad de la información 35

6.6. Responsabilidades de cumplimiento de seguridad de la información y función de control del cumplimiento de seguridad de la información 35

6.6.1. Función de control del cumplimiento de seguridad de la información 36
6.6.2. Programa de cumplimiento de seguridad de la información 37
6.6.3. Seguimiento de incidencias/no conformidades con la autoridad 37
6.6.4. Reacción inmediata ante un problema de seguridad 37
6.6.5. Medios de cumplimiento 38

6.7. Gestión de actividades y/o servicios contratados a otras organizaciones 38

7. CAMBIOS RELEVANTES DE ESTA EDICIÓN 40

1. OBJETO Y ALCANCE

El objeto de esta guía es establecer las pautas para la elaboración del Manual del Sistema de Gestión de Seguridad de la Información (en adelante, MSGSI) de una organización, según se dispone en los Reglamentos (UE) n.º 2022/1645 de la Comisión de 14 de julio 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) 748/2012 y (UE) 139/2014 de la Comisión, y por el que se modifican los Reglamentos (UE) 748/2012 y (UE) 139/2014 de la Comisión y el 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 Reglamento (UE) 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 748/2012 (UE) 1178/2011, (UE) 2015/340 de la Comisión y en los Reglamentos de Ejecución (UE) 2017/373, (UE) 139/2014 y (UE) 2021/664 de la Comisión, y por el que se modifican los Reglamentos (UE) 1178/2011, (UE) 748/2012, (UE) 2015/340 de la Comisión y los Reglamentos de Ejecución (UE) 2017/373 y (UE) 2021/664 de la Comisión.

Según los puntos normativos IS.I/D.OR.200 la organización deberá establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información que garantice que la organización:

1. Establece una política en materia de seguridad de la información que determina los principios generales de la organización con respecto a las posibles repercusiones de los riesgos relacionados con la seguridad de la información sobre la seguridad aérea;
2. Detecta y revisa los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.I/D.OR.205;
3. Define y aplica medidas de tratamiento de los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.I/D.OR.210;
4. Implanta un sistema interno de notificación en materia de seguridad de la información de conformidad con el punto IS.I/D.OR.215;
5. Define y aplica, de conformidad con el punto IS.I/D.OR.220, las medidas necesarias para detectar eventos de seguridad de la información, determina cuáles de ellos se consideran incidentes con posibles repercusiones sobre la seguridad aérea —salvo lo permitido en el punto IS.I/D.OR.205, letra e)— y responde a dichos incidentes de seguridad de la información y se recupera de ellos;
6. Aplica 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;
7. Toma las medidas adecuadas, de conformidad con el punto IS.I/D.OR.225, para abordar las incidencias notificadas por la autoridad competente;
8. Aplica un sistema externo de notificación de conformidad con el punto IS.I/D.OR.230 a fin de que la autoridad competente pueda adoptar las medidas adecuadas;

9. Cumple los requisitos del punto IS.I/D.OR.235 cuando contrata alguna parte de las actividades mencionadas en el punto IS.I/D.OR.200 a otras organizaciones;
10. Cumple los requisitos relativos al personal establecidos en el punto IS.I/D.OR.240;
11. Cumple los requisitos de conservación de registros establecidos en el punto IS.I/D.OR.245;
12. supervisa el cumplimiento de los requisitos del presente Reglamento por parte de la organización y proporciona información sobre las incidencias al gestor responsable, a fin de garantizar la aplicación efectiva de las medidas correctoras;
13. protege, 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.

Para establecer procesos y procedimientos, así como roles y responsabilidades, el Sistema de Gestión de Seguridad de la Información deberá ajustarse a (incluido cuando cambie durante el tiempo):

- La naturaleza y complejidad de sus actividades, sobre la base de una evaluación de los riesgos relacionados con la seguridad de la información inherentes a dichas actividades, tanto por su propia exposición al riesgo como los riesgos que puedan estar planteando para otras organizaciones.
- Sus necesidades y objetivos de seguridad de la información.
- Los requisitos de seguridad de la información.
- Estructura y tamaño de la organización.
- La necesidad de armonización con otros procesos de gestión ya existentes.

2. DEFINICIONES

Serán de aplicación los conceptos incluidos en las referencias normativas contempladas en el apartado REFERENCIAS de este documento.

3. APLICABILIDAD REGLAMENTO DE EJECUCIÓN (UE) 2023/203 DE LA COMISIÓN, DE 27 DE OCTUBRE DE 2022, PART-IS

Organización	Aplica RG 2023/203	Características	Aplicación Part-IS	Ver capítulo de esta guía
ATO / Operador FSTD	NO	-	Exento	N/A
ATO / Operador FSTD	SI	Cumple condiciones 2.1	Exento	N/A
ATO / Operador FSTD	SI	Cumple condiciones 2.2	Puede solicitar derogación	Parte 3
ATO / Operador FSTD	SI	2.3 No cumple condiciones 2.1 No cumple condiciones 2.2	SI	Parte 4

NOTA: Si en una organización existen varios ámbitos (aprobaciones) y en una de ellas es de obligado cumplimiento la PART-IS, no sería aplicable la derogación y la normativa aplicaría a toda la organización.

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 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.
- ATO / Operador FSTD que operen simuladores de vuelo de nivel de calificación (FNPT I y II).

3.2. Organizaciones susceptibles de derogación

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.

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:

- **Tipos de aeronaves.**
  - Aeronaves NO complejas por peso, 5700 kg(A) y 3175 Kg (H)
  - Aeronaves monomotor
  - ATOs que no tengan aeronaves o simuladores en propiedad y lo tengan subcontratado a un operador que cumpla con la Part-IS.

- **Tipo de formación.**
  - IFR de formación.
  - VFR diurno y nocturno.
  - ATOs cuya parte de vuelo se lleve a cabo en un proveedor que cumpla con la PART-IS.
  - ATO / Operador FSTD que operen simuladores de vuelo de nivel de calificación (FNPT II MCC, FTD y FFS).
- **Características organizativas y de alcance de la operación realizada.**
  - Registro de Entrenamiento: Uso predominante de registros en papel o sistemas digitales locales (hojas de cálculo simples en ordenadores no conectados en red corporativa compleja).
  - No se cuenta con proveedores que deban cumplir con Parte IS.
  - La actividad transfronteriza no existe o es marginal.
  - Estructura de gestión simplificada (p.ej., un único Responsable de Seguridad que asume múltiples roles compatibles).
  - ATOs que no dispongan de aeronaves en propio.
  - Número reducido y controlado de usuarios con acceso a la información sensible (expedientes, calificaciones, licencias). La ATO /Operador FSTD debe disponer de un sistema de control de accesos y permisos a la información sensible.

- No existen accesos remotos sistemáticos a los sistemas de la ATO/Operador FSTD (VPN, escritorios remotos, conexiones desde múltiples localizaciones)

Las organizaciones cuya actividad se desarrolle **al menos bajo un criterio por cada área** del anterior listado, 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. Organizaciones obligadas al cumplimiento

Por otro lado, más allá de las excepciones y derogaciones mencionadas anteriormente el cumplimiento del Reglamento (UE) 2023/203 es de obligado cumplimiento para todas aquellas organizaciones que desempeñan roles críticos en la cadena de seguridad de la aviación civil. El objetivo es garantizar que sus sistemas de información y datos estén protegidos contra amenazas que puedan comprometer la seguridad operacional (*safety*).

Teniendo en cuenta el punto IS.I.OR.100 del Reglamento (UE) 2023/203 las organizaciones que deben implementar los requisitos de seguridad de la información son entre otras:

- Organizaciones de Formación (ATO): Centros de formación aprobados que operen bajo el Reglamento (UE) nº 1178/2011 y que no cumplan los criterios de derogación del punto 4.2.

4. PROCEDIMIENTO DE DEROGACIONES A LA PARTE IS

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.

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.

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

- El formato de solicitud de derogación en el que se especifiquen los escenarios operativos y se incorpore la información relevante de la organización. Puede encontrar el formulario de solicitud de derogación FOR-ATO-DT01-F01, en la sección web de AESA **Organización de Entrenamiento Aprobada ATO**
-
- El operador de simuladores o la ATO deberá adjuntar un **Análisis de Riesgos específico** que justifique la viabilidad de la derogación solicitada. Puede encontrar el formulario de análisis de riesgos FOR-ATO-DT01-F02, en la sección web de AESA **Organización de Entrenamiento Aprobada ATO**

La derogación podrá ser solicitada por aquellos Operadores de FSTD y ATOs a los que les aplique el Reglamento 2023/203.

4.1. 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 todas las áreas.

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.
3. Identificar a continuación las diferentes amenazas presentes, caracterizando el escenario de la organización en los siguientes aspectos: o Fuentes de amenazas de seguridad de la información.

o Vectores de ataque y camino a través de la organización hasta el activo amenazado.

o Controles de seguridad de la información que podrían mitigar el ataque (posibles barreras).

o 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:
o Se deberá asignar un nivel de riesgo conforme a la clasificación establecida por la organización.

o Cada riesgo se deberá relacionar con su correspondiente elemento/categoría (interfaz con otra organización, área de la operación, etc).

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.

4.2. 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 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.

4.3. 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.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Un sistema de gestión de la seguridad de la información (SGSI) es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente el estado de la seguridad de la información de una organización. Su objetivo es proteger los **activos de información**, de modo que los objetivos operativos y de seguridad de una organización puedan alcanzarse de forma eficaz, eficiente y con una consciencia de los riesgos.

En términos generales, un SGSI establece un proceso de gestión de riesgos de seguridad de la información, basado en los resultados de los análisis de impacto de la seguridad de la información, que básicamente determinan su alcance. Si las violaciones de la seguridad de la información pueden causar o contribuir a consecuencias para la seguridad de la aviación, los requisitos de seguridad de la información deben limitar su impacto a niveles de seguridad de la aviación que se consideren aceptables. Por lo tanto, todas las funciones, procesos o sistemas de información que puedan causar o contribuir a las consecuencias para la seguridad aérea entran en el ámbito de aplicación del Reglamento (UE) 2023/203 y Reglamento (UE) 2022/1645. El SGSI proporciona los medios para decidir sobre los controles de seguridad de la información necesarios para todas las capas arquitectónicas (gobernanza, negocio, aplicaciones, tecnología, datos) y dominios (organizativos, humanos, físicos, técnicos). Además, permite gestionar la selección, implementación y operación de controles de seguridad de la información. Por último, permite gestionar la gobernanza, la gestión de riesgos y el cumplimiento dentro del ámbito del SGSI.

5.1. Implementación y mantenimiento del SGSI

El SGSI debe integrarse con los procesos y la estructura de gestión general de la organización o incluso, al menos parcialmente, con salvaguardas para su integridad respectiva **y, según sea razonablemente aplicable, con un sistema de gestión global que comprenda la seguridad de la información, la seguridad de la aviación y la gestión de la calidad**.

La ilustración 2 ofrece una descripción de alto nivel de los aspectos que son más destacados en la fase de implementación y los que caracterizan la fase operativa, así como la revisión y la posible mejora, si las funciones no funcionan según lo previsto.

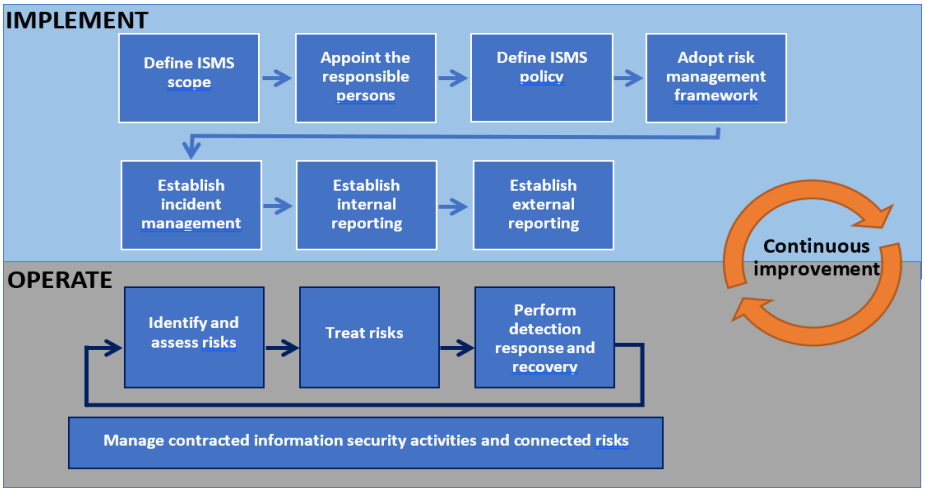


Ilustración 2. Representación de los requisitos de la Parte-IS desde la perspectiva del ciclo de vida de un SGSI.

En este proceso de implementación y mantenimiento del SGSI es importante tener en cuenta que:

- **AESA aprobará la edición inicial del MSGSI y conservará una copia**. El MSGSI se modificará por la organización 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 MSGSI.

- **Las modificaciones del MSGSI se gestionarán mediante un procedimiento establecido por la organización**. Este procedimiento incluirá las modificaciones no sujetas a aprobación por parte de AESA. 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/D.OR.255, letra b), serán aprobadas por la autoridad competente.

- **La organización podrá integrar el MGSI con otros 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**.

5.2. Pilares de un sistema de gestión

Un Sistema de Gestión de Seguridad de la Información es un Sistema de Gestión y, por tanto, su marco está integrado por los siguientes cuatro componentes:

5.2.1. Política y objetivos de seguridad

El compromiso y el liderazgo desde la Dirección en materia de seguridad son fundamentales para la implementación de un SGSI eficaz, y se afirman mediante la política de seguridad de la información y el establecimiento de objetivos en la materia. El compromiso de la Dirección respecto de la

seguridad se demuestra mediante la toma de decisiones y la asignación de recursos; estas decisiones y medidas deberían ser siempre coherentes con la política y objetivos de seguridad de la información a efectos de desarrollar una cultura de seguridad positiva.

La política de seguridad de la información debería ser desarrollada y apoyada por la Dirección y llevar la firma de, al menos, el Director Responsable (DR) o Persona Responsable Común (CRP)[1], único para el Sistema de Gestión. El personal clave de seguridad y, cuando corresponda, los órganos representativos del personal (foros de empleados, sindicatos) deberían consultarse para la elaboración de una política de seguridad de la información y sus objetivos a efectos de promover un sentido de responsabilidad compartida.

5.2.2. Gestión de riesgos de seguridad

El proceso de gestión de riesgos identifica sistemáticamente los peligros que existen en el contexto de la entrega de los productos o servicios de la organización. Puede que los peligros sean resultado de los sistemas que son deficientes en su diseño, función técnica, interfaz humana o interacciones con otros procesos y sistemas. También pueden resultar de una falla de los procesos o sistemas existentes para adaptar los cambios en el entorno de operación del proveedor de servicios. A menudo, un análisis cuidadoso de estos factores puede identificar posibles peligros en cualquier punto de la operación o del ciclo de vida de la actividad.

Se pueden descubrir peligros durante el ciclo de vida operacional a partir de fuentes internas y externas. Deberán revisarse continuamente las evaluaciones y mitigaciones de riesgos de seguridad de la información para asegurar que permanecen vigentes.

5.2.3. Aseguramiento de la seguridad

El aseguramiento de la seguridad consta de procesos y actividades realizadas por la organización para determinar si el SGSI funciona de acuerdo con las expectativas y los requisitos. Esto involucra la observación continua de sus procesos internos, así como su entorno de operación para detectar cambios o desviaciones que puedan introducir riesgos de seguridad emergentes o el deterioro de los controles de riesgos existentes. Dichos cambios o desviaciones pueden entonces abordarse mediante el proceso de gestión de riesgos.

Las actividades de aseguramiento de la seguridad deberían incluir el desarrollo e implementación de las medidas adoptadas en respuesta a los problemas identificados con posibles consecuencias para la seguridad. Estas acciones mejoran continuamente el rendimiento del SGSI de la organización.

5.2.4. Promoción de la seguridad

La promoción de la seguridad alienta una cultura de seguridad positiva y contribuye a alcanzar los objetivos de seguridad del proveedor de servicios mediante la combinación de competencias técnicas que mejoran continuamente con la instrucción y la educación, la comunicación eficaz y la

[1] Entiéndase según aplique reglamentariamente la definición de Director Responsable (DR), Persona Responsable Común (CRP) o Gerente Responsable (GR).

distribución de información. La dirección proporciona el liderazgo para promover la cultura de seguridad en toda la organización.

La gestión eficaz de la seguridad no puede lograrse solamente siguiendo una orden o una adherencia estricta a las políticas y procedimientos. La promoción de la seguridad afecta el comportamiento tanto individual como institucional y complementa las políticas, procedimientos y procesos de la organización, proporcionando un sistema de valores que respalda las actividades de seguridad.

La organización debería establecer e implementar procesos y procedimientos que faciliten la comunicación eficaz en ambos sentidos a través de todos los niveles. Esto debería comprender una clara dirección estratégica desde los estratos más altos de la organización y la habilitación de la comunicación "jerárquica ascendente" que fomenta los comentarios abiertos y constructivos de todo el personal.

6. ESTRUCTURA DEL MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MSGSI)

6.1. Generalidades

La organización describirá su Sistema de Gestión de Seguridad de la Información, el cual deberá abarcar los ámbitos recogidos en ORO.GEN.200A y/o IS.I/D.OR.200, según aplique, detallados a continuación, y ser coherente con el tamaño de la organización y la naturaleza y complejidad de sus actividades.

El sistema de gestión de seguridad de la información de la organización debe abarcar todas las actividades realizadas por ella en virtud de sus aprobaciones, tanto si las realiza con personal propio o contratadas a otras organizaciones o entidades.

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES
1. Política y Objetivos de Seguridad	Política de Seguridad
	Política de Cultura Justa
	Programa o Plan de Seguridad de la Organización
	Sistema de Notificación de sucesos/eventos
	Organigrama de la organización
	Procedimiento de Rendición de cuentas y funciones y responsabilidades del DR y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización
	Plan de respuesta ante Emergencias
	Procedimiento para gestionar la documentación y registro del sistema de gestión.
2. Gestión de riesgos de seguridad	Procedimiento para la identificación de peligros.
	Procedimiento/Método de evaluación y mitigación del riesgo.
	Procedimiento de implementación y efectividad de medidas mitigadoras.
	Procedimiento de rendimiento de la seguridad

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES
3. Aseguramiento de la Seguridad	Programa de indicadores de seguridad
	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.
	Procedimiento de Gestión del Cambio
4. Promoción de la Seguridad	Programa de entrenamiento del sistema de gestión (gestión del riesgo y control de conformidad)
	Procedimiento para la promoción de la seguridad
5. Control de conformidad y cumplimiento	Función de control de conformidad
	Programa de auditoría e inspecciones
	Procedimiento de seguimiento de no conformidades de la Autoridad
	Procedimiento de reacción inmediata ante un problema de seguridad.
	Procedimiento para medios alternativos de cumplimiento (AltMoc).
6. Gestión de actividades contratadas a otras organizaciones	Procedimiento para la gestión de servicios y/o actividades contratadas a otras organizaciones.

En la tabla siguiente se recogen los procedimientos y programas a desarrollar por la organización en relación con el sistema de gestión de seguridad de la información.

	MSG	MSGSI	
PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
1. Política y Objetivos de Seguridad	Política de Seguridad	Política de Seguridad de la Información	IS.I/D.OR.200(a)(1) IS.I.D.OR.250(a)(1), (a)(4)
	Política de Cultura Justa	Política de Cultura Justa	IS.I/D.OR.200(a)(1) IS.I/D.OR.200(a)(13)
	Programa o Plan de Seguridad de la Organización	Programa o Plan de Seguridad de la Organización	IS.I/D.OR.200 (a)(1);(a)(2); (a)(3) IS.I/D.205 (a)(b)(c) IS.I/D.OR.210 IS.I/D.OR.220 IS.I/D.OR.250 (a)(4)
	Sistema de Notificación de sucesos/eventos	Sistema de Notificación de sucesos/eventos	Reg. 376/2014 Art.4, Art.5, Art.13, Art.16 IS.I/D.OR.200 (a)(4) IS.I/D.OR.215 IS.I/D.OR.250(a)(8) IS.I/D.OR.200 (a)(8) IS.I/D.OR.230 IS.I/D.OR.220(a)
	Organigrama de la organización	Organigrama de la organización	IS.I/D.OR.250(a)(7) IS.I/D.OR.200(d)

	MSG	MSGSI	
PROCESO	**POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES**	**POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES**	**REQUISITO NORMATIVO**
	Procedimiento de Rendición de cuentas y funciones y responsabilidades del DR y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización	Procedimiento de rendición de cuentas y funciones del DR/CRP y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización e incluyendo la identidad y la fiabilidad del personal que tenga acceso a los sistemas de información y a los datos.	IS.I/D.OR.200(a)(10) IS.I/D.OR.240 IS.I/D.OR.200(d) IS.I./D.OR.250(a)(9) IS.I/OR.250(a)(2), (a)(3), (a)(5), (a)(6),
	Plan de respuesta ante Emergencias	Plan de respuesta ante Emergencias	IS.I/D.OR.220(c)
	Procedimiento para gestionar la documentación y registro del sistema de gestión de seguridad de la información.	Procedimiento para gestionar la documentación y registro del sistema de gestión de seguridad de la información.	IS.I/D.OR.200(a)(11) IS.I/D.OR.245 IS.I/D.OR.200(c) IS.I./D.OR.250(a)(9) IS.I/D.OR.200(d)
2. Gestión de riesgos de seguridad	Procedimiento para la identificación de peligros.	Procedimiento para la identificación de peligros.	IS.I/D.OR.200 (a)(2) IS.I/D.205 (a)(b) IS.I/D.OR.200(c)(d) IS.I./D.OR.250(a)(9)
	Procedimiento/Método de evaluación y mitigación del riesgo.	Procedimiento/Método de evaluación y mitigación del riesgo.	IS.I/D.OR.200 (a)(2) IS.I/D.205 (c)(d) IS.I/D.OR.200(c)(d) IS.I./D.OR.250(a)(9) IS.I/D.OR.210(a) IS.I/D.OR.220
3. Aseguramiento de la Seguridad	Procedimiento de implementación y efectividad de medidas mitigadoras.	Procedimiento de implementación y efectividad de medidas mitigadoras.	IS.I/D.OR.200 (a)(3); (a)(5) IS.I/D.OR.210 (a)(b) IS.I/D.OR.220 IS.I/D.OR.200(c)(d) IS.I./D.OR.250(a)(9)
	Procedimiento de rendimiento de la seguridad operacional	Procedimiento de rendimiento de la seguridad operacional	IS.OR.200(a)(1) ;(b) IS.I./D.OR.250(a)(9) IS.I./D.OR.260
	Programa de indicadores de seguridad operacional	Programa de indicadores de seguridad operacional	IS.I/D.OR.200(a)(2) IS.I/D.OR.200(d) IS.I/D.OR.205
	Procedimiento de Gestión del Cambio	Procedimientos de Gestión del Cambio	IS.I/D.200 (c) IS.I/D.OR.255 IS.I./D.OR.250(a)(9) IS.I/D.OR.250(c)

	MSG	MSGSI	
PROCESO	**POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES**	**POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES**	**REQUISITO NORMATIVO**
	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	IS.I/D.OR.200(b) IS.I./D.OR.250(a)(9) IS.I/D.OR.260
4. Promoción de la Seguridad	Programa de entrenamiento del sistema de gestión (gestión del riesgo y control de conformidad/calidad)	Programa de entrenamiento del sistema de gestión de seguridad de la información	IS.I/D.OR.200 (a)(10) IS.I/D.OR.240 (g)
	Procedimiento para la promoción de la seguridad	Procedimiento para la promoción de la seguridad	AMC1 IS.I/D.OR.200 (a)(1); (h) IS.I./D.OR.250(a)(9)
5. Control de conformidad y cumplimiento	Función de control de conformidad	Función de control de conformidad	IS.I/D.OR.200(a)(12) IS.I/D.OR.200(d) IS.I./D.OR.250(a)(9)
	Programa de auditoría e inspecciones	Programa de auditoría e inspecciones	IS.I/D.OR.200(a)(12) IS.I/D.OR.200(c)(d) IS.I./D.OR.250(a)(9)
	Procedimiento de seguimiento de no conformidades con la Autoridad	Procedimiento de seguimiento de no conformidades con la Autoridad	IS.I/D.OR.200 (a)(7) IS.I/OR/225 IS.I/D.OR.200(c)(d) IS.I./D.OR.250(a)(9)
	Procedimiento de reacción inmediata ante un problema de seguridad.	Procedimiento de reacción inmediata ante un problema de seguridad de la información.	IS.I/D.OR.200 (a)(6) IS.I/D.OR.200(d) IS.I/D.OR.220 (b) IS.I./D.OR.250(a)(9)
	Procedimiento para medios de cumplimiento.	Procedimiento para medios de cumplimiento.	IS.I/D.OR.250(a)(10) IS.I./D.OR.250(a)(9)
6. Gestión de actividades contratadas a otras organizaciones	Procedimiento para la gestión de servicios y/o actividades contratadas y/o subcontratadas a otras organizaciones.	Procedimiento para la gestión de actividades contratadas a otras organizaciones.	IS.I/D.OR.200 (a)(9) IS.I/D.OR.235 IS.I/D.OR.200(c)(d) IS.I./D.OR.250(a)(9) IS.I/D.OR.215 (c)(d)

6.2. Política y objetivos de seguridad

6.2.1. Naturaleza y complejidad.

Los procesos, procedimientos, roles y responsabilidades establecidos por la organización deberán corresponder a la naturaleza y complejidad de sus actividades, basándose en una evaluación de

los riesgos de seguridad de la información inherentes a esas actividades, y pueden integrarse dentro de otros sistemas de gestión existentes ya implementados por la organización.

6.2.2. Alcance

Se definirá y documentará el alcance del Sistema de Gestión de Seguridad de la Información determinando actividades, procesos, sistemas de soporte, e identificando cuáles de ellos pueden repercutir en impactos a la seguridad operacional.

El alcance (por ejemplo, servicios, sistemas, activos, procesos, interfaces y perímetro) del MSGSI se debe definir con justificaciones adecuadas del resultado y cualquier exclusión.

6.2.3. Compromiso de la dirección

6.2.3.1. Política de seguridad

La declaración firmada por el Director Responsable debe confirmar que la organización trabajará en todo momento de conformidad con el anexo Parte IS.I/D (según aplique) y con el MSGSI; si el Director Responsable no es el Director Ejecutivo (consejero delegado) de la organización, este deberá refrendar la declaración.

La organización puede optar por documentar la política en documentos separados, pero debe dirigir sus propias actividades de seguridad de la información. En este caso, debe asegurarse de que el manual contenga referencias adecuadas a cualquier documento que se mantenga por separado. Cualquier documento de este tipo debe considerarse una parte integral del manual del sistema de gestión de seguridad de la información de la organización.

La política incluirá los siguientes aspectos con un impacto potencial en la seguridad operacional:

- Debe comprometerse a cumplir con la legislación aplicable, considerar las normas pertinentes y las mejores prácticas;
- Debe establecer objetivos y medidas de rendimiento para la gestión de la seguridad de la información;
- Debe definir principios generales, actividades y procesos para que la organización proteja adecuadamente los sistemas y datos de las tecnologías de la información y la comunicación;
- Debe comprometerse a aplicar los requisitos del SGSI en los procesos de la organización;
- Debe comprometerse a mejorar continuamente hacia niveles más altos de madurez de los procesos de seguridad de la información;
- Debe comprometerse a cumplir con los requisitos aplicables en materia de seguridad de la información y su gestión proactiva y sistemática y a proporcionar los recursos adecuados para su implementación y operación;
- Debe asignar la seguridad de la información como una de las responsabilidades esenciales de todo el personal clave;

- Debe comprometerse a promover la política de seguridad de la información a través de sesiones de formación o concienciación dentro de la organización para todo el personal de forma periódica o previos cambios;
- Debe fomentar la «cultura justa» y la notificación de vulnerabilidades, sucesos sospechosos/anómalos y/o incidentes de seguridad de la información;
- Debe comprometerse a comunicar la política de seguridad de la información a todas las partes relevantes, según corresponda.

6.2.3.2. Política de cultura justa

Se definirá una política de Cultura Justa y los principios que identifican claramente los comportamientos aceptables e inaceptables para promoverla.

La aplicación de la política de cultura justa y la notificación de vulnerabilidades, sucesos sospechosos/anómalos y/o incidentes de seguridad de la información debe ser fomentada, entre otros, a través de su inclusión en la política de seguridad de la información.

Se garantizará que protege, sin perjuicio de los requisitos aplicables de notificación de incidentes, la confidencialidad de cualquier información que la organización pueda haber recibido de otras organizaciones, de acuerdo con su nivel de sensibilidad. Por tanto, la organización debe implementar y mantener controles de seguridad de la información que sean lo suficientemente robustos y efectivos para proteger la información y garantizar el principio de necesidad de saber (es decir, limitar el acceso a la información solo a aquellos que la necesitan para realizar sus funciones). Debe proteger la fuente de información de conformidad con las disposiciones pertinentes establecidas en el Reglamento (UE) 2018/1139. También debe cumplir lo dispuesto en el Reglamento (UE) n.º 376/2014.

6.2.3.3. Programa o plan de seguridad

Se establecerá un procedimiento para establecer los objetivos de seguridad de la información que sean consistentes con la política de seguridad de seguridad de la información y se definirán los medios para comunicarlos en toda la organización.

Los objetivos de seguridad de la información y las actuaciones asociadas deberán recogerse en un Programa o Plan de Seguridad de Seguridad de la Información de la organización.

Debe establecer los objetivos estratégicos y tácticos más importantes, los objetivos generales de seguridad de la información, o una especificación de un marco (quién, cómo) para establecer los objetivos de seguridad de la información, y medidas de rendimiento para la gestión de la seguridad de la información.

6.2.3.4. Sistema de notificación de Sucesos/Eventos en materia de seguridad de la información

6.2.3.4.1. Sistema Interno de Notificación:

La organización integrará en otros sistemas de notificación establecidos o implantará y describirá un sistema interno de notificación confidencial en materia de seguridad de la información que garantice la desidentificación de la fuente y permita la recopilación y evaluación del suceso de

seguridad de la información[3], incluidos los que deben notificarse a la autoridad competente a fin de que se puedan adoptar las medidas adecuadas.

6.2.3.4.2. Sistema Externo de Notificación

Las responsabilidades se definirán complementariamente conforme al IS.I/D.OR.230(b) y al Reglamento (UE) 376/2014 para garantizar el cumplimiento de todos los requisitos en cuanto a categorización y análisis de seguridad requerido a los sucesos.

Estas obligaciones de información podrán cumplirse utilizando un único canal de denuncia.

La organización debe establecer un procedimiento para notificar los sucesos de obligatorios a AESA en materia de seguridad de la información, estos son:

- Cualquier suceso contemplado en el Reglamento (UE) n.º 376/2014 que tenga su origen en interacciones electrónicas intencionadas no autorizadas;
- Incidentes de seguridad de la información que puedan entrañar un riesgo significativo para la seguridad aérea no contemplados en el Reglamento (UE) n.º 376/2014. Incluidos incidentes que indiquen la posible materialización de riesgos inaceptables y que puedan tener un impacto potencial en la seguridad aérea.
- Vulnerabilidades que plantean un riesgo significativo para la seguridad de la aviación y que aún no se han mitigado adecuadamente de conformidad con una estrategia de gestión de vulnerabilidades aprobada. Incluidas vulnerabilidades que indiquen la posible materialización de riesgos inaceptables y que puedan tener un impacto potencial en la seguridad aérea.

En materia de seguridad de la información, asegurará que la organización presente una notificación tan pronto como sea posible, un informe como máximo en las 72 horas siguientes al momento que se haya tenido conocimiento del suceso, salvo circunstancias excepcionales, y un informe de seguimiento elaborado según definido por AESA tan pronto se determinen las medidas que adopte la organización para recuperarse del incidente y las que propone para evitar incidentes similares a:

- AESA de cualquier incidente o vulnerabilidad que pueda representar un riesgo significativo para la seguridad aérea.
- En su caso, cuando tal incidente o vulnerabilidad afecte a una aeronave o a un sistema o componente asociado, la organización lo notificará también al titular de la aprobación de diseño.
- En su caso, cuando tal incidente o vulnerabilidad afecte a un sistema o componente utilizado por la organización, esta lo notificará a la organización responsable del diseño del sistema o componente.

6.2.4. Rendición de cuentas y responsabilidades de seguridad. Designación del personal clave

Se entiende por obligación de rendición de cuentas (*accountability*) la relativa al logro de los objetivos de seguridad establecidos.

Se entiende por responsabilidad la relativa al cumplimiento con la función asignada.

La organización documentará los roles, responsabilidades, competencias y recursos requeridos para la implementación y operación de un SGSI eficaz y establecerá un proceso para modificar dicha documentación. Los cambios que se produzcan en esos procesos, procedimientos, funciones y responsabilidades se gestionarán de conformidad con lo indicado en los apartados "Documentación del SG" y apartado "Gestión del Cambio".

La rendición de cuentas y responsabilidades de seguridad se corresponderá con la naturaleza y complejidad de sus actividades, basado en la evaluación de riesgos de seguridad de la información inherente a dichas actividades y puede estar integrada en otros Manuales de Gestión de la organización. Estar adaptada al propósito de la organización.

La organización deberá incluir un organigrama recogiendo las líneas de responsabilidad y obligación de rendición de cuentas a través de la organización.

6.2.4.1. Responsable de Seguridad de la Información

En esta sección se designará un Responsable de Seguridad de la Información (RSI) competente, indicando nombre, deberes, obligaciones de rendición de cuentas, responsabilidades y autoridades, que sea la persona de contacto y el responsable del desarrollo, administración y mantenimiento de un SGSI eficaz, con una línea directa de reporte al DR o CRP, por ejemplo, reuniones programadas y regulares. Deberá indicarse, además, el cargo que lo sustituye en caso de ausencia. Este o estos Responsable/s pueden ser conocido como Cybersecurity Risk Manager y/o Cyber Incident Responder. En el caso de organizaciones con varias aprobaciones dentro del ámbito de aplicación del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución que comparten un Sistema de Gestión de Seguridad de la Información conjunto, podrá existir un responsable para cada aprobación, siempre que se designe un "*focal point*" con línea directa de reporte al DR o CRP.

NOTA: En el caso de las organizaciones que hayan conseguido una aprobación de su solicitud de derogación, no tendrán que nominar una persona con el cargo de RSI, sin embargo, la organización:

i. Deberá identificar en este punto una persona o grupo de personas encargadas de asegurar que las condiciones que permitieron la obtención de la derogación se siguen manteniendo.

ii. Esta persona o grupo de personas no serán considerados como personal responsable aceptado por AESA.

iii. Esta persona o grupo de personas deberá poseer los conocimientos necesarios de la *"Part-IS"*, así como conocimiento suficiente para poder evaluar y controlar que las condiciones de la derogación se mantienen dentro de la organización.

El RSI debe demostrar una comprensión completa de los requisitos del Reglamento (UE) 2023/203 o Reglamento (UE) 2022/1645 para poder garantizar que los procesos y normas de la organización reflejen con precisión los requisitos aplicables, y disponer de conocimiento y experiencia previa en seguridad de la información.

El RSI debe reconocer, de manera trazable y verificable, que comprende las funciones asignadas y las responsabilidades de seguridad de la información asociadas.

Las funciones del responsable de seguridad incluyen, entre otras:

- Garantizar que el cumplimiento se gestione de forma proactiva y que se documente y se actúe en consecuencia.
- Gestionar los riesgos relacionados con la ciberseguridad de la organización alineados con la estrategia de la organización.
- Desarrollar, mantener y comunicar los procesos e informes de gestión de riesgos.
- Desarrollar la estrategia de gestión de riesgos de ciberseguridad de una organización, incorporando consideraciones de seguridad, para identificar y evaluar los riesgos que podrían afectar a la seguridad operativa. Esto incluye la evaluación de los posibles riesgos de seguridad derivados de las amenazas cibernéticas y las vulnerabilidades en OT, y la priorización de las opciones de tratamiento de riesgos que aborden eficazmente tanto los riesgos de ciberseguridad como los de seguridad operativa.
- Mantener un inventario de los activos de la organización, teniendo en cuenta los sistemas críticos para la seguridad y sus dependencias. Esto implica identificar y categorizar los activos en función de su impacto en la seguridad para garantizar que se apliquen las medidas de ciberseguridad adecuadas para proteger la integridad y la seguridad operativa de los activos críticos.
- Identificar y evaluar las amenazas y vulnerabilidades relacionadas con la ciberseguridad de los sistemas TIC (IT y OT), centrándose en su posible impacto en la seguridad operativa. Al evaluar las amenazas y vulnerabilidades, tener en cuenta los aspectos críticos para la seguridad, como la funcionalidad del sistema, la integridad y disponibilidad de la información y los datos.
- Identificar el panorama de amenazas, incluidos los perfiles de los adversarios y la estimación del potencial de los ataques.
- Evaluar los riesgos de ciberseguridad y proponer las opciones de tratamiento de riesgos más adecuadas, incluidos los controles de seguridad y la mitigación y prevención de riesgos que mejor aborden la estrategia y los requisitos de seguridad de la organización. Esto implica recomendar controles de seguridad y estrategias de mitigación de riesgos que aborden de manera efectiva los objetivos de ciberseguridad y seguridad operativa, garantizando un enfoque integral de gestión de riesgos.
- Supervisar la eficacia de los controles de ciberseguridad y evaluar continuamente los niveles de riesgo desde una perspectiva de seguridad. Evaluar periódicamente la idoneidad de los controles establecidos para mantener la seguridad operativa, teniendo en cuenta la evolución de las amenazas y vulnerabilidades.
- Garantizar que todos los riesgos de ciberseguridad se mantengan en un nivel aceptable para la organización y sus interfaces, con un enfoque específico en la seguridad operativa. Evaluar y reevaluar continuamente los riesgos para garantizar que los riesgos relacionados con la seguridad estén dentro de límites aceptables y que las medidas de ciberseguridad no comprometan la seguridad operativa.
- Desarrollar, mantener, informar y comunicar el ciclo completo de gestión de riesgos, haciendo hincapié en las implicaciones de seguridad de los riesgos identificados y las opciones de tratamiento de riesgos. Esto incluye proporcionar informes claros y concisos que destaquen los

riesgos de seguridad, la eficacia del control y los esfuerzos continuos para alinear las prácticas de ciberseguridad con los objetivos de seguridad operativa.

- Monitorizar el estado de la ciberseguridad de la organización, gestionar los incidentes durante los ciberataques y asegurar la continuidad del funcionamiento de los sistemas TIC (IT y OT).
- El aspecto de la seguridad es crucial en cualquier Plan de Respuesta a Incidentes. Es esencial priorizar el retorno a un nivel aceptable de seguridad, preservando la integridad de las operaciones y minimizando el daño potencial para todas las personas que puedan verse afectadas por un incidente o situación de emergencia.
- Desarrollar, implementar y evaluar procedimientos relacionados con el manejo de incidentes, con un fuerte enfoque en la seguridad en cada etapa del proceso.
- Identificar, analizar, mitigar y comunicar los incidentes de ciberseguridad que afectan a la seguridad.
- Evaluar y gestionar las vulnerabilidades técnicas con un enfoque orientado a la seguridad. Abordar las vulnerabilidades que puedan plantear riesgos para la seguridad y priorizar la aplicación de parches o la mitigación de esas vulnerabilidades para proteger los sistemas y los usuarios de posibles daños.
- Evaluar la resiliencia de los controles de ciberseguridad y las acciones de mitigación tomadas después de un incidente de ciberseguridad o violación de datos para garantizar que mantengan el nivel de seguridad necesario. Reevaluar los controles desde una perspectiva de seguridad para prevenir futuros incidentes que podrían tener impactos en la seguridad.
- Adoptar y desarrollar técnicas de prueba de manejo de incidentes que simulen escenarios operativos del mundo real, incluidos aquellos que pueden tener impactos en la seguridad. Medir la eficacia de las medidas de seguridad y los procedimientos de respuesta para mejorar continuamente las capacidades de gestión de incidentes.
- Establecer procedimientos para el análisis de los resultados de los incidentes y la presentación de informes sobre el manejo de incidentes, haciendo hincapié en la importancia del impacto de la seguridad y las lecciones aprendidas. Utilizar los datos de incidentes para mejorar la gestión de riesgos de seguridad y garantizar una mejor protección contra posibles incidentes futuros.
- Documentar el análisis de los resultados de los incidentes y las acciones de gestión de incidentes, destacando el impacto en la seguridad y las lecciones aprendidas. Mantener registros detallados para mejorar continuamente las medidas de seguridad y las estrategias de respuesta.
- Cooperar con los Centros de Operaciones Seguras (SOC) y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), priorizando la seguridad como objetivo común. Colaborar para garantizar respuestas oportunas y efectivas a incidentes que puedan tener un impacto en la seguridad.
- Cooperar con el personal clave para la notificación de incidentes de seguridad de acuerdo con el marco legal aplicable, asegurando que los incidentes con posibles implicaciones de seguridad se informen con prontitud y precisión a las autoridades competentes.

La dedicación del RSI debe ser tal que se garantice que la carga de trabajo que genere el mantenimiento y control del sistema sea asumible por este y por su personal de apoyo a través del departamento u oficina de seguridad de la información, considerando:

- Las estructuras organizativas, las políticas, los procesos y los procedimientos sujetos a la gestión de la seguridad de la información.
- El grado de coordinación necesario con otras organizaciones, contratistas y proveedores.
- El nivel de riesgo asociado a las actividades realizadas por la organización.

Con respecto a cualquier rol y tarea asignada, la organización debe especificar todas las responsabilidades de seguridad de la información que tiene un empleado de manera clara y transparente.

6.2.4.2. Identidad y confiabilidad del personal

La organización deberá incluir procedimientos que establezcan adecuadamente la identidad y la confiabilidad del personal que tenga acceso a los sistemas de información y a los datos sujetos a la Parte IS.

- La identidad debe determinarse sobre la base de pruebas documentales.
- Para la confiabilidad la organización debe contar con un proceso documentado y criterios adecuados para garantizar que se pueda confiar en las personas para desempeñar su función.

La confiabilidad puede establecerse, por ejemplo, mediante:

- Antes de la contratación, una verificación de antecedentes realizada de conformidad con las normas aplicables del Derecho de la Unión y nacional. Esta verificación puede incluir la verificación de:
    - Educación, empleo previo y cualquier brecha en los años anteriores.
    - Ausencia de antecedentes penales.

La ausencia de antecedentes penales podrá verificarse mediante un certificado expedido por la autoridad responsable del Estado miembro de conformidad con el Reglamento (UE) 2016/1191.

En el caso de los futuros empleados extranjeros, los controles mencionados pueden llevarse a cabo sobre la base de certificados equivalentes emitidos por el país de origen, como un «certificado de buena conducta».

    - Cualquier otra información o inteligencia relevante que se considere relevante para la idoneidad de una persona para trabajar en el puesto previsto.

- Durante el empleo, controlar el compromiso y la conducta del empleado.

Además, el proceso y los criterios para determinar la fiabilidad del personal pueden tener en cuenta si:

- Los sistemas de información y los datos a los que se ha de acceder se han asociado con una alta gravedad de las consecuencias para la seguridad del proceso de evaluación de riesgos.

- Los controles o medidas de mitigación para el tratamiento de riesgos identificados durante el análisis de riesgos se basan en procedimientos organizativos/operativos, por ejemplo, la configuración y administración correctas de las tecnologías de la información, las operaciones de bases de datos, el monitoreo de la seguridad de la información, etc.

En tales casos, el personal que tenga derechos de administrador o acceso no supervisado e ilimitado a los sistemas y datos o el personal que aplique las medidas contempladas podrá estar sujeto a criterios más estrictos.

6.2.4.3. Descripción general y organigrama

La organización incluirá un organigrama en el que se indique la relación de rendición de cuentas y responsabilidad de las personas responsables designadas por el DR y de aquellas personas clave en la implementación del Sistema de Gestión de Seguridad de la información según el punto IS.I/D.OR.200.

Se incluirá una descripción general del número y las categorías de personal y del sistema establecido para planificar la disponibilidad de personal.

6.2.5. Documentación del SGSI

En este apartado la organización debe describir su sistema de gestión de la documentación de los procesos clave del sistema de gestión.

En esta sección se detallará la documentación del SGSI que incluye las políticas y procesos que describen el sistema y los procesos de gestión de seguridad de la información de la organización.

6.3. Gestión de riesgos de seguridad

A lo largo de esta sección la organización describirá los procesos/métodos/procedimientos y las responsabilidades asociadas para la gestión de riesgos de la seguridad.

6.3.1. Identificación de peligros

En esta sección la organización deberá desarrollar un proceso sistemático para identificar los peligros en el sistema, entendiéndose peligro como una condición que puede causar o contribuir a un incidente o accidente de la aeronave.

En esta sección existirá un procedimiento que describa cómo se realiza la identificación de peligros asociados a la actividad de la organización. El sistema de identificación de peligros debe asegurar que todos los elementos que puedan tener impacto en la seguridad de la aviación son identificados e incluidos. Para ello deberá incluir una evaluación de los peligros preliminar de alto nivel que establezca un criterio de inclusión o exclusión de todos estos posibles peligros.

El nivel de detalle de este análisis corresponderá a un proceso iterativo proporcional al nivel de riesgo de cada **elemento** evaluado, identificando:

- Inputs y outputs relativos a los **funciones y servicios** de la organización, pudiendo proceder de fuentes internas o externas.

- Los **activos** (software, hardware, network) utilizados para crear, procesar, transmitir, almacenar o recibir los mencionados inputs o outputs.
- Los **entornos de trabajo** (oficinas, áreas restringidas o de acceso público o diferentes ubicaciones/instalaciones).
- Para cada activo incluido, identificación de los métodos específicos, procesos y recursos que se emplearán para gestionar, operar y mantener cada uno de dichos activos incluyendo los recursos internos o externos y contratistas que gestionen remotamente los activos (proveedores de servicios).

La organización también debe, como parte de esa evaluación de peligros, identificar las **interfaces** con otras compañías (proveedores de servicios, proveedores, contratistas, subcontratistas, etc.) basándose en los datos e información intercambiados, así como los medios empleados para dicho intercambio, identificando aquellos que puedan suponer un incremento del riesgo para la seguridad de la aviación para ellos mismos o para otras organizaciones.

6.3.2. Evaluación y mitigación de riesgos de seguridad

La organización ha de describir en esta sección su proceso formal para la evaluación y mitigación de riesgos, este proceso debe ser tal que asegure:

- Reproducibilidad de la evaluación para inputs similares.
- Repetitividad en el tiempo de la evaluación que permita comparar los resultados y cambios.
- La selección de inputs relevantes, en particular:
    - La información que permite determinar las consecuencias sobre la seguridad.
    - La información que permite determinar el potencial de ocurrencia del peligro.
- Proceso iterativo que permita un ajuste de los escenarios de los inputs con el objetivo de reducir las incertidumbres y vulnerabilidades o mejorar la eficacia de los controles existentes y las dependencias exteriores, en particular:
    - Redefinir los riesgos de alto nivel con mayor detalle a medida que se dispone de mayor información.
    - Mejorar la información de las vulnerabilidades conocidas mediante un proceso de actualización continua de la información.
    - Revisar la efectividad de los controles existentes y considerar la inclusión de nuevos controles.
    - Redefinir la comprensión de las dependencias con terceros y sus implicaciones en el perfil de riesgo de la organización.

La organización deberá revisar y actualizar la evaluación de riesgos cuando:

- Hay un cambio en los elementos sujetos a riesgos de seguridad de la información.
- Hay un cambio en las interfaces entre la organización y otras organizaciones, o en los riesgos comunicados por las otras organizaciones.

- Hay un cambio en la información o conocimiento utilizado para la identificación, análisis y clasificación de riesgos.
- Hay lecciones aprendidas del análisis de incidentes de seguridad de la información.

Se definirá el nivel de riesgo que la organización está dispuesta a aceptar y se indicará qué personal responsable de la organización tiene capacidad para tomar decisiones relativas a la tolerabilidad de los riesgos.

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

Ilustración 6. Ejemplo de matriz de aceptación de riesgos.

La organización tendrá un procedimiento para decidir y aplicar los controles o mitigaciones de riesgo apropiados. En el procedimiento se debe indicar cómo se asignan las responsabilidades para la implementación de las acciones y el plazo del que se dispone.

Para dicho análisis de riesgos, se deberá tener en cuenta los siguientes aspectos:

- Protección (EUROCAE ED-203A).
- Reducción de la exposición (EUROCAE ED-203A).
- Intento de ataque (EUROCAE ED-203A).
- Criterio de aceptación del riesgo.

Para los riesgos identificados como inaceptables, la organización deberá desarrollar medidas para corregirlos, implementarlas y comprobar su efectividad. Estas medidas deben permitir a la organización:

- Controlar las circunstancias que contribuyan a la ocurrencia de la amenaza;
- Reducir las consecuencias para la seguridad de la aviación como consecuencia de la amenaza;
- Evitar los riesgos.

Estas medidas no deben introducir nuevos riesgos.

El DR y el RCC, así como cualquier otro personal involucrado debe ser informado de los riesgos y sus resultados del análisis realizado, las amenazas evaluadas y de las medidas mitigadoras a implementar.

Además, la organización deberá informar a cualquier otra con la que exista una interfaz con riesgos compartidos.

Basado en este análisis de riesgos y sus medidas de corrección, la organización deberá implantar medidas en tres pasos: Detección, respuesta y recuperación.

Detección: La organización deberá implantar medidas de detección que revelen los posibles incidentes y vulnerabilidades que indiquen la materialización de estos riesgos y que puedan tener un impacto en la seguridad de la aviación.

Para ello, deberán identificar desviaciones del funcionamiento normal y activar alarmas/avisos para iniciar las medidas adecuadas en caso de desviación.

Respuesta: Estas medidas de respuesta deben permitir a la organización:

- Iniciar la reacción ante esos avisos/alarmas activando los recursos y procedimientos.
- Contener el ataque evitando su propagación evitando la completa materialización de la amenaza.
- Controlar el "modo de fallo" de los elementos afectados.

Recuperación: Deberá implementar medidas enfocadas a la recuperación de estos incidentes, incluyendo medidas de emergencia si fueran necesarias. Estas medidas deben permitir a la organización:

- Eliminar la situación que ha causado el incidente o reducirlo a un nivel tolerable;
- Alcanzar un nivel seguro de los elementos afectados en un tiempo de recuperación previamente definido.

6.4. Aseguramiento de la seguridad de la información

En esta sección la organización describirá los procesos/métodos/procedimientos y las responsabilidades asociadas para el aseguramiento de la seguridad.

6.4.1. Observación y medición del rendimiento en materia de seguridad de la información

6.4.1.1. Implementación y efectividad de medidas mitigadoras

La organización debe describir su proceso y responsabilidades asociadas para la observación, medición y evaluación del rendimiento y efectividad en materia de seguridad de la información de dicha organización en comparación con lo establecido en la política y objetivos de seguridad de la información.

Deberán tratarse al menos los siguientes aspectos:

- Finalidad del proceso de observación y medición del rendimiento en materia de seguridad de la información.
- Indicadores clave de rendimiento derivados de la evidencia de monitorización y la medición de los procesos del SGSI.
- Herramientas para la observación y medición del rendimiento. Se contemplarán al menos las mencionadas a continuación, y para cada una de ellas se detallará quién/cómo/cuándo usará dicha herramienta de cara a la observación y medición del rendimiento.
    - Los sistemas de notificación de sucesos (obligatorio y voluntario).
    - El estudio de seguridad.
    - Las revisiones de seguridad, incluyendo revisión de tendencias.
    - Las auditorías.
    - Las encuestas de seguridad.

Existirá un procedimiento para evaluar si la mitigación de riesgos se aplica y es efectiva.

6.4.1.2. Rendimiento e indicadores de seguridad de la información

Existirá un procedimiento para medir el rendimiento y efectividad en seguridad de la información de la organización, incluidos los indicadores de rendimiento de seguridad de la información y las metas relacionadas con los objetivos de seguridad de la información la organización.

La organización debe establecer indicadores de seguridad que permitan medir, entre otros:

- Las actuaciones del SGSI de manera sistémica (número de mitigaciones o barreras de seguridad establecidas, peligros y riesgos identificados, tiempos de resolución, etc.).
- La gestión del cambio.
- La cultura de seguridad.
- La seguridad de las actividades relacionadas (incidentes, vulnerabilidades, sucesos
- específicos, …).
- La promoción de seguridad de la información (boletines de seguridad, cursos, …).
- La efectividad de las mitigaciones de riesgo y de las medidas para detectar la posible materialización de riesgos inaceptables y que pueden tener un impacto potencial en la seguridad de la aviación.

Los indicadores de seguridad de la información establecidos por la organización se detallarán en un documento donde se incluya la descripción del indicador, el objetivo de este, el valor de referencia, la meta, cómo se recogen los datos, periodicidad de recogida de datos, responsable de la recogida de datos, periodicidad y responsable del control de indicador.

El seguimiento de los indicadores permitirá identificar tendencias y obtener información para la toma de decisiones del DR o CRP.

Además del seguimiento de los indicadores para medir el rendimiento en seguridad de la información de la organización, es necesario establecer auditorías de seguridad de la información, en el marco del programa de control de conformidad (ver apartado siguiente) para comprobar que la estructura del sistema es sólida en términos de niveles de competencia y el cumplimiento con los requisitos aplicables.

6.4.2. Gestión del cambio

Sin perjuicio del procedimiento de cambios aprobado para su correspondiente aprobación CAMO, 145 o POA, en este punto la organización debe describir las responsabilidades y procedimientos asociados a la gestión del cambio, que debe cubrir al menos los siguientes aspectos:

- La naturaleza y el propósito del cambio.
- El plan de implementación del cambio.
- El plan de verificación del cambio.
- La notificación a AESA ante una desviación en el plan de implementación del cambio.
- El impacto potencial en la seguridad de la aviación que introduce el cambio o su reevaluación ante una desviación en el plan de implementación del cambio.

Los cambios en el SGSI pueden ser gestionados y notificados a la autoridad competente en un procedimiento desarrollado por la organización. Este procedimiento deberá ser aprobado por la autoridad competente.

En cuanto a los cambios en el SGSI no cubiertos por el procedimiento anterior, la organización deberá solicitar y obtener una aprobación emitida por la autoridad competente.

6.4.3. Mejora continua del SGSI. Supervisión y revisión de la efectividad del sistema de gestión de seguridad de la información

En este apartado la organización deberá describir los procedimientos y responsabilidades asociadas para una mejora continua de la gestión de seguridad de la información.

La organización deberá evaluar, utilizando indicadores de desempeño adecuados, la efectividad y madurez del SGSI. Esa evaluación se llevará a cabo en un calendario predefinido por la organización o tras un incidente de seguridad de la información.

La organización debe tener un proceso en marcha para monitorizar, medir, evaluar y revisar la efectividad de su SGSI que defina:

- Quién monitorea, mide, analiza y evalúa los resultados y toma decisiones responsables.
- Cuándo deben realizarse los pasos anteriores.
- Qué métodos para la monitorización, medición, análisis y evaluación se aplican para asegurar resultados comparables y reproducibles.

El calendario de las evaluaciones debe ser acorde con el nivel máximo de riesgo establecido.

El proceso para monitorizar, medir, evaluar y revisar la efectividad del SGSI de la organización debe incluir como mínimo:

- La recopilación y retención de métricas de las actividades, e información adicional que podría ser útil para fines de monitorización.
- El análisis de las métricas con el fin de identificar tendencias y desviaciones de los objetivos de rendimiento predefinidos.

La organización debe evaluar la madurez utilizando un modelo de madurez adecuado para identificar áreas de mejora en el MSGSI (ver modelos en GM1 IS.I.OR.260 (a)). Para ello, la organización debe:

- Definir o adoptar un modelo de madurez que represente un conjunto de procesos y capacidades importantes y relevantes que se espera que se implementen y mantengan.
- Para cada proceso o capacidad evaluada, ha de asegurar que el modelo defina criterios contra los cuales se deben evaluar y justificar aspectos específicos, características y efectividad al determinar un nivel de madurez.
- Definir para cada proceso o capacidad evaluada su nivel de madurez objetivo deseado.

Para cada proceso o capacidad de seguridad de la información evaluado que contenga el modelo de madurez, la organización debe:

- Evaluar y justificar el nivel de madurez actual.
- Identificar cualquier área de mejora que deba realizar para alcanzar el nivel de madurez previsto.

6.5. Promoción de la seguridad

6.5.1. Instrucción y educación

La organización deberá tener un proceso para garantizar que el personal tenga la competencia necesaria para desempeñar sus tareas.

Para determinar la competencia necesaria del personal que realiza las actividades, se deben considerar los siguientes elementos:

- Los roles laborales y las tareas asociadas.
- Los conocimientos, habilidades y capacidades requeridos.

Como parte del proceso para garantizar que el personal mantenga la competencia necesaria, la organización debe:

- Evaluar las calificaciones y la experiencia del personal con respecto a la competencia requerida para los roles laborales asignados para identificar gaps.
- Alinear las calificaciones y la experiencia del personal con la competencia esperada para cumplir con sus roles organizando programas de aprendizaje adecuados para los miembros del personal existentes, reclutando nuevos recursos o una combinación de ambos.

- Mantener la competencia del personal durante el tiempo que estén asignados al rol laboral.

6.5.2. Comunicación de la seguridad de la información

En este punto la organización debe incluir procedimientos y responsabilidades asociadas para el establecimiento de un sistema de comunicación en materia de seguridad efectivo, teniendo en cuenta lo siguiente:

- Asegurar la comunicación a las partes interesadas internas y externas para lograr un nivel suficiente de concienciación sobre la seguridad de la información y la formación de todas las partes involucradas.
- La organización establece y mantiene canales de comunicación de seguridad de la información apropiados con la organización contratada.
- La organización debe comunicar la política y los objetivos de seguridad y es accesible a todo el personal a través de formación o sesiones de concienciación con todo el personal de la organización regularmente o cada vez que se modifique. Así como a todas las partes relevantes, según corresponda.

En este cuarto apartado del manual, las organizaciones que posean un Sistema de Gestión implantado y quieran aprovechar esta situación y desarrollar un Sistema de Gestión de Seguridad de la Información en el mismo manual, deberán asegurarse de:

La formación y la comunicación tanto interna como externa y las interfaces con otras empresas deberá también incluir la seguridad de la información

6.6. Responsabilidades de cumplimiento de seguridad de la información y función de control del cumplimiento de seguridad de la información

A lo largo de esta sección la organización deberá describir las responsabilidades en cuanto a cumplimiento con los requisitos aplicables relativos a la seguridad de la información y el funcionamiento de su función de control de cumplimiento de los mismos, tratando los siguientes aspectos:

- Responsabilidades y rendimiento de cuentas en cuanto a asegurar que las actividades de la organización se desarrollan cumpliendo los requisitos exigibles.
- Procedimientos para asegurar el cumplimiento de los requisitos.
- Funciones y responsabilidades del Responsable de Control del Cumplimiento de Seguridad de la Información, auditores e inspectores.
- Programa de control de conformidad (auditorías e inspecciones).

El programa de control de conformidad desarrollado por la organización permite asegurar el cumplimiento con los requisitos aplicables.

6.6.1. Función de control del cumplimiento de seguridad de la información

Los requisitos aplicables a la organización deben haber sido identificados y adecuadamente transcritos a los manuales y procedimientos de la organización.

La rendición de cuentas y las responsabilidades en materia de control del cumplimiento de seguridad de la información se definirán para todo el personal. Los cargos aprobados o responsables productivos de cada ámbito de la organización (gestión de la aeronavegabilidad, mantenimiento, operaciones vuelo, entrenamiento de tripulaciones, operaciones tierra, etc.) serán responsables de garantizar que las actividades bajo su responsabilidad se desarrollan de acuerdo con los requisitos aplicables. La persona designada con la responsabilidad de gestionar la función de supervisión del cumplimiento de la Parte IS puede ser la misma persona que, o reportar a, el RCC aprobado para la aprobación.

La rendición de cuentas y las responsabilidades del DR en materia de control cumplimiento de seguridad de la información estarán documentadas. En concreto, en cuanto a asegurar que hay suficientes recursos para asegurar el cumplimiento con los requisitos aplicables a la organización.

Se documentará que hay una persona o grupo de personas con responsabilidades para la función de control del cumplimiento de seguridad de la información, incluida la persona que actúa como Responsable del cumplimiento de seguridad de la información. Esta persona puede ser la misma, o reportar a aquella que desempeña la función de control de conformidad en la organización (RCC/RC) con acceso directo al DR. Deberá indicarse, además, el cargo que lo sustituye en caso de ausencia. En el caso de organizaciones con varias aprobaciones dentro del ámbito de aplicación del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución que comparten un Sistema de Gestión conjunto, podrá existir un RCC/RC para cada aprobación, siempre que se designe un “focal point” con línea directa de reporte al DR. El RCC debe reconocer, de manera trazable y verificable, que comprende las funciones asignadas y las responsabilidades de seguridad de la información asociadas.

Esta persona es responsable de asegurar que el programa de control de conformidad está adecuadamente implementado y es revisado continuamente para garantizar su mejora continua.

El responsable de control de cumplimiento de seguridad de la información no podrá ser responsable de ninguno de los ámbitos productivos de la organización y tiene que demostrar conocimiento de las actividades desarrolladas por el operador, o la organización de los requisitos normativos aplicables y experiencia en actividades de control normativo.

La organización debe demostrar que el responsable de control de cumplimiento de seguridad de la información tiene acceso a todas las partes de la organización y organizaciones subcontratadas, si las hubiese.

Teniendo en cuenta todo lo anterior, se debe desarrollar un procedimiento que describa cómo se garantiza que las actividades de la organización se desarrollan de acuerdo con los requisitos aplicables.

Se documentará de tal forma que se logre la independencia de la función de control de cumplimiento de seguridad de la información. En concreto, se debe garantizar que las auditorías e inspecciones no son realizadas por el personal responsable de la función auditada.

La organización debe definir un entrenamiento para los cargos aprobados y el personal con responsabilidades relacionadas con el control de cumplimiento, que incluya, entre otros, los requisitos relativos a control de no conformidades, los procedimientos y manuales aplicables, las técnicas de auditoría, reporte y registro.

La organización debe definir un briefing relativo a la función de control de cumplimiento de seguridad de la información para el resto de personal de la organización.

6.6.2. Programa de cumplimiento de seguridad de la información

La organización debe identificar y definir todos los procesos y procedimientos clave, así como los esquemas de informes internos y externos, que se utilizarán para mantener el cumplimiento con los objetivos de este Reglamento a lo largo del ciclo de vida del MSGSI. La organización puede ajustar los procesos o procedimientos existentes para el cumplimiento. Así como, identificar y documentar cualquier otra información que se utilizará para mantener el cumplimiento de los objetivos de la Parte IS.

La organización debe definir un programa de control de cumplimiento de seguridad de la información que incluya detalles de planificación de actividades y procedimientos de monitorización para auditorías e inspecciones, informes, seguimiento y registros.

El alcance de este programa debe ser tal que, al menos, garantice el control de cumplimiento de seguridad de la información.

Las no conformidades se recogerán en un informe de no conformidades.

La organización tendrá procedimientos documentados para la identificación y el seguimiento de acciones correctoras y correctivas.

Existirá un procedimiento sobre cómo se comunican los resultados de la auditoría al DR y a la alta dirección.

Se describirá la interfaz entre la función de control de cumplimiento de seguridad de la información y los procesos de gestión del riesgo de seguridad.

6.6.3. Seguimiento de incidencias/no conformidades con la autoridad

La organización deberá incluir en este punto la descripción del procedimiento de gestión de las incidencias o no conformidades notificadas por la autoridad competente, incluyendo detalle de las responsabilidades asociadas del personal de la organización (quién plantea las medidas correctoras y correctivas según el área de las incidencias, quién firma los formatos de seguimiento de deficiencias, quién los envía a la Autoridad, quién hace el seguimiento de las incidencias hasta el cierre, cumplimiento de plazos, etc.).

Dicho procedimiento de gestión de incidencias debe garantizar la aplicación de medidas correctoras a satisfacción de la autoridad competente y dentro del plazo acordado con dicha autoridad.

6.6.4. Reacción inmediata ante un problema de seguridad

Deberá incluirse en esta sección una descripción de responsabilidades y procedimientos requeridos para la gestión satisfactoria de un problema de seguridad que le sea comunicado a la organización.

La organización definirá un procedimiento para establecer las responsabilidades y actuaciones necesarias para identificar desviaciones de las actuaciones funcionales esperadas de los sistemas y activar warnings en su caso para iniciar la respuesta ante ellas, así como dicha respuesta para contener la amenaza y volver al estado seguro anterior al incidente.

El procedimiento también debe especificar qué acciones debe tomar la organización cuando, por parte de AESA, como consecuencia de una inspección o auditoría, se comunica que hay un problema de seguridad de la información que tiene que ser corregido inmediatamente. Esto es un nivel 1 de no conformidad.

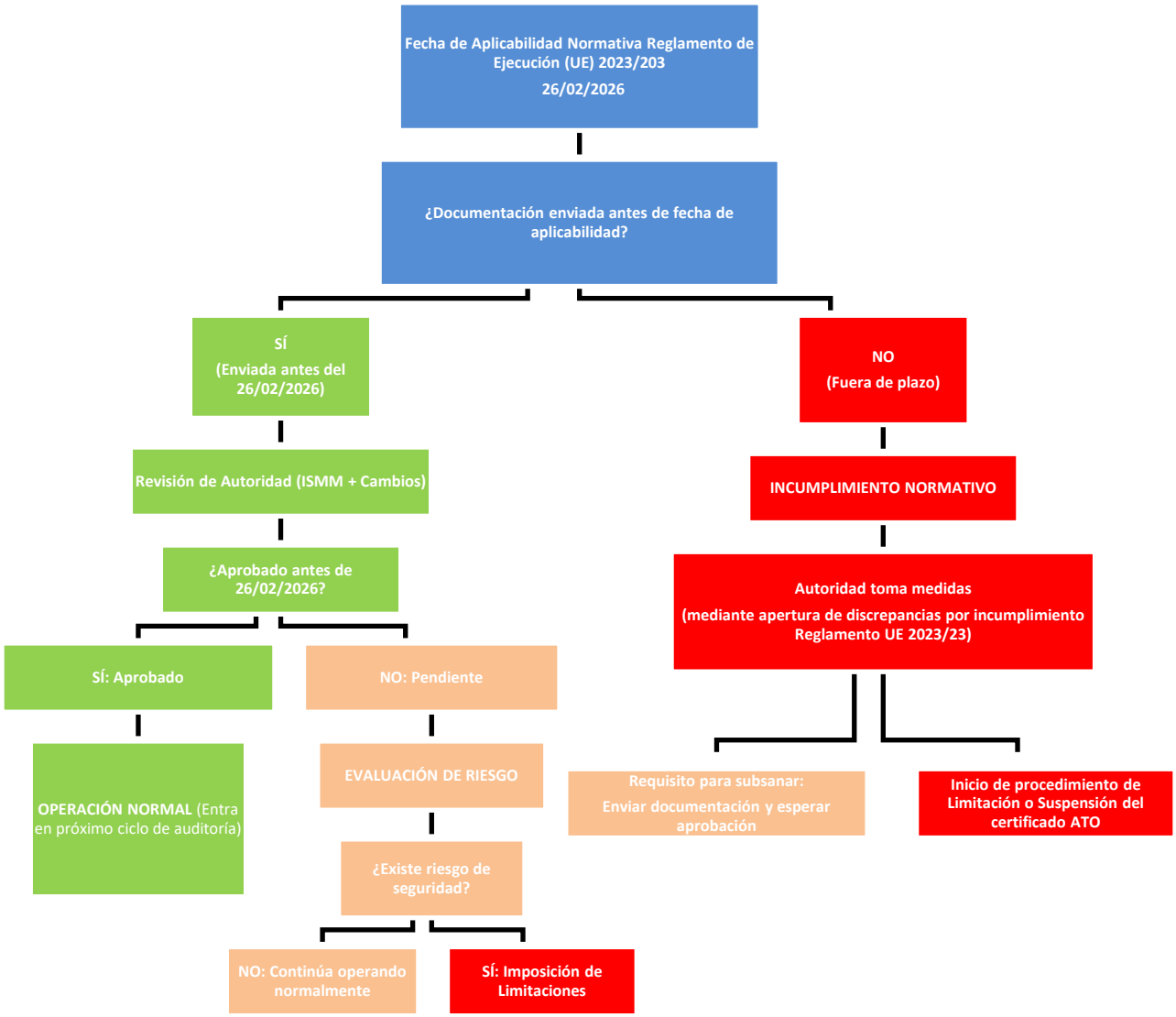
6.6.5. Medios de cumplimiento

La organización deberá incluir en este punto cómo gestionar otras formas de cumplimiento a las establecidas por EASA y/o AESA con los requisitos aplicables, de acuerdo con IS.I/D.OR.250(a)(10).

La organización debe desarrollar un procedimiento para garantizar el cumplimiento con los requisitos aplicables en el caso de que se implementen otros medios de cumplimiento alternativos a los establecidos en la regulación aplicable, siempre y cuando sean aprobados previamente por AESA.

6.7. Gestión de actividades y/o servicios contratados a otras organizaciones

La organización debe identificar y categorizar todas las organizaciones contratadas relevantes utilizadas para implementar el SGSI. La organización debe definir y documentar procedimientos para la gestión de interfaces y coordinación entre la organización y otras organizaciones, incluidas las organizaciones contratadas;



7. CAMBIOS RELEVANTES DE ESTA EDICIÓN

Primera edición