Agencia Estatal
de Seguridad Aérea

Guía del Manual del Sistema de Gestión

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	10/03/2023	– Edición inicial: – Cambio en la codificación de procedimientos, formatos y guías según ***SIG-GD-P01-ITR01***, por lo que la edición pasa a ed. 01. – Sustituye a la guía ***G-DSA-SG-02***. – Se amplía contenido y se añaden apartados para incluir la información relacionada con la información correspondiente con la inclusión del Sistema de Gestión en las organizaciones Parte 145 y POAs
02	05/12/2024	- Se aclara que un Sistema de Gestión (SG) estará integrado por un Sistema de Gestión de la Seguridad Operacional (SMS) y una Función de Control de la Conformidad. - Se modifican los puntos normativos correspondientes a POA de la tabla incluida en el apartado 3.1. - Se incluye la referencia a la guía ***DSA-SG-P01-GU03***. - Se aclara el requisito de elaborar un ERP para determinadas organizaciones.
03	09/07/2025	Los principales cambios introducidos en esta edición son los siguientes: - Se adecúa la trazabilidad entre el Manual del sistema de gestión y el MOE, modificándose los apartados 3.1.3, 3.2.1.1, 3.6.2 y 3.7.1 de esta guía. - Se mejora la coherencia entre las guías de ambos manuales para estos puntos.
04	Desde publicación	Se añade un anexo que recoge la guía para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) integrado dentro del Sistema de Gestión de Seguridad Operacional (SMS) de la organización. Además se recoge la normativa aplicable al respecto de la Seguridad de la Información. Este anexo es de aplicación únicamente para operadores aéreos. Ver los cambios concretos en el apartado 4. *Los cambios incorporados respecto a la anterior edición del procedimiento están marcados en azul.

REFERENCIAS	
CÓDIGO	**TÍTULO**
LEY 21/2003	LEY 21/2003, DE 7 DE JULIO, DE SEGURIDAD AÉREA.
LEY 39/2015	LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS
REAL DECRETO 98/2009	REAL DECRETO 98/2009, DE 6 DE FEBRERO, POR EL QUE SE APRUEBA EL REGLAMENTO DE INSPECCIÓN AERONÁUTICA Y MODIFICACIONES POSTERIORES
ORDEN FOM/2140/2005	ORDEN FOM/2140/2005, DE 27 DE JUNIO, POR LA QUE SE REGULAN LOS ENCARGOS A REALIZAR POR LA SOCIEDAD ESTATAL DE ENSEÑANZAS AERONÁUTICAS CIVILES, S.A. PARA LA EJECUCIÓN DE ACTUACIONES MATERIALES PROPIAS DE LA INSPECCIÓN AERONÁUTICA
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
REGLAMENTO (UE) Nº 2018/1139	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) Nº 1321/2014	REGLAMENTO (UE) N.º 1321/2014 DE LA COMISIÓN DE 26 DE NOVIEMBRE DE 2014 SOBRE EL MANTENIMIENTO DE LA AERONAVEGABILIDAD DE LAS AERONAVES Y PRODUCTOS AERONÁUTICOS, COMPONENTES Y EQUIPOS Y SOBRE LA APROBACIÓN DE LAS ORGANIZACIONES Y PERSONAL QUE PARTICIPAN EN DICHAS TAREAS. (REFUNDICIÓN DEL REGLAMENTO (CE NO 2042/2003).

REFERENCIAS	
CÓDIGO	**TÍTULO**
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
REGLAMENTO (CE) Nº 1008/2008	REGLAMENTO (CE) N.º 1008/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 24 DE SEPTIEMBRE DE 2008, SOBRE NORMAS COMUNES PARA LA EXPLOTACIÓN DE SERVICIOS AÉREOS EN LA COMUNIDAD.
REGLAMENTO (UE) Nº 748/2012	REGLAMENTO (UE) N.º 748/2012 DE LA COMISIÓN DE 3 DE AGOSTO DE 2012 POR EL QUE SE ESTABLECEN LAS DISPOSICIONES DE APLICACIÓN SOBRE LA CERTIFICACIÓN DE AERONAVEGABILIDAD Y MEDIOAMBIENTAL DE LAS AERONAVES Y LOS PRODUCTOS, COMPONENTES Y EQUIPOS RELACIONADOS CON ELLAS, ASÍ COMO SOBRE LA CERTIFICACIÓN DE LAS ORGANIZACIONES DE DISEÑO Y DE PRODUCCIÓN
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.
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) 748/2012 Y (UE) 139/2014 DE LA COMISIÓN.

** En todas las referencias anteriores se aplica la última edición en vigor. Por otro lado, se omiten las referencias a las Decisiones del Director Ejecutivo de EASA, que publican los medios aceptables de cumplimiento y material guía aplicables a los reglamentos de la Unión Europea, entendiéndose que aplican todas las Decisiones publicadas en la web oficial de EASA.*

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
AD	DIRECTIVA DE AERONAVEGABILIDAD (*AIRWORTHINESS DIRECTIVE*)
AESA	AGENCIA ESTATAL DE SEGURIDAD AÉREA
AMC	MEDIOS ACEPTABLES DE CUMPLIMIENTO (*ACCEPTABLE MEANS OF COMPLIANCE*)
AOC	CERTIFICADO DE OPERADOR AÉREO (*AIR OPERATOR CERTIFICATE*)
CAME	MANUAL DE LA ORGANIZACIÓN DE GESTIÓN DE MANTENIMIENTO DE LA AERONAVEGABILIDAD (*CONTINUING AIRWORTHINESS MANAGEMENT EXPOSITION*)
CAMO	ORGANIZACIÓN DE GESTIÓN DE MANTENIMIENTO DE LA AERONAVEGABILIDAD (*CONTINUING AIRWORTHINESS MANAGEMENT ORGANISATION*)
CIAIAC	COMISIÓN DE INVESTIGACIÓN DE ACCIDENTES E INCIDENTES DE AVIACIÓN CIVIL
DR	DIRECTOR RESPONSABLE
CRP	PERSONA RESPONSABLE COMÚN
EASA	AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD AÉREA (*EUROPEAN UNION AVIATION SAFETY AGENCY*)
ERP	PLAN DE RESPUESTA ANTE EMERGENCIAS (*EMERGENCY RESPONSE PLAN*)
FDM	MONITORIZACIÓN DE DATOS DE VUELO (*FLIGHT DATA MONITORING*)
FTE	FULL TIME EMPLOYEE
GM	MATERIAL GUÍA (GUIDANCE MATERIAL)
MOE	MANUAL DE ORGANIZACIÓN DE MANTENIMIENTO
MSG	MANUAL DEL SISTEMA DE GESTIÓN
MSGI	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

OACI	ORGANIZACIÓN DE AVIACIÓN CIVIAL INTERNACIONAL
PISO	PORTAL DE INDICADORES DE SEGURIDAD OPERACIONAL
POA	ORGANIZACIÓN DE PRODUCCIÓN
POE/MEOP	MANUAL DE ORGANIZACIÓN DE PRODUCCIÓN
SAG	GRUPO DE ACCIÓN DE SEGURIDAD (*SAFETY ACTION GROUP*)
SD	DIRECTIVA DE SEGURIDAD (*SAFETY DIRECTIVE*)
SG	SISTEMA DE GESTIÓN
SGSI	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
SIB	BOLETÍN DE INFORMACIÓN DE SEGURIDAD *(SAFETY INFORMATION BULLETIN)*
SMS	SISTEMA DE GESTIÓN DE LA SEGURIDAD OPERACIONAL
SPI	INDICADOR DE RENDIMIENTO DE SEGURIDAD (*SAFETY PERFORMANCE INDICATOR*)
SRB	COMITÉ DE SEGURIDAD (*SAFETY REVIEW BOARD*)
RCC/RC	RESPONSABLE DE CONTROL DE CONFORMIDAD / RESPONSABLE DE CALIDAD (RC SOLO APLICABLE A POA)

ÍNDICE

1. OBJETO Y ALCANCE

El objeto de esta guía es establecer las pautas para la elaboración del Manual del Sistema de Gestión (en adelante, MSG) de una organización, y para el caso de operadores aéreos ~~(y optativamente para organizaciones de Aeronavegabilidad Continuada asociadas al operador aéreo que pretendan integrar su MGSI/SGSI en su actual MGS/SGS ya compartido con el operador~~), las pautas para la integración de los requisitos relativos al Sistema de Seguridad de la Información, según se dispone en el *Reglamento (UE) n.º 965/2012 de 5 de octubre de 2012, el Reglamento (UE) n.º 1321/2014 de 26 de noviembre de 2014, el Reglamento (UE) n.º 748/2012 de 3 de agosto de 2012, el Reglamento de Ejecución (UE) 2023/203 de 27 de octubre de 2022 y el Reglamento Delegado (UE) 2022/1645 de 14 de julio de 2022*[1].

El alcance de este documento incluye a todas las organizaciones dentro del ámbito de aplicación del Reglamento (UE) n.º 965/2012, Reglamento (UE) n.º 1321/2014 y el Reglamento (UE) n.º 748/2012 que reglamentariamente requieran de establecer, aplicar y mantener un Sistema de Gestión.

Este documento aplica a todos los operadores sujetos a cumplimiento del Anexo III (Parte ORO) del Reglamento (UE) n.º 965/2012, a todas las organizaciones sujetas al cumplimiento del Anexo Vc (Parte CAMO) y del Anexo II (Parte 145) del Reglamento (UE) n.º 1321/2014 y a todas las organizaciones de producción (POA) del Reglamento (UE) n.º 748/2012.

La organización a la que aplique deberá desarrollar un Manual del Sistema de Gestión que tenga en cuenta los aspectos indicados en este documento o bien incluirlo en su Manual de Organización, si tiene una aprobación única y así lo considera.

Según **los puntos normativos ORO.GEN.200, CAMO.A.200 y 145.A.200**, la organización deberá establecer, implementar y mantener un Sistema de Gestión que incluya líneas de responsabilidad y rendición de cuentas claramente definidas para toda la organización, una descripción de los principios generales de la organización con respecto a la seguridad denominada política de seguridad, la identificación de los peligros para la seguridad que conlleven las actividades de la organización, la evaluación y gestión de los riesgos asociados de dichos peligros, el mantenimiento de personal capacitado y competente para realizar sus tareas, la documentación de todos los procesos clave del sistema de gestión y una función para supervisar el cumplimiento de los requisitos pertinentes por parte de la organización.

El Sistema de Gestión deberá corresponder al tamaño de la organización y a la naturaleza y complejidad de sus actividades, teniendo en cuenta los peligros y riesgos asociados inherentes a estas actividades.

De acuerdo con ORO.GEN.205, al contratar o comprar cualquier servicio o producto como parte de sus actividades, el operador deberá garantizar que los servicios o productos contratados o adquiridos cumplen con los requisitos aplicables, que cualquier riesgo para la seguridad aérea asociado a los servicios o productos contratados o adquiridos sea considerado por el sistema de gestión del operador.

[1] Para mayor detalle de las referencias normativas a aplicar, véase la Tabla de Referencias al comienzo del documento.

Según CAMO.A.205, la organización garantizará que cuando contrate el mantenimiento o subcontrate alguna parte de sus actividades de gestión del mantenimiento de la aeronavegabilidad, los peligros para la seguridad aérea asociados con dicha contratación o subcontratación se consideren como parte del SG de la organización.

Si una organización solicita o posee un certificado de Organización de Gestión del Mantenimiento de la Aeronavegabilidad (CAMO), su SG deberá ser:

- En el caso de que la organización sea **titular de uno o más certificados** de organización adicionales al de CAMO, dentro del ámbito de aplicación del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución, su Sistema de Gestión **puede** integrarse con aquellos exigidos por esos certificados adicionales. Por ejemplo, una CAMO con 145 y POA.
- En el caso de las **compañías aéreas** con licencia concedida con arreglo al Reglamento (CE) n.º 1008/2008, en las que el operador es el responsable del mantenimiento de la aeronavegabilidad de la aeronave que opere y debe estar aprobado como CAMO, su Sistema de Gestión **será** una parte integrada del Sistema de Gestión conjunto con el operador (AOC + CAMO), excepto,
- en el caso de que **forme parte de una única agrupación empresarial de compañías aéreas**, que como los operadores podrán **contratar** a una CAMO dentro de esa agrupación para que gestione el mantenimiento de la aeronavegabilidad de las aeronaves operadas por ellas según se indica en el punto M.A.201(ea), su Sistema de Gestión deberá estar **armonizado** con los SG de los operadores que formen parte de dicha agrupación empresarial y tengan contrato con la misma.

En el caso de que la organización sea titular de uno o más certificados de organización adicionales al de la Parte 145 y estos certificados estén dentro del ámbito de aplicación del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución, su Sistema de Gestión **puede** integrarse con aquellos exigidos por esos certificados adicionales o desarrollarse de forma Propia incluyendo solo la aprobación como organización Parte 145. Ejemplos, de un SG conjunto pueden ser el de un AOC, con CAMO y 145 o un 145 y una POA.

Según el punto **21.A.139**, en el caso de que la organización sea titular de uno o más certificados de organización adicionales al de la Parte 21 y estos certificados estén dentro del ámbito de aplicación del Reglamento (UE) n.º 2018/1139 y sus actos delegados y de ejecución, su Sistema de Gestión puede integrarse con aquellos exigidos por esos certificados adicionales o desarrollarse de forma Propia incluyendo solo la aprobación como organización POA.

En esta guía el término "*organización*" se refiere a la entidad que elabora el Manual del Sistema de Gestión. Esta puede ser un operador, una organización CAMO, una organización de mantenimiento Parte 145, una organización de producción POA. La terminología utilizada por OACI, equivalente al término "organización" utilizado en esta guía, y que aparece en las referencias al Anexo 19, es "proveedor de servicios".

Los apartados titulados con el término "*Operadores"* hacen referencia a requisitos específicos que deben cumplir las organizaciones que dispongan de AOC y se rijan por el Reglamento (UE) n.º 965/2012. Los apartados titulados con el término "*CAMO"* hacen referencia a requisitos específicos

que deben cumplir organizaciones CAMO (también de aplicación a las CAMO integradas en un operador con AOC) que se rigen por el Reglamento (UE) n.º 1321/2014. Los apartados titulados con el término "*145*" hacen referencia a los requisitos específicos que deben cumplir las organizaciones de mantenimiento Parte 145 que se rigen por el Reglamento (UE) n.º 1321/2014. Los apartados titulados con el término "*POA*" hacen referencia a los requisitos específicos que deben cumplir las organizaciones de producción que se rigen por el Reglamento (UE) n.º 748/2012.

Esta guía es una herramienta que puede ayudar a asegurar que todos los procesos del Sistema de Gestión de la organización están "Presentes" y son "Adecuados", y sirve como guía para el desarrollo del Manual del Sistema de Gestión de la organización.

En cuanto al Reglamento (UE) n.º 2023/203 de requisitos relativos a la Seguridad de la Información, el alcance de este documento se limita a los operadores aéreos dentro del ámbito del Reglamento (UE) n.º 965/2012 y su integración con el Sistema de Gestión del operador se detalla en el Apéndice al presente documento.

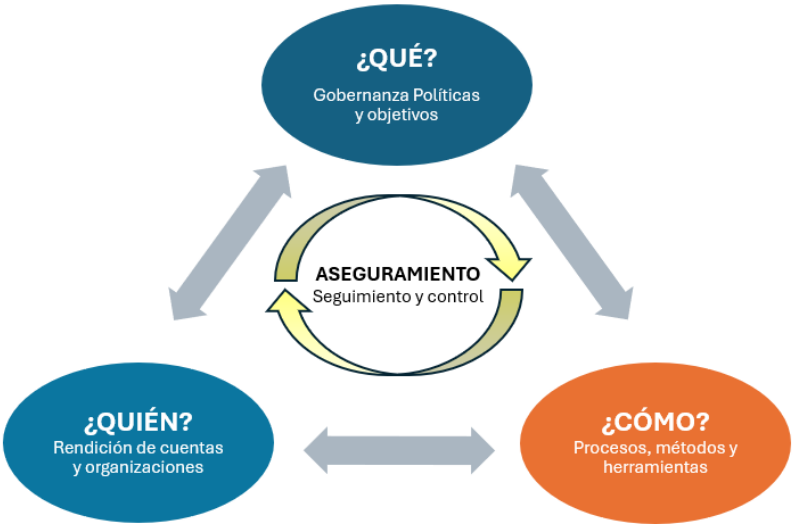
2. SISTEMA DE GESTIÓN (SG)

Se define ***Sistema de Gestión*** (SG) como el conjunto de elementos interrelacionados o que interactúan para establecer políticas y objetivos comunes y alcanzarlos.

Este conjunto de cuatro componentes clave permiten a una organización desarrollar:

1. El "Qué": las normas y la gobernanza:
   - que se traduzcan en procesos y responsabilidades de la organización (en relación con los componentes «Quién» y «Cómo»).
   - que serán bien comprendidas por todas las personas de la organización (en relación con el componente «Quién»).
2. El "Cómo": los medios y procesos que utilizará la organización:
   - garantizar que el funcionamiento de la organización sea coherente con las normas y los objetivos (en relación con el componente «Qué»)
   - garantizar que el modo de funcionamiento de la organización sea descrito y seguido por las personas de la organización (vinculado con el componente «Quién»).
3. El "Quién": la rendición de cuentas, las responsabilidades y las definiciones de las misiones asociadas:
   - garantizar que las personas actúan de acuerdo con las normas y políticas (vinculado con el componente «Qué»)
   - garantizar que las personas se atengan a los procesos y formas de trabajar descritos en la organización o empresa (vinculado con el componente «Cómo»).

4. El “Aseguramiento”: el seguimiento y control para garantizar el buen funcionamiento de otros los tres componentes de acuerdo con las normas y objetivos establecidos por la organización (enfoque de rendimiento).



Por otro lado, la Organización de Aviación Civil Internacional (OACI) define la **Seguridad Operacional** como “*el estado en el que los riesgos asociados a las actividades de aviación relativas a la operación de las aeronaves, o que apoyan directamente dicha operación, se reducen y controlan a un nivel aceptable*”.

A su vez, en el Anexo 19 al Convenio sobre Aviación Civil Internacional (Convenio de Chicago, 1944) se describe un **Sistema de Gestión de la Seguridad Operacional *(SMS)*** como un enfoque sistemático para la gestión de la seguridad operacional, que incluye las estructuras orgánicas, la obligación de rendición de cuentas, las políticas y los procedimientos necesarios.

Este Sistema de Gestión de la Seguridad Operacional se integrará con una Función para el Control de la Conformidad/Cumplimiento con los requisitos aplicables, y ambos formarán el **Sistema de Gestión (SG)** de las organizaciones. En el sistema normativo de la Unión Europea, un SG cubre el SMS y la función de supervisión del cumplimiento; y también puede cubrir subelementos relevantes en el sector, como un Sistema de Gestión de Riesgos de Fatiga (FRMS) para operadores aéreos (más explicaciones en GM1 de CAMO.A.200).

El **sistema de gestión de la seguridad operacional** se sostiene mediante los cuatro pilares que se definen en los subapartados siguientes.

2.1. Pilares de un sistema de gestión de la seguridad operacional

Su marco está integrado por los siguientes **cuatro** componentes:

2.1.1. *Política y objetivos de seguridad*

El compromiso y el liderazgo desde la Dirección en materia de seguridad son fundamentales para la implementación de un SG eficaz, y se afirman mediante la política de seguridad 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 a efectos de desarrollar una cultura de seguridad positiva.

La política de seguridad debería ser desarrollada y apoyada por la Dirección y llevar la firma de, al menos, el Director Responsable (DR), 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 y sus objetivos a efectos de promover un sentido de responsabilidad compartida.

2.1.2. *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 para asegurar que permanecen vigentes.

2.1.3. *Aseguramiento de la seguridad*

El aseguramiento de la seguridad consta de procesos y actividades realizadas por la organización para determinar si el SG 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 SG de la organización.

2.1.4. *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 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.

3. ESTRUCTURA DEL MANUAL DEL SISTEMA DE GESTIÓN (MSG)

3.1. Generalidades

La organización describirá su Sistema de Gestión, el cual deberá abarcar los ámbitos recogidos en ORO.GEN.200 y/o CAMO.A.200 y/o 145.A.200 y/o 21.A.139 y 21.A.143, según aplique, detallados a continuación, y ser coherente con el tamaño de la organización y la naturaleza y complejidad de sus actividades.

La organización podrá documentar su política de seguridad, sus objetivos de seguridad y todos los procesos clave de su sistema de gestión en un manual independiente (MSG) o en su manual de la organización (CAME, MOE, etc.). Las organizaciones que solicitan o que son titulares de varios certificados de organización dentro del ámbito de aplicación del Reglamento (UE) 2018/1139 que decidan compartir un Sistema de Gestión conjunto deberán utilizar un manual independiente para evitar duplicidades y en los manuales correspondientes a las aprobaciones que engloba el SG, únicamente se incluirá una referencia a la edición y revisión del MSG.

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

En caso de que las organizaciones subcontratadas contaran con un Sistema de Gestión propio, deberán establecerse los mecanismos de coordinación adecuados entre los Sistemas de Gestión de cada organización, aunque la responsabilidad final siempre será de la organización primera.

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

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
1. Política y Objetivos de Seguridad	Política de Seguridad	ORO.GEN.200(a)(2), (a)(6) CAMO.A.200 (a)(1), (a)(2), (a)(5), (a)(6) 145.A.200 (a)(1), (a)(2), (a)(5), (a)(6) 21.A.139(c)(1)

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
	Política de Cultura Justa	Reg. 376/2014 Art.16(11) / ORO.GEN.200 (a)(2) CAMO.A.200 (a)(2) 145.A.200 (a)(2) 21.A.139(c)(1) y AMC1 21.A.139(c)(3)y(4)(d)
	Programa o Plan de Seguridad de la Organización	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3) 145.A.200 (a)(3) 21.A.139(c)(3)
	Sistema de Notificación de sucesos/eventos	Reg. 376/2014 Art.4, Art.5, Art.13, Art.16 ORO.GEN.160 CAMO.A.160, CAMO.A.202 145.A.60, 145.A.202 21.A.139(c)(6), 21.A.3A y AMC1 21.A.139(c)(3)y(4)(d)
	Organigrama de la organización	ORO.GEN.210 (b), ORO.AOC.135 / CAMO.A.305 (a)(5) 145.A.30 (a) y (c) 21.A.143(a)
	Procedimiento de Rendición de cuentas y funciones y responsabilidades del DR y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización	ORO.GEN.200 (a)(1), (a)(5), ORO.GEN.210 (a), (b) / CAMO.A.200 (a)(1), (a)(2), (a)(5), CAMO.A.305 (a) 145.A.200 (a)(1), (a)(2), (a)(5), 145.A.30 (a) y (ca) 21.A.143(a)
	Plan de respuesta ante Emergencias	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3) 145.A.200 (a)(3) Parte 21 (N/A)
	Procedimiento para gestionar la documentación y registro del sistema de gestión.	ORO.GEN.220 CAMO.A.200 (a)(5) y CAMO.A.220 (b) 145.A.200 (a)(5) y 145.A.55 (c) 21.A.139(d)(2)(i) y(d)(2)(x)
2. Gestión de riesgos de seguridad	Procedimiento para la identificación de peligros.	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3) 145.A.200 (a)(3) 21.A.139(c~~b~~)(3~~1~~) y AMC1 21.A.139(c)(3)y(4)(a)y(c)
	Procedimiento/Método de evaluación y mitigación del riesgo.	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3) 145.A.200 (a)(3) 21.A.139(c)(3) y AMC1 21.A.139(c)(3)y(4)(b)y(c)
3. Aseguramiento de la Seguridad	Procedimiento de implementación y efectividad de medidas mitigadoras.	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3)

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
		145.A.200 (a)(3) 21.A.139(c)(4) y AMC1 21.A.139(c)(3)y(4)(e)
	Procedimiento de rendimiento de la seguridad operacional	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3) 145.A.200 (a)(3) 21.A.139(c)(4) AMC1 21.A.139(c)(3)y(4)(e)
	Programa de indicadores de seguridad operacional	ORO.GEN.200 (a)(3) CAMO.A.200 (a)(3) 145.A.200 (a)(3) 21.A.139(c)(4)(i) AMC1 21.A.139(c)(3)y(4)(e)
	Procedimiento de Gestión del Cambio	ORO.GEN.200 (a)(3), ORO.GEN.130 CAMO.A.200 (a)(3), CAMO.A.130 145.A.200 (a)(3), 145.A.85 21.A.139(c)(4)(ii), 21.A.147 y AMC1 21.A.139(c)(3)y(4)(f)
	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	Reg. 2018/1139 Annex II 3.1.(b), Annex V 8.1.(c) ORO.GEN.200 (a)(3), (a)(6) CAMO.A.200 (a)(3), (a)(6) 145.A.200 (a)(3), (a)(6) 21.A.139(c)(4)(iii) y AMC1 21.A.139(c)(3)y(4)(g)
4. Promoción de la Seguridad	Programa de entrenamiento del sistema de gestión (gestión del riesgo y control de conformidad/calidad)	ORO.GEN.200 (a)(4) CAMO.A.200 (a)(4) 145.A.200 (a)(4) 21.A.139(c)(5)(i) y 21.A.139(d)(2)(xi)
	Procedimiento para la promoción de la seguridad	ORO.GEN.200 (a)(4), (a)(5) CAMO.A.200 (a)(4), (a)(5) 145.A.200 (a)(4), (a)(5) 21.A.139 (c)(5)
5. Control de conformidad y cumplimiento	Función de control de conformidad	ORO.GEN.200 (a)(6) CAMO.A.200 (a)(6) 145.A.200 (a)(6) 21.A.139(e)
	Programa de auditoría e inspecciones	ORO.GEN.200 (a)(6) CAMO.A.200 (a)(6) 145.A.200 (a)(6) 21.A.139(d)(2)(ii) y (xiv)
	Procedimiento de seguimiento de no conformidades con la Autoridad	ORO.GEN.150 CAMO.A.150 145.A.95 21.A.139(d), AMC2 21.A.139(d)(2)(ii)(7) GM1 21.A.139(d)(2)(ii) y AMC1 21.A.139(e) 21.A.139(d)(2)(xiv)

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
	Procedimiento de reacción inmediata ante un problema de seguridad.	ORO.GEN.155 CAMO.A.155 145.A.155 Parte 21 (N/A)
	Procedimiento para medios de cumplimiento.	ORO.GEN.120 CAMO.A.120 145.A.120 21.A.134A
6. Gestión de actividades contratadas a otras organizaciones	Procedimiento para la gestión de servicios y/o actividades contratadas y/o subcontratadas a otras organizaciones.	ORO.GEN.205 CAMO.A.205 145.A.205 21.A.139(d)(2)(ii), GM1y2 21.A.139(d)(1) y AMC1 21.A.139 (d)(2)(ii) (b)(1)(ii)

3.1.1. *Operadores. Complejidad de la organización*

En esta sección el operador incluirá una declaración sobre su complejidad, y se declarará como compleja o no compleja en lo que respecta a las necesidades de su Sistema de Gestión.

Un sistema de gestión no complejo tiene alivios en lo que respecta a la manera de cumplir con los requisitos exigibles.

AMC1 ORO.GEN.200 (b)

Todos los operadores se considerarán complejos salvo que el operador presente una propuesta que resulte satisfactoria para la Autoridad justificando su consideración de organización no compleja basada, entre otros, en los siguientes aspectos:

- Tener menos de 20 FTE (deberá tenerse en cuenta el personal subcontratado).
- El alcance y nivel de subcontratación.
- No realizar operaciones que requieran una aprobación específica de acuerdo con la parte SPA.
- No realizar operaciones con diferentes tipos de aeronave.
- No realizar operaciones comerciales de alto riesgo.
- No realizar operaciones en entornos de riesgo (off shore, áreas montañosas…).
- Volumen de operaciones.

3.1.2. *CAMO*

En el medio aceptable de cumplimiento AMC1 CAMO.A.300 **se propone** una estructura para el Manual de la Organización de Gestión de la Aeronavegabilidad (CAME) que incluye en el capítulo 2 los procedimientos del Sistema de Gestión. La correspondencia entre dichos epígrafes y la estructura que se propone en esta guía se recoge en la siguiente tabla:

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	ÍNDICE EASA AMC1 CAMO.A.300
1. Política y Objetivos de Seguridad	Política de Seguridad	0.1
	Política de Cultura Justa	2.2
	Programa o Plan de Seguridad de la Organización	2.3
	Sistema de Notificación de sucesos/eventos	2.2, 2.11
	Organigrama de la organización	0.4, 2.8.6
	Procedimiento de Rendición de cuentas y funciones y responsabilidades del DR y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización	2.8.6, 2.9
	Plan de respuesta ante Emergencias	2.7
	Procedimiento para gestionar la documentación y registro del sistema de gestión.	2.10
2. Gestión de riesgos de seguridad	Procedimiento para la identificación de peligros.	2.1
	Procedimiento/Método de evaluación y mitigación del riesgo.	2.1
3. Aseguramiento de la Seguridad	Procedimiento de implementación y efectividad de medidas mitigadoras.	2.4
	Procedimiento de rendimiento de la seguridad	2.4
	Programa de indicadores de seguridad	2.4
	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	2.4
	Procedimiento de Gestión del Cambio	2.5
4. Promoción de la Seguridad	Programa de entrenamiento del sistema de gestión (gestión del riesgo y control de conformidad)	2.6
	Procedimiento para la promoción de la seguridad	2.6
5. Control de conformidad y cumplimiento	Función de control de conformidad	2.8.2, 2.8.3, 2.8.4
	Programa de auditoría e inspecciones	2.8.1
	Procedimiento de seguimiento de no conformidades de la Autoridad	0.5, 0.6
	Procedimiento de reacción inmediata ante un problema de seguridad.	2.7
	Procedimiento para medios alternativos de cumplimiento (AltMoc).	0.7
6. Gestión de actividades contratadas a otras organizaciones	Procedimiento para la gestión de servicios y/o actividades contratadas a otras organizaciones.	2.8.5

La organización podrá elegir entre las dos estructuras y, en el caso de seleccionar la del AMC1 CAMO.A.300, se deberá incluir una tabla de referencias cruzadas con la dispuesta en esta guía.

En el caso de las compañías aéreas que forman parte de una **única agrupación empresarial**, en las que uno o varios operadores podrán contratar a una CAMO dentro de esa agrupación para que gestione el mantenimiento de la aeronavegabilidad de las aeronaves operadas por ellas, el Sistema de Gestión de la CAMO deberá estar **armonizado** con el de los operadores que formen parte de

dicha agrupación empresarial. Se recomienda la lectura de la guía ***DSA-SG-P01-GU03***, de Sistemas de Gestión *entre AOC y CAMO con contrato*.

3.1.3. *145*

En el medio aceptable de cumplimiento AMC1 145.A.70(a) **se propone** una estructura para el Manual de la Organización de Mantenimiento (MOE), que incluye en el capítulo 3 los procedimientos del Sistema de Gestión. La correspondencia entre dichos epígrafes y la estructura descrita en esta guía se recoge en la siguiente tabla:

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	APARTADO GUÍA MSG	ÍNDICE EASA AMC1 145.A.70 (a)
1. Política y Objetivos de Seguridad	Política de Seguridad	3.2.1.1, 3.2.1.1.1	1.2
	Política de Cultura Justa	3.2.1.2	3.2
	Programa o Plan de Seguridad de la Organización	3.2.1.3	3.3
	Sistema de Notificación de sucesos/eventos	3.2.1.4, 3.2.1.4.1	3.2, 2.18
	Organigrama de la organización	3.2.2	1.5
	Procedimiento de Rendición de cuentas y funciones y responsabilidades del DR y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización	3.2.2	3.12, 1.4
	Plan de respuesta ante Emergencias	3.2.3	3.7
	Procedimiento para gestionar la documentación y registro del sistema de gestión.	3.2.4	3.22
2. Gestión de riesgos de seguridad	Procedimiento para la identificación de peligros.	3.3.1	3.1
	Procedimiento/Método de evaluación y mitigación del riesgo.	3.3.2	3.1
3. Aseguramiento de la Seguridad	Procedimiento de implementación y efectividad de medidas mitigadoras.	3.4.1.1	3.4
	Procedimiento de rendimiento de la seguridad	3.4.1.2	3.4
	Programa de indicadores de seguridad	3.4.1.2	3.4
	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	3.4.3	3.4
	Procedimiento de Gestión del Cambio	3.4.2, 3.4.2.3	3.5
4. Promoción de la Seguridad	Programa de entrenamiento del sistema de gestión (gestión del riesgo y control de conformidad)	3.5.1	3.6
	Procedimiento para la promoción de la seguridad	3.5	3.6
5. Control de conformidad y cumplimiento	Función de control de conformidad	3.6.1	1.3, 1.4
	Programa de auditoría e inspecciones	3.6.2, 3.6.2.1	3.8
	Procedimiento de seguimiento de no conformidades de la Autoridad	3.6.3	3.8

PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	APARTADO GUÍA MSG	ÍNDICE EASA AMC1 145.A.70 (a)
	Procedimiento de reacción inmediata ante un problema de seguridad.	3.6.4	3.7
	Procedimiento para medios alternativos de cumplimiento (AltMoc).	3.6.5	1.12
6. Gestión de actividades contratadas a otras organizaciones	Procedimiento para la gestión de servicios y/o actividades contratadas a otras organizaciones.	3.7, 3.7.1	3.18

3.1.4. *POA*

En esta sección la POA deberá elaborar y mantener una Memoria Explicativa de la Organización de Producción (POE) que todo su personal este familiarizado con su contenido y sus obligaciones dentro de la Organización y, debe proporcionar directamente o por referencia cruzada la información relacionada con el sistema de gestión de la producción descrito en el punto 21.A.139 tal que:

21.A.143(a):

1. Según AMC1 21.A.143(a)(1):
   1.1. Declaración del Gerente Responsable.
   1.2. Descripción del esquema interno de informes de seguridad de acuerdo con el punto 21.A.3A(a)(1)(ii).
   1.3. Procedimientos de gestión, garantía y promoción de la seguridad.
2. Personal Directivo.
3. Deberes y responsabilidades del Gerente Responsable y del Personal Directivo.
4. Organigrama de la Organización.
5. Lista del Personal Certificador.
6. Descripción general de los Recursos Humanos.
7. Descripción general de las instalaciones de producción y oficinas.
8. Alcance de la aprobación y descripción de los trabajos.
9. Procedimientos de notificación a AESA de los cambios en la Organización.
10. Procedimiento de enmienda y revisiones del POE.
11. Descripción del Sistema de Gestión de Producción.

12. Lista de Suministradores.
13. Manual de Operaciones de Ensayos en Vuelo.
    13.1. Descripción General de los Procesos.
    13.2. Tripulación.
    13.3. Transporte de Personal (no Tripulación).
    13.4. Gestión de Riesgos y Seguridad.
    13.5. Instrumentos y Equipos a Bordo.
    13.6. Lista de Ensayos en Vuelo.

21.A.143(c) Modificaciones: el POE se modificará cuando sea necesario a fin de reflejar una descripción actualizada de la organización.

3.2. Política y objetivos de seguridad

En esta sección, la organización incluirá su política de seguridad teniendo en cuenta lo siguiente: la política de seguridad describe los principios, procesos y métodos del Sistema de Gestión de la organización para lograr los resultados deseados en materia de seguridad. La política es el medio mediante el cual la organización declara su intención de mantener y, donde sea posible, mejorar los niveles de seguridad en todas sus actividades para minimizar su contribución al riesgo de sufrir un accidente tanto como sea razonablemente factible. La política de seguridad debe ser adecuada a la dimensión y complejidad de la organización.

3.2.1. *Compromiso de la dirección*

3.2.1.1. Política de seguridad

Air Operations ORO.GEN.200 (a)(2) y (a)(6)
- Operador Complejo AMC1 ORO.GEN.200(a)(2)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5)(e)

Continuing Airworthiness CAMO.A.200 (a)(1) y (a)(6)

Maintenance 145.A.200 (a)(1) y (a)(6)

Production 21.A.139 (c)(1)

En esta sección existirá una política de seguridad firmada por el Director Responsable que incluya un compromiso de mejora continua, recoja todos los requisitos legales y estándares aplicables, y considere las mejores prácticas.

La política de seguridad:

- Debe ser comunicada a toda la organización con apoyo visible del Director Responsable. Se deberá indicar de forma expresa cómo se garantiza este conocimiento, debiendo adecuarse al tamaño de la organización y al tipo de personal.
- Debe identificar la seguridad como la más alta prioridad organizativa, por encima de presiones comerciales, operacionales, ambientales o sociales.
- Debe reflejar los compromisos organizativos con respecto a la seguridad.
- Debe indicar que será revisada periódicamente para garantizar su aplicabilidad.
- Debe incluir los principios a seguir para las notificaciones de seguridad, sobre los cuales se fundamentarán los procedimientos de notificación de seguridad.
- Debe incluir el compromiso de mejora de los niveles de seguridad, de cumplir los requisitos legales y normas aplicables, de tener en cuenta las buenas prácticas, de proveer los recursos necesarios y de hacer que la seguridad sea una de las principales responsabilidades de todo el personal nominado, gestores y del personal de la organización en general.
- Debe indicar que el objetivo de las notificaciones e investigaciones no es buscar culpables, sino mejorar la seguridad.
- Debe fomentar activamente la notificación efectiva de seguridad y distinguir entre un comportamiento aceptable (errores involuntarios), contra el que no se tomarán medidas disciplinarias, y uno inaceptable (imprudencia, negligencia, sabotaje, etc.), contra el que sí se podrá actuar, una vez sean identificados los responsables (cultura justa o "just culture").

Los cargos aprobados y gestores (personal de estructura de alto nivel en la organización) deberán promover de forma continua la política de seguridad entre todo el personal y demostrar su compromiso con ella, proveer los recursos humanos y financieros necesarios para su implantación y establecer objetivos de seguridad y normas de funcionamiento.

Air Operations ORO.GEN.200 (a)(2)
- Operador Complejo AMC1 ORO.GEN.200(a)(2)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (e)

Continuing Airworthiness CAMO.A.200 (a)(2)

Maintenance 145.A.200 (a)(2)

Production 21.A.139 (c)

La política de seguridad incluirá una declaración para proporcionar recursos apropiados.

Air Operations ORO.GEN.200 (a)(2)
- Operador Complejo AMC1 ORO.GEN.200(a)(2)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (e)

Continuing Airworthiness CAMO.A.200 (a)(2), CAMO.A.200 (a)(5).

Maintenance 145.A.200 (a)(2), 145.A.200 (a)(5)

Production 21.A.139 (c)(1)

Se indicarán los medios para la comunicación de la política de seguridad.

Air Operations ORO.GEN.200 (a)(2)
- Operador Complejo AMC1 ORO.GEN.200(a)(2)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (e)

Continuing Airworthiness CAMO.A.200 (a)(2)

Maintenance 145.A.200 (a)(2)

Production 21.A.139 (c)(1) y (c)(5)

El compromiso de la Dirección con la seguridad estará documentado dentro de la política de seguridad.

3.2.1.2. 145

AMC1 145.A.200(a)(2), apartado (b)(3)

Además, para organizaciones Parte 145, se deberá incluir en la declaración el compromiso en la aplicación de los principios de los factores humanos, incluida la consideración debida a los aspectos de la fatiga.

3.2.1.3. Política de cultura justa

Organization Reg. 376/2014 Art. 16(11)

Air Operations ORO.GEN.200 (a)(2)
- Operador Complejo AMC1 ORO.GEN.200(a)(2) (a)(4)

Continuing Airworthiness CAMO.A.200 (a)(2)

Maintenance 145.A.200 (a)(2)

Production 21.A.139 (c)(1) y AMC1 21.A.139 (c)(1)(b)(5)

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

3.2.1.4. Programa o plan de seguridad

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(2) (c)(3)
  AMC1 ORO.GEN.200(a)(3) (d)(1)
  AMC1 ORO.GEN.200(a)(5) (a)

Continuing Airworthiness CAMO.A.200 (a)(3)

Maintenance 145.A.200 (a)(3)

Production 21.A.139 (c)(1) y AMC1 21.A.139 (c)(1)(d)

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

Los objetivos de seguridad establecidos por la organización deben tener en cuenta los objetivos de seguridad establecidos por el Programa Estatal de Seguridad Operacional (PESO) y las acciones concretas del Plan de Acción de Seguridad Operacional de España (PASO). Los objetivos de seguridad y las actuaciones asociadas deberán recogerse en un Programa o Plan de Seguridad de la organización.

El seguimiento de los objetivos de seguridad debe garantizarse mediante indicadores que permitan medir el rendimiento en materia de seguridad. El seguimiento será periódico y se realizará a través del Comité de Seguridad de la organización, SRB (Safety Review Board).

3.2.1.5. Sistema de notificación de sucesos/eventos

Organization Reg. 376/2014 Art. 4 Art. 5 Art. 13 Art. 16
Air Operations ORO.GEN.160
Continuing Airworthiness CAMO.A.160, CAMO.A.202
Maintenance 145.A.60, 145.A.202
Production 21.A.139 (c)(6) y 21.A.3A

Existirá un sistema de reporte confidencial para capturar sucesos, que garantice la desidentificación de la fuente, la retroalimentación y el registro de los sucesos en una base de datos. El sistema de notificación de sucesos establecido por la organización es una fuente de identificación de peligros del sistema de gestión.

La organización debe establecer un procedimiento para notificar los sucesos obligatorios a AESA. Las responsabilidades se definirán conforme 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.

El procedimiento identificará cómo se activan los reportes y definirá escalas de tiempo para los sucesos de reporte obligatorio (reporte a la Autoridad tan pronto como sea posible y siempre dentro de las 72 horas desde que la organización tiene conocimiento del suceso, salvo circunstancias excepcionales).

El procedimiento también debe incluir las consideraciones necesarias para notificar los incidentes y/o accidentes a la CIAIAC.

Puede encontrarse más información sobre la notificación de sucesos obligatoria y voluntaria en el *Material guía nuevo reglamento de sucesos 376/2014*, así como información sobre análisis y seguimiento de sucesos (follow-up) en la guía *para el Análisis y Seguimiento de Sucesos (Follow-Up)* disponibles en la web de AESA.

https://www.seguridadaerea.gob.es/es/ambitos/gestion-de-la-seguridad-operacional/sistema-de-notificaci%C3%B3n-de-sucesos/publicaciones-generales-del-sns

https://www.seguridadaerea.gob.es/es/ambitos/gestion-de-la-seguridad-operacional/sistema-de-notificaci%C3%B3n-de-sucesos/analisis-y-seguimiento-de-sucesos-follow-up

3.2.1.6. 145

En el caso de organizaciones Parte 145, se deberá desarrollar en el procedimiento lo siguiente:

1. Métodos para informar a AESA, al fabricante y al operador/CAMO de acuerdo con el Reglamento (UE) No 376/2014 del Parlamento Europeo y del Consejo de 3 de abril de 2014.

2. Defectos reportables (referencia: Reglamento (UE) No 376/2014 del Parlamento Europeo y del Consejo de 3 de abril de 2014 y anexo II del Reglamento de ejecución (UE) 2015/1018 de la Comisión de 29 de junio de 2015.
3. Sistema de notificación voluntaria: son sucesos de notificación voluntaria aquellos que no pertenecen a las tipologías de obligada notificación o aquellos que siendo de obligada notificación son notificados por personal que no está obligado a hacerlo. Procedimiento de determinación de qué sucesos voluntarios pueden ser notificados a la autoridad (aquellos que se determine que supongan un riesgo real o potencial para la seguridad).
4. Instrucciones para el rellenado de los formularios.
5. Campos obligatorios de notificación del anexo I del Reglamento (UE) No 376/2014 que se han de rellenar en las notificaciones.
6. Almacenamiento de los datos tanto obligatorios como voluntarios en base de datos compatible con ECCAIRs y ADREP para permitir el intercambio de información:

   *Formularios PDF de reporte off-line

   *Notificación on-line a través del portal europeo

   *Notificación a través de formato de archivo E5X

   *Uso del propio ECCAIRS

   *Notificación a través de plantillas Excel preestablecidas
7. Procedimiento de investigación y sistema de seguimiento. Procedimiento para determinar los riesgos, establecer medidas correctoras o preventivas y comunicar con regularidad a su personal información sobre el análisis y seguimiento de sucesos que son objeto de medidas correctoras/preventivas.
8. Personal que se encarga de la recogida, evaluación, tratamiento y almacenamiento de los datos salvaguarda la cultura justa.
9. Plazo para reportar (72 horas para reportar a la organización + 72 horas para comunicarlo a la autoridad desde que la organización tiene conocimiento del suceso).
10. Los reportes deben contener los resultados de las evaluaciones pertinentes (cuando son conocidos). Si la organización diagnostica deficiencias de seguridad reales o potenciales como resultado del análisis de un suceso, transmitirá a la autoridad en el plazo de 30 días desde la fecha de notificación del suceso los primeros resultados de los análisis realizados, así como cualquier medida que se haya adoptado. La organización deberá comunicar los resultados finales tan pronto como estén disponibles y en un plazo máximo de 3 meses.

    Para determinar los criterios de envío de Follow-ups por las organizaciones se ha desarrollado por parte de AESA la guía para el Análisis y Seguimiento de Sucesos (Follow-up).
11. Personas responsables de reportar (según el Reglamento (UE) No 376/2014).
12. Defectos reportados por las organizaciones subcontratadas.
13. Retención de datos. La información relacionada se divulga dentro de la organización sin datos personales. Limitación de acceso solo a personal autorizado.
14. Difusión de la cultura de notificación dentro de la organización.
15. Control de calidad para mejorar la coherencia de los datos (entre los que se notifican y los que se almacenan finalmente en la base de datos).

3.2.2. *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.

En esta sección deberán incluirse la obligación de rendición de cuentas y responsabilidades del Director Responsable (DR).

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

En el dimensionado del sistema de gestión deberán tenerse en cuenta las necesidades de personal que exigen los objetivos de seguridad establecidos.

Air Operations ORO.GEN.200 (a)(1) y ORO.GEN.210 (a)
- Operador Complejo AMC1 ORO.GEN.200(a)(2)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (e)

Continuing Airworthiness CAMO.A.200 (a)(2) y CAMO.A.305 (a)

Maintenance 145.A.200 (a)(2), 145.A.30 (a)

Production 21.A.139 (b)(2) y 21.A.145(c)(1)

En esta sección se nombrará un DR con plena responsabilidad y máxima rendición de cuentas sobre el SG. Deberá desarrollarse, además, un procedimiento de actuación en caso de ausencia del DR. 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, deberán tener un DR común.

El máximo responsable del SG es el DR, quien, sin importar otras funciones, tiene la responsabilidad final, en nombre de la organización, de implementar y mantener al SG. Las autoridades y responsabilidades del DR que no deben delegarse incluyen, entre otras:

- la disposición y asignación de recursos humanos, técnicos, financieros y de otro tipo necesarios para el rendimiento eficaz y eficiente del SG, de conformidad con los requisitos aplicables y con los manuales de la organización;
- garantizar que, si se produce una disminución en el nivel de recursos o circunstancias anormales que puedan afectar a la seguridad, se implantará la reducción requerida en el nivel de operaciones de la organización;
- la responsabilidad directa de la conducta de los asuntos de la organización;
- la autoridad final sobre las operaciones con certificación/aprobación de la organización;
- garantizar el cumplimiento con los requisitos normativos aplicables, las bases de certificación y el sistema de gestión de la seguridad de la organización;
- el establecimiento, la implantación y la promoción de la política de seguridad;

- el establecimiento de los objetivos de seguridad de la organización;
- actuar como promotor de la seguridad de la organización;
- tener la responsabilidad final para la resolución de todos los problemas de seguridad
- el establecimiento y mantenimiento de la competencia de la organización para aprender del análisis de los datos recopilados mediante su sistema de notificación de seguridad.

Además, el DR debe tener conocimiento y comprender los principios y las prácticas relacionados con los sistemas de gestión de la seguridad y los problemas clave de la gestión de riesgos dentro de la organización, y su forma de aplicación.

Ver la guía ***DSA-SG-P01-GU02***, sobre evaluación de cargos responsables del SG.

Air Operations ORO.GEN.200 (a)(1) y (a)(5), ORO.GEN.210 (a) y (b), y AMC1 ORO.GEN.200(a)(5)
- Operador Complejo AMC2 ORO.GEN.200(a)(5) y AMC1 ORO.GEN.200(a)(3) (b)(2)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (d)

Continuing Airworthiness CAMO.A.200 (a)(1) y (a)(5)

Maintenance 145.A.200 (a)(1) y (a)(5)

Production 21.A.139 (b)(2) y 21.A.145 (c)(1)

La rendición de cuentas de seguridad, las autoridades y las responsabilidades estarán claramente definidas y documentadas. Se establecerán las responsabilidades del DR en materia de seguridad. Entre estas responsabilidades se incluirán, al menos, la de establecer la tolerabilidad de riesgo de seguridad, es decir, el nivel de seguridad de las actividades de la organización.

Air Operations ORO.GEN.210 (b) y ORO.AOC.135
- Operador Complejo AMC1 ORO.GEN.200(a)(1) (a)(1)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (c)

Continuing Airworthiness CAMO.A.305 (a)(5)

Maintenance 145.A.30 (ca)

Production 21.A.139 (c)(3) y (4), AMC1 21.A.139 (c)(3) y (4)

En esta sección se designará un Responsable de Seguridad (RS) competente que sea responsable de la implementación y el mantenimiento del SG con una línea directa de reporte 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 RS para cada aprobación, siempre que se designe un "*focal point*" con línea directa de reporte al DR.

El RS es la persona de contacto y el responsable del desarrollo, administración y mantenimiento de un SG eficaz. El RS también aconseja al DR y al resto del personal sobre los asuntos de gestión de la seguridad y es responsable de coordinar y comunicar temas de seguridad dentro de la organización, así como también con proveedores externos y otras organizaciones. Las funciones del responsable de seguridad incluyen, entre otras:

- gestionar el plan de implementación del SG en nombre del Director Responsable;

- supervisar la implantación y el funcionamiento del SG;
- realizar/facilitar la identificación de peligros y el análisis de riesgos de seguridad;
- gestionar el sistema de notificación de seguridad;
- controlar las medidas correctivas y evaluar sus resultados;
- proporcionar informes periódicos sobre el rendimiento en materia de la seguridad de la organización;
- mantener registros y documentación de la seguridad;
- planificar y facilitar una capacitación de seguridad para el personal;
- proporcionar consejos independientes sobre asuntos de seguridad;
- iniciar y participar en las investigaciones internas de sucesos/accidentes;
- coordinarse y comunicarse (en nombre del DR) con AESA, según sea necesario, sobre temas relacionados con la seguridad;
- coordinarse y comunicarse (en nombre del DR) con organizaciones internacionales sobre temas relacionados con la seguridad;
- coordinar y gestionar el departamento u oficina de seguridad, si por las características de la organización ha sido definida.

La dedicación del RS 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.

Ver la guía ***DSA-SG-P01-GU02***, sobre evaluación de cargos responsables del SG.

También se incluirá el organigrama de la organización identificando cómo se han organizado las responsabilidades productivas que tendrán relación con la seguridad. Se indicarán también las funciones y responsabilidades de los diferentes cargos aprobados y gestores. Se podrá hacer referencia a otros manuales (manual de operaciones y/o gestión de la aeronavegabilidad y/o organización de mantenimiento y/o organización de producción) donde se describa la organización o viceversa.

3.2.2.1. Operadores complejos, CAMO y/o 145

En el caso de operadores complejos, CAMO y/o 145, en esta sección deberán incluirse las responsabilidades de los comités de seguridad (SRB), haciendo referencia a los métodos/procedimientos/procesos establecidos para cumplir con dichas responsabilidades.

Air Operations ORO.GEN.200 (a)(1) y AMC1 ORO.GEN.200(a)(1) puntos (b), (c) y (d)
Continuing Airworthiness CAMO.A.200 (a)(1) y AMC1 CAMO.A.200(a)(1)
Maintenance 145.A.200 (a)(1) y AMC1 145.A.200 (a)(1)

La organización establecerá comités de seguridad (SRB) apropiados que debatan y aborden los riesgos de seguridad y los problemas de cumplimiento e incluirán al DR y a los cargos aprobados o responsables de los distintos ámbitos de actividades relevantes de la organización con responsabilidad productiva.

En el caso de CAMO y 145, cuando esté justificado por su tamaño y la naturaleza y complejidad de sus actividades y sujeto a una evaluación de riesgos y a un acuerdo con AESA, es posible que la organización no necesite establecer un SRB y que estas tareas se asignen al RS.

Air Operations GM2 ORO.GEN.200(a)(1)
Continuing Airworthiness GM1 CAMO.A.200(a)(1)
Maintenance GM1 145.A.200 (a)(1)

En caso de que la organización haya establecido uno o varios grupos de acción de seguridad (SAG), deberá describir en esta sección las responsabilidades de dichos grupos haciendo referencia a los métodos/procedimientos/procesos establecidos para cumplir con dichas responsabilidades.

3.2.2.2. Operadores

Air Operations GM1 ORO.AOC.130 (e)(3)

En caso de que el operador esté obligado a implementar un programa de FDM deberá incluir en este punto las responsabilidades del grupo de FDM y detallar los métodos/procedimientos/procesos establecidos para cumplir con dichas responsabilidades.

Puede encontrarse información sobre el programa FDM en la guía ***GSO-FDM-DT01*** de *Seguimiento de Datos de Vuelo* disponible en la web de AESA, en el apartado "Material Guía de Sistemas de Gestión de Seguridad".

https://www.seguridadaerea.gob.es/es/prom-de-seguridad/directivas-y-material-guia

3.2.3. *Coordinación de la planificación de respuestas ante emergencias*

En esta sección la organización debe desarrollar, o si se ha desarrollado en un documento aparte, referenciarlo, su plan de respuesta ante emergencias (ERP) conteniendo las medidas a tomar por la organización o personas concretas durante una emergencia. Se recomienda desarrollar un documento específico.

Este ERP debe ser acorde al tamaño, naturaleza y complejidad de las actividades llevadas a cabo por la organización y debería cubrir al menos una transición ordenada y segura desde una situación normal a una de emergencia, la continuación de la provisión de servicios de forma segura, así como el retorno a la operación normal tan pronto como sea posible y la coordinación con los planes de respuesta de emergencia de otras organizaciones, cuando sea necesario. Quién toma las decisiones, cómo se obtiene la información, qué estructuras se crean para ello, etc. Debe indicarse en qué lugar del ERP se establecen los procedimientos, estructuras y metodologías que aseguran el cumplimiento con estos elementos.

Air Operations ORO.GEN.200 (a)(3) ▪ Operador Complejo AMC1 ORO.GEN.200(a)(3) (g) ▪ Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (f)
Continuing Airworthiness CAMO.A.200 (a)(3). AMC1 CAMO.A.200(a)(3).
Maintenance 145.A.200 (a)(3)

En esta sección se desarrollará y se indicará el método de distribución de un plan de respuesta de emergencia (ERP) apropiado que defina los procedimientos, roles, responsabilidades y acciones de las diversas organizaciones y del personal clave.

En el caso de organizaciones con aprobación CAMO y/o 145, se deberá desarrollar un procedimiento para actuar cuando se identifique un problema que pueda suponer un efecto inmediato en la seguridad del vuelo de las aeronaves que se gestionan y/o mantienen, en el que se incluyan instrucciones para contactar con el operador/propietario/CAMO. Adicionalmente, si aplica, se debe desarrollar un procedimiento para que la organización reaccione rápidamente cuando el operador active su ERP y requiera el apoyo de la CAMO y/o del 145.

3.2.4. *Documentación del SG*

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

Air Operations ORO.GEN.200 (a)(5) y AMC1 ORO.GEN.200(a)(5) punto (a)
- Operador Complejo AMC2 ORO.GEN.200(a)(5)

Continuing Airworthiness CAMO.A.200 (a)(5)

Maintenance 145.A.200 (a)(5)

Production 21.A.139

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

Air Operations ORO.GEN.220

AMC1 ORO.GEN.220(b)

Continuing Airworthiness CAMO.A.220 (b)

Maintenance 145.A.55 (c)

Production 21.A.143 (a)

La documentación del SG definirá las salidas (resultados/conclusiones) del SG y qué registros de las actividades del SG se almacenarán.

3.3. 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.

3.3.1. *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.

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(3) (a)(1)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (a) (b) y (d)

Continuing Airworthiness CAMO.A.200 (a)(3)

Maintenance 145.A.200 (a)(3)

Production 21.A.139 (c)(3) y (4) y 21.A.143 (a)(11)

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 deber ser reactivo y proactivo y debe tener en cuenta tanto fuentes internas como externas. El origen de los peligros identificados por la organización debe ser identificado, por ejemplo, si el peligro deriva de un suceso, de un cambio o de origen externo.

Entre las posibles fuentes de identificación de peligros internas se encuentran:

- Sistema de notificación.
- Encuestas de seguridad.
- Auditorías de seguridad.
- Análisis de tendencias de indicadores de seguridad.
- Análisis de tendencias del programa FDM, si aplica.
- Investigación y seguimiento de incidentes.

Entre las posibles fuentes de identificación de peligros externas se encuentran:

- Informes de accidentes.
- Sistema de notificación de sucesos de AESA.
- Comunicaciones de AESA, CIAIAC o cualquier otro organismo implicado en la seguridad.
- Otras organizaciones relacionadas con la actividad de la organización.
- SIBs de EASA.

3.3.2. *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 que garantice:

- Análisis, en términos de probabilidad y severidad de ocurrencia;
- Evaluación, en términos de tolerabilidad; y
- Control, en términos de mitigación, de los riesgos.

Lo anterior será requerido con independencia de la metodología que haya elegido la organización (metodología OACI, ARMS, BOW-TIE, etc.).

Se debe identificar al personal responsable de la organización con la capacidad de tomar decisiones relativas a la tolerabilidad de los riesgos.

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(3) (a)(1)

- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (a) (b) y (d)

Continuing Airworthiness CAMO.A.200 (a)(3)

Maintenance 145.A.200 (a)(3)

Production 21.A.139 (c)(3) y (4) y 21.A.143 (a)

En esta sección existirá un procedimiento para analizar y evaluar los riesgos de seguridad. 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.

La metodología de los diferentes procedimientos para gestionar riesgos puede ser común entre las distintas organizaciones. Sin embargo, no pueden ser comunes los valores de probabilidad y severidad, estos deben ser customizados y proporcionados a la actividad y volumen de operaciones de la organización.

El procedimiento establecido debe indicar cómo la organización va a tratar las recomendaciones de seguridad de los informes de la CIAIAC, de los SIB de EASA y de las emitidas por AESA dirigidas a la organización o que afecten a la actividad que desarrolla.

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(3) (b)

Continuing Airworthiness CAMO.A.200 (a)(3)

Maintenance 145.A.200 (a)(3)

Production 21.A.139 (c)(3)

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.

3.3.2.1. Operadores

Air Operations GM2 ORO.GEN.200 (a)(3)

Como caso particular, el operador establecerá en este apartado su procedimiento de gestión de riesgos de vuelo en entorno de cenizas volcánicas para lo cual dispone de la guía GM2 ORO.GEN.200(a)(3).

3.4. Aseguramiento de la seguridad

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

3.4.1. *Observación y medición del rendimiento en materia de seguridad*

3.4.1.1. Implementación y efectividad de medidas mitigadoras

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

Deberán tratarse al menos los siguientes aspectos:

- Finalidad del proceso de observación y medición del rendimiento en materia de seguridad.
- Indicadores de rendimiento de seguridad, definidos en OACI como "parámetro de seguridad basado en datos que se utiliza para observar y evaluar el rendimiento en materia de seguridad". Se deberán definir en esta sección los indicadores de rendimiento de seguridad (SPI) relacionados con aspectos clave de su sistema y operaciones. Deberán detallarse las responsabilidades, criterios y procedimientos para el desarrollo y revisión de los indicadores de rendimiento en materia de seguridad. Estos indicadores no se limitan a los de seguridad operacional que los operadores de transporte aéreo comercial reportan por medio del Portal de Indicadores de Seguridad Operacional (PISO).
- Metas de rendimiento de seguridad, definidas en OACI como el objetivo planificado o destinado para el/los indicador/es de rendimiento en materia de seguridad para un determinado periodo. Se deberán desarrollar metas de rendimiento cubriendo los aspectos clave de la organización y las operaciones. Deberán detallarse las responsabilidades, criterios y procedimientos para el desarrollo y revisión de las metas de rendimiento en materia de seguridad, teniendo en cuenta lo establecido en el RD 995/2013.
- 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.

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(3) (d)(1)

Continuing Airworthiness CAMO.A.200 (a)(3)

Maintenance 145.A.200 (a)(3)

Production 21.A.139 (c) y (4)

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

3.4.1.2. Rendimiento e indicadores de seguridad

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(3) (d)(1)

Continuing Airworthiness CAMO.A.200 (a)(3) Maintenance 145.A.200 (a)(3) Production 21.A.139 (4)

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

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

- Las actuaciones del SG de manera sistémica (número de mitigaciones o barreras de seguridad establecidas, actuaciones de los SAG, peligros y riesgos identificados, tiempos de resolución, etc.).
- La gestión del cambio.
- La cultura de seguridad.
- La seguridad de las actividades relacionadas (incidentes, sucesos específicos, …).
- La promoción de seguridad (boletines de seguridad, cursos, …).
- Los objetivos de seguridad establecidos en el programa o plan de acción de seguridad.
- La efectividad de las mitigaciones de riesgo.
- Los diferentes eventos y tendencias del programa de monitorización del vuelo (FDM), si aplica.

Los indicadores de seguridad establecidos por la organización se detallarán en un documento donde se incluya la descripción del indicador, el objetivo del mismo, 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. Estos indicadores no se limitarán a los indicadores de seguridad operacional que los operadores de transporte aéreo comercial reportan por medio del Portal de Indicadores de Seguridad Operacional (PISO).

El seguimiento de los indicadores permitirá identificar tendencias y obtener información para la toma de decisiones del DR a través del SRB.

Además del seguimiento de los indicadores para medir el rendimiento en seguridad de la organización, es necesario establecer auditorías de seguridad, 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.

3.4.2. *Gestión del cambio*

En este punto la organización debe describir las responsabilidades y procedimientos asociados a la gestión del cambio, que deben cubrir al menos los siguientes aspectos:

- Identificación de la naturaleza y alcance del cambio.
- Realización de un estudio previo de evaluación de impacto.
- Realización de un análisis de riesgos.
- Identificación del personal que llevará a cabo la implementación del cambio y de las medidas mitigadoras requeridas, resultado del proceso de gestión del cambio.

- Definición de un plan de implementación.
- Valoración de los costes económicos asociados.
- Comunicación del cambio propuesto al personal para lograr su implicación y apoyo al mismo.
- Implementación de las acciones definidas en el plan.
- Seguimiento de los efectos del cambio a través de las herramientas descritas en el punto 3.4.1 de observación y medición del rendimiento en materia de seguridad.

Air Operations ORO.GEN.200 (a)(3)
- Operador Complejo AMC1 ORO.GEN.200(a)(3) (e)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (b)

Continuing Airworthiness CAMO.A.200 (a)(3)

Maintenance 145.A.200 (a)(3)

Production 21.A.139 (c)(4) y 21.A.139 (d)(i)

En esta sección la organización establecerá un procedimiento de gestión del cambio para identificar si los cambios tienen un impacto en la seguridad y para gestionar los riesgos identificados de acuerdo con los procesos de gestión de riesgos de seguridad existentes.

Los peligros y riesgos identificados en la gestión del cambio se añadirán al registro de peligros y riesgos de la organización para su control y seguimiento.

La organización no llevará a cabo un cambio si el nivel de riesgo asociado está por encima de los límites establecidos por el DR para la organización.

3.4.2.1. Operadores

Según ORO.GEN.130, los siguientes cambios de la organización requerirán una aprobación previa por parte de AESA:

- Cambios que afecten al ámbito de aplicación del AOC, a las especificaciones de sus operaciones o a los elementos del sistema de gestión de ORO.GEN.200 (a)(1) y (a)(2).
- Cambios en el personal designado de conformidad con ORO.GEN.210, ORO.AOC.135 y ORO.GEN.200 y sus líneas jerárquicas con el DR.
- El procedimiento relacionado con los cambios que no requieren una aprobación previa desarrollado en el Manual de Operaciones. Procedimiento de notificación a la Autoridad (ORO.GEN.130 c).
- El procedimiento para la gestión de matrículas operadas por el AOC (ORO.GEN.130 c).
- El procedimiento para la gestión de bases operacionales (ORO.AOC.140).
- El procedimiento para la utilización de la aeronave del AOC por otro operador para operaciones no comerciales y comerciales especializadas (ORO.GEN.310).
- El entrenamiento de las tripulaciones (ORO.FC/CC/TC.).
- Programas alternativos de entrenamiento y cualificación (ORO.FC.245).
- La capacidad para la formación de las tripulaciones de cabina de pasajeros (ORO.FC.120).
- El procedimiento para que las tripulaciones operen en más de un tipo o variante (ORO.FC.240).

- El procedimiento para que los tripulantes de cabina de pasajeros operen más de 4 tipos de aeronaves (ORO.CC.250).
- El procedimiento para realizar operaciones no comerciales con aeronaves de más 19 asientos con menos de 19 pasajeros sin miembros de la tripulación de cabina (ORO.CC.100).
- Los esquemas de tiempo de vuelo de las tripulaciones (ORO.FTL.125).
- El programa de gestión de riesgos de fatiga de las tripulaciones (ORO.FTL.120).
- El uso de aeródromos aislados destino de operaciones con avión (CAT.GEN.MPA.106).
- El uso de los mínimos de aeródromo por debajo de los mínimos establecidos por el Estado (CAT.OP.MPA.110 a).
- Aproximaciones particulares no voladas como estabilizadas (CAT.OP.MPA.115 a).
- Aproximaciones de no precisión particulares no voladas con técnica CDFA (CAT.OP.MPA.115 b)2)).
- Uso de procedimientos instrumentales de salida o aproximación distintos a los establecidos por el Estado (CAT.OP.MPA.125 c).
- Operación extendida superior a 120 minutos (CAT.OP.MPA.140 a) 2)).
- Método de establecimiento de altitudes mínimas de vuelo (CAT.OP.MPA.145 b)).
- Política de combustible (CAT.OP.MPA.150).
- Procedimientos de descenso por debajo de altitudes mínimas de vuelo especificadas (CAT.OP.MPA.270 b).
- Utilización de masa de aterrizaje inferior a la certificada para determinar la velocidad indicada en el umbral (VAT) (CAT.OP.MPA.320 d)).
- Despegue con ángulos de alabeo incrementados (para aviones de performance clase A) (CAT.POL.MPA.A.240).
- Operaciones de aterrizaje corto (para aviones de performance clase A y B) (CAT.POL.MPA.A.250/350).
- Operaciones de distancia de aterrizaje requerida reducida (desde nov 2020) (CAT.POL.MPA.A.255/355).
- Procedimientos de Steep Approach (CAT.POL.A.245/345).
- Masa estándar para carga de pago distintas de las masas estándar para pasajeros y equipaje. (CAT.POL.MAB.100 e)).
- Procedimientos de selección de alternativos off shore para operaciones de helicópteros (CAT.OP.MPA.181 d) 6)).
- Operaciones con helicópteros en sitios de interés público (CAT.POL.H.225 a) 6)).
- Operaciones con helicópteros sin capacidad de aterrizaje forzoso seguro (CAT.POL.H.305).
- Operaciones de helicópteros sobre entorno hostil situado fuera de aéreas congestionadas (CAT.POL.H.420).
- Operaciones Específicas de acuerdo con la parte SPA, anexo V (RNP APPRCH AR, RVSM, ETOPS, LVO, EFB, DG, RNP 0.3, HEMS, NVIS, HHO, HOFO para helicópteros).

Para cualquiera de estos cambios, la organización se asegurará de contar con la aprobación formal de AESA para implementarlos y, durante la ejecución de los mismos, el operador ejercerá su actividad en las condiciones prescritas por AESA, según proceda.

No obstante, en función del riesgo y la madurez del sistema de gestión, AESA podrá establecer qué otros cambios son objeto de aprobación antes de la implementación por parte del operador. Al comienzo de las operaciones y una vez superado el proceso de certificación, el sistema de gestión del operador está documentado y es adecuado al tamaño, naturaleza y complejidad de las mismas. Sin embargo, todavía no está operativo ni puede ser efectivo. Por esta razón, se establece que los cambios en los procesos de un operador recién certificado serán aprobados. Cuando el operador demuestre que tiene capacidad para gestionar determinados cambios que no requieren aprobación, podrá proponer un procedimiento para la gestión y notificación de estos cambios. Una vez aprobado el procedimiento, el operador tendrá privilegios para gestionar los cambios sin aprobación dentro del alcance del procedimiento. Será condición necesaria que, al menos, el resultado de las primeras actividades de supervisión realizadas sea positivo.

Todos los cambios que no requieran aprobación previa serán gestionados y notificados a AESA según se haya definido en el procedimiento de notificación a la autoridad (ORO.GEN.130 c)), que deberá indicar cuáles son los cambios gestionados por el operador y cómo serán gestionados por el operador. Entre los cambios que pueden ser notificables por parte de la organización se encuentran:

- Revisiones de Manual de Operación,
- Revisiones del Manual del Sistema de Gestión,
- Equipamiento de aeronaves y las limitaciones asociadas, si no afectan a las especificaciones operativas del AOC,
- Datos de operación de las flotas relacionados con los manuales de certificación (AFMs, ...)
- La gestión de matrículas operadas bajo el AOC.

Air Operations ORO.GEN.130, AMC1 ORO.GEN.130 y AMC1 ORO.GEN.130(b) y (c)

Si el operador tiene privilegios para gestionar cambios sin aprobación y notificarlos a AESA, debe haber desarrollado un procedimiento donde se establezca el alcance de los cambios notificables y cómo se van a gestionar los cambios y la notificación de estos.

Un operador recién certificado no tendrá estos privilegios hasta que no se tengan evidencias que su sistema de gestión está operativo. Para ello, al menos el resultado de las primeras actividades de supervisión debe ser positivo. Cuando esto ocurra el operador puede proponer el procedimiento de gestión y notificación de cambio para su aprobación.

3.4.2.2. CAMO

Continuing Airworthiness CAMO.A.130, GM1 CAMO.A.130(a)(1) y GM2 CAMO.A.130(a)(1)

Según CAMO.A.130(a), los siguientes cambios en la organización requerirán una aprobación previa por parte de la autoridad:

- Cambios que afecten al alcance del certificado o a las condiciones de aprobación de la organización.
- Cambios en el personal designado de conformidad con la letra a), apartados 3 a 5, y la letra b), apartado 2, del punto CAMO.A.305.
- Los cambios en las líneas jerárquicas entre el personal designado indicado en el punto anterior, y el Director Responsable.
- El procedimiento relacionado con los cambios que no requieren una aprobación previa desarrollado en el CAME (CAMO.A.300(a)(11)(iv)).

Por otro lado, de acuerdo con CAMO.A.130(b), cualquier cambio en el que la norma disponga de manera explícita que ha de ser aceptado/autorizado/aprobado por parte de la autoridad, será considerado como cambio que requiere aprobación previa.

Para cualquiera de estos cambios la organización presentará a AESA una solicitud de modificación de la organización. Los cambios únicamente se introducen una vez que se ha recibido la aprobación formal de AESA y, durante la ejecución de los mismos, la CAMO ejercerá su actividad en las condiciones prescritas por la autoridad, según proceda.

Todos los cambios que no requieran aprobación previa serán gestionados y notificados a AESA según se haya definido en el procedimiento CAME (CAMO.A.300(a)(11)(iv)). AESA no aprobará aquellos cambios de los cuales la organización disponga de privilegio para aprobarlos ella misma (cambios que estén sujetos únicamente a notificación).

3.4.2.3. 145

Maintenance 145.A.85

Según 145.A.85, los siguientes cambios en la organización requerirán una aprobación previa por parte de la autoridad:

- Cambios que afecten al alcance del certificado o a las condiciones de aprobación de la organización.
- Cambios en el personal designado de conformidad con las letras a), b), c) y ca) del punto 145.A.30.
- Los cambios en las líneas jerárquicas entre el personal designado de conformidad con las letras b), c) y ca) del punto 145.A.30 y el Director Responsable.
- El procedimiento relacionado con los cambios que no requieren una aprobación previa desarrollado en el MOE (145.A.70(a)(10)).
- Centros adicionales de la organización distintos de los sujetos a lo dispuesto en el punto 145.A.75, letra c).
- Otros cambios que requieran aprobación previa de acuerdo con el anexo II (Parte 145).

Para cualquiera de estos cambios la organización presentará a AESA una solicitud de modificación de la organización. Los cambios únicamente se introducen una vez que se ha recibido la aprobación formal de AESA y, durante la ejecución de los mismos la organización 145 ejercerá su actividad en las condiciones prescritas por la autoridad, según proceda.

Todos los cambios que no requieran aprobación previa serán gestionados y notificados a AESA según se haya definido en el procedimiento 145 (145.A.70(a)(10)). AESA no aprobará aquellos cambios de los cuales la organización disponga de privilegio para aprobarlos ella misma (cambios que estén sujetos únicamente a notificación).

3.4.2.4. POA

Según 21.A.147 cada cambio en el sistema de gestión de producción que sea significativo para la demostración de la conformidad o las características de aeronavegabilidad y protección ambiental del producto, pieza o equipo, deberá ser aprobado por la autoridad competente antes de ser implementado. A continuación, se describen algunos ejemplos de cambios en la organización requerirán una aprobación previa por parte de la autoridad:

- Cambios significativos en la capacidad o los métodos de producción.
- Cambios en la estructura de la organización.
- Cambio del gerente responsable o de cualquier otra persona designada conforme al punto 21.A.145(c)(2).
- Cambios en los sistemas de producción o gestión de la calidad que puedan tener un impacto importante en la conformidad o la aeronavegabilidad de cualquier producto, pieza o equipo.
- Cambios en el lugar o control de trabajos subcontratados significativos o partes suministradas.
- Cambio de dirección de la Organización.
- Cambio de nombre o de propiedad de la Organización.
- Cambios de ubicación de la Organización.
- Cambio de alcance de la aprobación de la Organización.

Para cualquiera de estos cambios la organización presentará a AESA una solicitud de modificación de la organización. Para garantizar que los cambios no den como resultado el incumplimiento de la Parte 21, tanto la autoridad competente como el titular de la aprobación establecerán comunicación e intercambiaran información que permita realizar el trabajo de evaluación necesario antes de la implementación de un cambio.

AESA podrá establecer las condiciones en las que puede desarrollar su actividad la Organización durante la evaluación de un cambio. Si la organización introduce un cambio significativo en el sistema de gestión de la producción sin haber recibido la aprobación por parte AESA, se podrá considerar la necesidad de suspender, limitar o revocar el certificado de aprobación de la organización.

Los cambios únicamente se introducen una vez que se ha recibido la aprobación formal de AESA.

Con respecto a los cambios no significativos en el sistema de gestión de la producción, AESA incluirá su revisión en la supervisión continua que realice de conformidad. Si se detectase un incumplimiento, AESA lo notificará a la organización y pedirá que se introduzcan estos cambios.

3.4.3. *Mejora continua del SG. Supervisión y revisión de la efectividad del sistema de gestión*

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

Esta mejora podría conseguirse a través de:

- Valoraciones de cómo funciona la gestión de seguridad.
- Identificación y análisis de posibles retos asociados con el funcionamiento de la gestión de seguridad.
- Implementación de cambios para la mejora de la gestión de seguridad.
- Seguimiento y revisión de los efectos de cualquier cambio.

Cuando la gestión de la seguridad está funcionando bien, podría mejorarse su rendimiento a través de:

- Procedimientos de aprendizaje.
- Mejoras en las revisiones de seguridad, estudios de seguridad y auditorías.
- Mejoras en el sistema de reporte y herramientas de análisis.
- Mejoras en los procesos de identificación y evaluación de peligros y de concienciación en materia de riesgos en la organización.
- Mejoras en las relaciones con los subcontratistas, proveedores y clientes en lo relativo a la seguridad.
- Mejoras en los procesos de comunicación, incluyendo feedback del personal.

Air Operations Reg. 2018/1139 Annex V 8.1. (c)

ORO.GEN.200 (a)(3) y (a)(6)

- Operador Complejo AMC1 ORO.GEN.200(a)(3) (f)
- Operador No Complejo AMC1 ORO.GEN.200 (a)(1);(2);(3);(5) (e)

Continuing Airworthiness Reg. 2018/1139 Annex II 3.1. (b)

CAMO.A.200 (a)(3) y (a)(6)

Maintenance Reg. 2018/1139 Annex II 3.1. (b)

145.A.200 (a)(3) y (a)(6)

Production 21.A.139 (c)(4)

Existirá un procedimiento para supervisar y revisar la efectividad del SG utilizando los datos y la información disponibles.

3.5. Promoción de la seguridad

3.5.1. *Instrucción y educación*

Deberán incluirse los programas de entrenamiento inicial y recurrente en materia de seguridad para todo el personal de la organización y de otras organizaciones trabajando bajo la responsabilidad de la organización. Este entrenamiento debe ser acorde con sus responsabilidades y participación en materia de seguridad.

Deberá incluirse, al menos, para cada nivel de entrenamiento definido en función del perfil del alumno:

- Objetivo.
- Alcance.
- Perfil del instructor.
- Modalidad del curso (presencial, e-learning, autoestudio, etc.).
- Contenidos del curso, incluyendo:
    - política, objetivos y metas de seguridad;
    - estructura de la organización, funciones y responsabilidades relacionadas con la seguridad de cara a asegurar que el personal sea consciente de sus responsabilidades;
    - principios básicos de la gestión de riesgos de la seguridad, incluyendo funciones y responsabilidades de cada uno en este proceso;
    - sistemas de reporte de sucesos y peligros de la seguridad, informando de medios y procedimientos para reportar y sus beneficios;
    - principios de la mejora continua del rendimiento en materia de seguridad;
    - líneas de comunicación para la divulgación de información de seguridad;
    - responsabilidad de la organización sobre servicios subcontratados;
    - plan de respuesta de emergencia, funciones y responsabilidades asociadas.
- Cronograma.
- Método de evaluación, si procede.

La formación para los cargos de responsabilidad de las distintas áreas debe incluir el contenido relacionado con el cumplimiento de los requisitos de seguridad nacionales e institucionales, la asignación de recursos y la promoción activa del sistema de gestión de la seguridad, lo que incluye la comunicación eficaz de seguridad entre los departamentos. Además, la formación para estos cargos debe incluir material acerca del establecimiento de niveles de objetivos y metas del rendimiento en materia de seguridad.

La formación al DR debe proporcionarle una comprensión del sistema de gestión de la seguridad y su relación con la estrategia comercial general de la organización.

Air Operations ORO.GEN.200 (a)(4) y AMC1 ORO.GEN.200(a)(4) apartado (a)
Continuing Airworthiness CAMO.A.200 (a)(4)
Maintenance 145.A.200 (a)(4)

Production 21.A.139 (c)(5)

En esta sección existirá un programa de entrenamiento en el SG inicial y periódico. El entrenamiento abarcará los deberes de seguridad individuales (incluidos los roles, las responsabilidades y la rendición de cuentas) y cómo funciona el SG de la organización.

Existirá un procedimiento para garantizar que la organización tenga personal entrenado y competente.

3.5.2. *Comunicación de la seguridad*

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:

- El sistema de comunicación debe garantizar que todo el personal es conocedor de las actividades de gestión de la seguridad según corresponda a las responsabilidades de seguridad que tiene asignadas cada uno.
- El sistema debe comunicar la información de seguridad crítica, especialmente la relativa a peligros y riesgos analizados y evaluados.
- El sistema debe explicar por qué se toman determinadas acciones y por qué se generan nuevos procedimientos en materia de seguridad o se modifican los antiguos.
- La organización debe comunicar la política y los objetivos de seguridad a todo el personal.
- El Responsable de Seguridad debe comunicar regularmente información sobre las tendencias de rendimiento en materia de seguridad y temas de seguridad específicos mediante los boletines y las sesiones informativas. Además, también debe garantizar que las lecciones aprendidas a partir de las investigaciones o las experiencias ya sean internas o de otras organizaciones, se distribuyan ampliamente.
- En el caso de operadores que dispongan de un programa de FDM, el sistema debe permitir la difusión de las lecciones aprendidas del seguimiento de los datos de vuelo al personal, y a la industria/Autoridad si corresponde (asegurando previamente la desidentificación de los datos).
- El sistema debe alentar activamente al personal para que identifique e informe los peligros; de este modo el rendimiento en materia de seguridad será más eficiente.
- El sistema debe permitir que información y conocimientos de accidentes/incidentes relevantes puedan divulgarse a otras personas y organizaciones de forma que estos puedan aprender de los mismos.

Para divulgar información de seguridad podrían usarse, entre otras, las siguientes herramientas:

- Reuniones de seguridad con el personal, donde la información, acciones y procedimientos pueden ser discutidos.
- “Briefings” de seguridad.
- Email, correo, buzón de sugerencias.
- Campañas de seguridad.
- Información de seguridad de las autoridades, fabricantes, etc.

- Boletines con casos de estudio, reportes de auditoría, información de accidentes/incidentes internos y externos a la organización.
- Suscripción a publicaciones.

Organization Reg. 376/2014 Art. 13 (3)
Air Operations ORO.GEN.200 (a)(4) y (a)(5) ▪ Operador Complejo AMC1 ORO.GEN.200(a)(4) apartado (b)
Continuing Airworthiness CAMO.A.200 (a)(4) y (a)(5)
Maintenance 145.A.200 (a)(4) y (a)(5)
Production 21.A.139 (c)(5)

Esta sección definirá un procedimiento para determinar qué información de seguridad crítica se debe comunicar y cómo se comunica dentro de la organización a todo el personal según corresponda. Esto incluirá organizaciones y personal contratados cuando sea apropiado.

3.6. Responsabilidades de cumplimiento y función de control de conformidad / calidad

A lo largo de esta sección la organización deberá describir las responsabilidades en cuanto a cumplimiento con los requisitos aplicables y el funcionamiento de su función de control de conformidad, 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 de la Conformidad, 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.

3.6.1. *Función de control de conformidad / calidad*

Air Operations ORO.GEN.200 (a)(6) y AMC1 ORO.GEN.200 (a)(6)
Continuing Airworthiness CAMO.A.200 (a)(6)
Maintenance 145.A.200 (a)(6)
Production 21.A.139 (d)(1) y (e)

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 de conformidad 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 rendición de cuentas y las responsabilidades del DR en materia de control de conformidad 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 de conformidad, incluida la persona que actúa como Responsable de Control de Conformidad/Responsable de Calidad (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/RC es responsable de asegurar que el programa de control de conformidad está adecuadamente implementado y es revisado continuamente para garantizar su mejora continua.

El RCC/RC 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 RCC/RC tiene acceso a todas las partes de la organización y organizaciones subcontratadas, si las hubiese.

En caso de que el RCC/RC sea la misma persona que el RS de la organización, el DR debe asegurar que cuenta con los recursos suficientes para desarrollar ambas actividades. Se tendrá en cuenta el tamaño y complejidad de la organización.

En los operadores no complejos/CAMO/145, las funciones y responsabilidades del RCC pueden ser realizadas por el DR, si este cuenta con la experiencia y conocimientos necesarios para llevarlas a cabo.

Ver la guía ***DSA-SG-P01-GU02***, sobre evaluación de cargos responsables del SG.

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 conformidad. 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 conformidad para el resto de personal de la organización.

3.6.2. *Programa de control de la conformidad*

Air Operations ORO.GEN.200 (a)(6) y AMC1 ORO.GEN.200 (a)(6) (d)(2) (vi)
- Operador Complejo GM2 ORO.GEN.200(a)(6)
- Operador No Complejo GM3 ORO.GEN.200 (a)(6)

Continuing Airworthiness CAMO.A.200 (a)(6) y GM1 CAMO.A.200 (a)(6) and CAMO.B.300

Maintenance 145.A.200 (a)(6), GM1 145.A.200 (a)(6) and 145.B.300

Production 21.A.139 (d)(1) y (d)(2)

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

En caso de que se vayan a realizar auditorías en remoto, para organizaciones CAMO y 145, se ha de seguir lo establecido en GM1 CAMO.A.200(a)(6) y CAMO.B.300 y en GM1 145.A.200 (a)(6) y 145.B.300. Para las POAs se seguirá lo establecido en el GM1 21.A.139, 21.A.157, 21.A.239, 21.A.257, 21.B.120, 21.B.140, 21.B.220, 21.B.235 and 21.B.240.

El alcance de este programa debe ser tal que, al menos, garantice el control de conformidad con respecto a:

- Los privilegios de la organización según se recogen en los certificados/autorizaciones que permiten las actividades que realizan.
- Manuales y registros.
- Entrenamientos.
- Procedimientos y manual de sistema de gestión.
- Las actividades de los ámbitos productivos de la organización
- Las actividades desarrolladas por otras organizaciones subcontratadas y/o contratadas.

Para los operadores no complejos, el programa de auditorías e inspecciones puede realizarse a través de una checklist. 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 conformidad y los procesos de gestión del riesgo de seguridad.

3.6.2.1 145

En particular, para organizaciones Parte 145, deberán desarrollarse los siguientes procedimientos:

Plan de auditorías y procedimiento de auditorías

Debería describir cómo se organiza el sistema de auditoría interna.

1. Definición del sistema de control de conformidad
    a. Independencia
    b. Acceso al Director Responsable
    c. Composición y funciones del grupo de gestión de control de conformidad
2. Política de auditoría de la compañía
    a. Auditorías programadas, auditorías aleatorias y auditorías a realizar durante un mantenimiento (incluyendo turnos de noche)
    b. Notificación de la auditoría
    c. Informe de la auditoría (documentos a usar, auditor, puntos comprobados y discrepancias encontradas, fecha límite para su rectificación)
    d. Validación/aprobación interna del programa de auditorías
3. Plan anual de auditorías
    a. Principios de planificación del programa anual de auditorías
        - Instalaciones adecuadas
        - Verificación de que todos los aspectos de la organización son auditados en periodos no superiores a 12 meses, incluyendo cualquier procedimiento adicional de acuerdo con la Parte M o con la Parte ML, según aplique.
        - Estas auditorías deberán cubrir también al departamento de control de conformidad.
        - El máximo periodo entre auditorías de una estación línea no debiera exceder de 24 meses
        - Cumplimiento con los procedimientos aprobados
        - Fechas y plazos
        - Auditorías de productos
    b. Procedimientos de validación/aprobación interna del programa de auditorías y sus modificaciones
    c. Independencia de los auditores
    d. Mismos procedimientos de auditoría para varias líneas de producción
    e. Procedimiento de auditoría específico para una línea de producción
    f. Auditorías programadas y auditorías inesperadas durante la realización del mantenimiento, incluyendo turnos de noche si los hubiera
    g. Auditorías completas o varias auditorías parciales
    h. Principios a aplicar cuando se encuentran discrepancias en una línea de producción
    i. Agrupación de auditorías
    j. Auditoría del sistema de control de conformidad por un auditor independiente
4. Auditoría a subcontratistas y evaluación de proveedores
5. Registro de los informes de auditorías
    a. Duración/localización.

b. Tipo de documentos (notificación, informes, check list, programa de auditorías).

Al final de cada auditoría debe llevarse a cabo un informe de la misma que describa qué se ha auditado y las discrepancias detectadas.

Auditorías en remoto: Si la organización de mantenimiento quiere contar con la posibilidad de realizar auditorías de forma remota (ver definición), debe desarrollar un procedimiento que describa el proceso a seguir para la realización de este tipo de auditorías. El GM1 145.A.200(a)(6) y 145.B.300 contiene información sobre los aspectos a tener en cuenta y los requisitos mínimos que deben cumplirse.

Auditoría de producto e inspecciones

El plan de auditorías debe contemplar auditorías de producto y en ellas se comprobará que el estado de la aeronave, motor, componente o servicio especializado es consistente con la documentación aportada.

1. Política de auditoría de la compañía. Se debería añadir una política para las auditorías de producto, siempre que no entre en conflicto con la descrita en el párrafo anterior.
2. Programa de auditorías:
   a. Muestras de productos de cada línea de producción
   b. Fechas y plazos
3. Métodos de auditoría:
   a. Por muestreo
   b. Auditorías de investigación
4. Registros de los informes de auditoría:
   a. Duración/localización

Tipo de documentos (notificación, informes, check list, programa de auditorías)

Procedimiento para discrepancias y acciones correctoras de auditorías

1. Descripción del sistema de feedback de los informes de auditoría
2. Acción correctora y plazos:
   a. Planificación de las acciones correctoras y seguimiento:

      El plan de acciones correctoras debería estar diseñado de forma que se identifique y registre correctamente la discrepancia, y contenga:

      i) Acciones correctoras a corto plazo para subsanar las evidencias de las discrepancias detectadas en las auditorias
      ii) Análisis de la causa raíz y medidas correctoras a largo plazo para evitar la recurrencia de las discrepancias detectadas

b. Procedimiento que describa las acciones de la organización cuando el plazo de la acción correctora debe ser ampliado o cuando la respuesta no se recibe a tiempo

3. Gestión de la responsabilidad de la acción correctora y seguimiento
4. Registros de la auditoría y del feedback:
   a. Duración
   b. Tipo de documentos (respuestas, evidencias…)
5. Revisión de los resultados del sistema de control de conformidad:
   a. Reunión con el Director Responsable (incluyendo registro de la reunión)
   b. Reuniones regulares para comprobar el progreso de las acciones correctoras

En las organizaciones pequeñas, el seguimiento de las acciones correctoras no puede ser subcontratado.

3.6.3. *Seguimiento de incidencias/no conformidades con la autoridad*

Air Operations ORO.GEN.150 y AMC1 ORO.GEN.150(b)
Continuing Airworthiness CAMO.A.150
Maintenance 145.A.95
Production 21.A.139 (d)(1) y (d)(2)

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.

En el caso en que la autoridad competente sea AESA, se deberá tener en cuenta la obligación de presentar, en el plazo de 10 días desde la recepción del acta de inspección, un plan de acciones correctoras. Dicho plan de acciones deberá contener para cada incidencia la identificación de su causa raíz, así como la propuesta de las acciones necesarias para su resolución, con el mayor nivel de detalle posible, junto con el plazo de implementación de dichas acciones, así como las fechas de presentación a AESA de cualquier documentación que requiera aceptación/aprobación. Entre las acciones a tomar por la organización están:

- Acción correctora: acciones necesarias para evitar de forma inmediata que se siga incurriendo en un incumplimiento.
- Acción correctiva: acciones tendentes a evitar que puedan reproducirse aquellas discrepancias o no conformidades que fueron detectadas mediante el correspondiente análisis de causa raíz.

3.6.4. *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.

Air Operations ORO.GEN.155
Continuing Airworthiness CAMO.A.155
Maintenance 145.A.155
Production 21.A.139 (c)(6), (d)(1) y 21.A.3A

La organización definirá un procedimiento para establecer las responsabilidades y actuaciones necesarias para implementar las Directivas de Aeronavegabilidad (AD) y de Seguridad (SD) establecidas por EASA, AESA o cualquier otra autoridad competente de alguna de las actividades o productos de la organización.

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 que tiene que ser corregido inmediatamente. Esto es un nivel 1 de no conformidad.

3.6.5. *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 ORO.GEN.120 / CAMO.A.120 / 145.A.120 / 21.A.139 y 21.A.134, según aplique.

Air Operations ORO.GEN.120 y AMC1 ORO.GEN.120 (a)
Continuing Airworthiness CAMO.A.120
Maintenance 145.A.120
Production 21.A.139 (d)(1) y 21.A.134A

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.

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

Air Operations ORO.GEN.205
Continuing Airworthiness CAMO.A.205
Maintenance 145.A.205
Production 21.A.139 (d)(2)(ii)

Cuando la organización contrate/subcontrate un producto o servicio, debe asegurarse de que este cumple con los requisitos de aplicación, ya que la responsabilidad última del servicio o producto subcontratado recae sobre la organización. En esta sección, la organización debe definir las actuaciones que realizará sobre los contratistas/subcontratistas y sus servicios o productos antes de su contratación y durante la prestación de los servicios.

Además, los riesgos de las actividades desarrolladas por las organizaciones contratadas o subcontratadas deben estar bajo el control del sistema de gestión de la organización (ORO.GEN.205, CAMO.A.205 (a)(2), 145.A.205 (a)(2) y 21.A.139 (d)(2) (ii).

Ejemplos de algunas actividades susceptibles de ser contratadas/subcontratadas:

- Anti-icing/De-icing.
- Agente de handling.
- Soporte al vuelo (cálculo de performances, planes de vuelo, navegación, despacho); se verificará la integridad y la fiabilidad de los datos que se reciben de las subcontratas (análisis de aeropuertos, LCM, etc.).
- Entrenamiento; cuando el entrenamiento esté subcontratado, estas actuaciones deben verificar que el entrenamiento se imparte conforme a lo establecido en los manuales de la organización.
- Mantenimiento de aeronaves o de sus interiores.
- Ensayos no destructivos.
- Tareas de gestión del mantenimiento de la aeronavegabilidad como, por ejemplo, la elaboración de programas de mantenimiento.
- Gestión de implementación de directivas.
- Logística.
- Mecanizados.
- Tratamientos Superficiales.
- Montajes.
- Fabricación aditiva.
- Etc.

La organización debe desarrollar un procedimiento para establecer las responsabilidades adecuadas para la contratación de servicios a otras organizaciones. En el procedimiento se deben establecer las acciones necesarias para:

- Comunicar la política de seguridad y la formación de seguridad y control de conformidad a la organización contratada.
- Recibir y dar feedback sobre los sucesos relacionados con las actividades que desarrolla la organización contratada.
- La implementación de las acciones mitigadoras resultantes para que las actividades desarrolladas por la organización contratada se realicen con el nivel de seguridad establecido.
- La subsanación de las no conformidades detectadas a través del programa de control de conformidad de la organización.

- El acceso a las instalaciones y registros de la organización contratada por parte del personal de la organización contratante y de AESA.
- Establecer las responsabilidades necesarias en la organización contratada en cuanto a seguridad para garantizar que se cumplen los puntos anteriores.
- La responsabilidad de coordinar y controlar en la organización contratada y en la que contrata los aspectos de seguridad y control de conformidad exigidos.

En relación con este punto hay que considerar que una organización, aun contando con menos de 20 FTE, incluyendo al personal subcontratado, puede considerarse compleja desde el punto de vista del sistema de gestión teniendo en cuenta el alcance y el volumen de actividades y servicios contratados a otras organizaciones.

Cuanto mayor sea el volumen de contratación de servicios a otras organizaciones, mayor serán los FTE que la organización debe dedicar para controlar el cumplimiento de los requisitos normativos y el riesgo de las actividades contratadas.

El AMC1 ORO.GEN.205 b) establece que la manera de cumplir con estos requisitos, en un operador, es establecer en un contrato escrito el alcance de las actividades contratadas, los requisitos aplicables y las responsabilidades en cuanto a seguridad derivadas de dicho cumplimiento.

En caso de que la organización contratada cuente con un sistema de gestión certificado, el procedimiento para gestionar las actividades contratadas se simplifica notablemente pues la organización contratada ya cuenta con los responsables y procedimientos exigidos. Habrá que establecer la coordinación necesaria entre ambos sistemas de gestión.

En el caso concreto de contratación entre una CAMO y una organización de mantenimiento, además de lo indicado anteriormente, se deberá desarrollar el procedimiento requerido en la Parte 3 del CAME.

3.7.1 145

Además, para organizaciones Parte 145:

i. Equipo externo trabajando bajo su propia aprobación EASA Parte 145.

En este caso, al final del trabajo el equipo externo emitirá su propio CRS del trabajo realizado.

1. Separación entre dos organizaciones de mantenimiento trabajando en las mismas instalaciones.

2. Orden de trabajo proporcionada al equipo externo.

3. Tipo de apoyo (equipos/herramientas, instalaciones, etc.) que se pone a disposición del equipo externo.

4. Gestión del progreso del trabajo (reuniones, etc.)

5. Release to Service esperado del equipo de trabajo.

ii. Equipo externo trabajando sin aprobación EASA Parte 145.

En este caso, el equipo externo será considerado como un subcontratista y deberán seguirse los procedimientos desarrollados en el MOE, capítulo 2.1. La Organización deberá listarse en el MOE, capítulo 5.2 junto con el alcance de la autorización.

1. Control del subcontratista

2. Sistema de control de materiales, herramientas, instrucciones de trabajo y procedimientos.

3. Sistema de control de documentación como dibujos, modificaciones, reparaciones, etc.

4. Gestión del progreso del trabajo (reuniones, etc.)

5. Procedimiento de certificación del trabajo realizado por el equipo externo como: reparación, sustitución, modificación, overhaul, test, inspección.

6. Condiciones ambientales.

7. Certificación final.

8. Formación en procedimientos internos al personal externo.

4. CAMBIOS RELEVANTES DE ESTA EDICIÓN

Los principales cambios introducidos en esta edición son los siguientes:

- Adición de la normativa aplicable al respecto de los Sistemas de Seguridad de la Información y de los acrónimos derivados de ella.
- Modificación del apartado 1, definiendo el objeto alcance de esta guía y su apéndice sólo para operadores aéreos en lo que respecta al Reglamento (UE) n.º 2023/203.
- Generación de un apéndice íntegro que establece las pautas para integrar, dentro del Manual del Sistema de Gestión (MSG) del operador, las provisiones necesarias para el cumplimiento de los requisitos relativos a la Seguridad de la Información.

Apéndice

Integración del Sistema de Gestión de Seguridad de la Información (SGSI)

5. Apéndice

ÍNDICE

1. OBJETO Y ALCANCE

El objeto de este Apéndice es complementar las pautas proporcionadas por el cuerpo de esta Guía para incluir dentro del Manual del Sistema de Gestión (MSG) de un operador aéreo los aspectos propios del Sistema de Gestión de Seguridad de la Información, considerando los requisitos incluidos en el *Reglamento de Ejecución (UE) n.º 2023/203 de 27 de octubre de 2022.*

El alcance de este documento aplica a todos los operadores aéreos sujetos a cumplimiento del Anexo III (Parte ORO) del *Reglamento (UE) n.º 965/2012*, salvo a las que según el artículo 2 c) del Reglamento 2023/203 operan única y exclusivamente 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.

La organización a la que aplique deberá desarrollar un Manual del Sistema de Gestión de Seguridad de la Información (en adelante, MSGI) que tenga en cuenta los aspectos indicados en este documento y conforme al enfoque preferido de integrarlo dentro del MSG y por tanto englobado en su Sistema de Gestión (SGS) vigente.

Las potenciales ventajas de integrar el MSGI en el Manual de Gestión son:

- Aprovechar las políticas y procedimientos existentes: una organización puede utilizar sus políticas y procedimientos existentes como base para su SGSI. Esto puede ayudar a garantizar la coherencia y minimizar la necesidad de documentación adicional.
- Alinear el SGSI con su Sistema de Gestión de la Seguridad (SGS), para garantizar que sea coherente con el enfoque de gestión general de la organización.
- Utilizar los procesos de gestión de riesgos existentes: una organización puede utilizar sus procesos de gestión de riesgos existentes para identificar y evaluar los riesgos de Seguridad de la Información que pueden dar lugar a riesgos para la seguridad de la aviación.
- Reutilizar los controles existentes: una organización puede reutilizar los controles existentes, como los controles de acceso o el proceso de gestión de incidentes, para implementar los controles de seguridad de la información requeridos por el SGSI.

Según **los puntos normativos ORO.GEN.200, ORO.GEN.200A e IS.I.OR.200**, la organización deberá establecer, implementar y mantener un Sistema de Gestión (incluyendo de Seguridad de la Información) que incluya las posibles repercusiones de los riesgos relacionados con la seguridad de la información sobre la seguridad aérea, la detección y revisión de los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.I.OR.205, el tratamiento de los riesgos de seguridad de la información según el punto IS.I.OR.210, el mantenimiento de personal capacitado y competente para realizar sus tareas considerando los requisitos del punto IS.IOR.240,

la documentación de todos los procesos clave del sistema de gestión y la conservación de registros según IS.I.OR.245 y una función para supervisar el cumplimiento de los requisitos pertinentes por parte de la organización.

Asimismo, deberá implementarse un sistema de notificación tanto externo como interno en materia de seguridad de la información de conformidad con el punto IS.I.OR.215 integrándolo en el sistema de notificación de seguridad ya vigente. Además, definir y aplicar de conformidad con el punto IS.I.OR.220, las medidas necesarias para detectar eventos de seguridad de la información, determinar cuáles de ellos se consideran incidentes con posibles repercusiones sobre la seguridad aérea —salvo lo permitido en el punto IS.I.OR.205, letra e)— y responder a dichos incidentes de seguridad de la información y recuperarse de ellos (IS.I.OR.225, IS.I.OR.230 y IS.I.OR.235).

El Sistema de Gestión de Seguridad de la Información, debidamente integrado con el SGS, deberá corresponder al tamaño de la organización y a la naturaleza y complejidad de sus actividades, teniendo en cuenta los peligros y riesgos asociados inherentes a estas actividades desde la óptica de la seguridad de la información con potencial impacto en la seguridad operacional.

De acuerdo con IS.I.OR.235, al recibir o prestar cualquier servicio o producto como parte de sus actividades, el operador deberá garantizar que los servicios o productos contratados o adquiridos cumplen con los requisitos aplicables y que cualquier riesgo para la seguridad aérea asociado a los servicios o productos contratados o adquiridos, derivado de riesgos a la seguridad de la información, sea considerado por el sistema de gestión del operador.

El último apartado de este apéndice recoge una tabla resumen de los cambios que cada apartado del MGS debe incorporar para integrar el MGSI en su estructura.

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

Se define ***Sistema de Gestión de la Seguridad de la Información*** (SGSI) integrado en el Sistema de Gestión, como un enfoque sistemático para establecer, implementar, operar, monitorizar, 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.

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 se consideran dentro del ámbito de aplicación del Reglamento (UE) 2023/203. El SGSI, como parte del SGS, proporciona los medios para decidir sobre los controles de seguridad de la información necesarios para todas las capas de la organización (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.

El proceso de gestión de riesgos se basa en evaluaciones de riesgos de seguridad de la aviación y deriva de niveles de aceptación de riesgos de seguridad de la información con un impacto potencial en la seguridad de la aviación. La siguiente ilustración muestra en alto nivel y de manera no exhaustiva cómo las diferentes disciplinas de la evaluación de riesgos pueden necesitar colaborar para establecer una perspectiva común de riesgos.

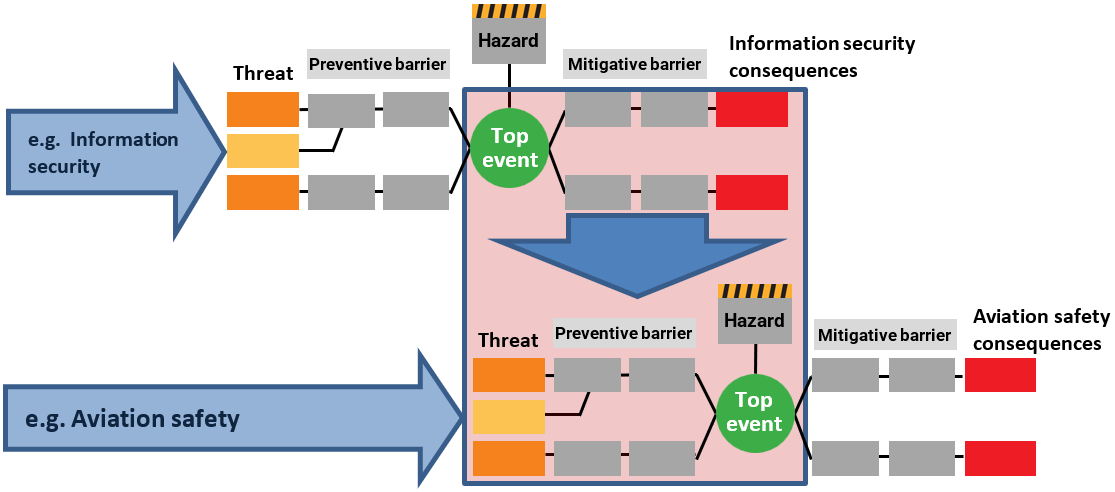


Ilustración 1. Representación de la gestión de los riesgos para la seguridad de la aviación que plantean las amenazas a la seguridad de la información. Extraída de GM del Reglamento 2023/203.

2.1. Pilares de un Sistema de Gestión de Seguridad de la Información

Se reproducen los mismos pilares mencionados en el apartado 2.1 de esta guía para el SGS.

2.1.1. *Política y objetivos de seguridad*

Son de aplicación los principios determinados por el apartado 2.1.2 de esta guía para el SGS, con la particularidad de que la política de seguridad deberá ser desarrollada y apoyada por la Dirección y llevar la firma de, al menos, el Director Responsable (DR) o Persona Responsable Común (CRP)[2], único para el Sistema de Gestión.

2.1.2. *Gestión de riesgos de seguridad*

Se considera recomendable mantener una gestión de riesgos de Seguridad de la Información coherente con la que el operador gestiona los riesgos de su SGS actual, determinando los procesos clave y los activos a los que afecta. Es de aplicación, por tanto, el apartado 2.1.2 del cuerpo de esta guía y debe aplicarse a aquellos riesgos de Seguridad de la Información que generen riesgos para la seguridad de la aviación.

[2] Entiéndase según aplique reglamentariamente la definición de Director Responsable (DR), Persona Responsable Común (CRP) o Gerente Responsable (GR). La figura del CRP es exclusiva del ámbito de Seguridad de la Información.

2.1.3. *Aseguramiento de la seguridad*

La observación continua de los procesos internos y de su entorno de operación para detectar Ver apartado 2.1.3 de esta guía, considerando siempre los aspectos de Seguridad de la Información.

2.1.4. *Promoción de la seguridad*

Conforme al apartado 2.1.4 de esta guía.

2.1.5. *Particularidades relativas a la gestión de la Seguridad de la Información*

Otros factores importantes para el éxito de la implementación y operación de un SGSI integrado en un SGS son los siguientes:

- **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 y la seguridad operacional**.
- El proceso de gestión de riesgos determina las características apropiadas de los controles preventivos para alcanzar y mantener niveles de riesgo aceptables.
- El proceso de gestión de incidentes garantiza que la organización detecte, reaccione y responda a los incidentes de Seguridad de la información de manera oportuna. Esto se logra definiendo responsabilidades, procedimientos, escenarios y planes de respuesta con anticipación para garantizar una respuesta coordinada, específica y eficiente.

El siguiente diagrama explicita las diferentes fases a seguir en el proceso de implementación (SGSI presente y adecuado) y su posterior operación (SGSI operativo o superiores).

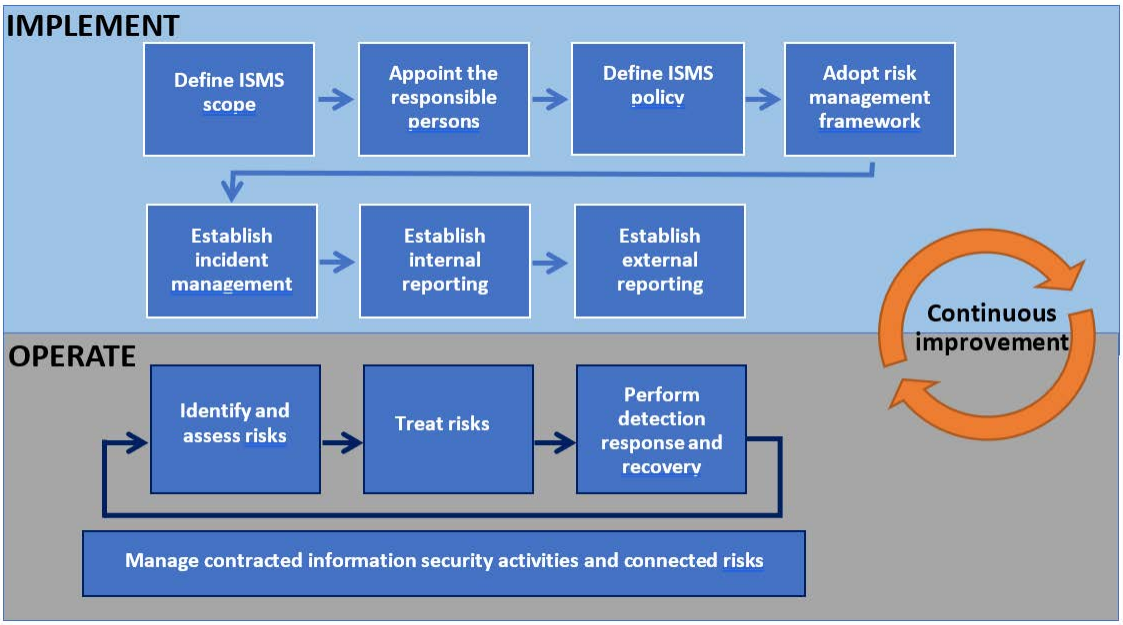


Ilustración 2. Representación de los requisitos de la Parte-IS desde la perspectiva del ciclo de vida de un SGSI.

Téngase en cuenta que:

- AESA aprobará de manera directa la edición inicial del MGSI como parte de una modificación del MSG.
- Las modificaciones del MSG que incluya el MSGI integrado se gestionarán mediante el procedimiento establecido por la organización para las modificaciones del MSG, que ahora deberá incluir las modificaciones relativas al MSGI y deberá ser aprobado por AESA.

2.2. Relación con ISO/IEC 27001

La norma internacional ISO/IEC 27001 es una norma ampliamente adoptada para la gestión de la Seguridad de la Información que especifica los requisitos genéricos para establecer, implementar, mantener y mejorar continuamente un SGSI. También incluye requisitos para la evaluación y el tratamiento de los riesgos de Seguridad de la Información. Los requisitos son aplicables a todas las entidades, independientemente de su tipo, tamaño o naturaleza. La ISO/IEC 27001 es compatible con otras normas de sistemas de gestión (calidad, seguridad, etc.).

La norma ISO/IEC 27001 permite a las entidades definir su propio alcance de auditoría y su propia tolerabilidad de riesgo organizativo. Esto, a su vez, conduce a requisitos de Seguridad de la Información que proporcionan al SGSI criterios para la aceptabilidad de los riesgos de Seguridad de la Información en línea con la tolerabilidad de riesgo de la entidad (véase la ilustración 4).

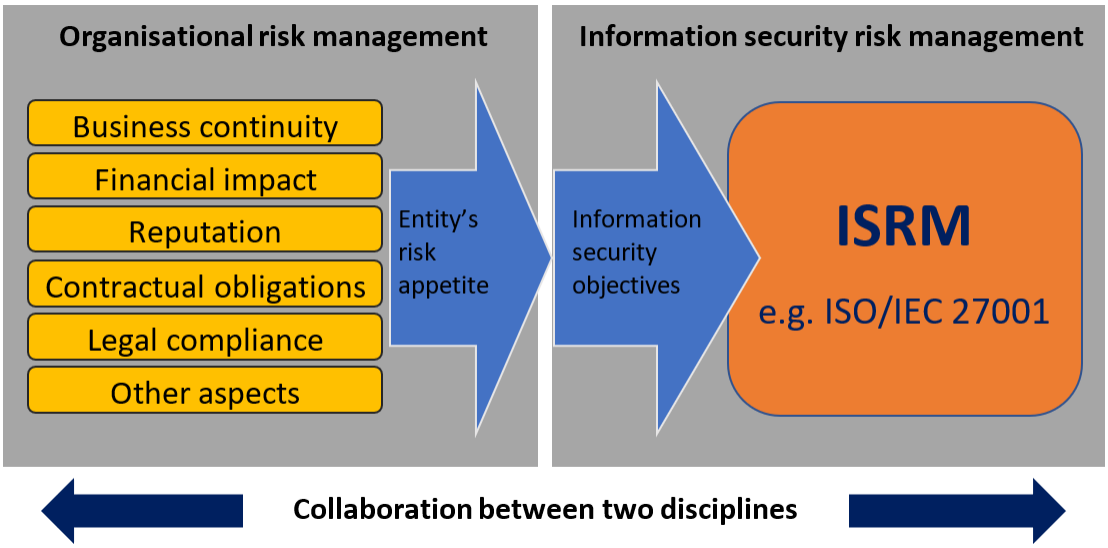


Ilustración 3. Relación entre tolerabilidad de Riesgos Organizacionales y Objetivos de Seguridad de la Información.

Los requisitos para un SGSI especificados por la Parte IS son en su mayoría coherentes y están alineados con la norma ISO/IEC 27001. ***No obstante, la Parte IS introduce disposiciones específicas en el contexto de la seguridad aérea***. Si una organización ya explota un SGSI basado en la norma

ISO/IEC 27001 para un ámbito y contexto diferentes, puede adaptarse y ampliarse al ámbito y contexto del Reglamento (UE) 2023/203 de manera sencilla sobre la base de un análisis del alcance y las diferencias determinando cuidadosamente los riesgos para la seguridad aérea, y considerando la integración con el propio SGS de la organización.

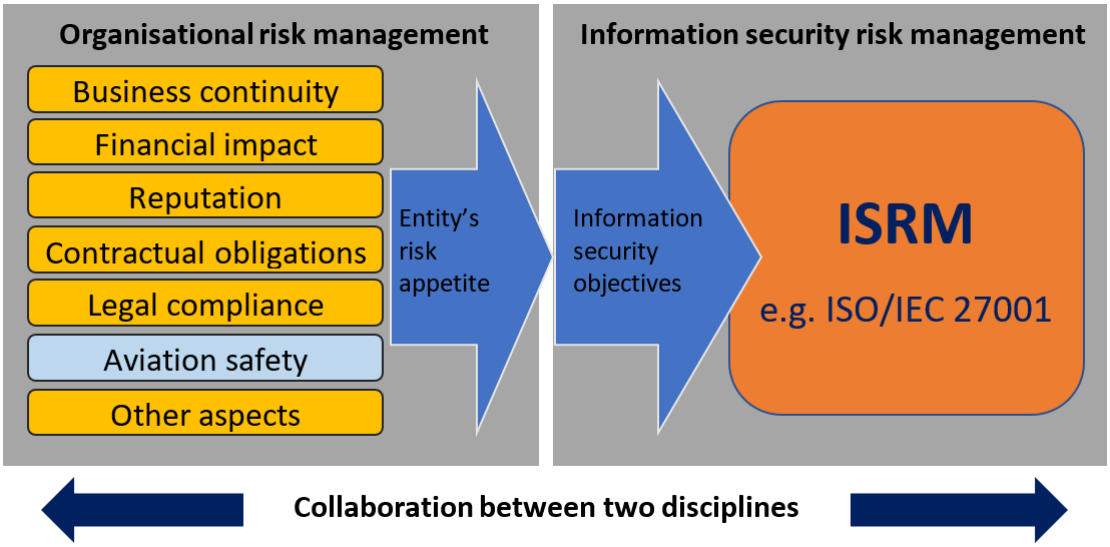


Ilustración 4. Introducción de los riesgos de aviación en la aceptación de riesgo de las organizaciones.

Para obtener una correspondencia entre las tareas principales requeridas en la Parte IS y las cláusulas y controles asociados en ISO/IEC 27001, se dispone del **Apéndice II de la Parte IS.I.OR**.

3. ESTRUCTURA DEL MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MSGI)

3.1. Generalidades

La organización describirá su Sistema de Gestión de Seguridad de la Información, el cual deberá abarcar los ámbitos recogidos en ORO.GEN.200, ORO.GEN.200A y IS.I.200 y ser coherente con el tamaño de la organización y la naturaleza y complejidad de sus actividades.

AESA recomienda para los operadores aéreos la integración del SGSI dentro del Sistema de Gestión de la organización, disponiendo de un único Manuel del Sistema de Gestión, y así se enfoca y describe este Apéndice. Deben abarcarse todas las actividades realizadas por la organización en virtud de sus aprobaciones, tanto si las realiza con personal propio o subcontratadas a otras organizaciones o entidades.

En caso de que las organizaciones subcontratadas contaran con un SGSI propio, deberán establecerse los mecanismos de coordinación adecuados entre los Sistemas de Gestión de cada organización, aunque la responsabilidad final siempre será de la organización primera.

En la tabla siguiente se recogen los procedimientos y programas a desarrollar por la organización en relación con el SGS y por su ampliación al SGSI.

	MSG		MSGSI	
PROCESO	**POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES**	**REQUISITO NORMATIVO**	**POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES**	**REQUISITO NORMATIVO**
1. Política y Objetivos de Seguridad	Política de Seguridad	ORO.GEN.200(a)(2), (a)(6)	Política de Seguridad de la Información	IS.I.OR.200(a)(1) IS.I.OR.250(a)(1), (a)(4)
	Política de Cultura Justa	Reg. 376/2014 Art.16(11) / ORO.GEN.200 (a)(2)	Política de Cultura Justa	IS.I.OR.200(a)(1) IS.I.OR.200(a)(13)
	Programa o Plan de Seguridad de la Organización	ORO.GEN.200 (a)(3)	Programa o Plan de Seguridad de la Organización	IS.I.OR.200 (a)(1); (a)(2); (a)(3) IS.I.205 (a)(b)(c) IS.I.OR.210 IS.I.OR.220 IS.I.OR.250 (a)(4)
	Sistema de Notificación de sucesos/eventos	Reg. 376/2014 Art.4, Art.5, Art.13, Art.16 ORO.GEN.160	Sistema de Notificación de sucesos/eventos	Reg. 376/2014 Art.4, Art.5, Art.13, Art.16 IS.I.OR.200 (a)(4) IS.I.OR.215 IS.I.OR.250(a)(8) IS.I.OR.200 (a)(8) IS.I.OR.230 IS.I.OR.220(a)
	Organigrama de la organización	ORO.GEN.210 (b), ORO.AOC.135 / CAMO.A.305 (a)(5) 145.A.30 (a) y (c) 21.A.143(a)	Organigrama de la organización	IS.I.OR.250(a)(7) IS.I.OR.200(d)
	Procedimiento de Rendición de cuentas y funciones y responsabilidades del DR y personal clave, incluyendo la responsabilidad de tolerabilidad del riesgo de la organización	ORO.GEN.200 (a)(1), (a)(5), ORO.GEN.210 (a), (b)	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.OR.200(a)(10) IS.I.OR.240 IS.I.OR.200(d) IS.I.OR.250(a)(9) IS.I.OR.250(a)(2), (a)(3), (a)(5), (a)(6)
	Plan de respuesta ante Emergencias	ORO.GEN.200 (a)(3)	Plan de respuesta ante Emergencias	IS.I.OR.220(c)

	MSG		MSGSI	
PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
	Procedimiento para gestionar la documentación y registro del sistema de gestión de seguridad de la información.	ORO.GEN.220	Procedimiento para gestionar la documentación y registro del sistema de gestión de seguridad de la información.	IS.I.OR.200(a)(11) IS.I.OR.245 IS.I.OR.200(c) IS.I.OR.250(a)(9) IS.I.OR.200(d)
2. Gestión de riesgos de seguridad	Procedimiento para la identificación de peligros.	ORO.GEN.200 (a)(3)	Procedimiento para la identificación de peligros.	IS.I.OR.200 (a)(2) IS.I.205 (a)(b) IS.I.OR.200(c)(d) IS.I.OR.250(a)(9)
	Procedimiento/Método de evaluación y mitigación del riesgo.	ORO.GEN.200 (a)(3)	Procedimiento/Método de evaluación y mitigación del riesgo.	IS.I.OR.200 (a)(2) IS.I.205 (c)(d) IS.I.OR.200(c)(d) IS.I.OR.250(a)(9) IS.I.OR.210(a) IS.I.OR.220
3. Aseguramiento de la Seguridad	Procedimiento de implementación y efectividad de medidas mitigadoras.	ORO.GEN.200 (a)(3)	Procedimiento de implementación y efectividad de medidas mitigadoras.	IS.I.OR.200 (a)(3); (a)(5) IS.I.OR.210 (a)(b) IS.I.OR.220 IS.I.OR.200(c)(d) IS.I.OR.250(a)(9)
	Procedimiento de rendimiento de la seguridad operacional	ORO.GEN.200 (a)(3)	Procedimiento de rendimiento de la seguridad operacional	IS.I.OR.200(a)(1) ;(b) IS.I..OR.250(a)(9) IS.I.OR.260
	Programa de indicadores de seguridad operacional	ORO.GEN.200 (a)(3)	Programa de indicadores de seguridad operacional	IS.I.OR.200(a)(2) IS.I.OR.200(d) IS.I.OR.205
	Procedimiento de Gestión del Cambio	ORO.GEN.200 (a)(3), ORO.GEN.130	Procedimientos de Gestión del Cambio	IS.I.200 (c) IS.I.OR.255 IS.I.OR.250(a)(9) IS.I.OR.250(c)
	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	Reg. 2018/1139 Annex II 3.1.(b), Annex V 8.1.(c) ORO.GEN.200 (a)(3), (a)(6)	Procedimiento para la supervisión y revisión de la efectividad del sistema de gestión.	IS.I.OR.200(b) IS.I.OR.250(a)(9) IS.I.OR.260
4. Promoción de la Seguridad	Programa de entrenamiento del sistema de gestión (gestión del riesgo y control de conformidad/calidad)	ORO.GEN.200 (a)(4)	Programa de entrenamiento del sistema de gestión de seguridad de la información	IS.I.OR.200 (a)(10) IS.I.OR.240 (g)
	Procedimiento para la promoción de la seguridad	ORO.GEN.200 (a)(4), (a)(5)	Procedimiento para la promoción de la seguridad	AMC1 IS.I.OR.200 (a)(1); (h) IS.I.OR.250(a)(9)
5. Control de conformidad y cumplimiento	Función de control de conformidad	ORO.GEN.200 (a)(6)	Función de control de conformidad	IS.I.OR.200(a)(12) IS.I.OR.200(d) IS.I.OR.250(a)(9)
	Programa de auditoría e inspecciones	ORO.GEN.200 (a)(6)	Programa de auditoría e inspecciones	IS.I.OR.200(a)(12) IS.I.OR.200(c)(d) IS.I.OR.250(a)(9)
	Procedimiento de seguimiento de no conformidades con la Autoridad	ORO.GEN.150	Procedimiento de seguimiento de no conformidades con la Autoridad	IS.I.OR.200 (a)(7) IS.I.OR.225 IS.I.OR.200(c)(d) IS.I.OR.250(a)(9)

	MSG		MSGSI	
PROCESO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO	POLITICAS / PROCEDIMIENTOS / PROGRAMAS / PLANES	REQUISITO NORMATIVO
	Procedimiento de reacción inmediata ante un problema de seguridad.	ORO.GEN.155	Procedimiento de reacción inmediata ante un problema de seguridad de la información.	IS.I.OR.200 (a)(6) IS.I.OR.200(d) IS.I.OR.220 (b) (c) IS.I.OR.250(a)(9)
	Procedimiento para medios de cumplimiento.	ORO.GEN.120	Procedimiento para medios de cumplimiento.	IS.I.OR.250(a)(10) IS.I.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.	ORO.GEN.205 CAMO.A.205 145.A.205 21.A.139(d)(2)(ii), GM1y2 21.A.139(d)(1) y AMC1 21.A.139 (d)(2)(ii) (b)(1)(ii)	Procedimiento para la gestión de actividades contratadas a otras organizaciones.	IS.I.OR.200 (a)(9) IS.I.OR.235 IS.I.OR.200(c)(d) IS.I.OR.250(a)(9) IS.I.OR.215 (c)(d)

3.2. Alcance

IS.I.OR.100; IS.I.OR.200 (a)(1)

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 MGSI se debe definir con justificaciones adecuadas del resultado y cualquier exclusión.

3.3. Política y objetivos de seguridad

En esta sección, la organización ampliará su política de seguridad contando ahora con los aspectos de Seguridad de la Información y considerando la dimensión y complejidad de la organización.

3.3.1. *Compromiso de la dirección*

3.3.1.1. Política de seguridad

IS.I.OR.250 (a)(1)

En esta sección se añadirá a la política de seguridad existente la de Seguridad de la Información firmada por el Director Responsable (en su caso por la Persona Responsable Común, CRP) que incluya un compromiso de mejora continua, recoja todos los requisitos legales y estándares aplicables, y considere las mejores prácticas. Además, debe confirmar que la organización trabajará en todo momento de conformidad con el anexo Parte IS.I.

La política de 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 de la gestión de la Seguridad de la Información 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;

Los cargos aprobados y gestores deberán promover de forma continua la política de Seguridad de la Información entre todo el personal, demostrar su compromiso con ella, proveer los recursos humanos y financieros necesarios y establecer objetivos de seguridad y normas de funcionamiento.

IS.I.OR.250 (a)(4)

La política de Seguridad de la Información incluirá una declaración para proporcionar recursos apropiados, al igual que ya se declara en la política del SGS.

Será revisada a intervalos periódicos o cuando ocurra un cambio que suponga una alteración o modificación notable con un impacto significativo en las operaciones de la organización, como un cambio estructural dentro de la organización debido a reorganizaciones, un cambio en los procesos de negocio (por ejemplo, trabajo desde casa, uso de dispositivos personales), una evolución tecnológica (por ejemplo, recursos informáticos distribuidos, inteligencia artificial/aprendizaje automático) o una evolución en el panorama de amenazas.

3.3.1.2. Política de cultura justa

IS.I.OR.200 (a)(1) y (a)(13)

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

3.3.1.3. Programa o plan de seguridad

IS.I.OR.200 (a)(1), (a)(2) y (a)(3); IS.I.205 (a)(b)(c); IS.I.OR.210; IS.I.OR.220; IS.I.OR.200(c)(d); IS.I.OR.250(a)(9); IS.I.OR.250 (a)(4), (a)(9)

Se establecerá un procedimiento para establecer los objetivos de Seguridad de la Información que sean consistentes con la política de seguridad y se definirán los medios para comunicarlos en toda la organización, en coherencia con los establecidos en el MGS.

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.

3.3.1.4. Sistema de notificación de sucesos/eventos

Organization Reg. 376/2014 Art. 4 Art. 5 Art. 13 Art. 16; IS.I.OR.200 (a)(4); IS.I.OR.215 ; IS.I.OR.250(a)(8); IS.I.OR.200 (a)(8); IS.I.OR.230; IS.I.OR.200(c)(d); IS.I.OR.250(a)(9); IS.I.OR.220(a)

Adicionalmente a lo especificado en esta guía para la notificación de sucesos de seguridad operacional, la organización integrará en su sistema de notificación ya descrito 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.

Este mecanismo será fácilmente accesible y comunicable y servirá para recopilar todas las notificaciones de eventos por parte del personal y de fuentes externas a la empresa, incluidos proveedores, socios, clientes, software de código abierto e investigadores de seguridad de la información. Las organizaciones deben llevar a cabo actividades de detección de incidentes[4] (IS.I.OR.220(a)) teniendo en cuenta el resultado de la evaluación de riesgos y la explotación de las nuevas vulnerabilidades[5] descubiertas.

Es una práctica común en las grandes organizaciones centralizar las operaciones de Seguridad de la Información en un centro de operaciones de seguridad (SOC) y hacer uso de un Sistema de gestión de eventos e información de Seguridad de la Información (SIEM). Un sistema SIEM recopila todos los eventos de fuentes, como archivos de registro, en una base de datos común y permite a los analistas y respondedores de un SOC conjunto revisar y actuar sobre estos eventos.

Las organizaciones que no tienen una capacidad SOC y no utilizan un sistema SIEM deben considerar cómo establecer procesos para cumplir con las capacidades de recopilación y evaluación requeridas, así como con los tiempos de detección y respuesta.

Este sistema interno de notificación de eventos de Seguridad de la Información permitirá:

- Determinar cuáles de los sucesos notificados se consideran incidentes o vulnerabilidades relacionadas con la Seguridad de la Información que pueden repercutir sobre la seguridad aérea.

---

[3] **«suceso de Seguridad de la Información»:** un suceso identificado de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o un fallo de los controles de seguridad de la información, o una situación previamente desconocida que puede ser pertinente para la seguridad de la información;

[4] **«incidente»:** todo suceso que tenga un efecto adverso real en la seguridad de las redes y los sistemas de información, tal como se definen en el artículo 4, apartado 7, de la Directiva (UE) 2016/1148.

[5] **«vulnerabilidad»:** defecto o debilidad presente en un activo o un sistema, en los procedimientos, en el diseño, en la aplicación o en las medidas de seguridad de la información que podría aprovecharse y dar lugar a un fallo o una violación de la política de seguridad de la información.

- Determinar cuáles son las causas de los incidentes y vulnerabilidades relacionados con la Seguridad de la Información determinados a partir de los sucesos notificados, así como los factores que contribuyen a ellos, y abordarlos en el contexto del proceso de gestión del riesgo relacionado con la Seguridad de la Información. La notificación, por tanto, es una fuente de identificación de peligros.
- Garantizar una evaluación de toda la información conocida y pertinente relativa a los incidentes y vulnerabilidades relacionados con la Seguridad de la Información notificados y evaluados, buscando repercusiones potenciales o reales en la seguridad de la aviación.
- Garantizar la aplicación de un método para distribuir internamente la información cuando sea necesario, recomendándose el uso del método ya establecido para los sucesos de seguridad de la aviación.

Los informes internos deben evaluarse de manera oportuna y, cuando el impacto potencial en la seguridad sea una condición insegura, proceder de acuerdo con el Sistema de Notificación de Sucesos del Sistema de Gestión. La organización cooperará en las investigaciones con cualquier otra organización que contribuya significativamente a la Seguridad de la información de sus propias actividades.

Toda entidad contratada que pueda exponer a la organización a riesgos relacionados con la Seguridad de la Información con posibles repercusiones sobre la seguridad aérea deberá notificar a la organización sus propios eventos de Seguridad de la Información como parte de la notificación interna y serán supervisados por la organización contratante.

Si las entidades contratadas también están sujetas a la Parte IS, el intercambio de información y la presentación de informes deben cubrirse en el marco de la gestión de riesgos compartidos y mediante el establecimiento de un acuerdo externo entre las organizaciones. El desarrollo de acuerdos externos se puede consultar en EUROCAE ED-201A, Capítulo 4.4 Acuerdos externos.

De manera más general, **cualquier contrato de servicios** debe incluir **cláusulas estándar relativas a las obligaciones de la organización contratada** de designar un punto de contacto para la gestión de incidentes y la posible gestión de crisis, de informar en un plazo acordado de los incidentes de Seguridad de la Información que puedan tener un impacto en la organización contratante y de notificar lo antes posible los que puedan dar lugar a condiciones inseguras y de tal manera que se cumpla la obligación de notificación externa;

Se contará también con un Sistema Externo de Notificación, que supondrá la ampliación del sistema de reporte del Sistema de Gestión para incluir las necesidades relativas a la Seguridad de la Información. Las responsabilidades se definirán complementariamente conforme al IS.I.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 de los sucesos.

Adicionalmente a los sucesos de notificación obligatoria definidos en el apartado 3.3.1.4 de la presente guía, se considerarán los siguientes en el ámbito de la Seguridad de la Información:

- 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.

La organización presentará una notificación tan pronto como sea posible, con un informe como máximo en las 72 horas siguientes al momento que se haya tenido conocimiento del suceso salvo circunstancias excepcionales, y conforme al procedimiento establecido por la organización. Este procedimiento deberá completarse en lo relativo a la Seguridad de la Información con un informe de seguimiento elaborado tan pronto se determinen las medidas que adopte la organización para recuperarse del incidente y las que propone para evitar incidentes similares, ante cualquier incidente o vulnerabilidad que pueda representar un riesgo significativo para la seguridad aérea.

La organización lo notificará también al titular de la aprobación de diseño de la aeronave o a la organización responsable del diseño del sistema o componente cuando tal incidente o vulnerabilidad afecte a una aeronave o a un sistema o componente asociado.

3.3.2. *Rendición de cuentas y responsabilidades de seguridad. Designación del personal clave*

En esta sección deberán incluirse la obligación de rendición de cuentas y responsabilidades del Director Responsable (DR) y, en su caso, la de la Persona Responsable Común (CRP) que es propio de organizaciones en las que se compartenestructuras organizativas, políticas, procesos y procedimientos de Seguridad de la Información con otras organizaciones o con áreas de su propia organización que no formen parte de la aprobación o declaración.

La organización deberá incluir un organigrama recogiendo las líneas de responsabilidad y obligación de rendición de cuentas a través de la organización, coordinado entre el personal del SGS y del SGSI.

IS.I.OR.200(a)(10); IS.I.OR.240; IS.I.OR.250 (a)(2), (a)(3), (a)(5), (a)(6), (a)(7), (a)(9)

Se nombrará un DR con plena responsabilidad y máxima rendición de cuentas sobre el SGSI, que deberá ser el mismo del SGS o, en caso contrario, determinarse un CRP.

El máximo responsable del SGSI es el DR (CRP), quien tiene la responsabilidad final, en nombre de la organización, de implementar y mantener al SGSI. Las autoridades y responsabilidades del DR (CRP) que no deben delegarse son análogas a las recogidas en el apartado 3.3.2 de esta guía, aplicadas lógicamente al cumplimiento de los requisitos de la Parte IS y a la propia Seguridad de la Información. Se añade la obligación de tener conocimiento básico del Reglamento (UE) 2023/203,

siendo capaz de explicar los objetivos generales del Reglamento y sus implicaciones para la organización y/o mediante realización de un curso de capacitación del Reglamento (UE) 2023/203.

Además, el DR debe tener conocimiento y comprender los principios y las prácticas relacionados con los sistemas de gestión de la Seguridad de la Información y los problemas clave de la gestión de riesgos dentro de la organización, y su forma de aplicación.

Se establecerán **medidas de coordinación** entre el Director Responsable de la organización y la Persona Responsable Común para garantizar una integración adecuada de la gestión de la Seguridad de la Información dentro de la organización garantizándose que:

- Se definen las responsabilidades y competencias en materia de Seguridad de la Información de la Persona Responsable Común.
- Se han establecido y comunicado a la Persona Responsable Común el alcance y los límites de las organizaciones.
- Se comunican y comparten los requisitos del reglamento con la Persona Responsable Común mediante una delegación adecuada, según sea necesaria, para aplicar los requisitos, incluyendo la autoridad y los medios financieros para establecer y controlar los recursos en todas las organizaciones, o partes de la organización involucradas.
- La Persona Responsable Común tiene acceso directo al DR.
- Los problemas se gestionan de forma proactiva y se documentan y se actúa en consecuencia contra cualquier señal de alerta temprana de incumplimiento.

Ver la guía ***DSA-SG-P01-GU02***, sobre evaluación de cargos responsables del SG y SGSI.

IS.I.OR.240 (b); IS.I.OR.250 (a)(2)

Adicionalmente 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 la vertiente del Sistema de Gestión enfocada a la Seguridad de Información. Podrá ser una figura independiente del RS o asumir éste la responsabilidad. El RSI dispondrá de una línea directa de reporte al DR o CRP como por ejemplo reuniones programadas y regulares. Deberá indicarse, además, el cargo que lo sustituye en caso de ausencia.

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 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 de la Información incluyen, entre otras:

- Garantizar cumplimiento normativo proactivo y documentado.
- Gestionar los riesgos relacionados con la ciberseguridad de la organización.
- Desarrollar, mantener y comunicar los procesos e informes de gestión de riesgos.
- Desarrollar la estrategia de gestión de riesgos de ciberseguridad, para identificar y evaluar los riesgos que podrían afectar a la seguridad operativa.
- Mantener un inventario identificado y categorizado de los activos de la organización, teniendo en cuenta los sistemas críticos para la seguridad y sus dependencias.
- 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.
- 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.
- Supervisar la eficacia de los controles de ciberseguridad y evaluar continuamente los niveles de riesgo desde una perspectiva de la seguridad operativa.
- 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.
- 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).
- Identificar, analizar, mitigar y comunicar los incidentes de ciberseguridad que afectan a la seguridad (Plan de Respuesta a Incidentes).
- Evaluar y gestionar las vulnerabilidades técnicas con un enfoque orientado a la seguridad.
- Evaluar (y reevaluar) 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.
- Establecer procedimientos para el análisis de incidentes, la presentación de informes sobre el manejo de incidentes y 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 manteniendo los registros adecuados.

- Cooperar con los Centros de Operaciones Seguras (SOC) y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT).

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.

Ver la guía ***DSA-SG-P01-GU02***, sobre evaluación de cargos responsables del SGS y del SGSI.

3.3.2.1. 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.

3.3.3. *Documentación del SGSI*

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

IS.I.OR.200 (c)

La organización, al crear y actualizar información documentada, debe asegurar una identificación y descripción apropiada (por ejemplo, un título, fecha, autor o número de referencia), así como una revisión y aprobación para su idoneidad y suficiencia. Y controlar la información documentada requerida por el SGSI para garantizar que esté disponible y sea adecuada para su uso, dónde y cuándo sea necesario. Además, debe asegurar que esté adecuadamente protegida (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad).

IS.I.OR.245

El formato de los registros será el especificado en los procedimientos de la organización para el SGS, identificando la informaciónde acuerdo con su nivel de clasificación de seguridad. Además se almacenarán utilizando medios que garanticen la integridad, autenticidad y acceso autorizado.

La organización deberá asegurarse de que se archiven, se evalúen periódicamente, se gestionen adecuadamente y sean trazables los siguientes registros durante al menos 5 años:

- Cualquier aprobación recibida y cualquier evaluación de riesgo de Seguridad de la Información asociada con el proceso de Derogación desde que la aprobación finalice su validez.
- Los contratos para actividades relacionadas para la implementación y mantenimiento del SGSI desde finalización o modificación de estos.
- Registros de los procesos clave.
- Registros de los riesgos identificados en la evaluación de riesgos junto con las medidas de tratamiento de riesgos asociadas.
- Registros de incidentes de Seguridad de la Información y vulnerabilidades reportados.

La organización deberá mantener registros de la cualificación y experiencia de su propio personal involucrado en actividades de gestión de Seguridad de la Información y los conservarán mientras la persona trabaje para la organización, y durante al menos 3 años después de que la persona la haya abandonado. El personal, a solicitud, tendrá acceso a sus registros individuales y la organización les proporcionará una copia de sus registros individuales al abandonar la organización.

Los registros deben mantenerse en papel o en formato electrónico o una combinación de ambos medios y permanecer accesibles siempre que sea necesario dentro de un tiempo razonable y utilizables durante todo el período de retención requerido. El período de retención comienza

cuando se ha creado el registro. La integridad de los datos de los registros, la disponibilidad y la autenticidad deben ser protegidas en coherencia con la protección de los datos operativos correspondientes, y estar dentro del alcance del SGSI.

Los sistemas de almacenamiento deben estar protegidos contra accesos no autorizados y, por lo tanto, deben tener medidas de Seguridad de la Información implementadas en coherencia con el nivel de riesgo de Seguridad de la Información asociado con ellos.

Una vez que ya no se requiere la retención de registros, la destrucción de registros y la desactivación de los activos utilizados para su almacenamiento deben implementarse de manera adecuada.

3.4. Gestión de riesgos de Seguridad de la Información

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.

3.4.1. *Identificación de peligros*

IS.I.OR.200(a)(2), IS.I.OR.205(a)(b)

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.

3.4.2. *Evaluación y mitigación de riesgos de Seguridad de la Información*

IS.I.OR.205(a)(b), IS.I.OR.210, IS.I.OR.220

En el caso de la evaluación y mitigación de riesgos de Seguridad de la Información se pueden consultar los documentos y metodologías EUROCAE ED-202A y EUROCAE ED-203. En todo caso, se

recomienda una coherencia y concordancia con el método usado por la organización para la evaluación de riesgos de seguridad. Así, se tendrán 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, a continuación implementar las medidas de mitigación 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 (CRP) 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.

3.5. Aseguramiento de la seguridad

En esta sección la organización describirá los procesos/métodos/procedimientos y las responsabilidades asociadas para el aseguramiento de la seguridad, siguiendo las mismas indicaciones ya mencionadas en el cuerpo de la Guía adaptadas a Seguridad de la Información.

IS.I.OR.200; IS.I.OR.210; IS.I.OR.255

3.5.1. *Gestión del cambio*

Conforme al punto IS.I.OR.255 la organización determinará, en un procedimiento que requiere de aprobación, los aspectos definidos en el apartado 3.4.2 de esta guía y los cambios que requieren aprobación previa.

Los peligros y riesgos identificados en la gestión del cambio se añadirán al registro de peligros y riesgos de la organización para su control y seguimiento.

Como regla general y por coherencia con los principios de la Gestión del Cambio del SGS, como mímino el procedimiento de la organización considerará como de aprobación previa por parte de AESA los descritos en el apartado 3.4.2 de esta guía:

- Cambios que afecten al ámbito de aplicación del AOC, a las especificaciones de sus operaciones o a los elementos del Sistema de Gestión de Seguridad de la Información de IS.I.OR.200 (a)(1) y (a)(2).
- Cambios en el personal designado de conformidad con IS.I.OR.200 y IS.I.OR.240 y sus líneas jerárquicas con el DR/CRP, incluyendo las responsabilidades y la rendición de cuentas.
- Cambios en la política de Seguridad de la Información y/o los objetivos de Seguridad de la Información con un impacto potencial en la seguridad de la aviación.
- El propio procedimiento de Gestión del Cambio relacionado en el primer párrafo de este apartado.

Por otro lado, no todos los cambios operativos relacionados con la Seguridad de la Información tienen un impacto en el SGSI teniendo que ser notificados o aprobados por AESA. Ejemplo de tales cambios pueden ser el lanzamiento de campañas de concienciación sobre ciberseguridad, cambios en herramientas de software de cifrado de archivos, reestructuraciones de índole comercial, etc.

3.5.2. *Mejora continua del SG. Supervisión y revisión de la efectividad del sistema de gestión*

La organización debe evaluar la madurez utilizando un modelo adecuado para identificar áreas de mejora en el MSG relativas a la Seguridad de la Información (ver modelos en GM1 IS.I.OR.260 (a)).

3.6. Promoción de la seguridad

3.6.1. *Instrucción y educación*

IS.I.OR.240 (g)

Existirá un programa de entrenamiento en el SGSI inicial y periódico. El entrenamiento abarcará los deberes de seguridad individuales (incluidos los roles, las responsabilidades y la rendición de cuentas) y cómo funciona el SGSI de la organización.

Existirá un procedimiento para garantizar que la organización tenga personal entrenado y competente.

Una organización puede utilizar, como guía inicial, un marco de competencia en ciberseguridad existente como el NICE (Iniciativa Nacional para la Educación en Ciberseguridad) basado en el Marco de Ciberseguridad del NIST (NIST CSF). En el Apéndice II de la Parte IS, se enumeran y mapean las tareas principales a las competencias derivadas del NIST CSF. Este mapeo puede usarse para establecer una línea base para identificar el gap de competencia. O bien, se recomienda más el uso del documento EASA "APPLICATION OF THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK TO AVIATION" para el gap de competencias. El cierre de este gap debe considerarse como el objetivo del programa de capacitación, que también debe incluir el alcance, contenido, los métodos de entrega (capacitación en aula, e-learning, notificaciones, capacitación en el trabajo) y • La frecuencia de la capacitación que mejor se ajuste a las necesidades de la organización, considerando el tamaño, alcance, competencias requeridas y complejidad de la organización.

Finalmente, a medida que la seguridad de la información/ciberseguridad evoluciona debido al aumento de nuevas amenazas, la organización debe revisar periódicamente la adecuación del programa de capacitación.

3.6.2. *Comunicación de la seguridad*

Las organizaciones que posean un Sistema de Gestión implantado y que integren su Sistema de Gestión de Seguridad de la Información en el mismo manual, deberán asegurarse de que la formación y la comunicación tanto interna como externa y las interfaces con otras empresas incluyen la Seguridad de la Información, siendo esta área gestionada por el RSI.

3.7. Responsabilidades de cumplimiento y función de control de conformidad

3.7.1. *Función de control de conformidad*

ORO.GEN.200A, IS.I.OR.200 (a) (12)

Se considera aplicable la guía proporcionada para el SGS.

3.7.2. *Programa de control de la conformidad*

IS.I.OR.200 (c) y (d); IS.I.OR.250 (a)(9)

Se considera aplicable la guía proporcionada para el SGS.

3.7.3. *Seguimiento de incidencias/no conformidades con la autoridad*

IS.I.OR.200 (a)(7)

Se considera aplicable la guía proporcionada para el SGS.

3.7.4. *Reacción inmediata ante un problema de seguridad*

IS.I.OR.220 (b) (c)

Se considera aplicable la guía proporcionada para el SGS.

Adicionalmente, 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 avisos (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.

3.7.5. *Medios de cumplimiento*

IS.I.OR.250(a)(10)

Se considera aplicable la guía proporcionada para el SGS.

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

IS.I.OR.200 (c) y (d); IS.I.OR.250 (a)(9)

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

Cuando la organización contrate un producto o servicio de Seguridad de la Información, debe asegurarse de que este cumple con los requisitos de aplicación, ya que la responsabilidad última del servicio o producto subcontratado recae sobre la organización. En esta sección, la organización debe definir las actuaciones que realizará sobre los contratistas y sus servicios o productos antes de su contratación y durante la prestación de los servicios.

Además, los riesgos de las actividades desarrolladas por las organizaciones contratadas deben estar bajo el control del sistema de gestión con atribuciones de Seguridad de la Información de la

organización (IS.I.OR.235). Para gestionar adecuadamente los riesgos asociados con las actividades contratadas, la organización debe cumplir con los siguientes criterios:

- Se lleva a cabo una evaluación previa de los proveedores antes de externalizar cualquier actividad de gestión de la Seguridad de la Información. La evaluación debe evaluar las competencias de los proveedores, la sostenibilidad, así como las calificaciones en relación con las actividades a contratar.
- Hay una evaluación de los riesgos asociados con la prestación de las actividades contratadas que ha sido acordada entre la organización bajo el Parte IS y la organización contratada.
- La organización establece y mantiene canales de comunicación adecuados sobre la Seguridad de la Información con la organización contratada.

Para valorar ejemplos de algunas actividades susceptibles de ser contratadas/subcontratadas ver GM3 IS.I.OR.235.

Para ejercer la supervisión de la organización contratada, la organización bajo la Parte IS debería tener:

- Un proceso para asegurar el cumplimiento de los requisitos de las actividades contratadas.
- Un proceso estructurado para seguir la ejecución esperada del contrato que incluya:
  - Definición y acuerdo sobre el alcance de las actividades.
  - Definición de los roles y responsabilidades de las partes (es decir, organización contratante y organización contratada).
  - Definición y revisión de los KPI.
  - Reacción ante desviaciones de las obligaciones contractuales.
  - Realización de auditorías de cumplimiento, de acuerdo con el alcance y los objetivos predefinidos, con el fin de evaluar las actividades operativas y de aseguramiento asociadas.
  - Provisión de retroalimentación sobre el resultado de las auditorías de cumplimiento tanto dentro de la organización como a la organización contratada, y respuesta a los hallazgos.

4. RESUMEN PARA INCLUIR EN EL MANUAL DEL SISTEMA DE GESTIÓN EL CONTENIDO DEL MANUAL DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN

MANUAL DEL SISTEMA DE GESTIÓN (MSG)	NUEVOS REQUISITOS AL MANUAL DEL SG	
	AFECTACIÓN	OBSERVACIONES
Política y objetivos de seguridad		
Alcance del SGSI	NUEVO	Desarrollar completamente
Compromiso de la dirección	Adaptar contenido	a) Refirmar compromiso del DR junto con los nuevos requisitos de la Parte IS b) En función del organigrama elegido por la organización (DR o

MANUAL DEL SISTEMA DE GESTIÓN (MSG)	NUEVOS REQUISITOS AL MANUAL DEL SG	
	AFECTACIÓN	OBSERVACIONES
		Responsable Común) estos requisitos podrán incluirse en una única declaración (punto a) o en varias declaraciones (SG y SGSI)
Rendición de cuentas y responsabilidades de seguridad	Adaptar contenido	a) Ampliar requisitos, responsabilidades del DR o Incorporar datos, requisitos y responsabilidades del Persona Responsable Común (CRP). En caso de este último desarrollar coordinación. b) Incorporar datos, requisitos y responsabilidades del Responsable de Seguridad de la Información (RSI). c) Incorporar 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.
Coordinación de la planificación	N/A	Punto no afectado por la Parte IS
Documentación del SGS	Adaptar contenido	La integridad de los datos de los registros, la disponibilidad y la autenticidad deben ser protegidas en coherencia con la protección de los datos operativos correspondientes, y como tal, deben estar dentro del alcance del SGSI.
Gestión de riesgos de seguridad		
Identificación de peligros	Adaptar contenido	El estudio, identificación y tratamiento de los peligros debe cubrir el alcance definido en este apéndice. Se debe tener en cuenta los riesgos relacionados con el personal (Ej.: Acceso no autorizado a sistemas)
Evaluación y mitigación de riesgos de seguridad	Adaptar contenido	La evaluación de riesgos deberá cubrir todos aquellos cambios de elementos, sujetos, interfaces, etc. relacionados con la seguridad de la información. Igualmente se deberá cubrir cualquier interfaz con riesgos compartidos con otras organizaciones.
Aseguramiento de la seguridad de la información		
Observación y medición del rendimiento en materia de seguridad	Adaptar contenido	Se deberán incorporar a los ya existentes propios del SGS, los indicadores de rendimiento de la información.
Gestión del cambio	Adaptar contenido	La Parte IS, introduce toda una serie de cambios con impacto en el SGSI que podrían llevar a un nivel inaceptable de riesgo que deben estar claramente definidos y clasificados como aprobables por AESA.
Mejora continua del SG	Adaptar contenido	Incorporar aspectos como evaluación de indicadores, monitorización de la efectividad de la parte del sistema de gestión relacionada con la Seguridad de la Información y personal encargo de realizarla.
Promoción de la seguridad		

MANUAL DEL SISTEMA DE GESTIÓN (MSG)	NUEVOS REQUISITOS AL MANUAL DEL SG	
	AFECTACIÓN	OBSERVACIONES
Instrucción y educación	Adaptar contenido	Incluir roles relacionados con la Parte IS y sus requisitos. Deberán incluirse los programas de entrenamiento inicial y recurrente en materia de seguridad para todo el personal de la organización y de otras organizaciones trabajando bajo la responsabilidad de la organización. Este entrenamiento debe ser acorde con sus responsabilidades y participación en materia de seguridad
Comunicación de la seguridad	Adaptar contenido	-
Responsabilidades de cumplimiento y función de control		
Función de control de conformidad	Adaptar contenido	Ampliar el contenido al concepto de "control del cumplimiento de Seguridad de la Información"
Programa de control de la conformidad	Adaptar contenido	Ampliar el contenido al concepto de "control del cumplimiento de Seguridad de la Información"
Seguimiento de incidencias	Adaptar contenido	-
Reacción inmediata ante un problema de seguridad	Adaptar contenido	-
Medios de cumplimiento	Adaptar contenido	Introducir en su programa de auditorías y sistema de control de conformidad los procedimientos y procesos clave que hayan sido identificados con el fin de controlar el cumplimiento de estos con la normativa vigente.
Gestión de actividades y/o servicios contratados		
Gestión de actividades y/o servicios contratados y/o subcontratados	Adaptar contenido	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. La Parte IS deberá estar claramente cubierta en todos los contratos (producto o servicio) relacionados con la de seguridad de la información, así como los riesgos de las actividades desarrolladas en dichos contratos.