BASE DE DATOS DE Norma CEF.-
Referencia: NCL013038

REGLAMENTO DELEGADO (UE) 2022/1645, DE LA COMISIÓN, de 14 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos relativos a la gestión de los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea destinados a las organizaciones contempladas en los Reglamentos (UE) n.º 748/2012 y (UE) n.º 139/2014 de la Comisión, y por el que se modifican los Reglamentos (UE) n.º 748/2012 y (UE) n.º 139/2014 de la Comisión.

(DOUE L 248, de 26 de septiembre de 2022)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) 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, y en particular su artículo 19, apartado 1, letra g), y su artículo 39, apartado 1, letra b),

Considerando lo siguiente:

(1) De conformidad con los requisitos esenciales establecidos en el anexo II, punto 3.1, letra b), del Reglamento (UE) 2018/1139, las organizaciones de diseño y producción deben aplicar y mantener un sistema de gestión para gestionar los riesgos de seguridad.

(2) Además, de conformidad con los requisitos esenciales establecidos en el anexo VII, puntos 2.2.1 y 5.2, del Reglamento (UE) 2018/1139, los operadores de aeródromos y las organizaciones responsables de proveer servicios de dirección de plataforma deben aplicar y mantener un sistema de gestión para gestionar los riesgos de seguridad.

(3) Los riesgos de seguridad mencionados en los considerandos 1 y 2 pueden surgir de diferentes fuentes, tales como los defectos de diseño y mantenimiento, los aspectos relacionados con el factor humano y las amenazas al medio ambiente y a la seguridad de la información. Por lo tanto, los sistemas de gestión que aplican las organizaciones mencionadas en los considerandos 1 y 2 deben tener en cuenta no solo los riesgos para la seguridad cuyo origen se encuentre en hechos fortuitos, sino también aquellos derivados de amenazas a la seguridad de la información, si los defectos existentes pueden ser aprovechados por individuos que actúen de mala fe. Estos riesgos relacionados con la seguridad de la información aumentan constantemente en el entorno de la aviación civil, ya que los sistemas de información actuales están cada vez más interconectados y se están convirtiendo con mayor frecuencia en el objetivo de este tipo de individuos.

(4) Los riesgos asociados a estos sistemas de información no se limitan a posibles ataques al ciberespacio, sino que abarcan también las amenazas que pueden afectar a los procesos y procedimientos, así como a la actuación de los seres humanos.

(5) Un número significativo de organizaciones ya utilizan normas internacionales, como la ISO 27001, para ocuparse de la seguridad de la información y los datos digitales. Es posible que estas normas no traten en su totalidad las especificidades de la aviación civil.

(6) Por lo tanto, conviene establecer requisitos para la gestión de los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea.

(7) Es esencial que estos requisitos cubran los distintos ámbitos de la aviación y sus interfaces, ya que la aviación es un sistema de sistemas altamente interconectado. Por lo tanto, deben aplicarse a todas las organizaciones que ya están obligadas a disponer de un sistema de gestión de conformidad con la legislación vigente en materia de seguridad aérea de la Unión.

(8) Los requisitos establecidos en el presente Reglamento deben aplicarse de manera coherente en todos los ámbitos de la aviación, generando al mismo tiempo un impacto mínimo sobre la legislación en materia de seguridad aérea de la Unión ya aplicable a dichos ámbitos.

(9) Los requisitos establecidos en el presente Reglamento deben entenderse sin perjuicio de los requisitos en materia de seguridad de la información y ciberseguridad establecidos en el punto 1.7 del anexo del Reglamento de Ejecución (UE) 2015/1998 de la Comisión y en el artículo 14 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo.

(10) La definición de «seguridad de la información» utilizada a efectos del presente acto jurídico no debe interpretarse como distinta de la definición de seguridad de las redes y sistemas de información establecida en la Directiva 2016/1148.

(11) A fin de evitar la duplicación de los requisitos legales, cuando las organizaciones cubiertas por el presente Reglamento ya estén sujetas a requisitos de seguridad derivados de los otros actos de la Unión mencionados en el considerando 9 que sean, en cuanto a su efecto, equivalentes a las disposiciones establecidas en el presente Reglamento, debe considerarse que el cumplimiento de aquellos requisitos de seguridad equivale al cumplimiento de los requisitos establecidos en el presente Reglamento.

(12) Las organizaciones cubiertas por el presente Reglamento que ya estén sujetas a los requisitos de seguridad derivados del Reglamento (UE) 2015/1998 deben cumplir asimismo los requisitos del anexo I (parte IS.D.OR.230, «Sistema externo de notificación sobre seguridad de la información») del presente Reglamento, ya que el Reglamento de Ejecución (UE) 2015/1998 no contiene ninguna disposición relativa a la notificación externa de incidentes relacionados con la seguridad de la información.

(13) Los Reglamentos (UE) n.º 748/2012 y (UE) n.º 139/2014 de la Comisión deben modificarse a fin de establecer el vínculo entre los sistemas de gestión prescritos en los Reglamentos antes citados y los requisitos de gestión de la seguridad de la información prescritos en el presente Reglamento.

(14) A fin de que las organizaciones dispongan de tiempo suficiente para garantizar el cumplimiento de las nuevas normas y procedimientos introducidos por el presente Reglamento, este debe aplicarse una vez transcurridos tres años desde su fecha de entrada en vigor.

(15) Los requisitos establecidos en el presente Reglamento se basan en el Dictamen n.º 03/2021, emitido por la Agencia de conformidad con el artículo 75, apartado 2, letras b) y c), y el artículo 76, apartado 1, del Reglamento (UE) 2018/1139.

(16) De conformidad con el artículo 128, apartado 4, del Reglamento (UE) 2018/1139, la Comisión consultó a los expertos designados por cada Estado miembro de acuerdo con los principios establecidos en el Acuerdo interinstitucional, de 13 de abril de 2016, sobre la mejora de la legislación.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1. *Objeto.*

El presente Reglamento establece los requisitos que deben cumplir las organizaciones mencionadas en el artículo 2 para detectar y gestionar riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea y afectar a los sistemas de tecnologías de la información y la comunicación y a los datos utilizados con fines de aviación civil, así como para detectar eventos de seguridad de la información y determinar cuáles de ellos se consideran incidentes de seguridad de la información con posibles repercusiones sobre la seguridad aérea, responder a dichos incidentes y recuperarse de ellos.

Artículo 2. *Ámbito de aplicación.*

1. El presente Reglamento se aplica a las organizaciones siguientes:

a) organizaciones de producción y organizaciones de diseño sujetas a las subpartes G y J de la sección A del anexo I (parte 21) del Reglamento (UE) n.º 748/2012, excepto las organizaciones de diseño y de producción que participan exclusivamente en el diseño o la producción de aeronaves ELA2, tal como se definen en el artículo 1, apartado 2, letra j), del Reglamento (UE) n.º 748/2012;

b) operadores de aeródromos y proveedores de servicios de dirección de plataforma sujetos al anexo III, «Parte relativa a los requisitos de las organizaciones (Parte ADR.OR)», del Reglamento (UE) n.º 139/2014.

2. El presente Reglamento se entiende sin perjuicio de los requisitos en materia de seguridad de la información y ciberseguridad establecidos en el punto 1.7 del anexo del Reglamento de Ejecución (UE) 2015/1998 de la Comisión y en el artículo 14 de la Directiva (UE) 2016/1148.

Artículo 3. *Definiciones.*

A los efectos del presente Reglamento, se entenderá por:

1) «seguridad de la información»: la preservación de la confidencialidad, integridad, autenticidad y disponibilidad de las redes y sistemas de información;
2) «evento de seguridad de la información»: un suceso detectado en el estado de un sistema, servicio o 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 desconocida hasta ese momento que puede tener importancia para la seguridad de la información;
3) «incidente»: todo hecho que tenga efectos adversos en la seguridad de las redes y sistemas de información, tal como se define en el artículo 4, apartado 7, de la Directiva (UE) 2016/1148;
4) «riesgo relacionado con la seguridad de la información»: el riesgo que implica la posibilidad de que se produzca un evento de seguridad de la información para las operaciones organizativas de la aviación civil, los activos, las personas y otras organizaciones; los riesgos relacionados con la seguridad de la información están asociados a la posibilidad de que las amenazas se aprovechen de las vulnerabilidades de un activo o grupo de activos de información;
5) «amenaza»: una posible violación de la seguridad de la información que existe desde el momento en que una entidad, circunstancia, acción o hecho puede ocasionar daños;
6) «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.

Artículo 4. *Requisitos derivados de otros actos legislativos de la Unión.*

1. Si una organización de las contempladas en el artículo 2 cumple requisitos de seguridad establecidos en el artículo 14 de la Directiva (UE) 2016/1148 que sean equivalentes a los requisitos establecidos en el presente Reglamento, se considerará que el cumplimiento de aquellos requisitos de seguridad constituye un cumplimiento de los requisitos establecidos en el presente Reglamento.

2. Si una organización de las contempladas en el artículo 2 es un operador o una entidad mencionada en los programas nacionales de seguridad para la aviación civil de los Estados miembros establecidos de conformidad con el artículo 10 del Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, los requisitos de ciberseguridad que figuran en el punto 1.7 del anexo del Reglamento de Ejecución (UE) 2015/1998 se considerarán equivalentes a los requisitos establecidos en el presente Reglamento, salvo en lo que respecta al punto IS.D.OR.230 del anexo del presente Reglamento, que deberá cumplirse.

3. La Comisión, previa consulta a la AESA y al Grupo de cooperación a que se refiere el artículo 11 de la Directiva (UE) 2016/1148, podrá emitir directrices para la evaluación de la equivalencia de los requisitos establecidos en el presente Reglamento y en la Directiva (UE) 2016/1148.

Artículo 5. *Autoridad competente.*

1. La autoridad responsable de certificar y supervisar el cumplimiento del presente Reglamento será:

a) en lo que respecta a las organizaciones contempladas en el artículo 2, letra a), la autoridad competente designada de conformidad con el anexo I (parte 21) del Reglamento (UE) n.º 748/2012;
b) en lo que respecta a las organizaciones contempladas en el artículo 2, letra b), la autoridad competente designada de conformidad con el anexo III (parte ADR.OR) del Reglamento (UE) n.º 139/2014.

2. A efectos del presente Reglamento, los Estados miembros podrán designar una entidad independiente y autónoma que desempeñe las funciones y responsabilidades asignadas a las autoridades competentes a que se refiere el apartado 1. En tal caso, se establecerán medidas de coordinación entre dicha entidad y las autoridades

competentes mencionadas en el apartado 1, a fin de garantizar una supervisión eficaz de todos los requisitos que debe cumplir la organización.

Artículo 6. *Modificación del Reglamento (UE) n.º 748/2012.*

El anexo I (parte 21) del Reglamento (UE) n.º 748/2012 se modifica como sigue:

1) El índice se modifica como sigue:

a) tras el título 21.A.139, se inserta el título siguiente:

«21.A.139A Sistema de gestión de la seguridad de la información»;

b) tras el título 21.A.239, se inserta el título siguiente:

«21.A.239A Sistema de gestión de la seguridad de la información».

2) Tras el punto 21.A.139, se inserta el punto 21.A.139A siguiente:

«21.A.139A Sistema de gestión de la seguridad de la información

Además del sistema de gestión de la producción exigido en el punto 21.A.139, la organización de producción deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento Delegado (UE) 2022/1645 de la Comisión a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»

3) Tras el punto 21.A.239, se inserta el punto 21.A.239A siguiente:

«21.A.239A Sistema de gestión de la seguridad de la información

Además del sistema de gestión del diseño exigido en el punto 21.A.239, la organización de diseño deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento Delegado (UE) 2022/1645 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»

Artículo 7. *Modificación del Reglamento (UE) n.º 139/2014.*

El anexo III (parte ADR.OR) del Reglamento (UE) n.º 139/2014 se modifica como sigue:

1) Tras el punto ADR.OR.D.005, se inserta el punto ADR.OR.D.005A siguiente:

«ADR.OR.D.005A Sistema de gestión de la seguridad de la información

El operador del aeródromo deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento Delegado (UE) 2022/1645 de la Comisión a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»

2) El punto ADR.OR.D.007 se sustituye por el texto siguiente:

«ADR.OR.D.007 Gestión de datos aeronáuticos e información aeronáutica

a) Como parte de su sistema de gestión, el operador del aeródromo implantará y mantendrá un sistema de gestión de la calidad que abarque las siguientes actividades:

1) sus actividades de datos aeronáuticos;
2) sus actividades de suministro de información aeronáutica.

b) Como parte de su sistema de gestión, el operador del aeródromo establecerá un sistema de gestión de la seguridad que garantice la protección de los datos operativos que reciba, produzca o utilice de otro modo, de manera que el acceso a dichos datos operativos esté limitado únicamente a las personas autorizadas.

c) El sistema de gestión de la seguridad definirá los siguientes elementos:

1) los procedimientos relativos al análisis y la mitigación de riesgos en materia de seguridad de los datos, al control y la mejora de la seguridad, a las evaluaciones de la seguridad y a la difusión de enseñanzas al respecto;

2) los medios elaborados para detectar fallos de seguridad y alertar al personal con los avisos oportunos;

3) los medios para controlar los efectos de los fallos de seguridad y determinar acciones de recuperación y procedimientos de reducción a fin de evitar que se repitan.

d) El operador del aeródromo garantizará la habilitación de seguridad de su personal en relación con la seguridad de los datos aeronáuticos.

e) Los aspectos relacionados con la seguridad de la información se gestionarán de conformidad con el punto ADR.OR. D.005A.»

3) Tras el punto ADR.OR.F.045, se inserta el punto ADR.OR.F.045A siguiente:

«ADR.OR.F.045A Sistema de gestión de la seguridad de la información

La organización responsable de la prestación de SDP deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento Delegado (UE) 2022/1645 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»

Artículo 8.

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*. Será aplicable a partir del 16 de octubre de 2025.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 14 de julio de 2022.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Seguridad de la información. requisitos de la organización

[PARTE-IS.D.OR]

IS.D.OR.100 Ámbito de aplicación
IS.D.OR.200 Sistema de gestión de la seguridad de la información

IS.D.OR.205 Evaluación de los riesgos relacionados con la seguridad de la información
IS.D.OR.210 Tratamiento de los riesgos relacionados con la seguridad de la información
IS.D.OR.215 Sistema interno de notificación en materia de seguridad de la información
IS.D.OR.220 Incidentes relacionados con la seguridad de la información: detección, respuesta y recuperación
IS.D.OR.225 Respuesta a las incidencias notificadas por la autoridad competente
IS.D.OR.230 Sistema externo de notificación en materia de seguridad de la información
IS.D.OR.235 Contratación de actividades de gestión de la seguridad de la información
IS.D.OR.240 Requisitos relativos al personal
IS.D.OR.245 Conservación de registros
IS.D.OR.250 Manual de gestión de la seguridad de la información (MGSI)
IS.D.OR.255 Cambios en el sistema de gestión de la seguridad de la información

IS.D.OR.260 Mejora continua
IS.D.OR.100 Ámbito de aplicación

En la presente parte se establecen los requisitos que deben cumplir las organizaciones contempladas en el artículo 2 del presente Reglamento.

IS.D.OR.200 Sistema de gestión de la seguridad de la información (SGSI)

a) A fin de alcanzar los objetivos establecidos en el artículo 1, la organización creará, implantará y mantendrá un sistema de gestión de la seguridad de la información (SGSI) que garantice que la organización:

1) establece una política en materia de seguridad de la información que determina los principios generales de la organización con respecto a las posibles repercusiones de los riesgos relacionados con la seguridad de la información sobre la seguridad aérea;
2) detecta y revisa los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.D. OR.205;
3) define y aplica medidas de tratamiento de los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.D.OR.210;
4) implanta un sistema interno de notificación en materia de seguridad de la información de conformidad con el punto IS.D.OR.215;
5) define y aplica, de conformidad con el punto IS.D.OR.220, las medidas necesarias para detectar eventos de seguridad de la información, determina cuáles de ellos se consideran incidentes con posibles repercusiones sobre la seguridad aérea -salvo lo permitido en el punto IS.D.OR.205, letra e)- y responde a dichos incidentes de seguridad de la información y se recupera de ellos;
6) aplica las medidas notificadas por la autoridad competente como reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea;
7) toma las medidas adecuadas, de conformidad con el punto IS.D.OR.225, para abordar las incidencias notificadas por la autoridad competente;
8) aplica un sistema externo de notificación de conformidad con el punto IS.D.OR.230 a fin de que la autoridad competente pueda adoptar las medidas adecuadas;
9) cumple los requisitos del punto IS.D.OR.235 cuando contrata alguna parte de las actividades mencionadas en el punto IS.D.OR.200 a otras organizaciones;
10) cumple los requisitos relativos al personal establecidos en el punto IS.D.OR.240;
11) cumple los requisitos de conservación de registros establecidos en el punto IS.D.OR.245;
12) supervisa el cumplimiento de los requisitos del presente Reglamento por parte de la organización y proporciona información sobre las incidencias al gestor responsable o, en el caso de las organizaciones de diseño, al responsable de la organización de diseño, a fin de garantizar la aplicación efectiva de las medidas correctoras;
13) protege, sin perjuicio de los requisitos de notificación de incidentes aplicables, la confidencialidad de cualquier información que la organización pueda haber recibido de otras organizaciones, en función de su nivel de sensibilidad.

b) A fin de cumplir ininterrumpidamente los requisitos contemplados en el artículo 1, la organización aplicará un proceso de mejora continua de conformidad con el punto IS.D.OR.260.
c) La organización documentará, de conformidad con el punto IS.D.OR.250, todos los procesos, procedimientos, funciones y responsabilidades clave necesarios para cumplir lo dispuesto en el punto IS.D.OR.200, letra a), y establecerá un proceso para modificar dicha documentación. Los cambios que se produzcan en esos procesos, procedimientos, funciones y responsabilidades se gestionarán de conformidad con el punto IS.D.OR.255.
d) Los procesos, procedimientos, funciones y responsabilidades establecidos por la organización para cumplir lo dispuesto en el punto IS.D.OR.200, letra a), corresponderán a la naturaleza y complejidad de sus actividades, sobre la base de una evaluación de los riesgos relacionados con la seguridad de la información inherentes a dichas actividades, y podrán integrarse en otros sistemas de gestión ya implantados por la organización.
e) Sin perjuicio de la obligación de cumplir los requisitos de información establecidos en el Reglamento (UE) n.º 376/2014 del Parlamento Europeo y del Consejo y los requisitos del punto IS.D.OR.200, letra a), punto 13, la autoridad competente podrá permitir que la organización no aplique los requisitos a que se refieren las letras a) a d), así como los requisitos relacionados que contienen los puntos IS.D.OR.205 a IS.D.OR.260, si demuestra a satisfacción de dicha autoridad que sus actividades, instalaciones y recursos, así como los servicios que gestiona, presta, recibe y mantiene, no plantean ningún riesgo relacionado con la seguridad de la información que pueda repercutir en la seguridad aérea, ni para ella misma ni para otras organizaciones. La aprobación se basará en una

evaluación del riesgo relacionado con la seguridad de la información documentada y realizada por la organización o un tercero de conformidad con el punto IS.D.OR.205 y revisada y aprobada por su autoridad competente.

El mantenimiento de la validez de dicha aprobación será revisado por la autoridad competente tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.

IS.D.OR.205 Evaluación de los riesgos relacionados con la seguridad de la información

a) La organización determinará, entre todos sus elementos, cuáles pueden estar expuestos a riesgos relacionados con la seguridad de la información. Esto incluirá:

1) las actividades, instalaciones y recursos de la organización, así como los servicios que la organización gestiona, presta, recibe o mantiene;

2) los equipos, sistemas, datos e información que contribuyan al funcionamiento de los elementos enumerados en el punto 1.

b) La organización identificará las interfaces que tiene con otras organizaciones y que podrían dar lugar a una exposición mutua a riesgos relacionados con la seguridad de la información.

c) Por lo que respecta a los elementos e interfaces a que se refieren las letras a) y b), la organización determinará los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea. Para cada riesgo identificado, la organización:

1) asignará un nivel de riesgo con arreglo a una clasificación predefinida establecida por la organización;

2) asociará cada riesgo y su nivel con el elemento o interfaz correspondiente determinado de conformidad con las letras a) y b).

La clasificación predefinida a que se refiere el punto 1 tendrá en cuenta el potencial para que suceda el escenario de amenaza y la gravedad de sus consecuencias para la seguridad. Atendiendo a dicha clasificación, y teniendo en cuenta si la organización tiene un proceso de gestión de riesgos estructurado y repetible para las operaciones, la organización deberá ser capaz de establecer si el riesgo es aceptable o debe tratarse de conformidad con el punto IS.D.OR.210.

A fin de facilitar la comparabilidad mutua de las evaluaciones de riesgos, la asignación del nivel de riesgo con arreglo al punto 1 tendrá en cuenta la información pertinente obtenida en coordinación con las organizaciones a que se refiere la letra b).

d) La organización revisará y actualizará la evaluación de riesgos efectuada de conformidad con las letras a), b) y c) en cualquiera de las situaciones siguientes:

1) si se produce un cambio en los elementos sujetos a riesgos relacionados con la seguridad de la información;

2) si se produce un cambio en las interfaces entre la organización y otras organizaciones, o en los riesgos comunicados por las otras organizaciones;

3) si se produce un cambio en la información o los conocimientos utilizados para la identificación, el análisis y la clasificación de riesgos;

4) si se han extraído enseñanzas del análisis de los incidentes relacionados con la seguridad de la información.

IS.D.OR.210 Tratamiento de los riesgos relacionados con la seguridad de la información

a) La organización elaborará medidas para hacer frente a los riesgos inaceptables detectados de conformidad con el punto IS.D.OR.205, las aplicará a su debido tiempo y comprobará que siguen siendo eficaces. Dichas medidas permitirán a la organización:

1) controlar las circunstancias que contribuyen a que suceda efectivamente el escenario de amenaza;

2) reducir las consecuencias para la seguridad aérea asociadas a la materialización del escenario de amenaza;

3) evitar los riesgos.

Dichas medidas no introducirán nuevos riesgos potenciales para la seguridad aérea que resulten inaceptables.

b) La persona a que se refiere el punto IS.D.OR.240, letras a) y b), y el resto del personal afectado de la organización serán informados del resultado de la evaluación de riesgos efectuada de conformidad con el punto IS.D.OR.205, los escenarios de amenaza correspondientes y las medidas que deban aplicarse.

La organización también informará a las organizaciones con las que tenga una interfaz de conformidad con el punto IS. D.OR.205, letra b), de cualquier riesgo compartido por ambas organizaciones.

IS.D.OR.215 Sistema interno de notificación en materia de seguridad de la información

a) La organización establecerá un sistema interno de notificación que permita la recopilación y evaluación de eventos de seguridad de la información, incluidos los que deben notificarse con arreglo al punto IS.D.OR.230.

b) Dicho sistema y el proceso a que se refiere el punto IS.D.OR.220 permitirán a la organización:

1) determinar cuáles de los hechos notificados con arreglo a la letra a) se consideran incidentes o vulnerabilidades relacionados con la seguridad de la información que pueden repercutir sobre la seguridad aérea;

2) identificar las causas de los incidentes y vulnerabilidades relacionados con la seguridad de la información determinados de acuerdo con el punto 1, 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 de conformidad con los puntos IS. D.OR.205 e IS.D.OR.220;

3) garantizar una evaluación de toda la información conocida y pertinente relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información determinados de acuerdo con el punto 1;

4) garantizar la aplicación de un método para distribuir internamente la información cuando sea necesario.

c) Toda organización 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 los eventos de seguridad de la información. Dichos informes se presentarán utilizando los procedimientos establecidos en los acuerdos contractuales específicos y se evaluarán de conformidad con la letra b).

d) La organización cooperará en las investigaciones con cualquier otra organización que contribuya significativamente a la seguridad de la información de sus propias actividades.

e) La organización podrá integrar ese sistema de notificación en otros sistemas de notificación que ya haya implantado.

IS.D.OR.220 Incidentes relacionados con la seguridad de la información: detección, respuesta y recuperación

a) Sobre la base del resultado de la evaluación de riesgos efectuada de conformidad con el punto IS.D.OR.205 y del resultado del tratamiento de los riesgos realizado de conformidad con el punto IS.D.OR.210, la organización aplicará medidas para detectar incidentes y vulnerabilidades que indiquen la posible materialización de riesgos inaceptables y que puedan repercutir sobre la seguridad aérea. Estas medidas de detección permitirán a la organización:

1) detectar desviaciones con respecto a los valores de referencia del rendimiento funcional predeterminados;

2) desencadenar avisos para activar medidas de respuesta adecuadas, en caso de desviación.

b) La organización aplicará medidas para responder a cualquier situación identificada de conformidad con la letra a) que pueda evolucionar o haber evolucionado hasta convertirse en un incidente relacionado con la seguridad de la información. Estas medidas de respuesta permitirán a la organización:

1) iniciar la reacción a los avisos mencionados en la letra a), punto 2, activando recursos y líneas de actuación predefinidos;

2) contener la propagación de un ataque e impedir la materialización plena de un escenario de amenaza;

3) controlar el modo de fallo de los elementos afectados definidos en el punto IS.D.OR.205, letra a).

c) La organización aplicará medidas destinadas a recuperarse de incidentes relacionados con la seguridad de la información, incluidas medidas de emergencia, en caso necesario. Estas medidas de recuperación permitirán a la organización:

1) eliminar la condición que causó el incidente o limitarla a un nivel tolerable;

2) alcanzar un estado de seguridad de los elementos afectados definidos en el punto IS.D.OR.205, letra a), dentro de un plazo de recuperación previamente definido por la organización.

IS.D.OR.225 Respuesta a las incidencias notificadas por la autoridad competente

a) Tras la recepción de la notificación de incidencias presentada por la autoridad competente, la organización:

1) identificará la causa o las causas principales del incumplimiento y los factores que contribuyeron a él;
2) definirá un plan de medidas correctoras;
3) demostrará que se ha corregido el incumplimiento a satisfacción de la autoridad competente.

b) Las acciones a que se refiere la letra a) se llevarán a cabo en el plazo acordado con la autoridad competente.

IS.D.OR.230 Sistema externo de notificación en materia de seguridad de la información

a) La organización aplicará un sistema de notificación en materia de seguridad de la información que cumpla los requisitos establecidos en el Reglamento (UE) n.º 376/2014 y sus actos delegados y de ejecución, si dicho Reglamento es aplicable a la organización.
b) Sin perjuicio de las obligaciones del Reglamento (UE) n.º 376/2014, la organización se asegurará de que se informe a su autoridad competente de cualquier incidente o vulnerabilidad en materia de seguridad de la información que pueda representar un riesgo significativo para la seguridad aérea. Además:

1) cuando tal incidente o vulnerabilidad afecte a una aeronave o a un sistema o componente asociado, la organización lo notificará también al titular de la aprobación de diseño;
2) cuando tal incidente o vulnerabilidad afecte a un sistema o componente utilizado por la organización, esta lo notificará a la organización responsable del diseño del sistema o componente.

c) La organización notificará las condiciones a que se refiere la letra b) del siguiente modo:

1) Presentará una notificación a la autoridad competente y, en su caso, al titular de la aprobación de diseño o a la organización responsable del diseño del sistema o componente, tan pronto como haya tenido conocimiento de la condición.
2) Presentará un informe a la autoridad competente y, en su caso, al titular de la aprobación de diseño o a la organización responsable del diseño del sistema o componente tan pronto como sea posible, pero, como máximo, en las 72 horas siguientes al momento en que haya tenido conocimiento de la condición, a no ser que circunstancias excepcionales lo impidan.
El informe se redactará en la forma definida por la autoridad competente y contendrá toda la información pertinente sobre la condición que la organización posea.
3) Presentará un informe de seguimiento a la autoridad competente y, en su caso, al titular de la aprobación de diseño o a la organización responsable del diseño del sistema o componente, en el que se detallen las medidas que la organización ha adoptado o tiene intención de adoptar para recuperarse del incidente y las que se propone tomar para evitar incidentes similares relacionados con la seguridad de la información en el futuro.
El informe de seguimiento se presentará tan pronto como se hayan determinado dichas medidas, y se elaborará en la forma definida por la autoridad competente.

IS.D.OR.235 Contratación de actividades de gestión de la seguridad de la información

a) La organización se asegurará de que, al contratar cualquier parte de las actividades mencionadas en el punto IS.D.OR.200 a otras organizaciones, las actividades contratadas cumplan los requisitos del presente Reglamento y la organización contratada trabaje bajo su supervisión. La organización velará por que los riesgos asociados a las actividades contratadas se gestionen adecuadamente.
b) La organización garantizará que la autoridad competente pueda tener acceso, previa solicitud, a la organización contratada para determinar si sigue cumpliendo los requisitos aplicables establecidos en el presente Reglamento.

IS.D.OR.240 Requisitos relativos al personal

a) El gestor responsable de la organización o, en el caso de las organizaciones de diseño, el responsable de la organización de diseño, designados de conformidad con el Reglamento (UE) n.º 748/2012 y el Reglamento (UE) n.º 139/2014, tal como se establece en el artículo 2, punto 1, letras a) y b), del presente Reglamento, tendrá

autoridad corporativa para garantizar que todas las actividades exigidas por el presente Reglamento puedan financiarse y llevarse a cabo. Dicha persona deberá:

1) garantizar que se dispone de todos los recursos necesarios para cumplir los requisitos del presente Reglamento;
2) establecer y promover la política de seguridad de la información a que se refiere el punto IS.D.OR.200, letra a), punto 1;
3) demostrar un conocimiento básico del presente Reglamento.

b) El gestor responsable o, en el caso de las organizaciones de diseño, el responsable de la organización de diseño, nombrará a una persona o grupo de personas que velarán por que la organización cumpla los requisitos del presente Reglamento, y definirá el alcance de su autoridad. Dicha persona o grupo de personas informará directamente al gestor responsable o, en el caso de las organizaciones de diseño, al responsable de la organización de diseño, y tendrá los conocimientos, la formación y la experiencia adecuados para ejercer sus responsabilidades. En los procedimientos deberá determinarse quién sustituye a una persona determinada en caso de ausencia prolongada de esta.
c) El gestor responsable o, en el caso de las organizaciones de diseño, el responsable de la organización de diseño, nombrará a una persona o grupo de personas con la responsabilidad de gestionar la función de control del cumplimiento mencionada en el punto IS.D.OR.200, letra a), punto 12.
d) Si la organización comparte estructura organizativa, 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, el gestor responsable o, en el caso de las organizaciones de diseño, el responsable de la organización de diseño podrá delegar sus actividades en una persona responsable común.
En tal caso, se establecerán medidas de coordinación entre el gestor responsable de la organización o, en el caso de las organizaciones de diseño, el responsable de la organización de diseño, y la persona responsable común para garantizar una integración adecuada de la gestión de la seguridad de la información en la organización.
e) El gestor responsable o el responsable de la organización de diseño, o bien la persona responsable común a que se refiere la letra d), tendrá autoridad corporativa para establecer y mantener las estructuras organizativas, políticas, procesos y procedimientos necesarios para aplicar el punto IS.D.OR.200.
f) La organización contará con un proceso que garantice que dispone de personal suficiente para llevar a cabo las actividades contempladas en el presente anexo.
g) La organización contará con un proceso que garantice que el personal a que se refiere la letra f) tenga la competencia necesaria para llevar a cabo sus tareas.
h) La organización contará con un proceso que garantice que el personal reconozca las responsabilidades asociadas a las funciones y tareas que tiene asignadas.
i) La organización velará por que se establezca adecuadamente la identidad y la fiabilidad del personal que tenga acceso a los sistemas de información y a los datos sujetos a los requisitos del presente Reglamento.

IS.D.OR.245 Conservación de registros

a) La organización conservará registros de sus actividades de gestión de la seguridad de la información.

1) La organización garantizará el archivo y la trazabilidad de los siguientes registros:

i) toda aprobación recibida y cualquier evaluación de los riesgos relacionados con la seguridad de la información asociada de conformidad con el punto IS.D.OR.200, letra e),
ii) contratos para las actividades mencionadas en el punto IS.D.OR.200, letra a), punto 9,
iii) registros de los procesos clave a que se refiere el punto IS.D.OR.200, letra d),
iv) registros de los riesgos detectados en la evaluación de riesgos a que se refiere el punto IS.D.OR.205, junto con las medidas asociadas de tratamiento de los riesgos a que se refiere el punto IS.D.OR.210,
v) registros de incidentes y vulnerabilidades relacionados con la seguridad de la información notificados de conformidad con los sistemas de notificación a que se refieren los puntos IS.D.OR.215 e IS.D.OR.230,
vi) registros de los eventos de seguridad de la información que puedan tener que reevaluarse para revelar incidentes o vulnerabilidades relacionados con la seguridad de la información no detectados.

2) Los registros a que se refiere el punto 1, inciso i), se conservarán al menos hasta cinco años después de que la aprobación haya perdido su validez.
3) Los registros a que se refiere el punto 1, inciso ii), se conservarán al menos hasta cinco años después de que el contrato haya sido modificado o resuelto.

4) Los registros a que se refiere el punto 1, incisos iii), iv) y v), se conservarán al menos durante un período de cinco años.

5) Los registros a que se refiere el punto 1, inciso vi), se conservarán hasta que dichos eventos de seguridad de la información se hayan vuelto a evaluar con arreglo a una periodicidad definida en un procedimiento establecido por la organización.

b) La organización llevará registros de la cualificación y experiencia del personal a su servicio que participe en actividades de gestión de la seguridad de la información.

1) Los registros de cualificación y experiencia del personal se conservarán mientras la persona trabaje para la organización y al menos hasta tres años después de que la persona haya abandonado la organización.

2) Los miembros del personal tendrán acceso, previa solicitud, a sus registros individuales. Además, previa solicitud, la organización les facilitará una copia de sus registros individuales al abandonar la organización.

c) El formato de los registros se especificará en los procedimientos de la organización.

d) Los registros deberán guardarse de forma que estén protegidos frente a daños, alteraciones y robo, y la información se clasificará, en caso necesario, de conformidad con su nivel de seguridad. La organización se asegurará de que los registros se almacenen utilizando métodos que garanticen la integridad, la autenticidad y el acceso autorizado.

IS.D.OR.250 Manual de gestión de la seguridad de la información (MGSI)

a) La organización pondrá a disposición de la autoridad competente un manual de gestión de la seguridad de la información (MGSI) y, en su caso, cualquier manual y procedimiento asociado referenciado que contenga:

1) una declaración firmada por el gestor responsable o, en el caso de las organizaciones de diseño, por el responsable de la organización de diseño, en la que se confirme que la organización trabajará en todo momento de conformidad con el presente anexo y con el MGSI; si el gestor responsable o, en el caso de las organizaciones de diseño, el responsable de la organización de diseño no es el director ejecutivo (consejero delegado) de la organización, este deberá refrendar la declaración;

2) el título, el nombre, las funciones, las obligaciones, las responsabilidades y las potestades de la persona o personas a que se refiere el punto IS.D.OR.240, letras b) y c);

3) el título, el nombre, las funciones, las obligaciones, las responsabilidades y las potestades de la persona responsable común a que se refiere el punto IS.D.OR.240, letras d), si procede;

4) la política de seguridad de la información de la organización a que se refiere el punto IS.D.OR.200, letra a), punto 1;

5) una descripción general del número y las categorías del personal y del sistema en vigor para planificar la disponibilidad de personal, como requiere el punto IS.D.OR.240;

6) el título, el nombre, las funciones, las obligaciones, las responsabilidades y las potestades de las personas clave responsables de la aplicación del punto IS.D.OR.200, incluida la persona o personas responsables de la función de control del cumplimiento a que se refiere el punto IS.D.OR.200, letra a), punto 12;

7) un organigrama que muestre las cadenas de obligaciones y responsabilidades asociadas de las personas a que se refieren los puntos 2 y 6;

8) la descripción del sistema interno de notificación a que se refiere el punto IS.D.OR.215;

9) los procedimientos que especifiquen la forma en que la organización garantiza el cumplimiento de la presente parte, y en particular:

i) el punto IS.D.OR.200, letra c), relativo a la documentación,

ii) los procedimientos que definen cómo controla la organización las actividades contratadas a que se refiere el punto IS.D.OR.200, letra a), punto 9,

iii) el procedimiento de modificación del MGSI definido en la letra c);

10) los detalles de los medios alternativos de cumplimiento aprobados.

b) La autoridad competente aprobará la edición inicial del MGSI y conservará una copia. El MGSI se modificará según sea necesario para seguir constituyendo una descripción actualizada del SGSI de la organización. Se entregará a la autoridad competente una copia de las modificaciones introducidas en el MGSI.

c) Las modificaciones del MGSI se gestionarán mediante un procedimiento establecido por la organización. Las modificaciones que no estén incluidas en el ámbito de este procedimiento, así como las modificaciones

relacionadas con los cambios a que se refiere el punto IS.D.OR.255, letra b), serán aprobadas por la autoridad competente.

d) La organización podrá integrar el MGSI con otras guías o manuales de gestión que posea, siempre que exista una referencia cruzada clara que indique qué partes de la guía o manual de gestión corresponden a los diferentes requisitos que figuran en el presente anexo.

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

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

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

Por lo que se refiere a estos cambios:

1) la solicitud deberá presentarse antes de que tenga lugar cualquiera de estos cambios, para que la autoridad competente pueda determinar si se sigue cumpliendo el presente Reglamento y, si fuera necesario, modificar el certificado de la organización y las correspondientes condiciones de aprobación que lleva adjuntas;

2) la organización pondrá a disposición de la autoridad competente toda la información que solicite para evaluar el cambio;

3) el cambio solo se aplicará tras la recepción de una aprobación formal por parte de la autoridad competente;

4) la organización operará bajo las condiciones prescritas por la autoridad competente durante la aplicación de dichos cambios.

IS.D.OR.260 Mejora continua

a) La organización evaluará, utilizando indicadores de rendimiento adecuados, la eficacia y madurez del SGSI. Dicha evaluación se llevará a cabo con arreglo a un calendario predefinido por la organización o a raíz de un incidente de seguridad de la información.

b) Si se detectan deficiencias tras la evaluación realizada de conformidad con la letra a), la organización adoptará las medidas de mejora necesarias para garantizar que el SGSI sigue cumpliendo los requisitos aplicables y mantiene los riesgos relacionados con la seguridad de la información a un nivel aceptable. Además, la organización reevaluará los elementos del SGSI afectados por las medidas adoptadas.