II

(Actos no legislativos)

REGLAMENTOS

REGLAMENTO DE EJECUCIÓN (UE) 2023/203 DE LA COMISIÓN

de 27 de octubre de 2022

por el que se establecen disposiciones de aplicación del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos relativos a la gestión de los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea destinados a las organizaciones contempladas en los Reglamentos (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011 y (UE) 2015/340 de la Comisión y los Reglamentos de Ejecución (UE) 2017/373 y (UE) 2021/664 de la Comisión, así como a las autoridades competentes contempladas en los Reglamentos (UE) n.º 748/2012, (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340 de la Comisión y en los Reglamentos de Ejecución (UE) 2017/373, (UE) n.º 139/2014 y (UE) 2021/664 de la Comisión, y por el que se modifican los Reglamentos (UE) n.º 1178/2011, (UE) n.º 748/2012, (UE) n.º 965/2012, (UE) n.º 139/2014, (UE) n.º 1321/2014 y (UE) 2015/340 de la Comisión y los Reglamentos de Ejecución (UE) 2017/373 y (UE) 2021/664 de la Comisión

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 ([1]), y en particular su artículo 17, apartado 1, letra b); su artículo 27, apartado 1, letra a); su artículo 31, apartado 1, letra b); su artículo 43, apartado 1, letra b); su artículo 53, apartado 1, letra a), y su artículo 62, apartado 15, letra c),

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 gestión del mantenimiento de la aeronavegabilidad y las organizaciones de mantenimiento 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 IV, punto 3.3, letra b), y punto 5, letra b), del Reglamento (UE) 2018/1139, las organizaciones de formación de pilotos y tripulantes de cabina de pasajeros, los centros de medicina aeronáutica para la tripulación y los operadores de dispositivos de simulación de vuelo para entrenamiento deben aplicar y mantener un sistema de gestión para gestionar los riesgos de seguridad.

(3) Asimismo, de conformidad con los requisitos esenciales establecidos en el anexo V, punto 8.1, letra c), del Reglamento (UE) 2018/1139, los operadores aéreos deben aplicar y mantener un sistema de gestión para gestionar los riesgos de seguridad.

(4) Por otra parte, de conformidad con los requisitos esenciales establecidos en el anexo VIII, punto 5.1, letra c), y punto 5.4, letra b), del Reglamento (UE) 2018/1139, los proveedores de servicios de gestión del tránsito aéreo y de navegación aérea, los proveedores de servicios de U-Space y los proveedores únicos de servicios de información común, así como las organizaciones de formación y los centros de medicina aeronáutica para los controladores de tránsito aéreo deben aplicar y mantener un sistema de gestión para gestionar los riesgos de seguridad.

([1]) DO L 212 de 22.8.2018, p. 1.

(5) Dichos riesgos de seguridad 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 la Agencia de la Unión Europea para la Seguridad Aérea («Agencia») y las organizaciones y autoridades nacionales competentes mencionadas en los considerandos anteriores deben tener en cuenta no solo los riesgos de 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.

(6) 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.

(7) 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 esas normas no traten en su totalidad las especificidades de la aviación civil. 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.

(8) Es esencial que estos requisitos cubran todos los ámbitos de la aviación y sus interfaces, ya que la aviación es un sistema de sistemas altamente interconectado. Por consiguiente, deben aplicarse a todas las organizaciones y autoridades competentes contempladas en los Reglamentos (UE) n.º 748/2012 ([2]), (UE) n.º 1321/2014 ([3]), (UE) n.º 965/2012 ([4]), (UE) n.º 1178/2011 ([5]), (UE) 2015/340 ([6]), (UE) n.º 139/2014 ([7]) de la Comisión y el Reglamento de Ejecución (UE) 2021/664 de la Comisión ([8]), también a aquellas 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. No obstante, algunas organizaciones deben quedar excluidas del ámbito de aplicación del presente Reglamento, a fin de garantizar la proporcionalidad adecuada con respecto a los menores riesgos relacionados con la seguridad de la información que plantean para el sistema de aviación.

(9) Los requisitos establecidos en el presente Reglamento deben garantizar una aplicación 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.

([2]) 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 (DO L 224 de 21.8.2012, p. 1).

([3]) 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 (DO L 362 de 17.12.2014, p. 1).

([4]) Reglamento (UE) n.º 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) n.º 216/2008 del Parlamento Europeo y del Consejo (DO L 296 de 25.10.2012, p. 1).

([5]) Reglamento (UE) n.º 1178/2011 de la Comisión, de 3 de noviembre de 2011, por el que se establecen requisitos técnicos y procedimientos administrativos relacionados con el personal de vuelo de la aviación civil en virtud del Reglamento (CE) n o 216/2008 del Parlamento Europeo y del Consejo (DO L 311 de 25.11.2011, p. 1).

([6]) Reglamento (UE) 2015/340 de la Comisión, de 20 de febrero de 2015, por el que se establecen requisitos técnicos y procedimientos administrativos relativos a las licencias y los certificados de los controladores de tránsito aéreo en virtud del Reglamento (CE) n.º 216/2008 del Parlamento Europeo y del Consejo, se modifica el Reglamento de Ejecución (UE) n.º 923/2012 de la Comisión y se deroga el Reglamento (UE) n.º 805/2011 de la Comisión (DO L 63 de 6.3.2015, p. 1).

([7]) Reglamento (UE) n.º 139/2014 de la Comisión, de 12 de febrero de 2014, por el que se establecen los requisitos y procedimientos administrativos relativos a los aeródromos, de conformidad con el Reglamento (CE) n.º 216/2008 del Parlamento Europeo y el Consejo (DO L 44 de 14.2.2014, p. 1).

([8]) Reglamento de Ejecución (UE) 2021/664 de la Comisión, de 22 de abril de 2021, sobre un marco regulador para el U-Space (DO L 139 de 23.4.2021, p. 161).

(10) 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 ([9]) y en el artículo 14 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([10]).

(11) Los requisitos de seguridad establecidos en los artículos 33 a 43 del título V «Seguridad del programa» del Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo ([11]) se consideran equivalentes a los requisitos establecidos en el presente Reglamento, salvo en lo que respecta al punto IS.I.OR.230 del anexo II del presente Reglamento, que debe cumplirse.

(12) Con el objetivo de proporcionar seguridad jurídica, la interpretación del término «seguridad de la información», tal como se define en el presente Reglamento, que refleja su uso común en la aviación civil a escala mundial, debe considerarse coherente con la del término «seguridad de las redes y sistemas de información», tal como se define en el artículo 4, apartado 2, de la Directiva (UE) 2016/1148. La definición de «seguridad de la información» utilizada a efectos del presente Reglamento no debe interpretarse como distinta de la definición de «seguridad de las redes y sistemas de información» establecida en la Directiva (UE) 2016/1148.

(13) 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 actos de la Unión mencionados en los considerandos (10) y 11 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.

(14) Las organizaciones cubiertas por el presente Reglamento que ya estén sujetas a los requisitos de seguridad derivados del Reglamento de Ejecución (UE) 2015/1998 o del Reglamento (UE) 2021/696, o ambos, deben cumplir asimismo los requisitos del anexo II (parte IS.I.OR.230, «Sistema externo de notificación sobre seguridad de la información») del presente Reglamento, ya que ninguno de los Reglamentos contiene disposiciones relativas a la notificación externa de incidentes relacionados con la seguridad de la información.

(15) En aras de la exhaustividad, los Reglamentos (UE) n.º 1178/2011, (UE) n.º 748/2012, (UE) n.º 965/2012, (UE) n.º 139/2014, (UE) n.º 1321/2014, (UE) 2015/340, y los Reglamentos de Ejecución (UE) 2017/373 de la Comisión ([12]) y (UE) 2021/664 deben modificarse para introducir los requisitos relativos al sistema de gestión de la seguridad de la información prescritos en el presente Reglamento, junto con los sistemas de gestión que en él se establecen, y para establecer los requisitos de las autoridades competentes en lo que respecta a la supervisión de las organizaciones que aplican dichos requisitos de gestión de la seguridad de la información.

(16) A fin de que las organizaciones dispongan de tiempo suficiente para garantizar el cumplimiento de las nuevas normas y procedimientos, el presente Reglamento debe aplicarse tres años después de su entrada en vigor, excepto en el caso del proveedor de servicios de navegación aérea del sistema europeo de navegación por complemento geoestacionario (EGNOS) definido en el Reglamento de Ejecución (UE) 2017/373, para el que, debido a la acreditación de seguridad en curso del sistema EGNOS y sus servicios de conformidad con el Reglamento (UE) 2021/696, debe ser aplicable a partir del 1 de enero de 2026.

(17) Los requisitos establecidos en el presente Reglamento se basan en el Dictamen n.º 03/2021 ([13]), 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.

([9]) Reglamento de Ejecución (UE) 2015/1998 de la Comisión, de 5 de noviembre de 2015, por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea (DO L 299 de 14.11.2015, p. 1).

([10]) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

([11]) Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo, de 28 de abril de 2021, por el que se crean el Programa Espacial de la Unión y la Agencia de la Unión Europea para el Programa Espacial y por el que se derogan los Reglamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 y (UE) n.º 377/2014 y la Decisión n.º 541/2014/UE (DO L 170 de 12.5.2021, p. 69).

([12]) Reglamento de Ejecución (UE) 2017/373 de la Comisión, de 1 de marzo de 2017, por el que se establecen requisitos comunes para los proveedores de servicios de gestión del tránsito aéreo/navegación aérea y otras funciones de la red de gestión del tránsito aéreo y su supervisión, por el que se derogan el Reglamento (CE) n.º 482/2008 y los Reglamentos de Ejecución (UE) n.º 1034/2011, (UE) n.º 1035/2011 y (UE) 2016/1377, y por el que se modifica el Reglamento (UE) n.º 677/2011 (DO L 62 de 8.3.2017, p. 1).

([13]) https://www.easa.europa.eu/document-library/opinions

(18) Los requisitos establecidos en el presente Reglamento se ajustan al dictamen del Comité para la aplicación de las normas comunes de seguridad en el ámbito de la aviación civil establecidas en el artículo 127 del Reglamento (UE) 2018/1139.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto

El presente Reglamento establece los requisitos que deben cumplir las organizaciones y las autoridades competentes para:

a) detectar y gestionar los 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 de las comunicaciones, así como a los datos utilizados con fines de aviación civil;

b) detectar eventos de seguridad de la información y determinar cuáles se consideran incidentes de seguridad de la información con posibles repercusiones sobre la seguridad aérea;

c) responder a dichos incidentes de seguridad de la información y recuperarse de ellos.

Artículo 2

Ámbito de aplicación

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

a) las organizaciones de mantenimiento sujetas a lo dispuesto en la sección A del anexo II (parte 145) del Reglamento (UE) n.º 1321/2014, excepto aquellas que participen exclusivamente en el mantenimiento de aeronaves de conformidad con el anexo V *ter* (parte ML) del Reglamento (UE) n.º 1321/2014;

b) las organizaciones de gestión del mantenimiento de la aeronavegabilidad («CAMO») sujetas a lo dispuesto en la sección A del anexo V *quater* (parte CAMO) del Reglamento (UE) n.º 1321/2014, excepto aquellas que participen exclusivamente en la gestión del mantenimiento de la aeronavegabilidad de las aeronaves de conformidad con el anexo V *ter* (parte ML) del Reglamento (UE) n.º 1321/2014;

c) los operadores aéreos sujetos a lo dispuesto en el anexo III (parte ORO) del Reglamento (UE) n.º 965/2012, excepto aquellos que participen exclusivamente en la operación de cualquiera de las siguientes aeronaves:

   i) una aeronave ELA2, tal como se define en el artículo 1, apartado 2, letra j), del Reglamento (UE) n.º 748/2012,

   ii) aviones monomotor propulsados por hélice con una configuración máxima operativa de asientos de pasajeros de cinco plazas o menos que no estén clasificados como aeronaves motopropulsadas complejas, cuando despeguen y aterricen en el mismo aeródromo o lugar de operación y operen de acuerdo con las reglas de vuelo visual (VFR) diurnas,

   iii) helicópteros monomotor con una configuración máxima operativa de asientos de pasajeros de cinco plazas o menos que no estén clasificados como aeronaves motopropulsadas complejas, cuando despeguen y aterricen en el mismo aeródromo o lugar de operación y operen de acuerdo con las VFR diurnas;

d) las organizaciones de instrucción reconocidas (ATO) sujetas a lo dispuesto en el anexo VII (parte ORA) del Reglamento (UE) n.º 1178/2011, excepto aquellas que participen exclusivamente en actividades de formación relacionadas con las aeronaves ELA2, tal como se definen en el artículo 1, apartado 2, letra j), del Reglamento (UE) n.º 748/2012, o en la formación teórica;

e) los centros de medicina aeronáutica para la tripulación sujetos a lo dispuesto en el anexo VII (parte ORA) del Reglamento (UE) n.º 1178/2011;

f) los operadores de dispositivos de simulación de vuelo para entrenamiento (FSTD) sujetos a lo dispuesto en el anexo VII (parte ORA) del Reglamento (UE) n.º 1178/2011, excepto aquellos que participen exclusivamente en la operación de FSTD para aeronaves ELA2, tal como se definen en el artículo 1, apartado 2, letra j), del Reglamento (UE) n.º 748/2012;

g) las organizaciones de formación de controladores de tránsito aéreo (ATCO TO) y los centros de medicina aeronáutica para ATCO sujetos a lo dispuesto en el anexo III (parte ATCO.OR) del Reglamento (UE) 2015/340;

h) las organizaciones sujetas a lo dispuesto en el anexo III (parte ATM/ANS.OR) del Reglamento de Ejecución (UE) 2017/373, excepto los siguientes proveedores de servicios:

i) los proveedores de servicios de navegación aérea titulares de un certificado limitado con arreglo al punto ATM/ANS.OR.A.010 de dicho anexo,

ii) los proveedores de servicios de información de vuelo que declaren sus actividades con arreglo al punto ATM/ANS.OR.A.015 de dicho anexo;

i) los proveedores de servicios de U-Space y los proveedores únicos de servicios de información común sujetos al Reglamento de Ejecución (UE) 2021/664.

2. El presente Reglamento se aplica a las autoridades competentes, incluida la Agencia de la Unión Europea para la Seguridad Aérea («Agencia»), mencionada en el artículo 6 del presente Reglamento y en el artículo 5 del Reglamento Delegado (UE) 2022/1645 de la Comisión ([14]).

3. El presente Reglamento también se aplica a la autoridad competente responsable de la expedición, prórroga, modificación, suspensión o revocación de las licencias de mantenimiento de aeronaves de conformidad con el anexo III (parte 66) del Reglamento (UE) n.º 1321/2014.

4. 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 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 reales 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;

([14]) Reglamento Delegado (UE) 2022/1645 de la Comisión, de 14 de julio de 2022, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos relativos a la gestión de los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea destinados a las organizaciones contempladas en los Reglamentos (UE) n.º 748/2012 y (UE) n.º 139/2014 de la Comisión, y por el que se modifican los Reglamentos (UE) n.º 748/2012 y (UE) n.º 139/2014 de la Comisión (DO L 248 de 26.9.2022, p. 18).

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 para las organizaciones y las autoridades competentes

1. Las organizaciones a que se refiere el artículo 2, apartado 1, deberán cumplir los requisitos establecidos en el anexo II (parte IS.I.OR) del presente Reglamento.

2. Las autoridades competentes a que se refiere el artículo 2, apartados 2 y 3, deberán cumplir los requisitos establecidos en el anexo I (parte IS.AR) del presente Reglamento.

Artículo 5

Requisitos derivados de otros actos legislativos de la Unión

1. Si una organización de las contempladas en el artículo 2, apartado 1, 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, apartado 1, 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 ([15]), 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.I.OR.230 del anexo II del presente Reglamento, que deberá cumplirse como tal.

3. Si la organización contemplada en el artículo 2, apartado 1, es el proveedor de servicios de navegación aérea del sistema europeo de navegación por complemento geoestacionario (EGNOS) a que se refiere el Reglamento (UE) 2021/696, los requisitos de seguridad que figuran en los artículos 33 a 43 del título V de dicho Reglamento se considerarán equivalentes a los requisitos establecidos en el presente Reglamento, salvo en lo que respecta al punto IS.I.OR.230 del anexo II del presente Reglamento, que deberá cumplirse como tal.

4. La Comisión, previa consulta a la Agencia 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 6

Autoridad competente

1. Sin perjuicio de las tareas encomendadas al Consejo de Acreditación de Seguridad a que se refiere el artículo 36 del Reglamento (UE) 2021/696, 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, apartado 1, letra a), la autoridad competente designada de conformidad con el anexo II (parte 145) del Reglamento (UE) n.º 1321/2014;

b) en lo que respecta a las organizaciones contempladas en el artículo 2, apartado 1, letra b), la autoridad competente designada de conformidad con el anexo V *quater* (parte CAMO) del Reglamento (UE) n.º 1321/2014;

([15]) Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n.º 2320/2002 (DO L 97 de 9.4.2008, p. 72).

c) en lo que respecta a las organizaciones contempladas en el artículo 2, apartado 1, letra c), la autoridad competente designada de conformidad con el anexo III (parte ORO) del Reglamento (UE) n.º 965/2012;

d) en lo que respecta a las organizaciones contempladas en el artículo 2, apartado 1, letras d) a f), la autoridad competente designada de conformidad con el anexo VII (parte ORA) del Reglamento (UE) n.º 1178/2011;

e) en lo que respecta a las organizaciones contempladas en el artículo 2, apartado 1, letra g), la autoridad competente designada de conformidad con el artículo 6, apartado 2, del Reglamento (UE) 2015/340;

f) en lo que respecta a las organizaciones contempladas en el artículo 2, apartado 1, letra h), la autoridad competente designada de conformidad con el artículo 4, apartado 1, del Reglamento de Ejecución (UE) 2017/373;

g) en lo que respecta a las organizaciones contempladas en el artículo 2, apartado 1, letra i), la autoridad competente designada de conformidad con el artículo 14, apartado 1 o 2, según proceda, del Reglamento de Ejecución (UE) 2021/664.

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.

3. La Agencia cooperará, respetando plenamente las normas aplicables en materia de protección del secreto, de los datos personales y de la información clasificada, con la Agencia de la Unión Europea para el Programa Espacial (EUSPA) y con el Consejo de Acreditación de Seguridad a que se refiere el artículo 36 del Reglamento (UE) 2021/696, a fin de garantizar una supervisión eficaz de los requisitos aplicables al proveedor de servicios de navegación aérea del EGNOS.

Artículo 7

Presentación de la información pertinente a las autoridades competentes en materia de SRI

Las autoridades competentes en virtud del presente Reglamento informarán, sin demora indebida, al punto de contacto único designado de conformidad con el artículo 8 de la Directiva (UE) 2016/1148 de cualquier información pertinente incluida en las notificaciones presentadas con arreglo al punto IS.I.OR.230 del anexo II del presente Reglamento y al punto IS.D.OR.230 del anexo I del Reglamento Delegado (UE) 2022/1645 por los operadores de servicios esenciales identificados de conformidad con el artículo 5 de la Directiva (UE) 2016/1148.

Artículo 8

Modificación del Reglamento (UE) n.º 1178/2011

Los anexos VI (parte ARA) y VII (parte ORA) del Reglamento (UE) n.º 1178/2011 se modifican de conformidad con el anexo III del presente Reglamento.

Artículo 9

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

El anexo I (parte 21) del Reglamento (UE) n.º 748/2012 se modifica de conformidad con el anexo IV del presente Reglamento.

Artículo 10

Modificación del Reglamento (UE) n.º 965/2012

Los anexos II (parte ARO) y III (parte ORO) del Reglamento (UE) n.º 965/2012 se modifican de conformidad con el anexo V del presente Reglamento.

Artículo 11

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

El anexo II (parte ADR.AR) del Reglamento (UE) n.º 139/2014 se modifica de conformidad con el anexo VI del presente Reglamento.

Artículo 12

Modificación del Reglamento (UE) n.º 1321/2014

Los anexos II (parte 145), III (parte 66) y V *quater* (parte CAMO) del Reglamento (UE) n.º 1321/2014 se modifican de conformidad con el anexo VII del presente Reglamento.

Artículo 13

Modificación del Reglamento (UE) 2015/340

Los anexos II (parte ATCO.AR) y III (parte ATCO.OR) del Reglamento (UE) 2015/340 se modifican de conformidad con el anexo VIII del presente Reglamento.

Artículo 14

Modificación del Reglamento de Ejecución (UE) 2017/373

Los anexos II (parte ATM/ANS.AR) y III (parte ATM/ANS.OR) del Reglamento de Ejecución (UE) 2017/373 se modifican de conformidad con el anexo IX del presente Reglamento.

Artículo 15

Modificación del Reglamento de Ejecución (UE) 2021/664

El Reglamento de Ejecución (UE) 2021/664 se modifica como sigue:

1) En el artículo 15, apartado 1, la letra f) se sustituye por la siguiente:

«f) aplican y mantienen un sistema de gestión de la protección de conformidad con el punto ATM/ANS.OR.D.010 de la subparte D del anexo III del Reglamento de Ejecución (UE) 2017/373 y un sistema de gestión de la seguridad de la información de conformidad con el anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203;».

2) En el artículo 18, se añade la letra l) siguiente:

«l) establecerán, aplicarán y mantendrán un sistema de gestión de la seguridad de la información de conformidad con el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203.».

Artículo 16

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 22 de febrero de 2026.

No obstante, en lo que respecta al caso del proveedor de servicios de navegación aérea del EGNOS sujeto al Reglamento de Ejecución (UE) 2017/373, será aplicable a partir del 1 de enero de 2026.

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

Hecho en Bruselas, el 27 de octubre de 2022.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

SEGURIDAD DE LA INFORMACIÓN. REQUISITOS APLICABLES A LAS AUTORIDADES

[PARTE IS.AR]

IS.AR.100 Ámbito de aplicación

En la presente parte se establecen los requisitos de gestión que deben cumplir las autoridades competentes contempladas en el artículo 2, apartado 2, del presente Reglamento.

Los requisitos que deben cumplir dichas autoridades competentes para el desempeño de sus actividades de certificación, supervisión y ejecución figuran en los Reglamentos mencionados en el artículo 2, apartado 1, del presente Reglamento y en el artículo 2 del Reglamento Delegado (UE) 2022/1645.

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

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

1) establece una política en materia de seguridad de la información que determina los principios generales de la autoridad competente 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.AR.205;

3) define y aplica medidas de tratamiento de los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.AR.210;

4) define y aplica, de conformidad con el punto IS.AR.215, 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 y responde a dichos incidentes de seguridad de la información y se recupera de ellos;

5) cumple los requisitos del punto IS.AR.220 cuando contrata alguna parte de las actividades descritas en el punto IS.AR.200 a otras organizaciones;

6) cumple los requisitos relativos al personal establecidos en el punto IS.AR.225;

7) cumple los requisitos de conservación de registros establecidos en el punto IS.AR.230;

8) supervisa el cumplimiento de los requisitos del presente Reglamento por parte de su propia organización y proporciona información sobre las incidencias a la persona a que se refiere el punto IS.AR.225, letra a), a fin de garantizar la aplicación efectiva de las medidas correctoras;

9) protege la confidencialidad de toda información que la autoridad competente pueda tener en relación con las organizaciones sujetas a su supervisión y la información recibida a través de los sistemas externos de notificación de la organización establecidos de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del presente Reglamento y el punto IS.I.OR.230 del anexo (parte IS.I.OR) del Reglamento Delegado (UE) 2022/1645;

10) notifica a la Agencia los cambios que afecten a la capacidad de la autoridad competente para desempeñar sus tareas y cumplir sus obligaciones, tal como se definen en el presente Reglamento;

11) define y pone en práctica procedimientos para compartir con otras autoridades y organismos competentes, así como organizaciones sujetas al presente Reglamento, según corresponda y de manera práctica y oportuna, la información pertinente que les permita efectuar evaluaciones eficaces de los riesgos de seguridad relacionados con sus actividades.

b) A fin de cumplir ininterrumpidamente los requisitos contemplados en el artículo 1, la autoridad competente aplicará un proceso de mejora continua de conformidad con el punto IS.AR.235.

c) La autoridad competente documentará todos los procesos, procedimientos, funciones y responsabilidades clave necesarios para cumplir lo dispuesto en el punto IS.AR.200, letra a), y establecerá un proceso para modificar dicha documentación.

d) Los procesos, procedimientos, funciones y responsabilidades establecidos por la autoridad competente para cumplir lo dispuesto en el punto IS.AR.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 autoridad competente.

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

a) La autoridad competente determinará, entre todos los elementos de su propia organización, cuáles pueden estar expuestos a riesgos relacionados con la seguridad de la información. Esto deberá incluir:

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

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

b) La autoridad competente identificará las interfaces que su propia organización 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 autoridad competente determinará los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea.

Para cada riesgo identificado, la autoridad competente:

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

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. Mediante dicha clasificación, y teniendo en cuenta si la autoridad competente tiene un proceso de gestión de riesgos estructurado y repetible para las operaciones, la autoridad competente deberá ser capaz de establecer si el riesgo es aceptable o debe tratarse de conformidad con el punto IS.AR.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 autoridad competente revisará y actualizará la evaluación de riesgos efectuada de conformidad con las letras a), b) y c) en cualquiera de los casos 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 de la autoridad competente 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.AR.210 Tratamiento de los riesgos relacionados con la seguridad de la información

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

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.AR.225, letra a), y el resto del personal afectado de la autoridad competente serán informados del resultado de la evaluación de riesgos efectuada de conformidad con el punto IS.AR.205, los escenarios de amenaza correspondientes y las medidas que deban aplicarse.

La autoridad competente también informará a las organizaciones con las que tenga una interfaz de conformidad con el punto IS.AR.205, letra b), de cualquier riesgo compartido entre la autoridad competente y la organización.

IS.AR.215 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.AR.205 y del resultado del tratamiento de los riesgos realizado de conformidad con el punto IS.AR.210, la autoridad competente aplicará medidas para detectar eventos que indiquen la posible materialización de riesgos inaceptables y que puedan repercutir sobre la seguridad aérea. Estas medidas de detección permitirán a la autoridad competente:

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 autoridad competente 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 autoridad competente:

1) iniciar la reacción de su propia organización 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.AR.205, letra a).

c) La autoridad competente 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 autoridad competente:

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

2) restablecer un estado de seguridad de los elementos afectados definidos en el punto IS.AR.205, letra a), dentro de un plazo de recuperación previamente definido por su propia organización.

IS.AR.220 Contratación de actividades de gestión de la seguridad de la información

La autoridad competente se asegurará de que, al contratar cualquier parte de las actividades mencionadas en el punto IS.AR.200 a otras organizaciones, las actividades contratadas cumplan los requisitos del presente Reglamento y la organización contratada trabaje bajo su supervisión. La autoridad competente velará por que los riesgos asociados a las actividades contratadas se gestionen adecuadamente.

IS.AR.225 Requisitos relativos al personal

La autoridad competente:

a) contará con una persona facultada para establecer y mantener las estructuras organizativas, las políticas, los procesos y los procedimientos necesarios para aplicar el presente Reglamento.

Esta persona:

1) estará facultada para acceder plenamente a los recursos necesarios para que la autoridad competente lleve a cabo todas las tareas requeridas por el presente Reglamento;

2) tendrá la delegación de poderes necesaria para llevar a cabo las tareas que le hayan sido asignadas;

b) contará con un proceso que garantice que dispone de personal suficiente para llevar a cabo las actividades contempladas en el presente anexo;

c) contará con un proceso que garantice que el personal a que se refiere la letra b) tenga la competencia necesaria para llevar a cabo sus tareas;

d) contará con un proceso que garantice que el personal reconozca las responsabilidades asociadas a las funciones y tareas que tiene asignadas;

e) 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.AR.230 Conservación de registros

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

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

i) contratos para las actividades mencionadas en el punto IS.AR.200, letra a), punto 5);

ii) registros de los procesos clave a que se refiere el punto IS.AR.200, letra d);

iii) registros de los riesgos detectados en la evaluación de riesgos a que se refiere el punto IS.AR.205, junto con las medidas asociadas de tratamiento de los riesgos a que se refiere el punto IS.AR.210;

iv) 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 el contrato haya sido modificado o resuelto.

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

4) Los registros a que se refiere el punto 1), inciso iv), 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 autoridad competente.

b) La autoridad competente 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 autoridad competente y al menos hasta tres años después de que la persona haya dejado de trabajar para la autoridad competente.

2) Los miembros del personal tendrán acceso, previa solicitud, a sus registros individuales. Además, previa solicitud, la autoridad competente les facilitará una copia de sus registros individuales al dejar de trabajar para la autoridad competente.

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

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 autoridad competente se asegurará de que los registros se almacenen utilizando métodos que garanticen la integridad, la autenticidad y el acceso autorizado.

IS.AR.235 Mejora continua

a) La autoridad competente evaluará, utilizando indicadores de rendimiento adecuados, la eficacia y madurez de su propio SGSI. La evaluación se realizará con arreglo a un calendario predefinido por la autoridad competente 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 autoridad competente 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 autoridad competente reevaluará los elementos del SGSI afectados por las medidas adoptadas.

ANEXO II

SEGURIDAD DE LA INFORMACIÓN. REQUISITOS DE LAS ORGANIZACIONES

[PARTE IS.I.OR]

IS.I.OR.100 Ámbito de aplicación

En la presente parte se establecen los requisitos que deben cumplir las organizaciones contempladas en el artículo 2, apartado 1, del presente Reglamento.

IS.I.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.I.OR.205;

3) define y aplica medidas de tratamiento de los riesgos relacionados con la seguridad de la información de conformidad con el punto IS.I.OR.210;

4) implanta un sistema interno de notificación en materia de seguridad de la información de conformidad con el punto IS.I.OR.215;

5) define y aplica, de conformidad con el punto IS.I.OR.220, las medidas necesarias para detectar eventos de seguridad de la información, determina cuáles de ellos se consideran incidentes con posibles repercusiones sobre la seguridad aérea —salvo lo permitido en el punto IS.I.OR.205, letra e)— y responde a dichos incidentes de seguridad de la información y se recupera de ellos;

6) aplica las medidas notificadas por la autoridad competente como reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea;

7) toma las medidas adecuadas, de conformidad con el punto IS.I.OR.225, para abordar las incidencias notificadas por la autoridad competente;

8) aplica un sistema externo de notificación de conformidad con el punto IS.I.OR.230 a fin de que la autoridad competente pueda adoptar las medidas adecuadas;

9) cumple los requisitos del punto IS.I.OR.235 cuando contrata alguna parte de las actividades mencionadas en el punto IS.I.OR.200 a otras organizaciones;

10) cumple los requisitos relativos al personal establecidos en el punto IS.I.OR.240;

11) cumple los requisitos de conservación de registros establecidos en el punto IS.I.OR.245;

12) supervisa el cumplimiento de los requisitos del presente Reglamento por parte de la organización y proporciona información sobre las incidencias al gestor responsable, a fin de garantizar la aplicación efectiva de las medidas correctoras;

13) protege, sin perjuicio de los requisitos de notificación de incidentes aplicables, la confidencialidad de cualquier información que la organización pueda haber recibido de otras organizaciones, en función de su nivel de sensibilidad.

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.I.OR.260.

c) La organización documentará, de conformidad con el punto IS.I.OR.250, todos los procesos, procedimientos, funciones y responsabilidades clave necesarios para cumplir lo dispuesto en el punto IS.I.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.I.OR.255.

d) Los procesos, procedimientos, funciones y responsabilidades establecidos por la organización para cumplir lo dispuesto en el punto IS.I.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 y los requisitos establecidos en el punto IS.I.OR.200, letra a), punto 13), la autoridad competente podrá permitir que la organización no aplique los requisitos a que se refieren las letras a) a d) ni los requisitos relacionados que figuran en los puntos IS.I.OR.205 a IS.I.OR.260 si demuestra a satisfacción de dicha autoridad que sus actividades, instalaciones y recursos, así como los servicios que gestiona, presta, recibe y mantiene, no plantean ningún riesgo relacionado con la seguridad de la información que pueda repercutir en la seguridad aérea, ni para ella misma ni para otras organizaciones. La aprobación se basará en una evaluación del riesgo relacionado con la seguridad de la información documentada y realizada por la organización o un tercero de conformidad con el punto IS.I.OR.205 y revisada y aprobada por su autoridad competente.

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

IS.I.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.I.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, según proceda, con las letras c) o e) 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.

e) Sin perjuicio de lo establecido en la letra c), las organizaciones que deban cumplir lo dispuesto en la subparte C del anexo III (parte ATM/ANS.OR) del Reglamento de Ejecución (UE) 2017/373 sustituirán el análisis de las repercusiones sobre la seguridad aérea por un análisis de las repercusiones sobre sus servicios con arreglo al estudio de seguridad exigido en el punto ATM/ANS.OR.C.005. Este estudio de seguridad se pondrá a disposición de los proveedores de servicios de tránsito aéreo a los que presten servicios, y dichos proveedores de servicios de tránsito aéreo serán responsables de evaluar las repercusiones sobre la seguridad aérea.

IS.I.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.I.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.I.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.I.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.I.OR.205, letra b), de cualquier riesgo compartido por ambas organizaciones.

IS.I.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.I.OR.230.

b) Dicho sistema y el proceso a que se refiere el punto IS.I.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) determinar cuáles son 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.I.OR.205 e IS.I.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.I.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.I.OR.205 y del resultado del tratamiento de los riesgos realizado de conformidad con el punto IS.I.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.I.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.I.OR.205, letra a), dentro de un plazo de recuperación previamente definido por la organización.

IS.I.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.I.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.I.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.I.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.I.OR.240 Requisitos relativos al personal

a) El gestor responsable de la organización designado de conformidad con los Reglamentos (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340, (UE) 2017/373 o el Reglamento de Ejecución (UE) 2021/664, según proceda, a que se refiere el artículo 2, apartado 1, 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.I.OR.200, letra a), punto 1);

3) demostrar un conocimiento básico del presente Reglamento.

b) El gestor responsable 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 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 nombrará a una persona o grupo de personas con la responsabilidad de gestionar la función de control del cumplimiento mencionada en el punto IS.I.OR.200, letra a), punto 12).

d) Si la organización comparte estructuras 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, el gestor responsable podrá delegar sus actividades en una persona responsable común.

En tal caso, se establecerán medidas de coordinación entre el gestor responsable de la organización 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 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.I.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.I.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.I.OR.200, letra e);

ii) contratos para las actividades mencionadas en el punto IS.I.OR.200, letra a), punto 9);

iii) registros de los procesos clave a que se refiere el punto IS.I.OR.200, letra d);

iv) registros de los riesgos detectados en la evaluación de riesgos a que se refiere el punto IS.I.OR.205, junto con las medidas asociadas de tratamiento de los riesgos a que se refiere el punto IS.I.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.I.OR.215 e IS.I.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.I.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 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 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 definidas en el punto IS.I.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 definida en el punto IS.I.OR.240, letra d), si procede;

4) la política de seguridad de la información de la organización a que se refiere el punto IS.I.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.I.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.I.OR.200, incluida la persona o personas responsables de la función de control del cumplimiento a que se refiere el punto IS.I.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.I.OR.215;

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

i) la documentación mencionada en el punto IS.I.OR.200, letra c);

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

iii) el procedimiento de modificación del MGSI a que se refiere 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.I.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.I.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.I.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.

ANEXO III

Los anexos VI (parte ARA) y VII (parte ORA) del Reglamento (UE) n.º 1178/2011 se modifican como sigue:

1) El anexo VI (parte ARA) se modifica como sigue:

a) en el punto ARA.GEN.125 se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203.»;

b) tras el punto ARA.GEN.135, se inserta el punto ARA.GEN.135A siguiente:

«**ARA.GEN.135A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto ARA.GEN.125, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.»;

c) en el punto ARA.GEN.200, se añade la letra e) siguiente:

«e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

d) el punto ARA.GEN.205 queda modificado como sigue:

i) el título se sustituye por el texto siguiente:

«**ARA.GEN.205 Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ORA.GEN.200A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto ARA.GEN.200, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

e) en el punto ARA.GEN.300, se añade la letra g) siguiente:

«g) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ORA.GEN.200A por parte de la organización, además de cumplir lo dispuesto en las letras a) a f), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.»;

f) tras el punto ARA.GEN.330, se inserta el punto ARA.GEN.330A siguiente:

«**ARA.GEN.330A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.I.OR.255, letra a), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto ARA.GEN.300. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto ARA.GEN.350.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.I.OR.255, letra b), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

2) El anexo VII (parte ORA) se modifica como sigue:

Tras el punto ORA.GEN.200, se inserta el punto ORA.GEN.200A siguiente:

«**ORA.GEN.200A Sistema de gestión de la seguridad de la información**

Además del sistema de gestión a que se refiere el punto ORA.GEN.200, la organización deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.».

ANEXO IV

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.B.20, se inserta el título siguiente:

"21.B.20A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea";

b) el título del punto 21.B.30 se sustituye por el siguiente:

"21.B.30 Atribución de tareas";

c) tras el título 21.B.240, se inserta el título siguiente:

"21.B.240A Cambios en el sistema de gestión de la seguridad de la información";

d) tras el título 21.B.435, se inserta el título siguiente:

"21.B.435A Cambios en el sistema de gestión de la seguridad de la información";

2) en el punto 21.B.15, se añade la letra c) siguiente:

"c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.D.OR.230 del anexo (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645.";

3) tras el punto 21.B.20, se inserta el punto 21.B.20A siguiente:

"21.B.20A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto 21.B.15, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.";

4) en el punto 21.B.25, se añade la letra e) siguiente:

"e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.";

5) el punto 21.B.30 queda modificado como sigue:

a) el título se sustituye por el texto siguiente:

“21.B.30 Atribución de tareas”;

b) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento de los puntos 21.A.139A y 21.A.239A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto 21.B.25, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

6) en el punto 21.B.221, se añade la letra g) siguiente:

“g) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto 21.A.139A por parte de la organización, además de cumplir lo dispuesto en las letras a) a f), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.”;

7) tras el punto 21.B.240, se inserta el punto 21.B.240A siguiente:

“**21.B.240A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.D.OR.255, letra a), del anexo (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto 21.B.221. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto 21.B.225.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.D.OR.255, letra b), del anexo (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.”;

8) en el punto 21.B.431, se añade la letra d) siguiente:

“d) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto 21.A.239A por parte de la organización, además de cumplir lo dispuesto en las letras a) a c), la autoridad competente se ajustará a los siguientes principios:

1) la autoridad competente revisará las interfaces y los riesgos asociados detectados de conformidad con el punto IS.D.OR.205, letra b), del anexo (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645 para cada organización sujeta a su supervisión;

2) si se detectan discrepancias en las interfaces mutuas y los riesgos asociados detectados por diferentes organizaciones, la autoridad competente las revisará con las organizaciones afectadas y, en caso necesario, planteará las conclusiones adecuadas para garantizar la aplicación de medidas correctoras;

3) cuando la revisión de la documentación con arreglo al punto 2) revele la existencia de riesgos importantes asociados a las interfaces con organizaciones sujetas a la supervisión de otra autoridad competente en el mismo Estado miembro, esta información se comunicará a la autoridad competente correspondiente.";

9) tras el punto 21.B.435, se inserta el punto 21.B.435A siguiente:

«**21.B.435A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.D.OR.255, letra a), del anexo (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto 21.B.431. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto 21.B.433.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.D.OR.255, letra b), del anexo (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio;».

ANEXO V

Los anexos II (parte ARO) y III (parte ORO) del Reglamento (UE) n.º 965/2012 se modifican como sigue:

1) El anexo II (parte ARO) se modifica como sigue:

a) en el punto ARO.GEN.125, se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203.»;

b) tras el punto ARO.GEN.135, se inserta el punto ARO.GEN.135A siguiente:

«**ARO.GEN.135A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto ARO.GEN.125, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.»;

c) en el punto ARO.GEN.200, se añade la letra e) siguiente:

«e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

d) el punto ARO.GEN.205 queda modificado como sigue:

i) el título se sustituye por el texto siguiente:

«**ARO.GEN.205 Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ORO.GEN.200A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto ARO.GEN.200, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

e) en el punto ARO.GEN.300, se añade la letra g) siguiente:

«g) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ORO.GEN.200A por parte de la organización, además de cumplir lo dispuesto en las letras a) a f), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.»;

f) tras el punto ARO.GEN.330, se inserta el punto ARO.GEN.330A siguiente:

«**ARO.GEN.330A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.I.OR.255, letra a), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto ARO.GEN.300. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto ARO.GEN.350.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.I.OR.255, letra b), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

2) El anexo III (parte ORO) se modifica como sigue:

tras el punto ORO.GEN.200, se inserta el punto ORO.GEN.200A siguiente:

«**ORO.GEN.200A Sistema de gestión de la seguridad de la información**

Además del sistema de gestión a que se refiere el punto ORO.GEN.200, el operador deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.».

ANEXO VI

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

1) En el punto ADR.AR.A.025, se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.D.OR.230 del anexo I (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645.».

2) Tras el punto ADR.AR.A.030, se inserta el punto ADR.AR.A.030A siguiente:

«**ADR.AR.A.030A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto ADR.AR.A.025, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.».

3) En el punto ADR.AR.B.005, se añade la letra d) siguiente:

«d) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.».

4) El punto ADR.AR.B.010 queda modificado como sigue:

i) el título se sustituye por el texto siguiente:

«**ADR.AR.B.010 Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ADR.OR.D.005A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto ADR.AR.B.005, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.».

5) En el apartado ADR.AR.C.005, se añade la letra f) siguiente:

«f) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ADR.OR.D.005A por parte de la organización, además de cumplir lo dispuesto en las letras a) a e), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.».

6) Tras el punto ADR.AR.C.040, se inserta el punto ADR.AR.C.040A siguiente:

«**ADR.AR.C.040A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.D.OR.255, letra a), del anexo I (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto ADR.AR.C.005. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto ADR.AR.C.055.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.D.OR.255, letra b), del anexo I (parte IS.D.OR) del Reglamento Delegado (UE) 2022/1645:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

ANEXO VII

Los anexos II (parte 145), III (parte 66) y V *quater* (parte CAMO) del Reglamento (UE) n.º 1321/2014 se modifican como sigue:

1) El anexo II (parte 145) se modifica como sigue:

a) el índice se modifica como sigue:

i) tras el título 145.A.200, se inserta el título siguiente:

«145.A.200A Sistema de gestión de la seguridad de la información»;

ii) tras el título 145.B.135, se inserta el título siguiente:

«145.B.135A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea»;

iii) el título del punto 145.B.205 se sustituye por el siguiente:

«145.B.205 Atribución de tareas»;

iv) tras el título 145.B.330, se inserta el título siguiente:

«145.B.330A Cambios en el sistema de gestión de la seguridad de la información»;

b) tras el punto 145.A.200, se inserta el punto 145.A.200A siguiente:

«145.A.200A **Sistema de gestión de la seguridad de la información**

Además del sistema de gestión a que se refiere el punto 145.A.200, la organización de mantenimiento deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

c) en el punto 145.B.125, se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203.»;

d) tras el punto 145.B.135, se inserta el punto 145.B.135A siguiente:

«145.B.135A **Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto 145.B.125, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.»;

e) en el punto 145.B.200, se añade la letra e) siguiente:

«e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

f) el punto 145.B.205 se modifica como sigue:

i) el título se sustituye por el texto siguiente:

«145.B.205 **Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto 145.A.200A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto 145.B.200, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

g) en el punto 145.B.300, se añade la letra g) siguiente:

«g) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto 145.A.200A por parte de la organización, además de cumplir lo dispuesto en las letras a) a f), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.»;

h) tras el punto 145.B.330, se inserta el punto 145.B.330A siguiente:

«145.B.330A **Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.I.OR.255, letra a), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto 145.B.300. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto 145.B.350.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.I.OR.255, letra b), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

2) El anexo III (parte 66) se modifica como sigue:

a) en el índice, tras el título 66.B.10, se inserta el título siguiente:

«66.B.15 Sistema de gestión de la seguridad de la información»;

b) tras el punto 66.B.10, se inserta el punto 66.B.15 siguiente:

«66.B.15 **Sistema de gestión de la seguridad de la información**

La autoridad competente establecerá, aplicará y mantendrá un sistema de gestión de la seguridad de la información de conformidad con el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 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) El anexo V *quater* (parte CAMO) se modifica como sigue:

a) el índice se modifica como sigue:

i) tras el título CAMO.A.200, se inserta el título siguiente:

«CAMO.A.200A Sistema de gestión de la seguridad de la información»;

ii) tras el título CAMO.B.135, se inserta el título siguiente:

«CAMO.B.135A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea»;

iii) el título del punto CAMO.B.205 se sustituye por el siguiente:

«CAMO.B.205 Atribución de tareas»;

iv) tras el título CAMO.B.330, se inserta el título siguiente:

«CAMO.B.330A Cambios en el sistema de gestión de la seguridad de la información»;

b) tras el punto CAMO.A.200, se inserta el punto CAMO.A.200A siguiente:

«CAMO.A.200A **Sistema de gestión de la seguridad de la información**

Además del sistema de gestión a que se refiere el punto CAMO.A.200, la organización deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

c) en el punto CAMO.B.125, se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203.».

d) tras el punto CAMO.B.135, se inserta el punto CAMO.B.135A siguiente:

«CAMO.B.135A **Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto CAMO.B.125, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.»;

e) en el punto CAMO.B.200, se añade la letra e) siguiente:

«e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

f) el punto CAMO.B.205 queda modificado como sigue:

i) el título se sustituye por el texto siguiente:

«CAMO.B.205 **Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto CAMO.A.200A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto CAMO.B.200, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

g) en el punto CAMO.B.300, se añade la letra g) siguiente:

«g) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto CAMO.A.200A por parte de la organización, además de cumplir lo dispuesto en las letras a) a f), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.»;

h) tras el punto CAMO.B.330, se inserta el punto CAMO.B.330A siguiente:

«CAMO.B.330A **Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.I.OR.255, letra a), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto CAMO.B.300. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto CAMO.B.350.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.I.OR.255, letra b), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

ANEXO VIII

Los anexos II (parte ATCO.AR) y III (parte ATCO.OR) del Reglamento (UE) 2015/340 se modifican como sigue:

1) El anexo II (parte ATCO.AR) se modifica como sigue:

a) en el punto ATCO.AR.A.020, se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información importante para la seguridad procedente de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203.»;

b) tras el punto ATCO.AR.A.025, se inserta el punto ATCO.AR.A.025A siguiente:

«**ATCO.AR.A.025A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto ATCO.AR.A.020 y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.»;

c) en el punto ATCO.AR.B.001, se añade la letra e) siguiente:

«e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

d) el punto ATCO.AR.B.005 queda modificado como sigue:

i) el título se sustituye por el texto siguiente:

«**ATCO.AR.B.005 Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ATCO.OR.C.001A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto ATCO.AR.B.001, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

e) en el apartado ATCO.AR.C.001, se añade la letra f) siguiente:

«f) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ATCO.OR.C.001A por parte de la organización, además de cumplir lo dispuesto en las letras a) a e), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.»;

f) tras el punto ATCO.AR.E.010, se inserta el punto ATCO.AR.E.010A siguiente:

«**ATCO.AR.E.010A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.I.OR.255, letra a), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto ATCO.AR.C.001. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto ATCO.AR.C.010.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.I.OR.255, letra b), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

2) El anexo III (parte ATCO.OR) se modifica como sigue:

Tras el punto ATCO.OR.C.001, se inserta el punto ATCO.OR.C.001A siguiente:

«**ATCO.OR.C.001A Sistema de gestión de la seguridad de la información**

Además del sistema de gestión a que se refiere el punto ATCO.OR.C.001, la organización de formación deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.».

ANEXO IX

Los anexos II (parte ATM/ANS.AR) y III (parte ATM/ANS.OR) del Reglamento de Ejecución (UE) 2017/373 se modifican como sigue:

1) El anexo II (parte ATM/ANS.AR) se modifica como sigue:

a) en el punto ATM/ANS.AR.A.020, se añade la letra c) siguiente:

«c) La autoridad competente del Estado miembro proporcionará a la Agencia lo antes posible la información de seguridad pertinente derivada de los informes sobre la seguridad de la información que haya recibido de conformidad con el punto IS.I.OR.230 del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203.»;

b) tras el punto ATM/ANS.AR.A.025, se inserta el punto ATM/ANS.AR.A.025A siguiente:

«**ATM/ANS.AR.A.025A Reacción inmediata a un incidente o una vulnerabilidad relacionados con la seguridad de la información que repercutan en la seguridad aérea**

a) La autoridad competente aplicará un sistema para recabar, analizar y difundir adecuadamente la información relativa a los incidentes y vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que sean notificados por las organizaciones. Esto se hará en coordinación con cualquier otra autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro, a fin de reforzar la coordinación y aumentar la compatibilidad de los sistemas de notificación.

b) La Agencia instaurará un sistema para analizar adecuadamente cualquier información de seguridad pertinente que reciba de conformidad con el punto ATM/ANS.AR.A.020, letra c), y proporcionar sin demora indebida a los Estados miembros y a la Comisión cualquier información, incluidas las recomendaciones o las medidas correctoras que deban adoptarse, necesaria para reaccionar oportunamente a los incidentes o vulnerabilidades relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea y que afecten a productos, componentes, equipos no instalados, personas u organizaciones sujetos al Reglamento (UE) 2018/1139 y a sus actos delegados y de ejecución.

c) Al recibir la información mencionada en las letras a) y b), la autoridad competente adoptará las medidas oportunas para abordar las posibles repercusiones en la seguridad aérea del incidente o la vulnerabilidad relacionados con la seguridad de la información.

d) Las medidas adoptadas de conformidad con la letra c) se notificarán de inmediato a todas las personas u organizaciones que deban cumplirlas en virtud del Reglamento (UE) 2018/1139 y sus actos delegados y de ejecución. La autoridad competente del Estado miembro también notificará dichas medidas a la Agencia y, cuando se requiera una actuación combinada, a las autoridades competentes de los demás Estados miembros afectados.»;

c) en el punto ATM/ANS.AR.B.001, se añade la letra e) siguiente:

«e) Además de los requisitos que figuran en la letra a), el sistema de gestión establecido y mantenido por la autoridad competente deberá cumplir lo dispuesto en el anexo I (parte IS.AR) del Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

d) el punto ATM/ANS.AR.B.005 se modifica como sigue:

i) el título se sustituye por el texto siguiente:

«**ATM/ANS.AR.B.005 Atribución de tareas**»;

ii) se añade la letra c) siguiente:

«c) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ATM/ANS.OR.B.005A por parte de la organización, la autoridad competente podrá atribuir tareas a entidades calificadas de conformidad con la letra a) o a cualquier autoridad pertinente responsable de la seguridad de la información o de la ciberseguridad en el Estado miembro. Al atribuir las tareas, la autoridad competente se cerciorará de que:

1) la entidad calificada o la autoridad pertinente coordinen y tengan en cuenta todos los aspectos relacionados con la seguridad aérea;

2) los resultados de las actividades de certificación y supervisión realizadas por la entidad calificada o la autoridad pertinente se integren en los expedientes generales de certificación y supervisión de la organización;

3) su propio sistema de gestión de la seguridad de la información establecido de conformidad con el punto ATM/ANS.AR.B.001, letra e), abarque todas las tareas de certificación y supervisión continua realizadas en su nombre.»;

e) en el punto ATM/ANS.AR.C.010, se añade la letra d) siguiente:

«d) Por lo que respecta a la certificación y la supervisión del cumplimiento del punto ATM/ANS.OR.B.005A por parte de la organización, además de cumplir lo dispuesto en las letras a) a c), la autoridad competente revisará toda aprobación concedida con arreglo al punto IS.I.OR.200, letra e), del presente Reglamento o al punto IS.D.OR.200, letra e), del Reglamento Delegado (UE) 2022/1645 tras el ciclo de auditoría de supervisión aplicable y cada vez que se introduzcan cambios en el ámbito de trabajo de la organización.»;

f) tras el punto ATM/ANS.AR.C.025, se inserta el punto ATM/ANS.AR.C.025A siguiente:

«**ATM/ANS.AR.C.025A Cambios en el sistema de gestión de la seguridad de la información**

a) Por lo que respecta a los cambios gestionados y notificados a la autoridad competente de conformidad con el procedimiento establecido en el punto IS.I.OR.255, letra a), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203, la autoridad competente incluirá la revisión de dichos cambios en su supervisión continua de conformidad con los principios establecidos en el punto ATM/ANS.AR.C.010. Si se detecta un incumplimiento, la autoridad competente lo notificará a la organización, pedirá que se introduzcan otros cambios y actuará de conformidad con el punto ATM/ANS.AR.C.050.

b) Por lo que respecta a otros cambios que requieran una solicitud de aprobación de conformidad con el punto IS.I.OR.255, letra b), del anexo II (parte IS.I.OR) del Reglamento de Ejecución (UE) 2023/203:

1) al recibir la solicitud de cambio, la autoridad competente comprobará que la organización cumple los requisitos aplicables antes de expedir la aprobación;

2) la autoridad competente establecerá las condiciones en las que la organización puede operar durante la aplicación del cambio;

3) si considera que la organización cumple los requisitos aplicables, la autoridad competente aprobará el cambio.».

2) El anexo III (parte ATM/ANS.OR) se modifica como sigue:

a) tras el punto ATM/ANS.OR.B.005, se inserta el punto ATM/ANS.OR.B.005A siguiente:

«**ATM/ANS.OR.B.005A Sistema de gestión de la seguridad de la información**

Además del sistema de gestión a que se refiere el punto ATM/ANS.OR.B.005, el proveedor de servicios deberá establecer, implantar y mantener un sistema de gestión de la seguridad de la información de conformidad con el Reglamento de Ejecución (UE) 2023/203 a fin de garantizar una gestión adecuada de los riesgos relacionados con la seguridad de la información que puedan repercutir en la seguridad aérea.»;

b) el punto ATM/ANS.OR.D.010 se sustituye por el texto siguiente:

«**ATM/ANS.OR.D.010 Gestión de la protección**

a) Los proveedores de servicios de navegación aérea y de gestión de afluencia del tránsito aéreo y el Gestor de la Red establecerán un sistema de gestión de la protección, como parte integrante de su sistema de gestión, tal como se exige en el punto ATM/ANS.OR.B.005, con objeto de garantizar:

1) la protección de sus instalaciones y de su personal, con el fin de evitar interferencias ilícitas que afecten a la prestación de servicios;

2) la protección de los datos operativos que reciban, produzcan o empleen, para que su acceso quede restringido a las personas autorizadas.

b) El sistema de gestión de la protección definirá:

1) el proceso y los procedimientos relativos al análisis y mitigación de riesgos en materia de protección, al control y a la mejora de la protección, los estudios sobre protección y la difusión de enseñanzas al respecto;

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

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

c) Los proveedores de servicios de navegación aérea y de gestión de afluencia del tránsito aéreo y el Gestor de la Red se asegurarán, cuando proceda, de que su personal tiene las autorizaciones de seguridad y se coordinarán con las autoridades civiles y militares pertinentes para garantizar la protección de sus instalaciones, de su personal y de sus datos.

d) Los aspectos relacionados con la seguridad de la información se gestionarán de conformidad con el punto ATM/ANS.OR.B.005A.».