Este texto constitui um instrumento de documentação e não tem qualquer efeito jurídico. As Instituições da União não assumem qualquer responsabilidade pelo respetivo conteúdo. As versões dos atos relevantes que fazem fé, incluindo os respetivos preâmbulos, são as publicadas no Jornal Oficial da União Europeia e encontram-se disponíveis no EUR-Lex. É possível aceder diretamente a esses textos oficiais através das ligações incluídas no presente documento

►B

REGULAMENTO DE EXECUÇÃO (UE) 2023/203 DA COMISSÃO

de 27 de outubro de 2022

que estabelece regras de execução do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, no que diz respeito aos requisitos de gestão dos riscos de segurança da informação com impacto potencial na segurança da aviação, para as organizações abrangidas pelos Regulamentos (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340 e os Regulamentos de Execução (UE) 2017/373 e (UE) 2021/664 da Comissão, e para as autoridades competentes abrangidas pelos Regulamentos (UE) n.º 748/2012, (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340 e os Regulamentos de Execução (UE) 2017/373, (UE) n.º 139/2014 e (UE) 2021/664 da Comissão, e que altera os Regulamentos (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 e os Regulamentos de Execução (UE) 2017/373 e (UE) 2021/664 da Comissão

(JO L 31 de 2.2.2023, p. 1)

Alterado por:

		Jornal Oficial		
		n.º	página	data
►M1	Regulamento de Execução (UE) 2023/1769 da Comissão de 12 de setembro de 2023	L 228	19	15.9.2023
►M2	Regulamento de Execução (UE) 2024/1109 da Comissão de 10 de abril de 2024	L 1109	1	23.5.2024
►M3	Regulamento de Execução (UE) 2025/2293 da Comissão de 10 de novembro de 2025	L 2293	1	11.11.2025

Retificado por:

►C1 Retificação, JO L 90857 de 3.11.2025, p. 1 (2023/203)

▼B

REGULAMENTO DE EXECUÇÃO (UE) 2023/203 DA COMISSÃO

de 27 de outubro de 2022

que estabelece regras de execução do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, no que diz respeito aos requisitos de gestão dos riscos de segurança da informação com impacto potencial na segurança da aviação, para as organizações abrangidas pelos Regulamentos (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340 e os Regulamentos de Execução (UE) 2017/373 e (UE) 2021/664 da Comissão, e para as autoridades competentes abrangidas pelos Regulamentos (UE) n.º 748/2012, (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340 e os Regulamentos de Execução (UE) 2017/373, (UE) n.º 139/2014 e (UE) 2021/664 da Comissão, e que altera os Regulamentos (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 e os Regulamentos de Execução (UE) 2017/373 e (UE) 2021/664 da Comissão

Artigo 1.º

Objeto

O presente regulamento estabelece os requisitos a cumprir pelas organizações e autoridades competentes para:

a) Identificar e gerir os riscos de segurança da informação com impacto potencial na segurança da aviação que possam afetar os sistemas de tecnologias da informação e comunicação e os dados utilizados para fins da aviação civil;

b) Detetar eventos relacionados com a segurança da informação e identificar aqueles que são considerados incidentes de segurança da informação com potencial impacto na segurança da aviação;

c) Responder a esses incidentes de segurança da informação e recuperar deles.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento é aplicável às seguintes organizações:

(a) Entidades de manutenção abrangidas pelo anexo II (parte 145), secção A, do Regulamento (UE) n.º 1321/2014, exceto as que estão exclusivamente envolvidas na manutenção de aeronaves, em conformidade com o anexo V-B (parte ML) do Regulamento (UE) n.º 1321/2014;

(b) Entidades de gestão da aeronavegabilidade permanente (CAMO) abrangidas pelo anexo V-C (parte CAMO), secção A, do Regulamento (UE) n.º 1321/2014, exceto as que estão exclusivamente envolvidas na gestão da aeronavegabilidade permanente das aeronaves, em conformidade com o anexo V-B (parte ML) do Regulamento (UE) n.º 1321/2014;

(c) Operadores aéreos abrangidos pelo anexo III (parte ORO) do Regulamento (UE) n.º 965/2012, com exceção dos exclusivamente envolvidos na operação de:

▼B

i) uma aeronave ELA 2, na aceção do artigo 1.º, n.º 2, alínea j), do Regulamento (UE) n.º 748/2012;

ii) aviões monomotor a hélice com uma configuração operacional máxima de lugares de passageiros igual ou inferior a 5, não classificados como aeronaves a motor complexas, quando descolam e aterram no mesmo aeródromo ou local de operação e operam de acordo com as regras de voo visual (VFR) diurnas;

iii) helicópteros monomotor com uma configuração operacional máxima de lugares de passageiros igual ou inferior a 5, não classificados como aeronaves a motor complexas, quando descolam e aterram no mesmo aeródromo ou local de operação e operam de acordo com as regras VFR diurnas.

(d) Organizações de formação certificadas (ATO) abrangidas pelo anexo VII (parte ORA) do Regulamento (UE) n.º 1178/2011, exceto as envolvidas exclusivamente em atividades de formação de aeronaves ELA2, tal como definidas no artigo 1.º, n.º 2, alínea j), do Regulamento (UE) n.º 748/2012, ou exclusivamente envolvidas em formação teórica;

(e) Centros de medicina aeronáutica da tripulação de voo abrangidos pelo anexo VII (parte ORA) do Regulamento (UE) n.º 1178/2011;

(f) Operadores de dispositivos de treino de simulação de voo (FSTD) abrangidos pelo anexo VII (parte ORA) do Regulamento (UE) n.º 1178/2011, exceto os envolvidos exclusivamente na operação de FSTD de aeronaves ELA2, tal como definidas no artigo 1.º, n.º 2, alínea j), do Regulamento (UE) n.º 748/2012;

(g) Organizações de formação de controladores de tráfego aéreo (ATCO TO) e centros de medicina aeronáutica de ATCO abrangidos pelo anexo III (parte ATCO.OR) do Regulamento (UE) 2015/340;

(h) Organizações abrangidas pelo anexo III (Parte-ATM/ANS.OR) do Regulamento de Execução (UE) 2017/373, exceto os seguintes prestadores de serviços:

i) prestadores de serviços de navegação aérea titulares de um certificado limitado em conformidade com a secção ATM/ /ANS.OR.A.010 do mesmo anexo;

ii) prestadores de serviços de informação de voo que declarem as suas atividades em conformidade com a secção ATM/ANS.OR. A.015 do mesmo anexo;

(i) Prestadores de serviços no espaço «U» e prestadores únicos de serviços de informação comum abrangidos pelo Regulamento de Execução (UE) 2021/664;

▼M1

(j) Entidades certificadas envolvidas no projeto ou na produção de sistemas ATM/ANS e componentes ATM/ANS abrangidas pelo Regulamento de Execução (UE) 2023/1769 da Comissão ([1]).

▼B

2. O presente regulamento aplica-se às autoridades competentes, incluindo a Agência da União Europeia para a Segurança da Aviação («Agência»), referidas no artigo 6.º do presente regulamento e no artigo 5.º do Regulamento Delegado (UE) 2022/1645 da Comissão ([2]).

3. O presente regulamento aplica-se igualmente à autoridade competente responsável pela emissão, renovação, alteração, suspensão ou revogação de licenças de manutenção aeronáutica, em conformidade com o anexo III (parte 66) do Regulamento (UE) n.º 1321/2014.

▼M2

3-A. O presente regulamento aplica-se igualmente à autoridade competente designada em conformidade com o anexo I (parte AR.UAS) do Regulamento de Execução (UE) 2024/1109 da Comissão ([3]).

▼B

4. O presente regulamento não deve prejudicar os requisitos de segurança da informação e de cibersegurança estabelecidos no ponto 1.7 do anexo do Regulamento de Execução (UE) 2015/1998 e no artigo 14.º da Diretiva (UE) 2016/1148.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

(1) «Segurança da informação», a preservação da confidencialidade, integridade, autenticidade e disponibilidade das redes e dos sistemas de informação;

([1]) Regulamento de Execução (UE) 2023/1769 da Comissão*, de 12 de setembro de 2023 que estabelece os requisitos técnicos e os procedimentos administrativos para a certificação das entidades envolvidas no projeto ou na produção de sistemas e componentes de gestão do tráfego aéreo/serviços de navegação aérea e que altera o Regulamento de Execução (UE) 2023/203 (JO L 228 de XX.9.2023, p. 19).

([2]) Regulamento Delegado (UE) 2022/1645 da Comissão, de 14 de julho de 2022, que estabelece regras de execução do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho no que respeita aos requisitos em matéria de gestão dos riscos de segurança da informação com potencial impacto na segurança da aviação para as entidades abrangidas pelos Regulamentos (UE) n.º 748/2012 e (UE) n.º 139/2014 da Comissão e que altera os Regulamentos (UE) n.º 748/2012 e (UE) n.º 139/2014 da Comissão (JO L 248 de 26.9.2022, p. 18).

([3]) Regulamento de Execução (UE) 2024/1109 da Comissão, de 10 de abril de 2024, que estabelece normas de aplicação do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho no que respeita aos requisitos relativos às autoridades competentes e aos procedimentos administrativos de certificação, supervisão e execução da aeronavegabilidade permanente dos sistemas de aeronaves não tripuladas e que altera o Regulamento de Execução (UE) 2023/203 (JO L, 2024/1109, 17.5.2024, ELI: http://data.europa.eu/eli//reg_impl/2024/1109/oj).

▼B

(2) «Incidente de segurança da informação», uma ocorrência identificada de um estado de um sistema, serviço ou rede que indique uma possível violação da política de segurança da informação ou uma falha dos controlos de segurança da informação, ou uma situação anteriormente desconhecida que possa ser relevante para a segurança da informação;

(3) «Incidente», um evento com um efeito adverso real na segurança das redes e dos sistemas de informação, tal como definido no artigo 4.º, ponto 7, da Diretiva (UE) 2016/1148;

(4) «Risco para a segurança da informação», o risco para as operações organizacionais da aviação civil, os ativos, as pessoas singulares e outras entidades devido ao impacto potencial de um evento de segurança da informação. Os riscos para a segurança da informação estão associados ao potencial de as ameaças explorarem as vulnerabilidades de um ativo de informação ou de um grupo de ativos de informação;

(5) «Ameaça», uma potencial violação da segurança da informação suscitada por uma entidade, circunstância, ação ou um evento suscetível de causar danos;

(6) «Vulnerabilidade», uma falha ou deficiência de um ativo ou sistema, dos procedimentos, da conceção, da aplicação ou de medidas de segurança da informação que possam ser exploradas e resultem numa infração ou violação da política de segurança da informação.

Artigo 4.º

Requisitos aplicáveis às organizações e autoridades competentes

1. As organizações referidas no artigo 2.º, n.º 1, devem cumprir os requisitos do anexo II (parte IS.I.OR) do presente regulamento.

▼M2

2. As autoridades competentes referidas no artigo 2.º, n.ºs 2, 3 e 3-A, devem cumprir os requisitos do anexo I (parte IS.AR) do presente regulamento.

▼B

Artigo 5.º

Requisitos decorrentes de outra legislação da União

1. Sempre que uma entidade referida no artigo 2.º, n.º 1, cumpra requisitos de segurança estabelecidos em conformidade com o artigo 14.º da Diretiva (UE) 2016/1148 equivalentes aos estabelecidos no presente regulamento, considera-se que o cumprimento desses requisitos de segurança equivale ao cumprimento dos requisitos estabelecidos no presente regulamento.

▼B

2. Se uma organização referida no artigo 2.º, n.º 1, for um operador ou uma entidade referida nos programas nacionais de segurança da aviação civil dos Estados-Membros estabelecidos em conformidade com o artigo 10.º do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho ([4]), os requisitos de cibersegurança constantes do ponto 1.7 do anexo do Regulamento de Execução (UE) 2015/1998 são considerados equivalentes aos requisitos estabelecidos no presente regulamento, exceto no que diz respeito à secção IS.I.OR.230 do anexo II do presente regulamento, que deve ser cumprida enquanto tal.

3. Se a organização a que se refere o artigo 2.º, n.º 1, for o prestador de serviços de navegação aérea do Serviço Europeu Complementar de Navegação Geoestacionária (EGNOS) referido no Regulamento (UE) 2021/696, os requisitos de segurança constantes dos artigos 33.º a 43.º do título V desse regulamento são considerados equivalentes aos requisitos estabelecidos no presente regulamento, exceto no que diz respeito à secção IS.I.OR.230 do anexo II do presente regulamento, que deve ser cumprida enquanto tal.

4. A Comissão, após consulta da Agência e do grupo de cooperação referido no artigo 11.º da Diretiva (UE) 2016/1148, pode emitir orientações para a avaliação da equivalência dos requisitos estabelecidos no presente regulamento e na Diretiva (UE) 2016/1148.

Artigo 6.º

Autoridade competente

1. Sem prejuízo das funções confiadas ao Comité de Acreditação de Segurança (SAB) a que se refere o artigo 36.º do Regulamento (UE) 2021/696, a autoridade responsável pela certificação e supervisão do cumprimento do presente regulamento é:

(a) No que respeita às organizações referidas no artigo 2.º, n.º 1, alínea a), a autoridade competente designada em conformidade com o anexo II (parte 145) do Regulamento (UE) n.º 1321/2014;

(b) No que respeita às organizações referidas no artigo 2.º, n.º 1, alínea b), a autoridade competente designada em conformidade com o anexo V-C (parte CAMO) do Regulamento (UE) n.º 1321/2014;

(c) No que respeita às organizações referidas no artigo 2.º, n.º 1, alínea c), a autoridade competente designada em conformidade com o anexo III (parte ORO) do Regulamento (UE) n.º 965/2012;

(d) No que respeita às organizações referidas no artigo 2.º, n.º 1, alíneas d) a f), a autoridade competente designada em conformidade com o anexo VII (parte ORA) do Regulamento (UE) n.º 1178/2011;

(e) No que respeita às organizações referidas no artigo 2.º, n.º 1, alínea g), a autoridade competente designada em conformidade com o artigo 6.º, n.º 2, do Regulamento (UE) 2015/340;

(f) No que respeita às organizações referidas no artigo 2.º, n.º 1, alínea h), a autoridade competente designada em conformidade com o artigo 4.º, n.º 1, do Regulamento de Execução (UE) 2017/373;

([4]) Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).

▼B

(g) No que respeita às organizações referidas no artigo 2.º, n.º 1, alínea i), a autoridade competente designada em conformidade com o artigo 14.º, n.º 1 ou n.º 2, conforme aplicável, do Regulamento de Execução (UE) 2021/664;

▼M1

(h) No que diz respeito às entidades a que se refere o artigo 2.º, n.º 1, alínea j), a autoridade competente designada em conformidade com o artigo 3.º, n.º 1, do Regulamento de Execução (UE) 2023/1769.

▼B

2. Para efeitos do presente regulamento, os Estados-Membros podem designar uma entidade independente e autónoma para desempenhar as funções e responsabilidades atribuídas às autoridades competentes a que se refere o n.º 1. Nesse caso, devem ser estabelecidas medidas de coordenação entre essa entidade e as outras autoridades competentes, a que se refere o n.º 1, a fim de assegurar uma supervisão eficaz de todos os requisitos a cumprir pela entidade.

3. A Agência deve cooperar, no pleno respeito das regras aplicáveis em matéria de sigilo, proteção dos dados pessoais e proteção das informações classificadas, com a Agência da União Europeia para o Programa Espacial (EUSPA) e com o SAB a que se refere o artigo 36.º do Regulamento (UE) 2021/696, a fim de assegurar uma supervisão eficaz dos requisitos aplicáveis ao prestador de serviços de navegação aérea EGNOS.

Artigo 7.º

Apresentação de informações relevantes às autoridades competentes em matéria de SRI

As autoridades competentes ao abrigo do presente regulamento devem informar, sem demora injustificada, o ponto de contacto único designado em conformidade com o artigo 8.º da Diretiva (UE) 2016/1148 de quaisquer informações relevantes incluídas nas notificações apresentadas nos termos da secção IS.I.OR.230 do anexo II do presente regulamento e da secção IS.D.OR.230 do anexo I do Regulamento Delegado (UE) 2022/1645 pelos operadores de serviços essenciais identificados em conformidade com o artigo 5.º da Diretiva (UE) 2016/1148.

Artigo 8.º

Alteração do Regulamento (UE) n.º 1178/2011

Os anexos VI (parte ARA) e VII (parte ORA) do Regulamento (UE) n.º 1178/2011 são alterados em conformidade com o anexo III do presente regulamento.

Artigo 9.º

Alteração do Regulamento (UE) n.º 748/2012

O anexo I (parte 21) do Regulamento (UE) n.º 748/2012 é alterado em conformidade com o anexo IV do presente regulamento.

▼B

Artigo 10.º

Alteração do Regulamento (UE) n.º 965/2012

Os anexos II (parte ARO) e III (parte ORO) do Regulamento (UE) n.º 965/2012 são alterados em conformidade com o anexo V do presente regulamento.

Artigo 11.º

Alteração do Regulamento (UE) n.º 139/2014

O anexo II (parte ADR.AR) do Regulamento (UE) n.º 139/2014 é alterado em conformidade com o anexo VI do presente regulamento.

Artigo 12.º

Alteração do Regulamento (UE) n.º 1321/2014

Os anexos II (parte 145), III (parte 66) e V-C (parte CAMO) do Regulamento (UE) n.º 1321/2014 são alterados em conformidade com o anexo VII do presente regulamento.

Artigo 13.º

Alteração do Regulamento (UE) n.º 2015/340

Os anexos II (parte ATCO.AR) e III (parte ATCO.OR) do Regulamento (UE) 2015/340 são alterados em conformidade com o anexo VIII do presente regulamento.

Artigo 14.º

Alteração do Regulamento de Execução (UE) n.º 2017/373

Os anexos II (parte ATM/ANS.AR) e III (parte ATM/ANS.OR) do Regulamento de Execução (UE) 2017/373 são alterados em conformidade com o anexo IX do presente regulamento.

Artigo 15.º

Alteração do Regulamento de Execução (UE) 2021/664

O Regulamento de Execução (UE) 2021/664 é alterado do seguinte modo:

(1) No artigo 15.º, n.º 1, a alínea f) passa a ter a seguinte redação:

«f) Implementar e manter um sistema de gestão da segurança em conformidade com a secção ATM/ANS.OR.D.010 do anexo III, subparte D, do Regulamento de Execução (UE) 2017/373, e um sistema de gestão da segurança da informação em conformidade com o anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.»;

(2) Ao artigo 18.º é aditada a seguinte alínea l):

«l) Estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203.».

▼B

Artigo 16.º

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

É aplicável a partir de 22 de fevereiro de 2026.

No entanto, no que respeita ao prestador de serviços de navegação aérea EGNOS abrangido pelo Regulamento de Execução (UE) 2017/373, o presente regulamento é aplicável a partir de 1 de janeiro de 2026.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

▼B

ANEXO I

SEGURANÇA DA INFORMAÇÃO — REQUISITOS APLICÁVEIS ÀS AUTORIDADES

[PARTE IS.AR]

IS.AR.100 Âmbito de aplicação

IS.AR.200 Sistema de gestão da segurança da informação (SGSI)

IS.AR.205 Avaliação dos riscos para a segurança da informação

IS.AR.210 Tratamento dos riscos para a segurança da informação

IS.AR.215 Incidentes de segurança da informação — deteção, resposta e recuperação

IS.AR.220 Adjudicação de atividades de gestão da segurança da informação

IS.AR.225 Requisitos em matéria de pessoal

IS.AR.230 Conservação de registos

IS.AR.235 Melhoria contínua

IS.AR.100 Âmbito de aplicação

A presente parte estabelece os requisitos de gestão a cumprir pelas autoridades competentes referidas no artigo 2.º, n.º 2, do presente regulamento.

Os requisitos a cumprir por essas autoridades competentes no desempenho das suas atividades de certificação, supervisão e fiscalização constam dos regulamentos referidos no artigo 2.º, n.º 1, do presente regulamento e no artigo 2.º do Regulamento Delegado (UE) 2022/1645.

IS.AR.200 Sistema de gestão da segurança da informação (SGSI)

a) A fim de alcançar os objetivos estabelecidos no artigo 1.º, a autoridade competente deve criar, aplicar e manter um sistema de gestão da segurança da informação (SGSI) que lhe permita assegurar que:

(1) estabelece uma política em matéria de segurança da informação que define os seus princípios gerais no que diz respeito ao potencial impacto dos riscos de segurança da informação na segurança da aviação;

(2) identifica e analisa os riscos de segurança da informação em conformidade com a secção IS.AR.205;

(3) define e aplica medidas de tratamento dos riscos de segurança da informação em conformidade com a secção IS.AR.210;

(4) define e aplica, em conformidade com a secção IS.AR.215, as medidas necessárias para detetar incidentes de segurança da informação, identifica os eventos considerados incidentes com potencial impacto na segurança da aviação e dá resposta a esses incidentes de segurança da informação e recupera desses incidentes;

(5) cumpre os requisitos constantes da secção IS.AR.220 ao subcontratar qualquer parte das atividades referidas na secção IS.AR.200 a outras organizações;

▼B

(6) cumpre os requisitos em matéria de pessoal estabelecidos na secção IS. AR.225;

(7) cumpre os requisitos de conservação de registos estabelecidos na secção IS.AR.230;

(8) controla a conformidade da sua própria organização com os requisitos do presente regulamento e fornece informações sobre as constatações à pessoa referida na secção IS.AR.225, alínea a), a fim de assegurar a aplicação eficaz das medidas corretivas;

(9) protege a confidencialidade de quaisquer informações que a autoridade competente possa ter relacionado com organizações sujeitas à sua supervisão e das informações recebidas através dos sistemas de comunicação externa da organização estabelecidos em conformidade com a secção IS.I.OR.230 do anexo II (parte IS.I.OR) do presente regulamento e com a secção IS.I.OR.230 do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645;

(10) notifica a Agência de alterações que afetem a capacidade da autoridade competente para desempenhar as suas funções e cumprir as responsabilidades que lhe incumbem, tal como definidas no presente regulamento;

(11) define e aplica procedimentos para partilhar, conforme adequado e de forma prática e atempada, informações relevantes para ajudar outras autoridades e agências competentes, bem como as organizações abrangidas pelo presente regulamento, a realizar avaliações eficazes dos riscos para a segurança relacionados com as suas atividades.

b) A fim de satisfazer continuamente os requisitos referidos no artigo 1.º, a autoridade competente deve implementar um processo de melhoria contínua em conformidade com a secção IS.AR.235.

c) A autoridade competente deve documentar todos os principais processos, procedimentos, funções e responsabilidades necessários para cumprir o disposto na secção IS.AR.200, alínea a), e estabelecer um processo de alteração dessa documentação.

d) Os processos, procedimentos, funções e responsabilidades estabelecidos pela autoridade competente para cumprir o disposto na secção IS.AR.200, alínea a), devem corresponder à natureza e complexidade das suas atividades, com base numa avaliação dos riscos para a segurança da informação inerentes a essas atividades, e podem ser integrados noutros sistemas de gestão existentes já implementados pela autoridade competente.

IS.AR.205 Avaliação dos riscos para a segurança da informação

a) A autoridade competente deve identificar todos os elementos da sua própria organização que possam estar expostos a riscos de segurança da informação, devendo estes incluir:

(1) as atividades, instalações e recursos da autoridade competente, bem como os serviços por ela operados, prestados, recebidos ou mantidos;

(2) os equipamentos, sistemas, dados e informações que contribuem para o funcionamento dos elementos enumerados no ponto (1).

b) A autoridade competente deve identificar as interfaces que tem com outras organizações e que possam resultar numa exposição mútua aos riscos de segurança da informação.

c) No que diz respeito aos elementos e interfaces referidos nas alíneas a) e b), a autoridade competente deve identificar os riscos para a segurança da informação que possam ter um impacto potencial na segurança da aviação.

▼B

Para cada risco identificado, a autoridade competente deve:

(1) atribuir um nível de risco de acordo com uma classificação predefinida estabelecida pela autoridade competente;

(2) associar cada risco e o seu nível ao elemento ou interface correspondente identificado em conformidade com as alíneas a) e b).

A classificação predefinida referida no ponto (1) deve ter em conta o potencial de ocorrência do cenário de ameaça e a gravidade das suas consequências para a segurança. Com base nessa classificação, e tendo em conta se a autoridade competente dispõe de um processo estruturado e repetível de gestão dos riscos para as operações, a autoridade competente deve ser capaz de determinar se o risco é aceitável ou se deve ser tratado em conformidade com a secção IS.AR.210.

A fim de facilitar a comparabilidade mútua das avaliações de riscos, a atribuição do nível de risco nos termos do ponto (1) deve ter em conta as informações relevantes obtidas em coordenação com as organizações referidas na alínea b).

d) A autoridade competente deve rever e atualizar a avaliação dos riscos efetuada em conformidade com as alíneas a), b) e c) em qualquer das seguintes situações:

(1) uma alteração dos elementos sujeitos a riscos para a segurança da informação;

(2) uma alteração nas interfaces entre a organização da autoridade competente e as demais organizações, ou nos riscos comunicados pelas outras organizações;

(3) uma alteração das informações ou dos conhecimentos utilizados para a identificação, análise e classificação dos riscos;

(4) ensinamentos retirados da análise dos incidentes de segurança da informação.

IS.AR.210 Tratamento dos riscos para a segurança da informação

a) A autoridade competente deve desenvolver medidas para fazer face aos riscos inaceitáveis identificados em conformidade com a secção IS.AR.205, aplicá-las em tempo útil e verificar a sua eficácia contínua. Essas medidas devem permitir à autoridade competente:

(1) controlar as circunstâncias que contribuem para a ocorrência efetiva do cenário de ameaça;

(2) reduzir as consequências para a segurança da aviação associadas à concretização do cenário de ameaça;

(3) evitar os riscos.

Essas medidas não devem introduzir quaisquer novos riscos potencialmente inaceitáveis para a segurança da aviação.

b) A pessoa referida na secção IS.AR.225, alínea a), e outro pessoal afetado da autoridade competente devem ser informados do resultado da avaliação dos riscos efetuada em conformidade com a secção IS.AR.205, dos cenários de ameaça correspondentes e das medidas a aplicar.

A autoridade competente deve também informar as organizações com as quais tenha uma interface, em conformidade com a secção IS.AR.205, alínea b), de quaisquer riscos que se coloquem a ambas.

▼B

IS.AR.215 Incidentes de segurança da informação — deteção, resposta e recuperação

a) Com base no resultado da avaliação dos riscos efetuada em conformidade com a secção IS.AR.205 e no resultado do tratamento dos riscos realizado em conformidade com a secção IS.AR.210, a autoridade competente deve aplicar medidas para detetar incidentes que indiquem a potencial materialização de riscos inaceitáveis e que possam ter um impacto potencial na segurança da aviação. Essas medidas de deteção devem permitir à autoridade competente:

(1) identificar desvios em relação às bases de referência do desempenho funcional predeterminado;

(2) desencadear avisos para ativar medidas de resposta adequadas, em caso de desvio.

b) A autoridade competente deve aplicar medidas para responder a qualquer situação identificada em conformidade com a alínea a) que possa desencadear ou se tenha transformado num incidente de segurança da informação. Essas medidas de resposta devem permitir à autoridade competente:

(1) iniciar a reação da sua própria organização aos alertas referidos na alínea a), ponto (2), ativando recursos predefinidos e ações;

(2) conter a propagação de um ataque e evitar a plena concretização de um cenário de ameaça;

(3) controlar o modo de avaria dos elementos afetados definidos na secção IS.AR.205, alínea a).

c) A autoridade competente deve aplicar medidas destinadas a recuperar de incidentes de segurança da informação, incluindo medidas de emergência, se necessário. Essas medidas de recuperação devem permitir à autoridade competente:

(1) eliminar a condição que causou o incidente ou limitá-lo a um nível tolerável;

(2) restaurar um estado seguro dos elementos afetados definidos na secção IS.AR.205, alínea a), num prazo de recuperação previamente definido pela sua própria organização.

IS.AR.220 Adjudicação de atividades de gestão da segurança da informação

A autoridade competente deve assegurar que, ao contratar qualquer parte das atividades a que se refere a secção IS.AR.200 a outras organizações, as atividades contratadas cumprem os requisitos do presente regulamento e a organização contratada trabalha sob a sua supervisão. A autoridade competente deve assegurar que os riscos associados às atividades contratadas são geridos de forma adequada.

IS.AR.225 Requisitos em matéria de pessoal

A autoridade competente deve:

a) Dispor de uma pessoa com autoridade para estabelecer e manter as estruturas organizativas, políticas, processos e procedimentos necessários para a aplicação do presente regulamento.

Essa pessoa deve:

(1) ter autoridade para aceder plenamente aos recursos necessários para que a autoridade competente possa desempenhar todas as funções exigidas pelo presente regulamento;

(2) dispor da delegação de poderes necessária para o desempenho das funções que lhe foram atribuídas;

▼B

b) Dispor de um processo que garanta que dispõe de pessoal em número suficiente para a consecução das atividades abrangidas pelo presente anexo;

c) Dispor de um processo para assegurar que o pessoal referido na alínea b) possui as competências necessárias para desempenhar as suas funções;

d) Dispor de um processo para assegurar que o pessoal reconhece as responsabilidades associadas às funções e tarefas que lhe são cometidas;

e) Assegurar que a identidade e a fiabilidade do pessoal que tem acesso aos sistemas de informação e aos dados sujeitos aos requisitos do presente regulamento são devidamente estabelecidas.

IS.AR.230 Conservação de registos

a) A autoridade competente deve conservar registos das suas atividades de gestão da segurança da informação.

(1) A autoridade competente deve assegurar que os seguintes registos são arquivados e rastreáveis:

i) contratos para as atividades referidas na secção IS.AR.200, alínea a), ponto (5);

ii) registos dos principais processos referidos na secção IS.AR.200, alínea d);

iii) registos dos riscos identificados na avaliação dos riscos referida na secção IS.AR.205, juntamente com as medidas associadas de tratamento dos riscos referidas na secção IS.AR.210;

iv) registos dos eventos relacionados com a segurança da informação que possam ter de ser reavaliados para revelar incidentes ou vulnerabilidades de segurança da informação não detetados.

(2) Os registos referidos no ponto 1, subalínea i), devem ser conservados pelo menos até 5 anos após a alteração ou rescisão do contrato.

(3) Os registos referidos no ponto 1, subalíneas ii) e iii), devem ser conservados pelo menos durante um período de 5 anos.

(4) Os registos referidos no ponto 1, subalínea iv), devem ser conservados até que esses eventos de segurança da informação tenham sido reavaliados de acordo com uma periodicidade definida num procedimento estabelecido pela autoridade competente.

b) A autoridade competente deve manter registos das qualificações e da experiência do seu pessoal envolvido em atividades de gestão da segurança da informação.

(1) Os registos relativos às qualificações e à experiência do pessoal devem ser conservados enquanto a pessoa trabalhar para a autoridade competente e durante, pelo menos, 3 anos após a pessoa ter deixado a autoridade competente.

(2) Os membros do pessoal devem, a seu pedido, ter acesso aos seus registos individuais. Além disso, a seu pedido, a autoridade competente deve fornecer-lhes uma cópia dos seus registos individuais quando deixam a autoridade competente.

c) O formato dos registos deve ser especificado nos procedimentos da autoridade competente.

▼B

d) Os registos devem ser conservados de um modo que assegure a proteção dos danos, das alterações e do furto, sendo as informações identificadas, sempre que requerido, de acordo com o seu nível de classificação de segurança. A autoridade competente assegura que os registos são conservados através de meios que garantam a integridade, a autenticidade e o acesso autorizado.

IS.AR.235 Melhoria contínua

a) A autoridade competente deve avaliar, utilizando indicadores de desempenho adequados, a eficácia e a maturidade do seu próprio SGSI. A avaliação deve ser efetuada com base num calendário predefinido, definido pela autoridade competente ou na sequência de um incidente de segurança da informação.

b) Se forem detetadas deficiências na sequência da avaliação efetuada em conformidade com a alínea a), a autoridade competente deve tomar as medidas de melhoria necessárias para assegurar que o SGSI continua a cumprir os requisitos aplicáveis e permite manter os riscos de segurança da informação a um nível aceitável. Além disso, a autoridade competente deve reavaliar os elementos do SGSI afetados pelas medidas adotadas.

▼B

ANEXO II

SEGURANÇA DA INFORMAÇÃO — REQUISITOS APLICÁVEIS ÀS ORGANIZAÇÕES

[PARTE IS.I.OR]

IS.I.OR.100 Âmbito de aplicação

IS.I.OR.200 Sistema de gestão da segurança da informação (SGSI)

IS.I.OR.205 Avaliação dos riscos para a segurança da informação

IS.I.OR.210 Tratamento dos riscos para a segurança da informação

IS.I.OR.215 Sistema de comunicação interna de informações sobre segurança da informação

IS.I.OR.220 Incidentes de segurança da informação — deteção, resposta e recuperação

IS.I.OR.225 Resposta a constatações notificadas pela autoridade competente

IS.I.OR.230 Sistema de comunicação externa sobre segurança da informação

IS.I.OR.235 Adjudicação de atividades de gestão da segurança da informação

IS.I.OR.240 Requisitos em matéria de pessoal

IS.I.OR.245 Conservação de registos

IS.I.OR.250 Manual de gestão da segurança da informação (MGSI)

IS.I.OR.255 Alterações ao sistema de gestão da segurança da informação

IS.I.OR.260 Melhoria contínua

IS.I.OR.100 Âmbito de aplicação

A presente parte estabelece os requisitos a cumprir pelas organizações referidas no artigo 2.º, n.º 1, do presente regulamento.

IS.I.OR.200 Sistema de gestão da segurança da informação (SGSI)

a) A fim de alcançar os objetivos estabelecidos no artigo 1.º, a entidade deve criar, aplicar e manter um sistema de gestão da segurança da informação (SGSI) que lhe permita assegurar que:

   (1) estabelece uma política em matéria de segurança da informação que define os seus princípios gerais no que diz respeito ao potencial impacto dos riscos de segurança da informação na segurança da aviação;

   (2) identifica e analisa os riscos de segurança da informação em conformidade com a secção IS.I.OR.205;

   (3) define e aplica medidas de tratamento dos riscos de segurança da informação em conformidade com a secção IS.I.OR.210;

   (4) aplica um sistema de comunicação interna de informações em matéria de segurança da informação, em conformidade com a secção IS.I. OR.215;

   (5) define e aplica, em conformidade com a secção IS.I.OR.220, as medidas necessárias para detetar incidentes de segurança da informação, identifica os eventos considerados incidentes com potencial impacto na segurança da aviação, exceto conforme permitido pela secção IS.I. OR.205, alínea e), dá resposta a esses incidentes de segurança da informação e recupera desses incidentes;

▼B

(6) aplica as medidas que tenham sido notificadas pela autoridade competente como reação imediata a um incidente de segurança da informação ou a uma vulnerabilidade com impacto na segurança da aviação;

(7) toma as medidas adequadas, em conformidade com a secção IS.I.OR.225, para dar resposta às constatações notificadas pela autoridade competente;

(8) aplica um sistema de comunicação externa em conformidade com a secção IS.I.OR.230, a fim de permitir que a autoridade competente tome as medidas adequadas;

(9) cumpre os requisitos constantes da secção IS.I.OR.235 ao subcontratar qualquer parte das atividades referidas na secção IS.I.OR.200 a outras organizações;

(10) cumpre os requisitos em matéria de pessoal estabelecidos na secção IS.I.OR.240;

(11) cumpre os requisitos de conservação de registos estabelecidos na secção IS.I.OR.245;

(12) controla a conformidade da sua própria organização com os requisitos do presente regulamento e fornece informações sobre as constatações ao administrador responsável a fim de assegurar a aplicação eficaz das medidas corretivas;

(13) protege, sem prejuízo dos requisitos aplicáveis em matéria de comunicação de incidentes, a confidencialidade de quaisquer informações que a organização possa ter recebido de outras organizações, de acordo com o seu nível de sensibilidade.

b) A fim de satisfazer continuamente os requisitos referidos no artigo 1.º, a organização deve implementar um processo de melhoria contínua em conformidade com a secção IS.I.OR.260.

c) A organização deve documentar, em conformidade com a secção IS.I.OR.250, todos os principais processos, procedimentos, funções e responsabilidades necessários para cumprir o disposto na secção IS.I.OR.200, alínea a), e estabelecer um processo de alteração dessa documentação. As alterações a esses processos, procedimentos, funções e responsabilidades devem ser geridas em conformidade com a secção IS.I.OR.255.

d) Os processos, procedimentos, funções e responsabilidades estabelecidos pela organização para cumprir o disposto na secção IS.I.OR.200, alínea a), devem corresponder à natureza e complexidade das suas atividades, com base numa avaliação dos riscos para a segurança da informação inerentes a essas atividades, e podem ser integrados noutros sistemas de gestão existentes já implementados pela organização.

e) Sem prejuízo da obrigação de cumprir os requisitos de comunicação de informações previstos no Regulamento (UE) n.º 376/2014 e os requisitos da secção IS.I.OR.200, alínea a), ponto (13), a autoridade competente pode autorizar a organização a não aplicar os requisitos referidos nas alíneas a) a d) e os respetivos requisitos constantes das secções IS.I.OR.205 até IS.I.OR.260, se demonstrar, a contento dessa autoridade, que as suas atividades, instalações e recursos, bem como os serviços que opera, fornece, recebe e mantém, não apresentam riscos de segurança da informação com um impacto potencial na segurança da aviação, nem para si própria nem para outras organizações. A certificação deve basear-se numa avaliação documentada dos riscos de segurança da informação realizada pela organização ou por terceiros em conformidade com a secção IS.I.OR.205 e revista e aprovada pela respetiva autoridade competente.

A manutenção da validade dessa aprovação será revista pela autoridade competente na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.

▼B

IS.I.OR.205 Avaliação dos riscos para a segurança da informação

a) A organização deve identificar todos os seus elementos que possam estar expostos a riscos de segurança da informação, incluindo:

(1) as atividades, instalações e recursos da organização, bem como os serviços que a organização opera, presta, recebe ou mantém;

(2) equipamentos, sistemas, dados e informações que contribuem para o funcionamento dos elementos enumerados no ponto (1).

b) A organização deve identificar as interfaces que tem com outras organizações e que possam resultar numa exposição mútua aos riscos de segurança da informação.

c) No que diz respeito aos elementos e interfaces referidos nas alíneas a) e b), a organização deve identificar os riscos para a segurança da informação que possam ter um impacto potencial na segurança da aviação. Para cada risco identificado, a organização deve:

(1) atribuir um nível de risco de acordo com uma classificação predefinida estabelecida pela organização;

(2) associar cada risco e o seu nível ao elemento ou interface correspondente identificado em conformidade com as alíneas a) e b).

A classificação predefinida referida no ponto (1) deve ter em conta o potencial de ocorrência do cenário de ameaça e a gravidade das suas consequências para a segurança. Com base nessa classificação, e tendo em conta se a organização dispõe de um processo estruturado e repetível de gestão dos riscos para as operações, a organização deve ser capaz de determinar se o risco é aceitável ou se deve ser tratado em conformidade com a secção IS.I.OR.210.

A fim de facilitar a comparabilidade mútua das avaliações de riscos, a atribuição do nível de risco nos termos do ponto (1) deve ter em conta as informações relevantes obtidas em coordenação com as organizações referidas na alínea b).

d) A organização deve rever e atualizar a avaliação dos riscos efetuada em conformidade com as alíneas a), b) e, consoante for aplicável, as alíneas c) ou e), em qualquer das seguintes situações:

(1) uma alteração dos elementos sujeitos a riscos para a segurança da informação;

(2) uma alteração nas interfaces entre a organização e outras organizações ou nos riscos comunicados pelas outras organizações;

(3) uma alteração das informações ou dos conhecimentos utilizados para a identificação, análise e classificação dos riscos;

(4) ensinamentos retirados da análise dos incidentes de segurança da informação.

e) Em derrogação da alínea c), as organizações obrigadas a cumprir o disposto na subparte C do anexo III (Parte-ATM/ANS.OR) do Regulamento de Execução (UE) 2017/373 devem substituir a análise do impacto na segurança da aviação por uma análise do impacto nos seus serviços de acordo com a avaliação do apoio à segurança exigida pela secção ATM/ANS.OR.C.005. Esta avaliação do apoio à segurança deve ser disponibilizada aos prestadores de serviços de tráfego aéreo a quem prestam serviços e esses prestadores de serviços de tráfego aéreo serão responsáveis pela avaliação do impacto na segurança da aviação.

▼B

IS.I.OR.210 Tratamento dos riscos para a segurança da informação

a) A organização deve desenvolver medidas para fazer face aos riscos inaceitáveis identificados em conformidade com a secção IS.I.OR.205, aplicá-las em tempo útil e verificar a sua eficácia contínua. Essas medidas devem permitir à organização:

(1) controlar as circunstâncias que contribuem para a ocorrência efetiva do cenário de ameaça;

(2) reduzir as consequências para a segurança da aviação associadas à concretização do cenário de ameaça;

(3) evitar os riscos.

Essas medidas não devem introduzir quaisquer novos riscos potencialmente inaceitáveis para a segurança da aviação.

b) A pessoa referida na secção IS.I.OR.240, alíneas a) e b), e outro pessoal afetado da organização devem ser informados do resultado da avaliação dos riscos efetuada em conformidade com a secção IS.I.OR.205, dos cenários de ameaça correspondentes e das medidas a aplicar.

A organização deve também informar as organizações com as quais tenha uma interface, em conformidade com a secção IS.I.OR.205, alínea b), de quaisquer riscos que se coloquem a ambas as organizações.

IS.I.OR.215 Sistema de comunicação interna de informações sobre segurança da informação

a) A organização deve estabelecer um sistema de comunicação interna que permita a recolha e a avaliação de eventos relacionados com a segurança da informação, incluindo os que devem ser comunicados nos termos da secção IS.I.OR.230.

b) Esse regime e o processo referido na secção IS.I.OR.220 devem permitir à organização:

(1) identificar quais dos eventos comunicados nos termos da alínea a) são considerados incidentes ou vulnerabilidades de segurança da informação com um impacto potencial na segurança da aviação;

(2) identificar as causas e os fatores que contribuem para os incidentes e as vulnerabilidades na segurança da informação identificados em conformidade com o ponto (1) e abordá-los no âmbito do processo de gestão dos riscos de segurança da informação, em conformidade com as secções IS.I.OR.205 e IS.I.OR.220;

(3) assegurar uma avaliação de todas as informações conhecidas e pertinentes relacionadas com os incidentes e as vulnerabilidades de segurança da informação identificados em conformidade com o ponto (1);

(4) assegurar a aplicação de um método de divulgação interna da informação, conforme necessário.

c) Qualquer organização contratada que possa expor a organização a riscos de segurança da informação com um impacto potencial na segurança da aviação deve comunicar as ocorrências de segurança da informação à organização. Esses relatórios são apresentados de acordo com os procedimentos estabelecidos nas disposições contratuais específicas e avaliados em conformidade com a alínea b).

d) A organização cooperará nas investigações com qualquer outra organização que preste um contributo significativo para a segurança da informação das suas próprias atividades.

e) A organização pode integrar esse regime de comunicação de informações noutros sistemas de comunicação de informações que já tenha implementado.

▼B

IS.I.OR.220 Incidentes de segurança da informação — deteção, resposta e recuperação

a) Com base no resultado da avaliação dos riscos efetuada em conformidade com a secção IS.I.OR.205 e no resultado do tratamento dos riscos realizado em conformidade com a secção IS.I.OR.210, a organização deve aplicar medidas para detetar incidentes e vulnerabilidades que indiquem a potencial materialização de riscos inaceitáveis e que possam ter um impacto potencial na segurança da aviação. Essas medidas de deteção devem permitir à organização:

(1) identificar desvios em relação às bases de referência do desempenho funcional predeterminado;

(2) desencadear avisos para ativar medidas de resposta adequadas, em caso de desvio.

b) A organização deve aplicar medidas para responder a qualquer situação identificada em conformidade com a alínea a) que possa desencadear ou se tenha transformado num incidente de segurança da informação. Essas medidas de resposta devem permitir à organização:

(1) iniciar a reação aos alertas referidos na alínea a) (2), ativando recursos predefinidos e ações;

(2) conter a propagação de um ataque e evitar a plena concretização de um cenário de ameaça;

(3) controlar o modo de avaria dos elementos afetados definidos na secção IS.I.OR.205, alínea a).

c) A organização deve aplicar medidas destinadas a recuperar de incidentes de segurança da informação, incluindo medidas de emergência, se necessário. Essas medidas de recuperação devem permitir à organização:

(1) eliminar a condição que causou o incidente ou limitá-lo a um nível tolerável;

(2) atingir um estado seguro dos elementos afetados definidos na secção IS.I.OR.205, alínea a), num prazo de recuperação previamente definido pela organização.

IS.I.OR.225 Resposta a constatações notificadas pela autoridade competente

a) Após receção da notificação de constatações apresentada pela autoridade competente, a organização deve:

(1) identificar a causa principal ou as causas principais e os fatores que contribuem para a não conformidade;

(2) definir um plano de medidas corretivas;

(3) demonstrar a retificação do incumprimento a contento da autoridade competente.

b) As ações referidas na alínea a) devem ser realizadas no prazo acordado com a autoridade competente.

IS.I.OR.230 Sistema de comunicação externa sobre segurança da informação

a) A organização deve implementar um sistema de comunicação de informações sobre segurança da informação que cumpra os requisitos estabelecidos no Regulamento (UE) n.º 376/2014 e nos seus atos delegados e de execução, caso esse regulamento seja aplicável à organização.

▼B

b) Sem prejuízo das obrigações previstas no Regulamento (UE) n.º 376/2014, a organização deve assegurar que qualquer incidente ou vulnerabilidade de segurança da informação que possa representar um risco significativo para a segurança da aviação seja comunicado à respetiva autoridade competente. Além disso:

(1) se tal incidente ou vulnerabilidade afetar uma aeronave ou um sistema ou componente associado, a organização deve também comunicá-lo ao titular da certificação de projeto;

(2) se tal incidente ou vulnerabilidade afetar um sistema ou componente utilizado pela organização, esta deve comunicá-lo à organização responsável pelo projeto do sistema ou componente.

c) A organização deve comunicar as condições referidas na alínea b) do seguinte modo:

(1) Deve ser apresentada uma notificação à autoridade competente e, se for caso disso, ao titular da certificação de projeto ou à organização responsável pelo projeto do sistema ou componente, logo que a organização tenha conhecimento da situação;

(2) Deve ser apresentado um relatório à autoridade competente e, se for caso disso, ao titular da certificação de projeto ou à organização responsável pelo projeto do sistema ou do componente, o mais rapidamente possível, mas no máximo 72 horas a contar do momento em que a organização tome conhecimento da situação, salvo em circunstâncias excecionais que o impeçam.

O relatório deve ser elaborado na forma definida pela autoridade competente e conter todas as informações pertinentes sobre a situação de que a organização tenha conhecimento;

(3) Deve ser apresentado um relatório de acompanhamento à autoridade competente e, se for caso disso, ao titular da certificação de projeto ou à organização responsável pelo projeto do sistema ou componente, com informações pormenorizadas sobre as medidas que a organização tomou ou tenciona tomar para recuperar do incidente e as medidas que tenciona tomar para evitar incidentes semelhantes em matéria de segurança da informação no futuro.

O relatório de acompanhamento deve ser apresentado logo que essas ações tenham sido identificadas e elaborado na forma definida pela autoridade competente.

IS.I.OR.235 Adjudicação de atividades de gestão da segurança da informação

a) A organização deve assegurar que, ao contratar qualquer parte das atividades a que se refere o ponto IS.I.OR.200 a outras organizações, as atividades contratadas cumprem os requisitos do presente regulamento e a organização contratada trabalha sob a sua supervisão. A organização deve assegurar que os riscos associados às atividades contratadas são geridos de forma adequada.

b) A organização deve assegurar que a autoridade competente possa ter acesso, a pedido, à organização contratada para determinar a conformidade permanente com os requisitos aplicáveis estabelecidos no presente regulamento.

IS.I.OR.240 Requisitos em matéria de pessoal

a) O administrador responsável da organização designada em conformidade com os Regulamentos (UE) n.º 1321/2014, (UE) n.º 965/2012, (UE) n.º 1178/2011, (UE) 2015/340, o Regulamento de Execução (UE) 2017/373 ou o Regulamento de Execução (UE) 2021/664, conforme aplicável, a que se refere o artigo 2.º, n.º 1, do presente regulamento, deve ser dotado dos poderes necessários para assegurar que todas as atividades exigidas pelo presente regulamento podem ser financiadas e realizadas. Deve:

▼B

(1) Assegurar a disponibilidade de todos os recursos necessários para cumprir os requisitos do presente regulamento;

(2) Estabelecer e promover a política de segurança da informação referida na secção IS.I.OR.200, alínea a), ponto (1);

(3) Demonstrar que possui um conhecimento básico do presente regulamento.

b) O administrador responsável nomeia uma pessoa ou um grupo de pessoas para assegurar que a organização cumpre os requisitos do presente regulamento e define as suas funções. Essa pessoa ou grupo de pessoas responde diretamente perante o administrador responsável e deve dispor dos conhecimentos, dos antecedentes e da experiência adequados para cumprir as suas responsabilidades. Os procedimentos devem estabelecer de forma clara quem substitui quem em caso de ausência prolongada da(s) pessoa(s) acima referida(s).

c) O administrador responsável nomeará uma pessoa ou um grupo de pessoas com a responsabilidade de gerir a função de controlo da conformidade a que se refere a secção IS.I.OR.200, alínea a), ponto (12).

d) Se a organização partilhar estruturas, políticas, processos e procedimentos organizacionais de segurança da informação com outras organizações ou com áreas da sua própria organização que não façam parte da certificação ou declaração, o administrador responsável poderá delegar as suas atividades numa pessoa responsável comum.

Nesse caso, devem ser estabelecidas medidas de coordenação entre o administrador responsável da organização e a pessoa responsável comum, a fim de assegurar a integração adequada da gestão da segurança da informação na organização.

e) O administrador responsável, ou a pessoa responsável comum a que se refere a alínea d), têm os poderes necessários para estabelecer e manter as estruturas, políticas, processos e procedimentos organizacionais necessários à aplicação da secção IS.I.OR.200.

f) A organização deve dispor de um processo que garanta que dispõe de pessoal em número suficiente para a consecução das atividades abrangidas pelo presente anexo.

g) A organização deve dispor de um processo para assegurar que o pessoal referido na alínea f) possui as competências necessárias para desempenhar as suas funções.

h) A organização deve dispor de um processo para assegurar que o pessoal reconhece as responsabilidades associadas às funções e tarefas que lhe são cometidas.

i) A organização deve assegurar que a identidade e a fiabilidade do pessoal que tem acesso aos sistemas de informação e aos dados sujeitos aos requisitos do presente regulamento são devidamente estabelecidas.

IS.I.OR.245 Conservação de registos

a) *A organização deve conservar registos das suas atividades de gestão da segurança da informação.*

(1) A organização deve assegurar que os seguintes registos são arquivados e rastreáveis:

i) qualquer aprovação recebida e qualquer avaliação dos riscos de segurança da informação associada, em conformidade com a secção IS.I.OR.200, alínea e);

ii) contratos para as atividades referidas na secção IS.I.OR.200, alínea a), ponto (9);

▼B

iii) registos dos principais processos referidos na secção IS.I.OR.200, alínea d);

iv) registos dos riscos identificados na avaliação dos riscos referida na secção IS.I.OR.205, juntamente com as medidas associadas de tratamento dos riscos referidas na secção IS.I.OR.210;

v) registos dos incidentes e vulnerabilidades de segurança da informação comunicados em conformidade com os sistemas de comunicação a que se referem as secções IS.I.OR.215 e IS.I.OR.230;

vi) registos dos eventos relacionados com a segurança da informação que possam ter de ser reavaliados para revelar incidentes ou vulnerabilidades de segurança da informação não detetados.

(2) Os registos referidos no ponto 1, subalínea i), devem ser conservados pelo menos até 5 anos após a aprovação ter perdido a sua validade.

(3) Os registos referidos no ponto 1, subalínea ii), devem ser conservados pelo menos até 5 anos após a alteração ou rescisão do contrato.

(4) Os registos referidos no ponto 1, subalíneas iii), iv) e v), devem ser conservados pelo menos durante um período de 5 anos.

(5) Os registos referidos no ponto 1, subalínea vi), devem ser conservados até que esses eventos de segurança da informação tenham sido reavaliados de acordo com uma periodicidade definida num procedimento estabelecido pela organização.

b) *A organização deve manter registos das qualificações e da experiência do seu pessoal envolvido em atividades de gestão da segurança da informação.*

(1) Os registos relativos às qualificações e à experiência do pessoal devem ser conservados enquanto a pessoa trabalhar para a organização e durante, pelo menos, 3 anos após a pessoa ter deixado a organização.

(2) Os membros do pessoal devem, a seu pedido, ter acesso aos seus registos individuais. Além disso, a seu pedido, a organização deve fornecer-lhes uma cópia dos seus registos individuais quando deixam a organização.

c) O formato dos registos deve ser especificado nos procedimentos da organização.

d) Os registos devem ser conservados de um modo que assegure a proteção dos danos, das alterações e do furto, sendo as informações identificadas, sempre que requerido, de acordo com o seu nível de classificação de segurança. A organização assegura que os registos são conservados através de meios que garantam a integridade, a autenticidade e o acesso autorizado.

IS.I.OR.250 Manual de gestão da segurança da informação (MGSI)

a) A organização deve disponibilizar à autoridade competente um manual de gestão da segurança da informação (MGSI) e, se for caso disso, quaisquer manuais e procedimentos associados referenciados, que contenham:

(1) Uma declaração assinada pelo administrador responsável, confirmando que a organização procederá sempre em conformidade com os requisitos do presente anexo e com o MGSI; Se o administrador responsável não for o diretor executivo (CEO) da organização, então este (CEO) deve assinar a declaração;

(2) O(s) título(s), o(s) nome(s), o(s) deveres, a(s) responsabilidades e os poderes da pessoa ou das pessoas a que se refere a secção IS.I.OR.240, alíneas b) e c);

▼B

(3) O título, o nome, os deveres, as responsabilidades e os poderes da pessoa ou das pessoas a que se refere a secção IS.I.OR.240, alínea d), se aplicável;

(4) A política de segurança da informação da organização a que se refere a secção IS.I.OR.200, alínea a), ponto (1);

(5) Uma descrição genérica dos recursos humanos e do sistema em vigor para planear a disponibilidade do pessoal, tal como exigido pela secção IS.I.OR.240;

(6) O(s) título(s), o(s) nome(s), o(s) deveres, a(s) responsabilidades e os poderes das principais pessoas responsáveis pela aplicação da secção IS.I.OR.200, incluindo a pessoa ou pessoas responsáveis pela função de controlo da conformidade a que se refere a secção IS.I.OR.200, alínea a), ponto (12);

(7) Um organograma que mostre as cadeias de responsabilização e de responsabilidade associadas às pessoas referidas nos pontos (2) e (6);

(8) Uma descrição do sistema de comunicação interna a que se refere a secção IS.I.OR.215;

(9) Os procedimentos que especificam a forma como a organização garante o cumprimento da presente parte e, em especial:

i) a documentação referida na secção IS.I.OR.200, alínea c);

ii) os procedimentos que definem a forma como a organização controla quaisquer atividades contratadas referidas na secção IS.I.OR.200, alínea a), ponto (9);

iii) o procedimento de alteração ao MGSI definido na alínea c);

(10) A lista de meios de conformidade alternativos aprovados.

▼M3

b) A versão original do MGSI deve ser aprovada e uma cópia deve ser conservada pela autoridade competente. As organizações declaradas não carecem de aprovação. O MGSI deve ser alterado na medida do necessário para manter uma descrição atualizada do SGSI da organização. Deve ser fornecida à autoridade competente uma cópia de quaisquer alterações ao MGSI.

c) As alterações ao MGSI são geridas segundo um procedimento estabelecido pela organização. As alterações não incluídas no âmbito desse procedimento e as alterações relacionadas com as alterações a que se refere a secção IS.I.OR.255, alínea b), devem ser aprovadas pela autoridade competente. As organizações declaradas não carecem de aprovação.

▼B

d) A organização pode integrar o MGSI noutros manuais, desde que exista uma referência cruzada clara que indique quais as partes do manual que correspondem aos diferentes requisitos constantes do presente anexo.

▼M3

IS.I.OR.255 Alterações ao sistema de gestão da segurança da informação

a) As alterações ao SGSI podem ser geridas e notificadas à autoridade competente mediante um procedimento desenvolvido pela organização. Esse procedimento deve ser aprovado pela autoridade competente, exceto no caso das organizações declaradas.

▼M3

b) No que diz respeito às alterações do SGSI não abrangidas pelo procedimento referido na alínea a), a organização deve solicitar e obter uma aprovação emitida pela autoridade competente, exceto no caso de organizações declaradas, que não carecem de aprovação.

No que diz respeito a estas alterações:

(1) O pedido deve ser apresentado antes da introdução de qualquer alteração, de modo a permitir à autoridade competente determinar a conformidade permanente com o disposto no presente regulamento e, se necessário, alterar o certificado da organização e os respetivos termos de certificação anexos a este;

(2) A organização deve disponibilizar à autoridade competente todas as informações que esta solicite para avaliar a alteração;

(3) A alteração só pode ser aplicada após a receção de uma aprovação formal pela autoridade competente, exceto no caso das organizações declaradas, que podem aplicar imediatamente a alteração;

(4) A organização deve operar nas condições prescritas pela autoridade competente durante a aplicação dessas alterações.

▼B

IS.I.OR.260 Melhoria contínua

▼C1

a) A organização deve avaliar, utilizando indicadores de desempenho adequados, a eficácia e a maturidade do SGSI. Essa avaliação deve ser efetuada numa base de calendário predefinida pela organização ou na sequência de um incidente de segurança da informação.

b) Se forem detetadas deficiências na sequência da avaliação efetuada em conformidade com a alínea a), a organização deve tomar as medidas de melhoria necessárias para assegurar que o SGSI continua a cumprir os requisitos aplicáveis e permite manter os riscos de segurança da informação a um nível aceitável. Além disso, a organização deve reavaliar os elementos do SGSI afetados pelas medidas adotadas.

▼B

ANEXO III

Os anexos VI (parte ARA) e VII (parte ORA) do Regulamento (UE) n.º 1178/2011 são alterados do seguinte modo:

(1) O anexo VI (parte ARA) é alterado do seguinte modo:

a) na secção ARA.GEN.125, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.I.OR.230 do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.»;

b) a seguir à secção ARA.GEN.135 é inserida a seguinte secção ARA.GEN.135A:

«ARA.GEN.135A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com a secção ARA.GEN.125, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

c) na secção ARA.GEN.200, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

d) a secção ARA.GEN.205 é alterada do seguinte modo:

i) o título passa a ter a seguinte redação:

▼B

«ARA.GEN.205 Atribuição de tarefas»;

ii) é aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com a secção ORA.GEN.200A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com a secção ARA.GEN.200, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

e) na secção ARA.GEN.300, é aditada a alínea g) com a seguinte redação:

«g) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção ORA.GEN.200A, para além de cumprir o disposto nas alíneas a) a f), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

f) a seguir à secção ARA.GEN.330 é inserida a seguinte secção ARA.GEN.330A:

«ARA.GEN.330A Alterações ao sistema de gestão da segurança da informação

a) No que diz respeito às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.I.OR.255, alínea a), do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203, a autoridade competente deve incluir a revisão dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos na secção ARA.GEN.300. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com a secção ARA.GEN.350.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.I.OR.255, alínea b), do anexo II (parte IS.I.OR), do Regulamento de Execução (UE) 2023/203:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

▼B

(2) O anexo VII (parte ORA) é alterado do seguinte modo:

a seguir à secção ORA.GEN.200 é inserida a seguinte secção ORA. GEN.200A:

«ORA.GEN.200A Sistema de gestão da segurança da informação

Para além do sistema de gestão referido na secção ORA.GEN.200, a organização deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.».

▼B

ANEXO IV

O anexo I (parte 21) do Regulamento (UE) n.º 748/2012 é alterado do seguinte modo:

(1) O índice é alterado do seguinte modo:

(a) A seguir ao título 21.B.20 é inserido o seguinte título:

«21.B.20A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação»;

(b) O título do ponto 21.B.30 passa a ter a seguinte redação:

«21.B.30 Atribuição de tarefas»;

(c) A seguir ao título 21.B.240 é inserido o seguinte título:

«21.B.240A Alterações ao sistema de gestão da segurança da informação»;

(d) A seguir ao título 21.B.435 é inserido o seguinte título:

«21.B.435A Alterações ao sistema de gestão da segurança da informação»;

(2) No ponto 21.B.15, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.D.OR.230 do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645.»;

(3) A seguir ao ponto 21.B.20 é inserido o seguinte ponto 21.B.20A:

«21.B.20A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com o ponto 21.B.15, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

▼B

(4) No ponto 21.B.25, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

(5) O ponto 21.B.30 é alterado do seguinte modo:

(a) O título passa a ter a seguinte redação:

«21.B.30 Atribuição de tarefas»;

(b) É aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com os pontos 21.A.139A e 21.A.239A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com o ponto 21.B.25, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

(6) No ponto 21.B.221, é aditada a alínea g) com a seguinte redação:

«g) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção 21.A.139A, para além de cumprir o disposto nas alíneas a) a f), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

(7) A seguir ao ponto 21.B.240 é inserido o seguinte ponto 21.B.240A:

«**21.B.240A Alterações ao sistema de gestão da segurança da informação**

a) Para as alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.D.OR.255, alínea a), do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645, a autoridade competente deve incluir a análise dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos no ponto 21.B.221. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com o ponto 21.B.225.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.D.OR.255, alínea b), do anexo (parte IS.D.OR), do Regulamento Delegado (UE) 2022/1645:

▼B

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

(8) No ponto 21.B.431, é aditada a alínea d) com a seguinte redação:

«d) Para a certificação e supervisão da conformidade da organização com o disposto no ponto 21.A.239A, para além do cumprimento do disposto nas alíneas a) a c), a autoridade competente deve respeitar os seguintes princípios:

(1) a autoridade competente deve rever as interfaces e os riscos associados identificados em conformidade com a secção IS.D.OR.205, alínea b), do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645 por cada organização sujeita à sua supervisão;

(2) se forem detetadas discrepâncias nas interfaces mútuas e riscos associados identificados por diferentes organizações, a autoridade competente revê-las-á com as organizações afetadas e, se necessário, apresenta as constatações adequadas para assegurar a aplicação de medidas corretivas;

(3) se a documentação analisada nos termos do ponto (2) revelar a existência de riscos significativos associados às interfaces com organizações sujeitas à supervisão de uma autoridade competente diferente no mesmo Estado-Membro, essas informações devem ser comunicadas à autoridade competente correspondente.»;

(9) A seguir ao ponto 21.B.435 é inserido o seguinte ponto 21.B.435A:

«**21.B.435A Alterações ao sistema de gestão da segurança da informação**

a) Para as alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.D.OR.255, alínea a), do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645, a autoridade competente deve incluir a análise dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos no ponto 21.B.431. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com o ponto 21.B.433.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.D.OR.255, alínea b), do anexo (parte IS.D.OR), do Regulamento Delegado (UE) 2022/1645:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações».

▼B

ANEXO V

Os anexos II (parte ARO) e III (parte ORO) do Regulamento (UE) n.º 965/2012 são alterados do seguinte modo:

(1) O anexo II (parte ARO) é alterado do seguinte modo:

a) Na secção ARO.GEN.125, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.I.OR.230 do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.»;

b) a seguir à secção ARO.GEN.135 é inserida a seguinte secção ARO. GEN.135A:

«**ARO.GEN.135A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação**

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com a secção ARO.GEN.125, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

c) na secção ARO.GEN.200, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

d) a secção ARO.GEN.205 é alterada do seguinte modo:

i) o título passa a ter a seguinte redação:

«**ARO.GEN.205 Atribuição de tarefas**»;

▼B

ii) é aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com a secção ORO.GEN.200A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com a secção ARO.GEN.200, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

e) na secção ARO.GEN.300, é aditada a alínea g) com a seguinte redação:

«g) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção ORO.GEN.200A, para além de cumprir o disposto nas alíneas a) a f), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

f) a seguir à secção ARO.GEN.330 é inserida a seguinte secção ARO.GEN.330A:

«**ARO.GEN.330A Alterações ao sistema de gestão da segurança da informação**

a) No que diz respeito às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.I.OR.255, alínea a), do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203, a autoridade competente deve incluir a revisão dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos na secção ARO.GEN.300. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com a secção ARO.GEN.350.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.I.OR.255, alínea b), do anexo II (parte IS.I.OR), do Regulamento de Execução (UE) 2023/203:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

▼B

(2) O anexo III (parte ORO) é alterado do seguinte modo:

a seguir à secção ORO.GEN.200 é inserida a seguinte secção ORO. GEN.200A:

«**ORO.GEN.200A Sistema de gestão da segurança da informação**

Para além do sistema de gestão referido na secção ORO.GEN.200, o operador deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.».

▼B

ANEXO VI

O anexo II (parte ADR.AR) do Regulamento (UE) n.º 139/2014 é alterado do seguinte modo:

(1) No ponto ADR.AR.A.025, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.D.OR.230 do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645.»;

(2) a seguir à secção ADR.AR.A.030 é inserida a seguinte secção ADR.AR.A.030A:

«**ADR.AR.A.030A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação**

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com a secção ADR.AR.A.025, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

(3) na secção ADR.AR.B.005, é aditada a alínea d) com a seguinte redação:

«d) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

(4) a secção ADR.AR.B.010 é alterada do seguinte modo:

i) o título passa a ter a seguinte redação:

«**ADR.AR.B.010 Atribuição de tarefas**»;

▼B

ii) é aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com a secção ADR.OR.D.005A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com a secção ADR.AR.B.005, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

(5) Na secção ADR.AR.C.005, é aditada a alínea f) seguinte:

«f) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção ADR.OR.D.005A, para além de cumprir o disposto nas alíneas a) a e), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

(6) A seguir ao ponto ADR.AR.C.040 é inserido o seguinte ponto ADR.AR.C.040A:

«**ADR.AR.C.040A Alterações ao sistema de gestão da segurança da informação**

a) Relativamente às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.D.OR.255, alínea a), do anexo (parte IS.D.OR) do Regulamento Delegado (UE) 2022/1645, a autoridade competente deve incluir a análise dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos no ponto ADR.AR.C.005. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com o ponto ADR.AR.C.055.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.D.OR.255, alínea b), do anexo (parte IS.D.OR), do Regulamento Delegado (UE) 2022/1645:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»

▼B

ANEXO VII

Os anexos II (parte 145), III (parte 66) e V-C (parte CAMO) do Regulamento (UE) n.º 1321/2014 são alterados do seguinte modo:

(1) O anexo II (parte 145) é alterado do seguinte modo:

(a) O índice é alterado do seguinte modo:

i) A seguir ao título 145.A.200 é inserido o seguinte título:

«145.A.200A Sistema de gestão da segurança da informação»;

ii) A seguir ao título 145.B.135 é inserido o seguinte título:

«145.B.135A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação»;

iii) O título do ponto 145.B.205 passa a ter a seguinte redação:

«145.B.205 Atribuição de tarefas»;

iv) A seguir ao título 145.B.330 é inserido o seguinte título:

«145.B.330A Alterações ao sistema de gestão da segurança da informação»;

(b) A seguir ao ponto 145.A.200 é inserido o seguinte ponto 145.A.200A:

«145.A.200A **Sistema de gestão da segurança da informação**

Para além do sistema de gestão referido no ponto 145.A.200, a organização de manutenção deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

(c) No ponto 145.B.125, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.I.OR.230 do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.».

(d) A seguir ao ponto 145.B.135 é inserido o seguinte ponto 145.B.135A:

«145.B.135A **Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação**

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

▼B

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com o ponto 145.B.125, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

(e) No ponto 145.B.200, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

(f) O ponto 145.B.205 é alterado do seguinte modo:

i) O título passa a ter a seguinte redação:

«145.B.205 **Atribuição de tarefas**»;

ii) É aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com o ponto 145.A.200A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com o ponto 145.B.200, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

▼B

(g) No ponto 145.B.300, é aditada a alínea g) com a seguinte redação:

«g) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção 145.A.200A, para além de cumprir o disposto nas alíneas a) a f), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

(h) A seguir ao ponto 145.B.330 é inserido o seguinte ponto 145.B.330A:

«145.B.330A **Alterações ao sistema de gestão da segurança da informação**

a) No que diz respeito às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.I.OR.255, alínea a), do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203, a autoridade competente deve incluir a revisão dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos no ponto 145.B.300. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com o ponto 145.B.350.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.I.OR.255, alínea b), do anexo II (parte IS.I.OR), do Regulamento de Execução (UE) 2023/203.».

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

(2) O anexo III (parte 66) é alterado do seguinte modo:

a) no índice, a seguir ao título 66.B.10 é inserido o seguinte título:

«66.B.15 Sistema de gestão da segurança da informação»;

b) a seguir ao ponto 66.B.10 é inserido o seguinte ponto 66.B.15:

«66.B.15 **Sistema de gestão da segurança da informação**

A autoridade competente deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

(3) O anexo V-C (parte CAMO) é alterado do seguinte modo:

a) O índice é alterado do seguinte modo:

i) a seguir ao título CAMO.A.200 é inserido o seguinte título:

«CAMO.A.200A Sistema de gestão da segurança da informação»;

▼B

ii) a seguir ao título CAMO.B.135 é inserido o seguinte título:

«CAMO.B.135A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação»;

iii) O título do ponto CAMO.B.205 passa a ter a seguinte redação:

«CAMO.B.205 Atribuição de tarefas»;

iv) a seguir ao título CAMO.B.330 é inserido o seguinte título:

«CAMO.B.330A Alterações ao sistema de gestão da segurança da informação»;

b) a seguir ao ponto CAMO.A.200 é inserido o seguinte ponto CAMO.A.200A:

«CAMO.A.200A **Sistema de gestão da segurança da informação**

Para além do sistema de gestão referido no ponto CAMO.A.200, a organização deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

c) No ponto CAMO.B.125, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.I.OR.230 do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.».

d) a seguir ao ponto CAMO.B.135 é inserido o seguinte ponto CAMO.B.135A:

«CAMO.B.135A **Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação**

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com o ponto CAMO.B.125, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

▼B

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

e) no ponto CAMO.B.200, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

f) o ponto CAMO.B.205 é alterado do seguinte modo:

i) o título passa a ter a seguinte redação:

«CAMO.B.205 **Atribuição de tarefas**»;

ii) é aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com o ponto CAMO.A.200A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com o ponto CAMO.B.200, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

g) no ponto CAMO.B.300, é aditada a alínea g) com a seguinte redação:

«g) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção CAMO.A.200A, para além de cumprir o disposto nas alíneas a) a f), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

▼B

h) a seguir ao ponto CAMO.B.330 é inserido o seguinte ponto CAMO.B.330A:

«CAMO.B.330A **Alterações ao sistema de gestão da segurança da informação**

a) No que diz respeito às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.I.OR.255, alínea a), do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203, a autoridade competente deve incluir a revisão dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos no ponto CAMO.B.300. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com o ponto CAMO.B.350.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.I.OR.255, alínea b), do anexo II (parte IS.I.OR), do Regulamento de Execução (UE) 2023/203:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

▼B

ANEXO VIII

Os anexos II (parte ATCO.AR) e III (parte ATCO.OR) do Regulamento (UE) 2015/340 são alterados do seguinte modo:

(1) O anexo II (parte ATCO.AR) é alterado do seguinte modo:

a) Na secção ATCO.AR.A.020, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.I.OR.230 do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.»;

b) a seguir à secção ATCO.AR.A.025 é inserida a seguinte secção ATCO.AR.A.025A:

«**ATCO.AR.A.025A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação**

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com a secção ATCO.AR.A.020 e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

c) na secção ATCO.AR.B.001, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

▼B

d) a secção ATCO.AR.B.005 é alterada do seguinte modo:

i) o título passa a ter a seguinte redação:

«**ATCO.AR.B.005 Atribuição de tarefas**»;

ii) é aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com a secção ATCO.OR.C.001A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com a secção ATCO.AR.B.001, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

e) Na secção ATCO.AR.C.001, é aditada a alínea f) seguinte:

«f) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção ATCO.OR.C.001A, para além de cumprir o disposto nas alíneas a) a e), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

f) a seguir à secção ATCO.AR.E.010 é inserida a seguinte secção ATCO.AR.E.010A:

«**ATCO.AR.E.010A Alterações ao sistema de gestão da segurança da informação**

a) No que diz respeito às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.I.OR.255, alínea a), do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203, a autoridade competente deve incluir a revisão dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos na secção ATCO.AR.C.001. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com a secção ATCO.AR.C.010.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.I.OR.255, alínea b), do anexo II (parte IS.I.OR), do Regulamento de Execução (UE) 2023/203:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

▼B

(2) ►C1 O anexo III (parte ATCO.OR) é alterado do seguinte modo: ◄

a seguir à secção ATCO.OR.C.001 é inserida a seguinte secção ATCO.OR.C.001A:

«**ATCO.OR.C.001A Sistema de gestão da segurança da informação**

Para além do sistema de gestão referido na secção ATCO.OR.C.001, a organização de formação deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.».

▼B

ANEXO IX

Os anexos II (parte ATM/ANS.AR) e III (parte ATM/ANS.OR) do Regulamento de Execução (UE) 2017/373 são alterados do seguinte modo:

(1) O anexo II (parte ATM/ANS.AR) é alterado do seguinte modo:

a) na secção ATM/ANS.AR.A.020, é aditada a alínea c) com a seguinte redação:

«c) A autoridade competente do Estado-Membro deve fornecer à Agência, o mais rapidamente possível, informações significativas para a segurança decorrentes dos relatórios de segurança da informação por ela recebidos nos termos da secção IS.I.OR.230 do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203.»;

b) a seguir à secção ATM/ANS.AR.A.025 é inserida a seguinte secção ATM/ANS.AR.A.025A:

«**ATM/ANS.AR.A.025A Resposta imediata a um incidente ou vulnerabilidade de segurança da informação com impacto na segurança da aviação**

a) A autoridade competente deve implementar um sistema de recolha, análise e divulgação adequadas de informações relacionadas com incidentes e vulnerabilidades de segurança da informação com potencial impacto na segurança da aviação que sejam comunicadas pelas organizações. Tal deve ser feito em coordenação com quaisquer outras autoridades pertinentes responsáveis pela segurança da informação ou pela cibersegurança no Estado-Membro, a fim de aumentar a coordenação e a compatibilidade dos sistemas de comunicação de informações.

b) A Agência deve implementar um sistema para analisar adequadamente quaisquer informações relevantes em matéria de segurança recebidas em conformidade com o ponto ATM/ANS.AR.A.020, alínea c), e, sem demora injustificada, fornecer aos Estados-Membros e à Comissão todas as informações, incluindo recomendações ou medidas corretivas a tomar, necessárias para reagir atempadamente a um incidente ou vulnerabilidade de segurança da informação com potencial impacto na segurança da aviação que envolva produtos, peças, equipamentos não instalados, pessoas ou organizações abrangidas pelo Regulamento (UE) 2018/1139 e pelos seus atos delegados e de execução.

c) Ao receber as informações referidas nas alíneas a) e b), a autoridade competente toma as medidas adequadas para fazer face ao potencial impacto na segurança da aviação do incidente ou da vulnerabilidade de segurança da informação.

d) As medidas tomadas ao abrigo da alínea c) serão imediatamente notificadas a todas as pessoas ou organizações visadas, nos termos do Regulamento (UE) 2018/1139 e dos seus atos delegados e de execução. A autoridade competente do Estado-Membro deve notificar também a Agência dessas medidas e, caso seja necessário adotar medidas concertadas, as autoridades competentes dos outros Estados-Membros em causa.»;

c) na secção ATM/ANS.AR.B.001, é aditada a alínea e) com a seguinte redação:

«e) Além dos requisitos constantes da alínea a), o sistema de gestão estabelecido e mantido pela autoridade competente deve cumprir o disposto no anexo I (parte IS.AR) do Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

▼B

d) a secção ATM/ANS.AR.B.005 é alterada do seguinte modo:

i) o título passa a ter a seguinte redação:

«**ATM/ANS.AR.B.005 Atribuição de tarefas**»;

ii) é aditada a alínea c) com a seguinte redação:

«c) No que diz respeito à certificação e supervisão da conformidade da organização com o ponto ATM/ ANS.OR.B.005A, a autoridade competente pode atribuir tarefas a entidades qualificadas em conformidade com a alínea a) ou a qualquer autoridade pertinente responsável pela segurança da informação ou pela cibersegurança no Estado-Membro. Aquando da atribuição de tarefas, a autoridade competente deve certificar-se de que:

(1) todos os aspetos relacionados com a segurança da aviação são coordenados e tidos em conta pela entidade qualificada ou pela autoridade pertinente;

(2) os resultados das atividades de certificação e supervisão realizadas pela entidade qualificada ou pela autoridade pertinente estão integrados nos processos globais de certificação e supervisão da organização;

(3) o seu próprio sistema de gestão da segurança da informação, estabelecido em conformidade com o ponto ATM/ANS.AR.B.001, alínea e), abrange todas as tarefas de certificação e supervisão contínua realizadas em seu nome.»;

e) na secção ATM/ANS.AR.C.010, é aditada a alínea d) com a seguinte redação:

«d) No que respeita à certificação e supervisão da conformidade da organização com o disposto na secção ATM/ANS.OR.B.005A, para além de cumprir o disposto nas alíneas a) a c), a autoridade competente deve rever qualquer aprovação concedida nos termos da secção IS.I.OR.200, alínea e), do presente regulamento ou da secção IS.D.OR.200, alínea e), do Regulamento Delegado (UE) 2022/1645, na sequência do ciclo de auditoria de supervisão aplicável e sempre que sejam introduzidas alterações no âmbito do trabalho da organização.»

f) a seguir à secção ATM/ANS.AR.C.025 é inserida a seguinte secção ATM/ANS.AR.C.025A:

«**ATM/ANS.AR.C.025A Alterações ao sistema de gestão da segurança da informação**

a) No que diz respeito às alterações geridas e notificadas à autoridade competente em conformidade com o procedimento estabelecido na secção IS.I.OR.255, alínea a), do anexo II (parte IS.I.OR) do Regulamento de Execução (UE) 2023/203, a autoridade competente deve incluir a revisão dessas alterações na sua supervisão contínua, em conformidade com os princípios estabelecidos no ponto ATM/ANS.AR.C.010. Se for detetado qualquer incumprimento, a autoridade competente deve notificar a organização, solicitar novas alterações e agir em conformidade com o ponto ATM/ANS.AR.C.050.

b) No que diz respeito a outras alterações que requeiram um pedido de aprovação em conformidade com a secção IS.I.OR.255, alínea b), do anexo II (parte IS.I.OR), do Regulamento de Execução (UE) 2023/203:

(1) ao receber o pedido de alteração, a autoridade competente deve verificar a conformidade da organização com os requisitos aplicáveis antes de emitir a aprovação;

▼B

(2) a autoridade competente deve estabelecer as condições em que a organização pode operar durante a aplicação da alteração;

(3) caso considere que a organização cumpre os requisitos aplicáveis, a autoridade competente aprova as alterações.»;

(2) O anexo III (parte ATM/ANS.OR) é alterado do seguinte modo:

a) a seguir à secção ATM/ANS.OR.B.005 é inserida a seguinte secção ATM/ANS.OR.B.005A:

«**ATM/ANS.OR.B.005A Sistema de gestão da segurança da informação**

Para além do sistema de gestão referido no ponto ATM/ANS.OR.B.005, o prestador de serviços deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento de Execução (UE) 2023/203, a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»;

b) a secção ATM/ANS.OR.D.010 passa a ter a seguinte redação:

«**ATM/ANS.OR.D.010 Gestão da segurança da aviação**

a) Os prestadores de serviços de navegação aérea e de gestão do fluxo de tráfego aéreo e o gestor da rede devem, como parte integrante do seu sistema de gestão, tal como previsto no ponto ATM/ANS.OR.B.005, estabelecer um sistema de gestão da segurança da aviação a fim de garantir:

(1) A proteção das suas instalações e pessoal por forma a prevenir interferências ilícitas na prestação de serviços;

(2) A proteção dos dados operacionais que recebem, produzem ou, de outro modo, utilizam por forma a que o acesso esteja limitado unicamente às pessoas autorizadas.

b) O sistema de gestão da segurança deve estabelecer:

(1) O processo e os procedimentos relacionados com a avaliação e a mitigação dos riscos para a segurança, o controlo e o reforço da segurança, as avaliações da segurança e a difusão de ensinamentos;

(2) Os meios para identificar, monitorizar e detetar falhas da segurança e alertar o pessoal através de avisos adequados;

(3) Os meios para controlar os efeitos de falhas na segurança e identificar ações de recuperação e procedimentos de mitigação dos riscos a fim de prevenir a repetição de ocorrências.

c) Os prestadores de serviços de navegação aérea e de gestão do fluxo de tráfego aéreo e o gestor da rede devem assegurar a credenciação de segurança do seu pessoal, se adequado, bem como coordenar-se com as autoridades civis e militares relevantes para assegurar a proteção das suas instalações, pessoal e dados.

d) Os aspetos relacionados com a segurança da informação devem ser geridos em conformidade com o ponto ATM/ANS.OR.B.005A.».