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

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil, que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho ([1]), nomeadamente o artigo 19.º, n.º 1, alínea g), e o artigo 39.º, n.º 1, alínea b)

Considerando o seguinte:

(1) Em conformidade com os requisitos essenciais estabelecidos no anexo II, ponto 3.1, alínea b), do Regulamento (UE) 2018/1139, as organizações que exercem atividades de projeto e produção devem aplicar e manter um sistema de gestão dos riscos para a segurança.

(2) Além disso, em conformidade com os requisitos essenciais estabelecidos no anexo VII, pontos 2.2.1 e 5.2, do Regulamento (UE) 2018/1139, os operadores de aeródromos e as organizações responsáveis pela prestação de serviços de gestão da placa de estacionamento devem implementar e manter um sistema de gestão dos riscos para a segurança.

(3) Os riscos para a segurança referidos nos considerandos 1 e 2 podem ter origens diversas, incluindo falhas de conceção e manutenção, aspetos relacionados com o desempenho humano, ameaças ambientais e ameaças à segurança da informação. Por conseguinte, os sistemas de gestão implementados pelas entidades, tal como referido nos considerandos 1 e 2, devem ter em conta não só os riscos para a segurança decorrentes de eventos aleatórios, mas também os riscos para a segurança decorrentes de ameaças à segurança da informação, nos casos em que as falhas existentes possam ser utilizadas por pessoas com intenção dolosa. Estes riscos para a segurança da informação estão a aumentar constantemente no ambiente da aviação civil, à medida que os atuais sistemas de informação vão estando cada vez mais interligados, tornando-se cada vez mais alvo de intervenientes mal-intencionados.

(4) Os riscos associados a esses sistemas de informação não se limitam a eventuais ataques ao ciberespaço, abrangendo também ameaças que podem afetar processos e procedimentos, bem como o desempenho dos seres humanos.

(5) Um número significativo de entidades já utiliza normas internacionais, como a ISO 27001, para abordar a segurança da informação e dos dados digitais. Estas normas podem não ter plenamente em conta todas as especificidades da aviação civil.

(6) Consequentemente, é conveniente adotar requisitos para a gestão dos riscos de segurança da informação com um impacto potencial na segurança da aviação.

(7) É essencial que esses requisitos abranjam os diferentes domínios da aviação e as suas interfaces, uma vez que a aviação constitui uma rede de sistemas altamente interligados. Por conseguinte, devem aplicar-se a todas as entidades que já são obrigadas a dispor de um sistema de gestão em conformidade com a legislação da União em vigor em matéria de segurança da aviação.

(8) Os requisitos estabelecidos no presente regulamento devem ser aplicados de forma coerente em todos os domínios da aviação, criando simultaneamente um impacto mínimo na legislação da União em matéria de segurança da aviação já aplicável a esses domínios.

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

(9) Os requisitos estabelecidos no presente regulamento não devem prejudicar os requisitos de segurança da informação e de cibersegurança estabelecidos no ponto 1.7 do anexo do Regulamento de Execução (UE) 2015/1998 da Comissão ([2]) e no artigo 14.º da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([3]).

(10) A definição de segurança da informação utilizada para efeitos do presente ato jurídico não deve ser interpretada como divergente da definição de segurança das redes e dos sistemas de informação estabelecida na Diretiva 2016/1148.

(11) A fim de evitar uma duplicação dos requisitos legais, caso as entidades abrangidas pelo presente regulamento já estejam sujeitas a requisitos de segurança decorrentes de outros atos da União referidos no considerando 9, que sejam, de facto, equivalentes às disposições estabelecidas no presente regulamento, o cumprimento desses requisitos de segurança deverá ser considerado como equivalente ao cumprimento dos requisitos estabelecidos no presente regulamento.

(12) As entidades abrangidas pelo presente regulamento que já estejam sujeitas a requisitos de segurança decorrentes do Regulamento de Execução (UE) 2015/1998 devem também cumprir os requisitos do anexo I (parte IS.D.OR.230 «Sistema de comunicação externa de informações sobre segurança da informação») do presente regulamento, uma vez que o Regulamento (UE) 2015/1998 não contém quaisquer disposições relativas à comunicação externa de incidentes de segurança da informação.

(13) Os Regulamentos (UE) n.º 748/2012 ([4]) e (UE) n.º 139/2014 da Comissão ([5]) devem ser alterados a fim de estabelecer um elo entre os sistemas de gestão previstos nos regulamentos acima enumerados e os requisitos de gestão da segurança da informação previstos no presente regulamento.

(14) A fim de proporcionar às entidades tempo suficiente para assegurarem o cumprimento das novas regras e dos procedimentos introduzidos pelo presente regulamento, este deve ser aplicável 3 anos após a sua data de entrada em vigor.

(15) Os requisitos estabelecidos no presente regulamento baseiam-se no Parecer n.º 03/2021 ([6]), emitido pela Agência em conformidade com o artigo 75.º, n.º 2, alíneas b) e c), e com o artigo 76.º, n.º 1, do Regulamento (UE) 2018/1139.

(16) Em conformidade com o artigo 128.º, n.º 4, do Regulamento (UE) 2018/1139, a Comissão consultou os peritos designados por cada Estado-Membro, de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([7]).

ADOTA O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto

O presente regulamento estabelece os requisitos a cumprir pelas entidades a que se refere o artigo 2.º a fim de identificar e gerir os riscos de segurança da informação com potencial impacto na segurança da aviação que possam afetar os sistemas de tecnologias da informação e comunicação e os dados utilizados para fins da aviação civil, de detetar incidentes de segurança da informação e de identificar os que são considerados incidentes de segurança da informação com potencial impacto na segurança da aviação, além de dar resposta a esses incidentes de segurança da aviação e de recuperar dos mesmos.

([2]) Regulamento de Execução (UE) 2015/1998 da Comissão, de 5 de novembro de 2015, que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação (JO L 299 de 14.11.2015, p. 1).

([3]) Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

([4]) Regulamento (UE) n.º 748/2012 da Comissão, de 3 de agosto de 2012, que estabelece as normas de execução relativas à aeronavegabilidade e à certificação ambiental das aeronaves e dos produtos, peças e equipamentos conexos, bem como à certificação das entidades de projeto e produção (JO L 224 de 21.8.2012, p. 1).

([5]) Regulamento (UE) n.º 139/2014 da Comissão, de 12 de fevereiro de 2014, que estabelece requisitos e procedimentos administrativos relativos aos aeródromos em conformidade com o Regulamento (CE) n.º 216/2008 do Parlamento Europeu e do Conselho (JO L 44 de 14.2.2014, p. 1).

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

([7]) JO L 123 de 12.5.2016, p. 1.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento é aplicável:

a) às entidades de produção e às entidades de projeto abrangidas pelo anexo I (parte 21), secção A, subpartes G e J, do Regulamento (UE) n.º 748/2012, exceto às entidades de projeto e produção que participam exclusivamente no projeto e/ou na produção de aeronaves ELA2, na aceção do artigo 1.º, n.º 2, alínea j), do Regulamento (UE) n.º 748/2012;

b) aos operadores de aeródromos e prestadores de serviços de gestão da placa de estacionamento sujeitos ao anexo III «Parte Requisitos aplicáveis às organizações (parte ADR.OR)» do Regulamento (UE) n.º 139/2014.

2. 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;

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», qualquer evento que tenha um efeito adverso na segurança das redes e dos sistemas informáticos, tal como definido no artigo 4.º, n.º 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 de 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 decorrentes de outra legislação da União

1. Sempre que uma entidade referida no artigo 2.º cumpra requisitos de segurança estabelecidos no 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.

2. Se uma entidade referida no artigo 2.º 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 ([8]), 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 aos requisitos incluídos no ponto IS.D.OR.230 do anexo do presente regulamento, que devem ser cumpridos.

([8]) 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).

3. A Comissão, após consulta da AESA 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 5.º

Autoridade competente

1. A autoridade responsável pela certificação e supervisão do cumprimento do presente regulamento é:

a) no que respeita às entidades referidas no artigo 2.º, alínea a), a autoridade competente designada em conformidade com o anexo I (parte 21) do Regulamento (UE) n.º 748/2012;

b) no que respeita às entidades referidas no artigo 2.º, alínea b), a autoridade competente designada em conformidade com o anexo III (parte ADR.OR) do Regulamento (UE) n.º 139/2014.

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.

Artigo 6.º

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

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.A.139 é inserido o seguinte título:

      «**21.A.139A Sistema de gestão da segurança das informações**»;

   b) a seguir ao título 21.A.239 é inserido o seguinte título:

      «**21.A.239A Sistema de gestão da segurança das informações**»;

2) a seguir ao ponto 21.A.139A é inserido o seguinte ponto 21.A.139:

   «**21.A.139A Sistema de gestão da segurança das informações**

   Para além do sistema de gestão da produção exigido pelo ponto 21.A.139, a entidade de produção deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento Delegado (UE) 2022/1645 da Comissão (*) a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.

   (*) 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) A seguir ao ponto 21.A.239A é inserido o seguinte ponto 21.A.239:

   «**21.A.239A Sistema de gestão da segurança das informações**

   Para além do sistema de gestão do projeto exigido pelo ponto 21.A.239, a entidade de projeto deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento Delegado (UE) 2022/1645 a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»

Artigo 7.º

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

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

1) A seguir ao ponto ADR.OR.D.005A é inserido o seguinte ponto ADR.OR.D.005:

«**ADR.OR.D.005A Sistema de gestão da segurança das informações**

O operador do aeródromo deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento Delegado (UE) 2022/1645 da Comissão (*) a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.

(*) 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)»;

2) O ponto ADR.OR.D.007 passa a ter a seguinte redação:

«**ADR.OR.D.007 Gestão de dados aeronáuticos e de informações aeronáuticas**

a) Como parte do seu sistema de gestão, o operador do aeródromo deve aplicar e manter um sistema de gestão da qualidade que abranja as atividades seguintes;

1) as suas atividades relacionadas com o fornecimento de dados aeronáuticos;

2) as suas atividades relacionadas com o fornecimento de informações aeronáuticas.

b) Como parte do seu sistema de gestão, o operador do aeródromo deve definir um sistema de gestão da segurança para garantir a segurança dos dados operacionais que recebe, produz ou utiliza, de forma a que o acesso a esses dados operacionais seja restrito exclusivamente às pessoas autorizadas.

c) O sistema de gestão da segurança deve definir os seguintes elementos:

1) os procedimentos relacionados com a avaliação e a atenuação dos riscos para a segurança dos dados, a monitorização e a melhoria da segurança, as revisões da segurança e a difusão de ensinamentos;

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

3) os meios para circunscrever os efeitos de falhas na segurança e identificar ações de recuperação e procedimentos de atenuação dos riscos a fim de prevenir a repetição da ocorrência.

d) O operador de aeródromo deve assegurar a credenciação de segurança do seu pessoal no que respeita à segurança dos dados aeronáuticos.

e) Os aspetos relacionados com a segurança da informação devem ser geridos em conformidade com o ponto ADR.OR.D.005A.»;

3) A seguir ao ponto ADR.OR.F.045A é inserido o seguinte ponto ADR.OR.F.045:

«**ADR.OR.F.045A Sistema de gestão da segurança das informações**

A entidade responsável pela prestação de AMS deve estabelecer, implementar e manter um sistema de gestão da segurança da informação em conformidade com o Regulamento Delegado (UE) 2022/1645 a fim de assegurar a gestão adequada dos riscos para a segurança da informação que possam ter impacto na segurança da aviação.»

Artigo 8.º

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

O presente regulamento é aplicável a partir de 16 de outubro de 2025.

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

Feito em Bruxelas, em 14 de julho de 2022.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

SEGURANÇA DA INFORMAÇÃO — REQUISITOS APLICÁVEIS ÀS ENTIDADES

[PARTE IS.D.OR]

IS.D.OR.100 Âmbito de aplicação

IS.D.OR.200 Sistema de gestão da segurança da informação

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

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

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

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

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

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

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

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

IS.D.OR.245 Conservação de registos

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

IS.D.OR.255 Alterações do sistema de gestão da segurança da informação

IS.D.OR.260 Melhoria contínua

IS.D.OR.100 Âmbito de aplicação

A presente parte estabelece os requisitos a cumprir pelas entidades referidas no artigo 2.º do presente regulamento.

IS.D.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 o ponto IS.D.OR.205;

   3) define e aplica medidas de tratamento dos riscos de segurança da informação em conformidade com o ponto IS.D.OR.210;

   4) aplica um sistema de comunicação interna de informações em matéria de segurança da informação, em conformidade com o ponto IS.D.OR.215;

   5) define e aplica, em conformidade com o ponto IS.D.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.D.OR.205, alínea e), dá resposta a esses incidentes de segurança da informação e recupera desses incidentes;

   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 o ponto IS.D.OR.225, para dar resposta às constatações notificadas pela autoridade competente;

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

   9) cumpre os requisitos constantes do ponto IS.D.OR.235 ao subcontratar qualquer parte das atividades referidas no ponto IS.D.OR.200 a outras entidades;

10) cumpre os requisitos em matéria de pessoal estabelecidos no ponto IS.D.OR.240;

11) cumpre os requisitos de conservação de registos estabelecidos no ponto IS.D.OR.245;

12) controla a conformidade da entidade com os requisitos do presente regulamento e fornece informações sobre as conclusões ao administrador responsável ou, no caso das entidades de projeto, ao chefe da entidade de projeto, 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 entidade possa ter recebido de outras entidades, de acordo com o seu nível de sensibilidade.

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

c) A entidade deve documentar, em conformidade com o ponto IS.D.OR.250, todos os principais processos, procedimentos, funções e responsabilidades necessários para cumprir o disposto no ponto IS.D.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 o ponto IS.D.OR.255.

d) Os processos, procedimentos, funções e responsabilidades estabelecidos pela entidade para cumprir o disposto no ponto IS.D.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 entidade.

e) Sem prejuízo da obrigação de cumprir os requisitos de comunicação de informações previstos no Regulamento (UE) n.º 376/2014 do Parlamento Europeu e do Conselho ([1]) e os requisitos do ponto IS.D.OR.200 (a) (13), a autoridade competente pode autorizar a entidade a não aplicar os requisitos referidos nas alíneas a) a d), bem como os requisitos conexos constantes dos pontos IS.D.OR.205 a IS.D.OR.260, se demonstrar, a contento dessa autoridade, que as suas atividades, instalações e recursos, bem como os serviços que explora, 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 entidades. A certificação deve basear-se numa avaliação documentada dos riscos de segurança da informação realizada pela entidade ou por terceiros em conformidade com a secção IS.D.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 entidade.

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

a) A entidade deve identificar todos os seus elementos que possam estar expostos a riscos de segurança da informação. Tal inclui:

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

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

b) A entidade deve identificar as interfaces que tem com outras entidades 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 entidade deve identificar os riscos para a segurança da informação que possam ter um impacto potencial na segurança da aviação. Para cada risco identificado, a entidade deve:

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

([1]) Regulamento (UE) n.º 376/2014 do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativo à comunicação, à análise e ao seguimento de ocorrências na aviação civil, que altera o Regulamento (UE) n.º 996/2010 do Parlamento Europeu e do Conselho e revoga a Diretiva 2003/42/CE do Parlamento Europeu e do Conselho, e os Regulamentos (CE) n.º 1321/2007 e (CE) n.º 1330/2007 da Comissão (JO L 122 de 24.4.2014, p. 18).

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 entidade dispõe de um processo estruturado e repetível de gestão dos riscos para as operações, a entidade deve ser capaz de determinar se o risco é aceitável ou se deve ser tratado em conformidade com o ponto IS.D.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 entidades referidas na alínea b).

d) A entidade 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 entidade e outras entidades ou nos riscos comunicados pelas outras entidades;

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.D.OR.210 Tratamento dos riscos para a segurança da informação

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

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.D.OR.240, alíneas a) e b), e outro pessoal afetado da entidade devem ser informados do resultado da avaliação dos riscos efetuada em conformidade com o ponto IS.D.OR.205, dos cenários de ameaça correspondentes e das medidas a aplicar.

A entidade deve também informar as entidade com as quais tenha uma interface, em conformidade com o ponto IS.D.OR.205, alínea b), de quaisquer riscos que se coloquem a ambas as entidades.

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

a) A entidade 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 do ponto IS.D.OR.230.

b) Esse regime e o processo referido o ponto IS.D.OR.220 devem permitir à entidade:

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 os pontos IS.D.OR.205 e IS.D.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 entidade contratada que possa expor a entidade a riscos de segurança da informação com um impacto potencial na segurança da aviação deve comunicar as ocorrências de segurança da informação à entidade. Esses relatórios são apresentados de acordo com os procedimentos estabelecidos nas disposições contratuais específicas e avaliados em conformidade com a alínea b).

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

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

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

a) Com base no resultado da avaliação dos riscos efetuada em conformidade com o ponto IS.D.OR.205 e no resultado do tratamento dos riscos realizado em conformidade com o ponto IS.D.OR.210, a entidade 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 entidade:

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 entidade 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 entidade:

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 no ponto IS.D.OR.205, alínea a).

c) A entidade 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 entidade:

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

2) atingir um estado seguro dos elementos afetados definidos no ponto IS.D.OR.205, alínea a), num prazo de recuperação previamente definido pela entidade.

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

a) Após receção da notificação de constatações apresentada pela autoridade competente, a entidade 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.D.OR.230 Sistema de comunicação externa sobre segurança da informação

a) A entidade 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 entidade.

b) Sem prejuízo das obrigações previstas no Regulamento (UE) n.º 376/2014, a entidade 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 entidade deve também comunicá-lo ao titular da certificação de projeto;

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

c) A entidade 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 entidade responsável pelo projeto do sistema ou componente, logo que a entidade 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 entidade responsável pelo projeto do sistema ou do componente, o mais rapidamente possível, mas no máximo 72 horas a contar do momento em que a entidade 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 entidade 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 entidade responsável pelo projeto do sistema ou componente, com informações pormenorizadas sobre as medidas que a entidade 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.D.OR.235 Adjudicação de atividades de gestão da segurança da informação

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

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

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

a) O administrador responsável da entidade ou, no caso das entidades de projeto, o chefe da entidade de projeto, designado em conformidade com o Regulamento (UE) n.º 748/2012 e o Regulamento (UE) n.º 139/2014, tal como referido no artigo 2.º, n.º 1, alíneas a) e b), do presente regulamento, tem os poderes necessários para assegurar que todas as atividades exigidas pelo presente regulamento possam ser financiadas e realizadas. Deve:

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 no ponto IS.D.OR.200 (a) (1);

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

b) O administrador responsável ou, no caso das entidades de projeto, o chefe da entidade de projeto, nomeia uma pessoa ou um grupo de pessoas para assegurar que a entidade cumpre os requisitos do presente regulamento e define as funções dessa(s) pessoa(s). Essa pessoa ou esse grupo de pessoas responde diretamente perante o administrador responsável ou, no caso das entidades de projeto, o chefe da entidade de projeto, e deve dispor dos conhecimentos, das competências e da experiência adequados para o desempenho das 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 ou, no caso das entidades de projeto, o chefe da entidade de projeto nomeará uma pessoa ou um grupo de pessoas com a responsabilidade de gerir a função de controlo da conformidade a que se refere o ponto IS.D.OR.200, alínea a) 12).

d) Se a entidade partilhar estruturas, políticas, processos e procedimentos organizacionais de segurança da informação com outras entidades ou com áreas da sua própria organização que não façam parte da certificação ou declaração, o administrador responsável ou, no caso das entidades de projeto, o chefe da entidade de projeto, poderá delegar as suas atividades numa pessoa responsável comum.

Nesse caso, devem ser estabelecidas medidas de coordenação entre o administrador responsável da entidade ou, no caso das entidades de projeto, o chefe da entidade de projeto e a pessoa responsável comum, a fim de assegurar a integração adequada da gestão da segurança da informação na entidade.

e) O administrador responsável ou o chefe da entidade de projeto, 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 do ponto IS.D.OR.200.

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

i) A entidade 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.D.OR.245 Conservação de registos

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

1) a entidade 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 o ponto IS.D.OR.200, alínea e);

ii) contratos para as atividades referidas no ponto IS.D.OR.200 a) 9);

iii) registos dos principais processos referidos no ponto IS.D.OR.200, alínea d);

iv) registos dos riscos identificados na avaliação dos riscos referida no ponto IS.D.OR.205, juntamente com as medidas associadas de tratamento dos riscos referidas no ponto IS.D.OR.210;

v) registos dos incidentes e vulnerabilidades de segurança da informação comunicados em conformidade com os sistemas de comunicação a que se referem os pontos IS.D.OR.215 e IS.D.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 cinco anos após a aprovação ter perdido a sua validade.

3) Os registos referidos no ponto 1, subalínea ii), devem ser conservados pelo menos até cinco 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 cinco 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 entidade.

b) A entidade 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 entidade e durante, pelo menos, três anos após a pessoa ter deixado a entidade.

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

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

d) Os registos devem ser conservados de modo a garantir a sua proteção contra danos, alterações e furto, sendo a informação identificada, quando exigido, de acordo com o nível de classificação de segurança. A entidade deve assegurar que os registos são conservados através de meios que garantam a integridade, a autenticidade e o acesso autorizado.

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

a) A entidade 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 ou, no caso das entidades de projeto, pelo chefe da entidade de projeto, confirmando que a entidade trabalhará sempre em conformidade com o presente anexo e com o MGSI. Se o administrador responsável ou, no caso das entidades de projeto, o chefe da entidade de projeto, não for o diretor executivo da entidade, esse diretor executivo 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 o ponto IS.D.OR.240, alíneas b) e c);

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

4) a política de segurança da informação da entidade a que se refere o ponto IS.D.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 pelo ponto IS.D.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 do ponto IS.D.OR.200, incluindo a pessoa ou pessoas responsáveis pela função de controlo da conformidade a que se refere o ponto IS.D.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 o ponto IS.D.OR.215;

9) os procedimentos que especificam a forma como a entidade garante o cumprimento da presente parte e, em especial:

i) o ponto IS.D.OR.200, alínea c), relativo à documentação,

ii) os procedimentos que definem a forma como a entidade controla quaisquer atividades contratadas referidas no ponto IS.D.OR.200, alínea a), ponto 9,

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

10) a lista de meios de conformidade alternativos aprovados.

b) A versão original do MGSI deve ser aprovada e uma cópia deve ser conservada pela autoridade competente. O MGSI deve ser alterado na medida do necessário para manter uma descrição atualizada do SGSI da entidade. 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 entidade. As alterações não incluídas no âmbito deste procedimento e as alterações relacionadas com as alterações a que se refere o ponto IS.D.OR.255, alínea b), devem ser aprovadas pela autoridade competente.

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

IS.D.OR.255 Alterações do sistema de gestão da segurança da informação

a) As alterações ao MGSI podem ser geridas e notificadas à autoridade competente mediante um procedimento desenvolvido pela entidade. O procedimento a que se refere a alínea b) deve ser aprovado pela autoridade competente.

b) No que diz respeito às alterações ao MGSI não abrangidas pelo procedimento referido na alínea a), a entidade deve solicitar e obter uma aprovação emitida pela autoridade competente.

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 entidade e os respetivos termos de certificação anexos a este;

2) a entidade 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;

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

IS.D.OR.260 Melhoria contínua

a) A entidade deve avaliar, utilizando indicadores de desempenho adequados, a eficácia e a maturidade do MGSI. Essa avaliação deve ser efetuada numa base de calendário predefinida pela entidade 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 entidade deve tomar as medidas de melhoria necessárias para assegurar que o MGSI continua a cumprir os requisitos aplicáveis e permite manter os riscos de segurança da informação a um nível aceitável. Além disso, a entidade deve reavaliar os elementos do MGSI afetados pelas medidas adotadas.