

Jornal Oficial

da União Europeia

L 72



Edição em língua
portuguesa

Legislação

58.º ano

17 de março de 2015

Índice

II Atos não legislativos

REGULAMENTOS

Regulamento de Execução (UE) 2015/434 da Comissão, de 16 de março de 2015, que estabelece os valores forfetários de importação para a determinação do preço de entrada de certos frutos e produtos hortícolas	1
---	---

DECISÕES

★ Decisão (UE) 2015/435 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2014, relativa à mobilização da Margem para Imprevistos	4
★ Decisão (UE) 2015/436 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2014, relativa à mobilização do Fundo de Solidariedade da União Europeia	6
★ Decisão (UE) 2015/437 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2014, relativa à mobilização do Fundo de Solidariedade da União Europeia	7
★ Decisão (UE) 2015/438 do Conselho, de 2 de março de 2015, que determina a posição a tomar em nome da União Europeia no Comité Misto criado pelo Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos, relativa à adoção de diretrizes comuns para a aplicação do Acordo	8
★ Decisão (PESC) 2015/439 do Conselho, de 16 de março de 2015, que prorroga o mandato do Representante Especial da União Europeia para o Sael	27
★ Decisão (PESC) 2015/440 do Conselho, de 16 de março de 2015, que prorroga o mandato do Representante Especial da União Europeia para o Corno de África	32
★ Decisão (PESC) 2015/441 do Conselho, de 16 de março de 2015, que altera e prorroga a Decisão 2010/96/PESC, relativa a uma missão militar da União Europeia que tem em vista contribuir para a formação das Forças de Segurança da Somália	37

PT

Os atos cujos títulos são impressos em tipo fino são atos de gestão corrente adotados no âmbito da política agrícola e que têm, em geral, um período de validade limitado.

Os atos cujos títulos são impressos em tipo negro e precedidos de um asterisco são todos os restantes.

★ Decisão (PESC) 2015/442 do Conselho, de 16 de março de 2015, que lança a Missão de Aconselhamento Militar PCSD da União Europeia na República Centro-Africana (EUMAM RCA) e que altera a Decisão (PESC) 2015/78	39
★ Decisão (UE, Euratom) 2015/443 da Comissão, de 13 de março de 2015, relativa à segurança na Comissão	41
★ Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE	53

II

(Atos não legislativos)

REGULAMENTOS

REGULAMENTO DE EXECUÇÃO (UE) 2015/434 DA COMISSÃO

de 16 de março de 2015

que estabelece os valores forfetários de importação para a determinação do preço de entrada de certos frutos e produtos hortícolas

A COMISSÃO EUROPEIA,

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

Tendo em conta o Regulamento (UE) n.º 1308/2013 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, que estabelece uma organização comum dos mercados dos produtos agrícolas e que revoga os Regulamentos (CEE) n.º 922/72, (CEE) n.º 234/79, (CE) n.º 1037/2001, (CE) n.º 1234/2007 do Conselho ⁽¹⁾,

Tendo em conta o Regulamento de Execução (UE) n.º 543/2011 da Comissão, de 7 de junho de 2011, que estabelece regras de execução do Regulamento (CE) n.º 1234/2007 do Conselho nos sectores das frutas e produtos hortícolas e das frutas e produtos hortícolas transformados ⁽²⁾, nomeadamente o artigo 136.º, n.º 1,

Considerando o seguinte:

- (1) O Regulamento de Execução (UE) n.º 543/2011 estabelece, em aplicação dos resultados das negociações comerciais multilaterais do «Uruguay Round», os critérios para a fixação pela Comissão dos valores forfetários de importação dos países terceiros relativamente aos produtos e aos períodos indicados no Anexo XVI, parte A.
- (2) O valor forfetário de importação é calculado, todos os dias úteis, em conformidade com o artigo 136.º, n.º 1, do Regulamento de Execução (UE) n.º 543/2011, tendo em conta os dados diários variáveis. O presente regulamento deve, por conseguinte, entrar em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Os valores forfetários de importação referidos no artigo 136.º do Regulamento de Execução (UE) n.º 543/2011 são fixados no anexo do presente regulamento.

⁽¹⁾ JO L 347 de 20.12.2013, p. 671.

⁽²⁾ JO L 157 de 15.6.2011, p. 1.

Artigo 2.º

O presente regulamento entra em vigor na data da sua publicação no *Jornal Oficial da União Europeia*.

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

Feito em Bruxelas, em 16 de março de 2015.

Pela Comissão

Em nome do Presidente,

Jerzy PLEWA

Diretor-Geral da Agricultura e do Desenvolvimento Rural

ANEXO

Valores forfetários de importação para a determinação do preço de entrada de certos frutos e produtos hortícolas

(EUR/100 kg)		
Código NC	Código países terceiros ⁽¹⁾	Valor forfetário de importação
0702 00 00	EG	65,8
	MA	84,9
	TR	86,4
	ZZ	79,0
0707 00 05	JO	229,9
	MA	183,9
	TR	185,1
	ZZ	199,6
0709 93 10	MA	119,5
	TR	192,4
	ZZ	156,0
0805 10 20	EG	45,8
	IL	72,7
	MA	56,7
	TN	57,3
	TR	63,6
	ZZ	59,2
	ZZ	59,2
0805 50 10	TR	61,4
	ZZ	61,4
0808 10 80	BR	70,9
	CA	81,0
	CL	100,9
	CN	91,1
	MK	25,2
	US	166,1
	ZZ	89,2
	ZZ	89,2
0808 30 90	AR	112,0
	CL	133,2
	US	124,8
	ZA	103,5
	ZZ	118,4

⁽¹⁾ Nomenclatura dos países fixada pelo Regulamento (UE) n.º 1106/2012 da Comissão, de 27 de novembro de 2012, que executa o Regulamento (CE) n.º 471/2009 do Parlamento Europeu e do Conselho relativo às estatísticas comunitárias do comércio externo com países terceiros, no que respeita à atualização da nomenclatura dos países e territórios (JO L 328 de 28.11.2012, p. 7). O código «ZZ» representa «outras origens».

DECISÕES

DECISÃO (UE) 2015/435 DO PARLAMENTO EUROPEU E DO CONSELHO

de 17 de dezembro de 2014

relativa à mobilização da Margem para Imprevistos

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta o Acordo Interinstitucional de 2 de dezembro de 2013 entre o Parlamento Europeu, o Conselho e a Comissão sobre a disciplina orçamental, a cooperação em matéria orçamental e a boa gestão financeira ⁽¹⁾, nomeadamente o ponto 14,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

- (1) O artigo 13.º do Regulamento (UE, Euratom) n.º 1311/2013 do Conselho ⁽²⁾ definiu uma Margem para Imprevistos que pode ir até 0,03 % do rendimento nacional bruto da União.
- (2) Nos termos do artigo 6.º do referido regulamento, a Comissão calculou o montante absoluto da Margem para Imprevistos para 2014 ⁽³⁾.
- (3) Depois de ter examinado todas as outras possibilidades financeiras para reagir a circunstâncias imprevistas que surgiram depois de o limite máximo de pagamentos do quadro financeiro plurianual para 2014 ter sido estabelecido pela primeira vez em fevereiro de 2013, afigura-se necessário mobilizar a Margem para Imprevistos para complementar as dotações de pagamento do orçamento geral da União Europeia para o exercício de 2014, acima do limite máximo de pagamentos.
- (4) Deverá ser incluído na mobilização da Margem para Imprevistos um montante de 350 milhões de EUR de dotações de pagamento, enquanto se aguarda um acordo sobre pagamentos relativo a outros instrumentos especiais.
- (5) Tendo em conta a situação muito particular que se verifica este ano, a condição de instrumento de último recurso referida no artigo 13.º, n.º 1, do Regulamento (UE, Euratom) n.º 1311/2013 está preenchida.
- (6) Em cumprimento do artigo 13.º, n.º 3, do Regulamento (UE, Euratom) n.º 1311/2013, a Comissão deverá apresentar uma proposta sobre a dedução do montante em causa dos limites máximos de pagamentos do QFP para um ou mais exercícios futuros, tendo devidamente em conta o acordo sobre pagamentos relativo a outros instrumentos especiais, e sem prejuízo das prerrogativas institucionais da Comissão,

⁽¹⁾ JO C 373 de 20.12.2013, p. 1.

⁽²⁾ Regulamento (UE, Euratom) n.º 1311/2013 do Conselho, de 2 de dezembro de 2013, que estabelece o quadro financeiro plurianual para o período 2014-2020 (JO L 347 de 20.12.2013, p. 884).

⁽³⁾ Comunicação da Comissão ao Conselho e ao Parlamento Europeu, de 20 de dezembro de 2013, relativa ao ajustamento técnico do quadro financeiro para 2014 em conformidade com a evolução do RNB [COM(2013) 928].

ADOTARAM A PRESENTE DECISÃO:

Artigo 1.º

Relativamente ao orçamento geral da União Europeia para o exercício de 2014, a Margem para Imprevistos deve ser utilizada para disponibilizar o montante de 3 168 233 715 EUR em dotações de pagamento para além do limite máximo de pagamentos do quadro financeiro plurianual.

Artigo 2.º

O montante de 2 818 233 715 EUR será deduzido em três frações das margens abaixo dos limites máximos de pagamento para os seguintes exercícios:

- a) 2018: 939 411 200 EUR
- b) 2019: 939 411 200 EUR
- c) 2020: 939 411 315 EUR

A Comissão é convidada a apresentar oportunamente uma proposta sobre o montante remanescente de 350 milhões de EUR.

Artigo 3.º

A presente decisão é publicada no *Jornal Oficial da União Europeia*.

Feito em Estrasburgo, em 17 de dezembro de 2014.

Pelo Parlamento Europeu

O Presidente

M. SCHULZ

Pelo Conselho

O Presidente

B. DELLA VEDOVA

DECISÃO (UE) 2015/436 DO PARLAMENTO EUROPEU E DO CONSELHO
de 17 de dezembro de 2014
relativa à mobilização do Fundo de Solidariedade da União Europeia

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta o Regulamento (CE) n.º 2012/2002 do Conselho, de 11 de novembro de 2002, que estabelece o Fundo de Solidariedade da União Europeia ⁽¹⁾, nomeadamente o artigo 4.º, n.º 3,

Tendo em conta o Acordo Interinstitucional, de 2 de dezembro de 2013, entre o Parlamento Europeu, o Conselho e a Comissão sobre a disciplina orçamental, a cooperação em matéria orçamental e a boa gestão financeira ⁽²⁾, nomeadamente o ponto 11,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

- (1) A União Europeia criou o Fundo de Solidariedade da União Europeia (a seguir designado «Fundo») para manifestar a sua solidariedade para com a população das regiões afetadas por catástrofes.
- (2) O artigo 10.º do Regulamento (UE, Euratom) n.º 1311/2013 ⁽³⁾ permite a mobilização do Fundo dentro de um limite máximo anual de 500 milhões de euros (a preços de 2011).
- (3) O Regulamento (CE) n.º 2012/2002 estabelece as disposições que permitem a mobilização do Fundo.
- (4) A Itália apresentou um pedido de mobilização do Fundo, na sequência de inundações.
- (5) A Grécia apresentou um pedido de mobilização do Fundo, na sequência de um terremoto.
- (6) A Eslovénia apresentou um pedido de mobilização do Fundo, na sequência de tempestades de gelo.
- (7) A Croácia apresentou um pedido de mobilização do Fundo, na sequência de tempestades de gelo seguidas de inundações,

ADOTARAM A PRESENTE DECISÃO:

Artigo 1.º

No quadro do orçamento geral da União Europeia para o exercício de 2014, é mobilizada a quantia de 46 998 528 euros em dotações de autorização, a título do Fundo de Solidariedade da União Europeia.

No quadro do orçamento geral da União Europeia para o exercício de 2015, é mobilizada a quantia de 46 998 528 euros em dotações de pagamento, a título do Fundo de Solidariedade da União Europeia.

Artigo 2.º

A presente decisão é publicada no *Jornal Oficial da União Europeia*.

Feito em Estrasburgo, em 17 de dezembro de 2014.

Pelo Parlamento Europeu

O Presidente

M. SCHULZ

Pelo Conselho

O Presidente

B. DELLA VEDOVA

⁽¹⁾ JO L 311 de 14.11.2002, p. 3.

⁽²⁾ JO C 373 de 20.12.2013, p. 1.

⁽³⁾ Regulamento (UE, Euratom) n.º 1311/2013 do Conselho, de 2 de dezembro de 2013, que estabelece o quadro financeiro plurianual para o período 2014-2020 (JO L 347 de 20.12.2013, p. 884).

DECISÃO (UE) 2015/437 DO PARLAMENTO EUROPEU E DO CONSELHO
de 17 de dezembro de 2014
relativa à mobilização do Fundo de Solidariedade da União Europeia

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta o Regulamento do Conselho (CE) n.º 2012/2002, de 11 de novembro de 2002, que institui o Fundo de Solidariedade da União Europeia ⁽¹⁾, nomeadamente o artigo 4.º, n.º 3,

Tendo em conta o Acordo Interinstitucional, de 2 de dezembro de 2013, entre o Parlamento Europeu, o Conselho e a Comissão sobre a disciplina orçamental, a cooperação em matéria orçamental e a boa gestão financeira ⁽²⁾, nomeadamente o ponto 11,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

- (1) A União Europeia criou o Fundo de Solidariedade da União Europeia («Fundo») para manifestar a sua solidariedade com a população das regiões afetadas por catástrofes.
- (2) O artigo 10.º do Regulamento (UE, Euratom) n.º 1311/2013 ⁽³⁾ permite a mobilização do Fundo dentro de um limite máximo anual de 500 milhões de euros (a preços de 2011).
- (3) O Regulamento (CE) n.º 2012/2002 estabelece as disposições que permitem a mobilização do Fundo.
- (4) A Sérvia apresentou um pedido de mobilização do Fundo, na sequência de inundações.
- (5) A Croácia apresentou um pedido de mobilização do Fundo, na sequência de inundações.
- (6) A Bulgária apresentou um pedido de mobilização do Fundo, na sequência de inundações,

ADOTARAM A PRESENTE DECISÃO:

Artigo 1.º

No quadro do orçamento geral da União Europeia para o exercício de 2014, é mobilizada a quantia de 79 726 440 euros em dotações de autorização, a título do Fundo de Solidariedade da União Europeia.

No quadro do orçamento geral da União Europeia para o exercício de 2015, é mobilizada a quantia de 79 726 440 euros em dotações de pagamento, a título do Fundo de Solidariedade da União Europeia.

Artigo 2.º

A presente decisão é publicada no *Jornal Oficial da União Europeia*.

Feito em Estrasburgo, em 17 de dezembro de 2014.

Pelo Parlamento Europeu
O Presidente
M. SCHULZ

Pelo Conselho
O Presidente
B. DELLA VEDOVA

⁽¹⁾ JO L 311 de 14.11.2002, p. 3.

⁽²⁾ JO C 373 de 20.12.2013, p. 1.

⁽³⁾ Regulamento (UE, Euratom) n.º 1311/2013 do Conselho, de 2 de dezembro de 2013, que estabelece o quadro financeiro plurianual para o período 2014-2020 (JO L 347 de 20.12.2013, p. 884).

DECISÃO (UE) 2015/438 DO CONSELHO**de 2 de março de 2015****que determina a posição a tomar em nome da União Europeia no Comité Misto criado pelo Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos, relativa à adoção de diretrizes comuns para a aplicação do Acordo**

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 77.º, n.º 2, alínea a), em conjugação com o artigo 218.º, n.º 9,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

- (1) O artigo 12.º do Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos ⁽¹⁾ («Acordo») criou um Comité Misto. O Comité Misto tem por missão, nomeadamente, acompanhar a aplicação do Acordo.
- (2) O Acordo entre a União Europeia e a Ucrânia que altera o Acordo entre a Comunidade Europeia e a Ucrânia sobre a facilitação da emissão de vistos ⁽²⁾ («Acordo modificativo») entrou em vigor em 1 de julho de 2013.
- (3) O Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho ⁽³⁾ estabeleceu os procedimentos e as condições para a emissão de vistos de trânsito ou de estada prevista no território dos Estados-Membros não superior a 90 dias em cada período de 180 dias.
- (4) Tendo em conta a sua responsabilidade, o Comité Misto fez notar a necessidade de diretrizes comuns, a fim de assegurar uma aplicação harmonizada do Acordo pelos consulados dos Estados-Membros e clarificar a relação entre as disposições do Acordo e as disposições das Partes Contratantes que continuam a ser aplicáveis às matérias relativas a vistos não abrangidas pelo Acordo.
- (5) O Comité Misto adotou as referidas diretrizes, em 25 de novembro de 2009, através da sua Decisão n.º 1/2009. Estas diretrizes deverão ser adaptadas às novas disposições do Acordo introduzidas pelo Acordo modificativo e à evolução do direito interno da União em matéria de política de vistos. No interesse da clareza, é conveniente substituir as referidas diretrizes.
- (6) É conveniente definir a posição a adotar em nome da União no âmbito do Comité Misto relativa à adoção das diretrizes comuns para a aplicação do Acordo,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

A posição a adotar em nome da União no Comité Misto criado pelo artigo 12.º do Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos quanto à adoção de diretrizes comuns para a aplicação do Acordo tem por base o projeto de decisão do Comité Misto que acompanha a presente decisão.

⁽¹⁾ JO L 332 de 18.12.2007, p. 68.

⁽²⁾ JO L 168 de 20.6.2013, p. 11.

⁽³⁾ Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece o Código Comunitário de Vistos (JO L 243 de 15.9.2009, p. 1).

Artigo 2.º

A presente decisão entra em vigor na data da sua adoção.

Feito em Bruxelas, em 2 de março de 2015.

Pelo Conselho
A Presidente
D. REIZNIECE-OZOLA

PROJETO

DECISÃO N.º .../2014 DO COMITÉ MISTO CRIADO PELO ACORDO ENTRE A UNIÃO EUROPEIA E A UCRÂNIA SOBRE A FACILITAÇÃO DA EMISSÃO DE VISTOS**de****relativa à adoção de diretrizes comuns para a aplicação do Acordo**

O COMITÉ MISTO,

Tendo em conta o Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos («Acordo»), nomeadamente o artigo 12.º,

Considerando que o Acordo entrou em vigor em 1 de janeiro de 2008,

DECIDE O SEGUINTE:

Artigo 1.º

As diretrizes comuns para a aplicação do Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos são estabelecidas no anexo da presente decisão.

Artigo 2.º

É revogada a Decisão n.º 1/2009 do Comité Misto.

Artigo 3.º

A presente decisão entra em vigor em na data da sua adoção.

Feito em, em

*Pela União Europeia**Pela Ucrânia*

ANEXO

**DIRETRIZES COMUNS PARA A APLICAÇÃO DO ACORDO ENTRE A UNIÃO EUROPEIA E A UCRÂNIA
SOBRE A FACILITAÇÃO DA EMISSÃO DE VISTOS**

O objetivo do Acordo entre a União Europeia e a Ucrânia sobre a facilitação da emissão de vistos, que entrou em vigor em 1 de janeiro de 2008, com a redação que lhe foi dada pelo Acordo entre a União Europeia e a Ucrânia de 23 de julho de 2012, que entrou em vigor em 1 de julho de 2013 («Acordo»), consiste em facilitar, numa base de reciprocidade, os procedimentos de emissão de vistos para estadas não superiores a 90 dias em cada período de 180 dias para os cidadãos ucranianos.

O Acordo estabelece, numa base de reciprocidade, direitos e obrigações juridicamente vinculativos destinados a simplificar os procedimentos de emissão de vistos para os cidadãos ucranianos.

As presentes diretrizes, adotadas pelo Comité Misto criado pelo artigo 12.º do Acordo («Comité Misto»), têm por objetivo assegurar a aplicação correta e harmonizada das disposições desse Acordo pelas missões diplomáticas e postos consulares dos Estados-Membros. Estas diretrizes não fazem parte do Acordo e, por conseguinte, não são juridicamente vinculativas. No entanto, recomenda-se vivamente que o pessoal diplomático as consulte e respeite sistematicamente na aplicação das disposições do Acordo.

As presentes diretrizes devem ser atualizadas à luz da experiência obtida na aplicação do Acordo sob a responsabilidade do Comité Misto. As diretrizes adotadas pelo Comité Misto em 25 de novembro de 2009 foram adaptadas em conformidade com o Acordo entre a União Europeia e a Ucrânia que altera o Acordo entre a Comunidade Europeia e a Ucrânia sobre a facilitação da emissão de vistos («Acordo modificativo») e com a nova legislação da União, como o Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho ⁽¹⁾ («Código de Vistos»).

I. QUESTÕES GERAIS**1.1. Objetivo e âmbito de aplicação**

O artigo 1.º do Acordo estabelece que: «O objetivo do presente acordo consiste em facilitar a emissão de vistos aos cidadãos da Ucrânia para estadas não superiores a 90 dias em cada período de 180 dias.».

O Acordo aplica-se a todos os cidadãos ucranianos que solicitam um visto de curta duração, independentemente do país em que residem.

O artigo 1.º, n.º 2, do Acordo estabelece que: «A Ucrânia só pode reintroduzir a obrigação de visto para os cidadãos ou determinadas categorias de cidadãos de todos os Estados-Membros e não para os cidadãos ou determinadas categorias de cidadãos de Estados-Membros individuais. Se a Ucrânia reintroduzir a obrigação de visto para os cidadãos da UE ou para determinadas categorias de cidadãos da UE, serão aplicáveis automaticamente a estes as mesmas facilidades concedidas nos termos do presente acordo aos cidadãos ucranianos, com base na reciprocidade.».

De acordo com as decisões tomadas pelo governo ucraniano, a partir de 1 de maio de 2005 ou de 1 de janeiro de 2008, respetivamente, os cidadãos da UE estão isentos da obrigação de visto quando viajam para a Ucrânia por um período não superior a 90 dias ou quando transitam pelo território da Ucrânia. Esta disposição não prejudica o direito de o governo ucraniano alterar tais decisões.

1.2. Âmbito de aplicação do Acordo

O artigo 2.º do Acordo estabelece que:

«1. As medidas de facilitação de vistos previstas no presente acordo são aplicáveis aos cidadãos da Ucrânia apenas na medida em que estes não estejam isentos da obrigação de visto pelas disposições legislativas e regulamentares da Comunidade ou dos seus Estados-Membros, pelo presente acordo ou por outros acordos internacionais.

2. As questões não contempladas pelas disposições do presente acordo, como a recusa de emissão de visto, o reconhecimento dos documentos de viagem, a prova de meios de subsistência suficientes, a recusa de entrada e as medidas de expulsão, são reguladas pelo direito nacional da Ucrânia ou dos Estados-Membros ou pelo direito da União Europeia.».

⁽¹⁾ Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece o Código Comunitário de Vistos (JO L 243 de 15.9.2009, p. 1).

Sem prejuízo do disposto no seu artigo 10.º (que prevê a isenção da obrigação de visto para os titulares de passaportes diplomáticos e passaportes de serviço biométricos da Ucrânia), o Acordo não afeta as normas em vigor em matéria de obrigação e de isenção de visto. Por exemplo, o artigo 4.º do Regulamento (CE) n.º 539/2001 do Conselho ⁽¹⁾ autoriza os Estados-Membros a isentar da obrigação de visto a tripulação civil de aviões e navios, entre outras categorias.

As regras de Schengen e, em certos casos, o direito nacional, continuam a ser aplicáveis a todas as questões não abrangidas pelo Acordo, como a recusa de emissão de visto, o reconhecimento de documentos de viagem, a prova de meios de subsistência suficientes, a recusa de entrada e as medidas de expulsão. O mesmo se aplica às regras de Schengen que determinam o Estado-Membro responsável pelo tratamento de um pedido de visto. Por conseguinte, um cidadão ucraniano deve continuar a solicitar um visto no consulado do Estado-Membro de destino principal das suas deslocações; se não houver um destino principal, deve dirigir-se ao consulado do Estado-Membro da primeira entrada no espaço Schengen.

Mesmo que as condições previstas no Acordo estejam preenchidas, por exemplo, o requerente de visto apresenta os documentos comprovativos da finalidade da viagem para as categorias mencionadas no artigo 4.º, a emissão do visto ainda pode ser recusada caso as condições estabelecidas no artigo 5.º do Regulamento (CE) n.º 562/2006 do Parlamento Europeu e do Conselho ⁽²⁾ («Código das Fronteiras Schengen») não estejam preenchidas, ou seja, se a pessoa não estiver na posse de um documento de viagem válido, se tiver sido emitida uma indicação no SIS, se a pessoa for considerada uma ameaça para a ordem pública ou a segurança interna, etc.

O Código de Vistos continua a prever outras possibilidades de flexibilidade na emissão de vistos. Por exemplo, podem ser emitidos vistos de entradas múltiplas com um longo período de validade — até cinco anos — para categorias de pessoas não mencionadas no artigo 5.º do Acordo, se as condições previstas pelo Código de Vistos forem respeitadas (ver artigo 24.º, n.º 2, do Código de Vistos). Do mesmo modo, continuam a ser aplicáveis as disposições do Código de Vistos que permitem a isenção ou redução dos emolumentos de visto (ver ponto II. 2.1.1).

1.3. Tipos de vistos abrangidos pelo âmbito de aplicação do Acordo

O artigo 3.º, alínea d), do Acordo define «visto» como «uma autorização emitida por um Estado-Membro ou uma decisão tomada por esse Estado necessária para:

- a entrada para uma estada prevista nesse Estado-Membro ou em mais Estados-Membros por um período total não superior a 90 dias,
- a entrada para trânsito no território desse Estado-Membro ou de mais Estados-Membros».

O seguinte tipo de visto é abrangido pelo Acordo:

- Vistos «C» (vistos de curta duração).

As medidas de facilitação previstas no Acordo aplicam-se tanto aos vistos uniformes válidos para a totalidade do território dos Estados-Membros como aos vistos com validade territorial limitada (VTL).

1.4. Cálculo da duração da estada autorizada por um visto e, em especial, a questão de como determinar o período de seis meses

A recente alteração do Código das Fronteiras Schengen redefiniu a noção de curta duração. A atual definição tem a seguinte redação: «90 dias em qualquer período de 180 dias, o que implica ter em conta o período de 180 dias anterior a cada dia de estada.».

O dia de entrada e o dia de saída correspondem, respetivamente, ao primeiro e ao último dia da estada no território dos Estados-Membros. A noção de «qualquer» requer a aplicação de um período de referência «móvel» de 180 dias, analisando retrospectivamente cada dia de estada coberto pelo período de 180 dias, a fim de verificar se a regra de 90 dias em cada período de 180 dias continua a ser respeitada. Isso significa que uma ausência por um período ininterrupto de 90 dias permite uma nova estada até 90 dias.

Esta definição entrou em vigor em 18 de outubro de 2013. A calculadora pode ser consultada em linha no seguinte endereço: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm.

⁽¹⁾ Regulamento (CE) n.º 539/2001 do Conselho, de 15 de março de 2001, que fixa a lista dos países terceiros cujos nacionais estão sujeitos à obrigação de visto para transporem as fronteiras externas e a lista dos países terceiros cujos nacionais estão isentos dessa obrigação (JO L 81 de 21.3.2001, p. 1).

⁽²⁾ Regulamento (CE) n.º 562/2006 do Parlamento Europeu e do Conselho, de 15 de março de 2006, que estabelece o código comunitário relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen) (JO L 105 de 13.4.2006, p. 1).

Exemplo de cálculo da duração da estada com base na nova definição:

Uma pessoa titular de um visto de entradas múltiplas válido por um ano (de 18.4.2014 a 18.4.2015) entra no território dos Estados-Membros pela primeira vez em 19.4.2014 e permanece três dias. Entra novamente em 18.6.2014 e permanece por 86 dias. Qual é a situação dessa pessoa, tendo em conta as datas específicas? Quando é que esta pessoa pode entrar de novo?

Em 11.9.2014: durante os últimos 180 dias (de 16.3.2014 a 11.9.2014) a pessoa permaneceu três dias (de 19 a 21.4.2014) mais 86 dias (de 18.6.2014 a 11.9.2014) = 89 dias = o prazo autorizado não foi excedido. A pessoa pode ainda permanecer mais um dia.

A partir de 16.10.2014: a pessoa poderá entrar para uma estada de três dias suplementares (em 16.10.2014, a estada em 19.4.2014 torna-se irrelevante por ficar fora do período de 180 dias); em 17.10.2014, a estada de 20.4.2014 torna-se irrelevante (fora do período de 180 dias, etc.).

A partir de 15.12.2014: a pessoa poderá entrar para uma estada de 86 dias suplementares (em 15.12.2014, a estada de 18.6.2014 torna-se irrelevante por ficar fora do período de 180 dias); em 16.12.2014, a estada de 19.6.2014 torna-se irrelevante, etc.

1.5. Situação relativa aos Estados-Membros que ainda não aplicam a totalidade do acervo de Schengen, aos Estados-Membros que não participam na política comum de vistos da UE e aos países associados.

Os Estados-Membros que aderiram à União em 2004 (a República Checa, Estónia, Chipre, Letónia, Lituânia, Hungria, Malta, Polónia, Eslovénia e Eslováquia), em 2007 (Bulgária e Roménia) e em 2013 (Croácia) estão vinculados pelo Acordo desde a sua entrada em vigor.

Apenas a Bulgária, a Croácia, Chipre e a Roménia ainda não aplicam a totalidade do acervo de Schengen e continuarão a emitir vistos nacionais com uma validade limitada ao seu próprio território nacional. Esses Estados-Membros continuarão a aplicar o Acordo quando passarem a aplicar integralmente o acervo de Schengen.

O direito nacional continua a ser aplicável a todas as matérias não abrangidas pelo Acordo até à data de aplicação integral do acervo de Schengen pelos Estados-Membros. A partir dessa data, as regras de Schengen/as legislações nacionais aplicam-se às matérias não reguladas pelo Acordo.

A Bulgária, Chipre, a Croácia e a Roménia estão autorizados a reconhecer os títulos de residência, os vistos do tipo D e os vistos de curta duração emitidos pelos Estados Schengen e países associados para estadas de curta duração no seu território.

Em conformidade com o artigo 21.º da Convenção de Aplicação do Acordo de Schengen de 14 de junho de 1985 relativo à supressão gradual dos controlos nas fronteiras comuns, todos os Estados Schengen devem reconhecer os vistos para estadas de longa duração e os títulos de residência emitidos pelos outros Estados-Membros como válidos para estadas de curta duração no respetivo território. Os Estados Schengen aceitam os títulos de residência, os vistos do tipo D e os vistos de curta duração dos países associados para a entrada e permanência de curta duração e vice-versa.

O Acordo não se aplica à Dinamarca, à Irlanda e ao Reino Unido, mas inclui declarações conjuntas sobre a conveniência desses Estados-Membros concluírem acordos bilaterais de facilitação de vistos com a Ucrânia.

Um acordo bilateral sobre a facilitação de vistos entre a Dinamarca e a Ucrânia entrou em vigor em 1 de março de 2009. Não há negociações em curso sobre a facilitação de vistos entre a Ucrânia e, respetivamente, a Irlanda e o Reino Unido.

Embora sejam países associados a Schengen, o Acordo não se aplica à Islândia, ao Liechtenstein, à Noruega e à Suíça, mas inclui declarações conjuntas sobre a conveniência desses Estados Schengen celebrarem acordos bilaterais de facilitação de vistos com a Ucrânia.

A Noruega assinou um acordo bilateral de facilitação de vistos em 13 de fevereiro de 2008. Esse acordo entrou em vigor em 1 de setembro de 2011.

A Suíça concluiu as negociações de um acordo bilateral sobre a facilitação de vistos em novembro de 2011. A Islândia indicou que as negociações com a Ucrânia tiveram início.

1.6. Acordo/acordos bilaterais

O artigo 13.º, n.º 1, do Acordo estabelece que:

- «1. A partir da sua entrada em vigor, o presente acordo prevalece sobre o disposto noutros acordos ou convénios bilaterais ou multilaterais celebrados entre os Estados-Membros e a Ucrânia, na medida em que as disposições destes últimos cubram matérias abrangidas pelo presente acordo.».

A partir da data de entrada em vigor do Acordo, as disposições dos acordos bilaterais em vigor entre os Estados-Membros e a Ucrânia sobre matérias abrangidas pelo Acordo deixaram de ser aplicáveis. Em conformidade com o direito da União, os Estados-Membros têm de tomar as medidas necessárias para eliminar as incompatibilidades entre os seus acordos bilaterais e o Acordo.

No entanto, o artigo 13.º, n.º 2, do Acordo estabelece que:

«2. As disposições dos acordos ou convénios bilaterais entre Estados-Membros individuais e a Ucrânia celebrados antes da entrada em vigor do presente Acordo que preveem a isenção da obrigação de visto para os titulares de passaportes de serviço não biométricos continuam a ser aplicáveis, sem prejuízo do direito dos Estados-Membros em causa ou da Ucrânia de denunciarem ou suspenderem a aplicação desses acordos ou convénios bilaterais.».

Os Estados-Membros seguintes celebraram acordos bilaterais com a Ucrânia que preveem a isenção da obrigação de visto para os titulares de passaportes de serviço: Bulgária, Croácia, Chipre, Letónia, Lituânia, Hungria, Polónia, Roménia e Eslováquia.

Em conformidade com o artigo 13.º, n.º 1 do Acordo, na medida em que esses acordos bilaterais abrangem os titulares de passaportes de serviço biométricos, o artigo 10.º, n.º 2, do Acordo prevalece sobre esses acordos bilaterais. Em conformidade com o artigo 13.º, n.º 2 do Acordo, esses acordos bilaterais, que foram celebrados antes da entrada em vigor do Acordo modificativo, continuam a ser aplicáveis, na medida em que sejam aplicáveis aos titulares de passaportes de serviço não biométricos, sem prejuízo do direito dos Estados-Membros em causa ou da Ucrânia de denunciarem ou suspenderem a aplicação desses acordos ou convénios bilaterais. A isenção da obrigação de visto para os titulares de passaportes de serviço não biométricos concedida por um Estado-Membro só se aplica para viajar no território desse Estado-Membro e não para viagens com destino a outros Estados Schengen.

Caso um Estado-Membro tenha celebrado um acordo ou convénio bilateral com a Ucrânia sobre matérias não abrangidas pelo Acordo, tal isenção deve continuar a aplicar-se após a entrada em vigor do Acordo.

1.7. Declaração da Comunidade Europeia sobre o acesso dos requerentes de visto às informações relativas aos procedimentos de emissão de vistos de curta duração e relativas à harmonização dos documentos a apresentar com um pedido de visto de curta duração

Em conformidade com a referida declaração da Comunidade Europeia que acompanha o Acordo I, as informações de base comuns sobre o acesso dos requerentes de visto às missões diplomáticas e aos postos consulares dos Estados-Membros e sobre os procedimentos, as condições de emissão e a validade dos vistos emitidos foram elaboradas de forma a assegurar que os requerentes recebem informações coerentes e uniformes. Essas informações estão disponíveis no sítio Web da Delegação da UE na Ucrânia: http://eeas.europa.eu/delegations/ukraine/index_en.htm.

As missões diplomáticas e os postos consulares dos Estados-Membros são convidados a divulgar amplamente esta informação (em quadros informativos, folhetos, sítios Web, etc.) e a divulgar igualmente informações exatas sobre as condições da emissão de vistos, a representação dos Estados-Membros da UE na Ucrânia e a lista harmonizada de documentos de apoio necessários.

II. DIRETRIZES SOBRE DISPOSIÇÕES ESPECÍFICAS

2.1. Regras aplicáveis a todos os requerentes de visto.

Importante: note-se que as medidas de facilitação referidas em seguida no que se refere aos emolumentos a cobrar pelo tratamento de pedidos de visto, ao prazo de tratamento dos pedidos, à partida em caso de documentos perdidos ou roubados e à prorrogação do visto em circunstâncias excecionais, se aplicam a todos os requerentes de visto e titulares de vistos ucranianos.

2.1.1. Emolumentos de visto.

O artigo 6.º, n.º 1, do Acordo estabelece que:

«A taxa a cobrar pelo tratamento de um pedido de visto de cidadãos da Ucrânia é de 35 EUR. O montante acima mencionado pode ser revisto nos termos do n.º 4 do artigo 14.º.».

Em conformidade com o artigo 6.º, n.º 1, a taxa a cobrar pelo tratamento de um pedido de visto é de 35 EUR. Essa taxa será aplicada a todos os requerentes de visto ucranianos (incluindo turistas) e diz respeito a vistos de curta duração, independentemente do número de entradas. É igualmente aplicável aos pedidos de visto apresentados nas fronteiras externas.

O artigo 6.º, n.º 2, do Acordo estabelece que:

«Se a Ucrânia reintroduzir a obrigação de visto para os cidadãos da UE, a taxa de visto que pode exigir não pode ser superior a 35 EUR ou ao montante acordado se a taxa for revista nos termos do n.º 4 do artigo 14.º.».

O artigo 6.º, n.º 3, do Acordo estabelece que:

«Os Estados-Membros cobram uma taxa de 70 EUR pelo tratamento dos vistos nos casos em que, devido à distância entre o lugar de residência do requerente e o lugar de apresentação do pedido, o requerente pedir que seja tomada uma decisão no prazo de três dias a contar da apresentação deste último e o consulado deferir esse pedido.».

É cobrada uma taxa de 70 EUR pelo tratamento dos pedidos de vistos quando um pedido e os respetivos documentos justificativos forem apresentados por um requerente cujo local de residência seja numa região na qual o Estado-Membro que o requerente pretende visitar não tem representação consular (se não houver qualquer consulado na região, nem centro de vistos, nem consulados dos Estados-Membros que celebraram acordos de representação com o Estado-Membro que o requerente pretende visitar), e quando a missão diplomática ou o posto consular concordar em tomar uma decisão sobre um pedido de visto no prazo de três dias. A prova do lugar de residência do requerente de visto é fornecida no formulário de pedido de visto.

Em princípio, o artigo 6.º, n.º 3 do Acordo pretende facilitar o pedido de visto pelos requerentes que vivem a grande distância do consulado. Se for necessária uma longa viagem para solicitar o visto, o objetivo é emití-lo rapidamente para que o requerente possa receber o visto sem ter de se deslocar duas vezes.

Por este motivo, nos casos em que a duração de tratamento «normal» de um pedido de visto por determinada missão diplomática ou posto consular seja igual ou inferior a três dias, é cobrada a taxa normal de 35 EUR.

Nas missões diplomáticas e postos consulares que têm um sistema de marcação de entrevistas, o prazo para marcar a entrevista não é contabilizado na duração do tratamento (ver também II.2.1.2).

O artigo 6.º, n.º 4, do Acordo estabelece que:

«4. Sem prejuízo do disposto no n.º 5, estão dispensadas do pagamento dos emolumentos relativos ao tratamento de um pedido de visto as seguintes categorias de pessoas:

- a) Familiares próximos — cônjuges, filhos (incluindo filhos adotados), pais (incluindo tutores), avós e netos — de cidadãos da Ucrânia que residam legalmente no território dos Estados-Membros ou cidadãos da União Europeia que residam no território do Estado-Membro de que são nacionais;»

(N.B. Esse ponto diz respeito aos familiares próximos ucranianos que viajem para os Estados-Membros para visitar cidadãos ucranianos que residem legalmente no território dos Estados-Membros ou para visitar cidadãos da União Europeia que residam no território do Estado-Membro de que são nacionais. Os requerentes de visto ucranianos que sejam membros da família de um cidadão da União, na aceção do artigo 5.º, n.º 2, da Diretiva 2004/38/CE do Parlamento Europeu e do Conselho ⁽¹⁾, obtêm o seu visto gratuitamente, o mais rapidamente possível e com base num procedimento acelerado.)

- «b) Membros de delegações oficiais que, na sequência de um convite oficial dirigido à Ucrânia, participem em reuniões, consultas, negociações ou programas de intercâmbio, bem como em eventos realizados no território de um dos Estados-Membros por organizações intergovernamentais;
- c) Membros dos Governos e Parlamentos nacionais e regionais e membros dos Tribunais Constitucional e Supremo que não estejam isentos da obrigação de visto por força do presente acordo;
- d) Alunos, estudantes, incluindo de cursos de pós-graduação, e professores acompanhantes que realizem viagens para efeitos de estudo ou de formação;
- e) Pessoas com deficiência e eventuais acompanhantes;» (N.B.: para beneficiar da isenção da taxa, deve ser fornecida prova de que todos os requerentes de visto são abrangidos por esta categoria).
- «f) Pessoas que justificaram devidamente a necessidade da viagem por razões humanitárias, incluindo a necessidade de receber tratamento médico urgente, bem como os seus acompanhantes, ou para comparecer no funeral de um familiar próximo ou visitar um familiar próximo gravemente doente;
- g) Participantes em eventos desportivos internacionais e seus acompanhantes;» (N.B.: apenas são abrangidos os acompanhantes que viajarem a título profissional, pelo que os adeptos não são considerados acompanhantes).

⁽¹⁾ Diretiva 2004/38/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros, que altera o Regulamento (CEE) n.º 1612/68 e que revoga as Diretivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE (JO L 158 de 30.4.2004, p. 77).

- «h) Participantes em atividades científicas, culturais e artísticas, incluindo programas de intercâmbio universitário ou outros;
- i) Participantes em programas de intercâmbio oficiais organizados por cidades geminadas e outras entidades municipais;
- j) Jornalistas e equipa técnica que os acompanha a título profissional;» (N.B.: os jornalistas abrangidos pelo artigo 4.º, n.º 1, alínea e), do Acordo são abrangidos por esta alínea).
- «k) Pensionistas;» (N.B.: a fim de beneficiar da isenção da taxa de visto para esta categoria, os requerentes têm de comprovar a sua qualidade de pensionista).
- «l) Condutores que efetuam serviços de transporte internacional de mercadorias e de passageiros no território dos Estados-Membros em veículos registados na Ucrânia;
- m) Pessoal de carruagem, de carruagens frigoríficas e de locomotivas de comboios internacionais que circulam no território dos Estados-Membros;
- n) Menores de 18 anos e filhos a cargo com menos de 21 anos.» (N.B.: a fim de beneficiar da isenção da taxa de visto para esta categoria, os requerentes têm de comprovar a sua idade, bem como, no caso de idade inferior a 21 anos, a sua condição de filhos a cargo);
- «o) Representantes das comunidades religiosas;
- p) Profissionais que participam em exposições, conferências, simpósios ou seminários internacionais ou outros eventos semelhantes realizados no território dos Estados-Membros;
- q) Participantes, com idade até aos 25 anos, em seminários, conferências e eventos desportivos, culturais ou educativos organizados por organizações sem fins lucrativos;
- r) Representantes de organizações da sociedade civil que viajam para efeitos de formação, seminários e conferências, incluindo no âmbito de programas de intercâmbio;
- s) Participantes em programas oficiais de cooperação transfronteiriça da União Europeia, nomeadamente no contexto do Instrumento Europeu de Vizinhança e Parceria (IEVP).

O primeiro parágrafo também se aplica aos casos em que a finalidade da viagem seja o trânsito.».

O artigo 6.º, n.º 4, segundo parágrafo, do Acordo só se aplica se o objetivo da viagem para o país terceiro for equivalente a um dos objetivos enumerados no artigo 6.º, n.º 4, alíneas a) a s), do Acordo, por exemplo, se o trânsito for necessário para participar num seminário, visitar familiares, participar num programa de intercâmbio de organizações da sociedade civil, etc. no país terceiro.

As categorias de pessoas acima referidas beneficiam de isenção total da taxa. Além disso, segundo o artigo 16.º, n.º 6, do Código de Vistos, «em casos individuais, podem ser concedidas isenções ou reduções dos emolumentos quando tal sirva para promover interesses culturais ou desportivos, bem como interesses no domínio da política externa, da política de desenvolvimento e noutros domínios de interesse público vital, ou por razões humanitárias.».

No entanto, essa regra não pode ser aplicada para suprimir, em casos individuais, a taxa de 70 EUR pelo tratamento do pedido de visto, quando este último e os respetivos documentos justificativos são apresentados por um requerente cujo lugar de residência seja distante da missão diplomática ou posto consular do Estado-Membro e que pertença a uma das categorias isentas enumeradas no artigo 6.º, n.º 4, do Acordo.

Importa igualmente recordar que as categorias de pessoas isentas da taxa de visto podem estar sujeitas a uma taxa de serviço quando um Estado-Membro cooperar com um prestador de serviços externo.

O artigo 6.º, n.º 5, do Acordo estabelece que:

«5. Se um Estado-Membro cooperar com um prestador de serviços externo para efeitos da emissão de vistos, esse prestador pode cobrar uma taxa pelos seus serviços, que deve ser proporcional aos custos decorrentes da execução das suas tarefas e que não pode exceder 30 EUR. Os Estados-Membros devem continuar a permitir que os requerentes apresentem os pedidos de visto diretamente nos seus consulados. Se for necessário marcar dia e hora para a apresentação do pedido, a marcação deve ter lugar, em regra, nas duas semanas seguintes à data em que tiver sido solicitada.».

Manter a possibilidade de os requerentes apresentarem os pedidos diretamente no consulado, em vez de se dirigirem a um prestador de serviços externo, implica que seja realmente possível escolher entre estas duas opções. Ainda que o acesso direto não tenha de ser organizado em condições idênticas ou semelhantes às do prestador de serviços, deve evitar-se que, na prática, o acesso direto se torne impossível. Ainda que, no caso do acesso direto, a existência de diferentes tempos de espera para obter uma entrevista seja aceitável, a duração da espera não deve ser tão longa que, na prática, tornem o acesso direto impossível.

2.1.2. *Prazo de tratamento dos pedidos de visto.*

O artigo 7.º do Acordo estabelece que:

- «1. As missões diplomáticas e postos consulares dos Estados-Membros decidem sobre um pedido de emissão de visto no prazo de 10 dias a contar da data de receção do pedido e dos documentos exigidos para o efeito.
2. Em casos individuais, o prazo para tomar uma decisão sobre um pedido de visto pode ser prorrogado até 30 dias, nomeadamente quando for necessária uma análise complementar do pedido.
3. Em casos urgentes, o prazo para tomar uma decisão sobre um pedido de visto pode ser reduzido a 2 dias úteis ou a um período inferior.».

Em princípio, a decisão sobre o pedido de visto deve ser tomada no prazo de 10 dias a contar da data da receção do pedido de visto completo e dos documentos comprovativos.

Esse prazo pode ser prorrogado até 30 dias no máximo quando for necessária uma análise mais aprofundada, por exemplo, para consultar as autoridades centrais.

Todos esses prazos têm início apenas quando o processo do pedido estiver completo, ou seja, a partir da data de receção do pedido e dos documentos comprovativos.

Nas missões diplomáticas e postos consulares que disponham de um sistema de marcação de entrevistas, o prazo para marcar a entrevista não é contabilizado na duração do tratamento. Ao marcar uma entrevista, deve ter-se em conta a eventual urgência pedida pelo requerente de visto tendo em vista a aplicação do artigo 7.º, n.º 3, do Acordo. Regra geral, as entrevistas devem realizar-se no prazo de duas semanas a contar da data em que foram solicitadas (ver artigo 6.º, n.º 5, do Acordo). Um prazo mais longo deve ser uma exceção, mesmo nos períodos de maior afluência. O Comité Misto vai acompanhar atentamente esta questão. Os Estados-Membros envidarão esforços para garantir que as entrevistas dos membros das delegações oficiais da Ucrânia, com vista à apresentação de pedidos de visto nas missões diplomáticas e postos consulares, se realizam o mais rapidamente possível, de preferência no prazo de dois dias úteis, em casos urgentes e quando o convite tenha sido enviado com atraso.

A decisão de redução do prazo de decisão sobre um pedido de visto, prevista no artigo 7.º, n.º 3, do Acordo, é tomada pelo funcionário consular.

2.1.3. *Prorrogação do visto em circunstâncias excecionais.*

O artigo 9.º do Acordo estabelece que:

«Os cidadãos da Ucrânia que, por motivo de força maior, não tiverem a possibilidade de sair do território dos Estados-Membros até à data indicada nos seus vistos, podem obter a sua prorrogação gratuitamente nos termos da legislação aplicada pelo Estado de acolhimento pelo período necessário para o seu regresso ao Estado de residência.».

Quanto à possibilidade de prorrogar a validade do visto em casos de força maior, por exemplo, internamento hospitalar por motivos imprevistos/repentinos, doença/acidente, quando o titular do visto não tenha a possibilidade de sair do território dos Estados-Membros até à data indicada no visto, aplicam-se as disposições do artigo 33.º, n.º 1, do Código de Vistos, desde que estas sejam compatíveis com o Acordo (por exemplo, o visto prorrogado continua a ser um visto uniforme que autoriza a entrada no território de todos os Estados Schengen para os quais o visto era válido no momento da sua emissão). No entanto, nos termos do Acordo, a prorrogação do visto em caso de força maior é concedida a título gratuito.

2.2. Regras aplicáveis a certas categorias de requerentes de visto.

2.2.1. Documentos comprovativos da finalidade da viagem

Para todas as categorias de pessoas enumeradas no artigo 4.º, n.º 1, do Acordo, incluindo os condutores que efetuam serviços de transporte internacional de mercadorias e de passageiros, os documentos comprovativos indicados só são exigidos para justificar a finalidade da viagem. Para estas categorias de requerentes não devem ser solicitados quaisquer outros documentos relacionados com a finalidade da estada. Como indicado no artigo 4.º, n.º 3 do Acordo, não é exigida qualquer outra justificação, convite ou validação da finalidade da viagem.

Quando, em casos individuais, subsistam dúvidas sobre a verdadeira finalidade da viagem, o requerente de visto deve ser convocado para uma entrevista aprofundada (adicional) na embaixada/consulado, onde pode ser questionado sobre o objetivo real da estada ou a intenção de regressar ao seu país de proveniência — ver artigo 21.º, n.º 8, do Código de Vistos. Nesses casos individuais, podem ser fornecidos pelo requerente, ou excepcionalmente requeridos pelo funcionário consular, documentos suplementares. O Comité Misto acompanhará de perto esta questão.

Para as categorias de pessoas mencionadas no artigo 4.º, n.º 1, do Acordo, continuam a ser aplicáveis as regras atuais em matéria de documentos comprovativos do objetivo da viagem. O mesmo se aplica aos documentos em matéria de consentimento dos pais para a deslocação dos filhos menores de 18 anos.

As regras de Schengen ou as legislações nacionais aplicam-se às matérias não abrangidas pelas disposições do Acordo, como o reconhecimento dos documentos de viagem, o seguro médico de viagem, as garantias relativas ao regresso e a prova de meios de subsistência suficientes (ver ponto I.1.2).

Em consonância com a «Declaração da União Europeia sobre os documentos a apresentar juntamente com um pedido de visto de curta duração» que acompanha o Acordo modificativo, «A União Europeia estabelecerá uma lista harmonizada de documentos comprovativos em conformidade com o artigo 48.º, n.º 1, alínea a), do Código de Vistos, a fim de assegurar que sejam exigidos aos requerentes da Ucrânia, em princípio, os mesmos documentos comprovativos.»; os consulados dos Estados-Membros, atuando no âmbito da cooperação Schengen local, devem ainda garantir que os requerentes de visto ucranianos recebem informações de base coerentes e uniformes e que, em princípio, lhes são solicitados os mesmos documentos comprovativos independentemente do consulado do Estado-Membro em que apresentam o pedido.

Em princípio, o original do pedido ou do certificado exigido pelo artigo 4.º, n.º 1, do Acordo, devem ser entregues juntamente com o pedido de visto. No entanto, o consulado pode começar a processar o pedido de visto com base num fax ou numa cópia do pedido ou do certificado. Em todo o caso, o consulado pode solicitar o documento original no caso de um primeiro pedido e em casos individuais, quando haja dúvidas.

Dado que, por vezes, as listas das autoridades enumeradas em seguida contêm igualmente o nome da pessoa habilitada a assinar os respetivos pedidos/certificados, as autoridades ucranianas devem informar a cooperação local Schengen quando essas pessoas forem substituídas.

Artigo 4.º do Acordo estabelece que:

«1. Para as seguintes categorias de cidadãos da Ucrânia, os documentos a seguir indicados são suficientes para justificar a finalidade da viagem ao território da outra parte:

a) Para os membros das delegações oficiais que, na sequência de um convite oficial dirigido à Ucrânia, participem em reuniões, consultas, negociações ou programas de intercâmbio, bem como em eventos realizados no território de um dos Estados-Membros por organizações intergovernamentais:

— uma carta enviada por uma autoridade ucraniana confirmando que o requerente é membro da sua delegação em viagem ao território da outra parte para participar nos eventos acima mencionados, acompanhada de uma cópia do convite oficial;»

O nome do requerente deve ser indicado na carta emitida pela autoridade competente, confirmando que a pessoa faz parte da delegação que se desloca ao território da outra Parte para participar na reunião oficial. O nome do requerente não tem necessariamente de ser indicado no convite oficial para participar na reunião, embora tal possa ser o caso quando o convite oficial é dirigido a uma pessoa específica.

Essa disposição aplica-se aos membros de delegações oficiais, independentemente do tipo de passaporte de que são titulares (de serviço não biométrico ou passaporte ordinário).

«b) Para os empresários e representantes de organizações empresariais:

— um pedido por escrito de uma pessoa coletiva ou empresa anfitriã, ou de um seu departamento ou filial, de autoridades centrais ou locais dos Estados-Membros ou de comités organizadores de exposições comerciais e industriais, conferências e simpósios realizados no território dos Estados-Membros;

- c) Para os condutores que efetuam serviços de transporte internacional de mercadorias e de passageiros no território dos Estados-Membros em veículos registados na Ucrânia:

— um pedido por escrito da associação nacional de transportadores ucranianos que efetuam serviços de transporte rodoviário internacional, indicando a finalidade, a duração, o ou os destinos e a frequência das viagens;»

As autoridades competentes em matéria de transporte rodoviário internacional responsáveis por indicar a finalidade, duração, destinos e frequência das viagens dos condutores que efetuam serviços de transporte internacional de mercadorias e de passageiros no território dos Estados-Membros em veículos registados na Ucrânia, são as seguintes:

1. Associação dos transportadores rodoviários internacionais da Ucrânia (AsMAP/«АсМАП»)

O endereço postal da AsMAP é o seguinte:

11, Shorsa str.

Kyiv, 03150, Ucrânia

Os funcionários habilitados a assinar os pedidos são os seguintes:

Kostiuchenko Leonid — Presidente da AsMAP da Ucrânia;

Dokil' Leonid — Vice-Presidente da AsMAP da Ucrânia;

Kuchynskiy Yurii — Vice-Presidente da AsMAP da Ucrânia.

2. Empresa pública «Serviço dos transportes rodoviários internacionais» («SIRC — EP»)

O endereço postal da SIRC — EP é:

57, av. Nauka

Kyiv, 03083, Ucrânia

Tel. +38 044 524 21 01

Fax +38 044 524 00 70

Os funcionários habilitados a assinar os pedidos são os seguintes:

Tkachenko Anatolij — Diretor da SIRC — EP;

Neronov Oleksandr — Primeiro Diretor-adjunto da SIRC — EP.

3. União dos transportes rodoviários e logística da Ucrânia

O endereço postal da União dos transportes rodoviários e logística da Ucrânia é:

28, Predslavinska str.

Kyiv, 03150, Ucrânia

Tel./fax +38 044 528 71 30/+38 044 528 71 46/+38 044 529 44 40

O funcionário habilitado a assinar os pedidos é o seguinte:

Lypovskiy Vitalij — Presidente da União

4. Associação ucraniana dos transportadores de automóveis (AAAC/Всеукраїнська асоціація автомобільних перевізників)

O endereço postal da AAAC é o seguinte:

139, Velyka Vasylkivska str.

Kyiv, 03150, Ucrânia

Tel./fax: +38044-538-75-05, +38044-529-25-21

Os funcionários habilitados a assinar os pedidos são os seguintes::

Reva Vitalii (Віталій Рева) — Presidente da AAAC

Glavatskyi Petro (Петро Главатський) — Vice-Presidente da AAAC

Endereço eletrónico: vaap@i.com.ua

5. Associação ucraniana dos transportadores de automóveis (AAAC/Всеукраїнська асоціація автомобільних перевізників)

O endereço postal da AAAC é:

3, Rayisy Okipnoyi str.

Kyiv, 02002, Ucrânia

Tel./fax: +38044-517-44-31, +38044-516-47-26

Os funcionários habilitados a assinar os pedidos são os seguintes:

Vakulenko Volodymyr (Вакуленко Володимир Михайлович) — Vice-Presidente da AAAC

6. Empresa pública ucraniana «Ukrinteravtoservice» (Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів «Укрінтеравтосервіс»)

O endereço postal da empresa pública ucraniana «Ukrinteravtoservice» é:

57, av. Nauky

Kyiv, 03083, Ucrânia

Os funcionários habilitados a assinar os pedidos são os seguintes:

Dobrohod Serhii (Доброход Сергій Олександрович) — Diretor-Geral da empresa pública ucraniana «Ukrinteravtoservice» (telefone: +38 044 524-09-99; telemóvel: +38 050 463-89-32);

Kubalska Svitlana (Кубальська Світлана Сергіївна) — Diretora-Geral Adjunta da empresa pública ucraniana «Ukrinteravtoservice» (telefone: +38 044 524-09-99; Telemóvel: +38 050 550-82-62);

Tendo em conta os atuais problemas relacionados com essa categoria de requerentes de visto o Comité Misto vai acompanhar de perto a aplicação dessa disposição.

«d) Para o pessoal de carruagem, de carruagens frigoríficas e de locomotivas de comboios internacionais que circulam no território dos Estados-Membros:

— um pedido por escrito da empresa de caminhos-de-ferro competente da Ucrânia, indicando a finalidade, a duração e a frequência das viagens;»

A autoridade competente no domínio do transporte ferroviário da Ucrânia é o Serviço Estatal dos Transportes Ferroviários da Ucrânia («Ukrzaliznytsia»/«Укрзалізниця»).

O endereço postal da Ukrzaliznytsia é:

5-7 Tverskaya str.

Kyiv, 03680, Ucrânia

De acordo com a atribuição de responsabilidades na direção do «Ukrzaliznytsia», os funcionários competentes incumbidos de prestar informações sobre a finalidade, duração e frequência das viagens do pessoal de carruagem, de carruagens frigoríficas e de locomotivas de comboios internacionais que circulam no território dos Estados-Membros são:

Bolobolin Serhii (Болоболін Сергій Петрович) — Primeiro Diretor-Geral do Ukrzaliznytsia (telefone: +38 044 465 00 10);

Serhiyenko Mykola (Сергієнко Микола Іванович) — Primeiro Diretor-Geral Adjunto do Ukrzaliznytsia (telefone: +38 044 465 00 01);

Zhurakivskyi Vitaliy (Жураківський Віталій Олександрович) — Primeiro Diretor-Geral Adjunto do Ukrzaliznytsia (telefone: +38 044 465 00 41);

Slipchenko Oleksiy (Сліпченко Олексій Леонтійович) — Diretor-Geral Adjunto do Ukrzaliznytsia (telefone: +38 044 465 00 14);

Naumenko Petro (Науменко Петро Петрович) — Diretor-Geral Adjunto do Ukrzaliznytsia (telefone: +38 044 465 00 12);

Chekalov Pavlo (Чекалов Павло Леонтійович) — Diretor-Geral Adjunto do Ukrzaliznytsia (telefone: +38 044 465 00 13);

Matviiv Igor — Chefe do departamento de relações internacionais do Ukrzaliznytsia (telefone: +38 044 465 04 25).

«e) Para os jornalistas e a equipa técnica que os acompanha a título profissional:

- um certificado ou outro documento emitido por uma organização profissional ou pelo empregador do requerente comprovativo de que o interessado é jornalista profissional e que indique que a viagem tem por finalidade realizar um trabalho jornalístico ou comprove que o interessado é membro da equipa técnica que acompanha o jornalista a título profissional;»

Esta categoria não inclui os jornalistas independentes.

Devem ser apresentados o certificado ou documento comprovativo de que o interessado é um jornalista profissional e o documento original emitido pelo seu empregador declarando que a viagem tem por finalidade realizar um trabalho jornalístico ou comprovando que a pessoa é membro da equipa técnica que acompanha o jornalista a título profissional.

A organização profissional ucraniana competente para comprovar que a pessoa em causa é um jornalista qualificado é:

1. Sindicato Nacional dos Jornalistas da Ucrânia (NSJU) (Національна спілка журналістів України — НСЖУ).

O NSJU emite as carteiras de jornalista profissional para os trabalhadores qualificados dos órgãos de comunicação social nacionais e internacionais, de acordo com os padrões estabelecidos pela Federação Internacional de Jornalistas.

O endereço postal do NSJU é o seguinte:

27-a Khreschatyk str.

Kyiv, 01001, Ucrânia

A pessoa autorizada do NSJU é a seguinte:

Nalyvaiko Oleg Igorovych (Наливайко Олег Ігорович) — Diretor do NSJU

Telefone/Fax: +38044-234-20-96; +38044-234-49-60; +38044-234-52-09

Endereço eletrónico: spilka@nsju.org; admin@nsju.org.

2. União dos Meios de Comunicação Social Independentes da Ucrânia (IMUU) («Незалежна медіа-профспілка України»).

O endereço postal da IMUU é o seguinte:

Office 25,

27 — A, Khreshchatyk Str.,

Kyiv, 01001, Ucrânia

As pessoas autorizadas são as seguintes:

Lukanov Yurii (Луканов Юрій Вадимович) — Diretor da IMUU

Vynnychuk Oksana (Оксана Винничук) — Secretária-Executiva da IMUU

Telefone + 38 050 356 57 58

Endereço eletrónico: secretar@profspilka.org.ua

«f) Para os participantes em atividades científicas, culturais e artísticas, incluindo programas de intercâmbio universitário ou outros:

- um pedido de participação nessas atividades redigido pela organização anfitriã;

g) Para alunos, estudantes, incluindo de cursos de pós-graduação, e professores acompanhantes que realizem viagens de estudo ou de formação, nomeadamente no âmbito de programas de intercâmbio, bem como de outras atividades conexas:

- um pedido por escrito ou um certificado da inscrição por parte da universidade, colégio ou escola anfitriã, ou um cartão de estudante ou um certificado dos cursos a frequentar;»

Um cartão de estudante só pode ser aceite como justificação da finalidade da viagem quando for emitido pela universidade, colégio ou escola de acolhimento onde os estudos ou a formação terão lugar.

«h) Para os participantes em eventos desportivos internacionais e acompanhantes a título profissional:

- um pedido por escrito da organização anfitriã: autoridades competentes, federações desportivas nacionais e Comitês Olímpicos nacionais dos Estados-Membros;»

A lista dos acompanhantes, em caso de eventos desportivos internacionais, limita-se às pessoas que acompanham o desportista a título profissional: treinadores, massagistas, agente, médicos desportivos e dirigentes do clube. Os adeptos não são considerados acompanhantes.

«i) Participantes em programas de intercâmbio oficiais organizados por cidades geminadas e outras entidades municipais;

- um pedido redigido pelo chefe da administração/Presidente da Câmara das cidades ou entidades municipais em causa;»

O chefe da administração/presidente da câmara de cidades ou entidades municipais competente para emitir o convite escrito é o chefe da administração/presidente da câmara da cidade de acolhimento ou geminada onde a atividade de geminação vai ter lugar. Esta categoria abrange unicamente as geminações oficiais.

«j) Para os familiares próximos — cônjuges, filhos (incluindo filhos adotados), pais (incluindo tutores), avós e netos — em visita a cidadãos da Ucrânia que residam legalmente no território dos Estados-Membros ou a cidadãos da União Europeia que residam no território do Estado-Membro de que são nacionais:

- um pedido por escrito da pessoa anfitriã;»

Esda alínea diz respeito aos familiares próximos ucranianos que viajem para os Estados-Membros para visitar cidadãos ucranianos que residem legalmente no território dos Estados-Membros ou cidadãos da União Europeia que residam no território do Estado-Membro de que são nacionais.

A autenticidade da assinatura da pessoa anfitriã deve ser certificada pela autoridade competente de acordo com a legislação nacional do país de residência.

Também é necessário comprovar a residência legal da pessoa anfitriã e o laço de parentesco, por exemplo, juntando ao convite escrito da pessoa anfitriã cópias de documentos que expliquem o seu estatuto, como uma fotocópia do título de residência e um atestado dos laços familiares.

Essa disposição aplica-se também aos familiares do pessoal das missões diplomáticas e consulados que viajam para visitar familiares até 90 dias no máximo no território dos Estados-Membros, exceto quanto à necessidade de comprovar a residência legal e os laços familiares.

Em consonância com a Declaração da União Europeia sobre medidas de facilitação da emissão de vistos para os familiares anexada ao Acordo modificativo, «a fim de facilitar a mobilidade de um número alargado de pessoas que possuem laços familiares (em especial, irmãs, irmãos e respetivos filhos) com cidadãos da Ucrânia que residam legalmente no território dos Estados-Membros ou com cidadãos da União Europeia que residam no território do Estado-Membro de que são nacionais, a União Europeia convida os serviços consulares dos Estados-Membros a utilizar plenamente as possibilidades previstas no Código de Vistos para facilitar a emissão de vistos para esta categoria de pessoas, nomeadamente simplificando os documentos comprovativos solicitados aos requerentes, isentando-os dos emolumentos devidos pelo tratamento dos pedidos e, se necessário, emitindo-lhes vistos de entradas múltiplas.».

«k) Familiares de visita por motivo de cerimónias fúnebres:

- um documento oficial comprovativo do óbito, bem como dos laços familiares ou outros entre o requerente e a pessoa falecida;»

O Acordo não especifica quais são as autoridades nacionais que devem emitir o documento oficial acima referido: o país está situado o cemitério onde se realiza a cerimónia fúnebre ou o país de residência da pessoa que deseja estar presente nessa cerimónia. Deve aceitar-se que as autoridades competentes de ambos os países podem emitir esse tipo de documento oficial.

É necessário apresentar o referido documento oficial comprovativo do óbito, bem como dos laços familiares ou outros entre o requerente e a pessoa falecida, por exemplo, certidões de nascimento e/ou de casamento.

«l) Para pessoas que visitam cemitérios militares e civis:

- um documento oficial comprovativo da existência e conservação da sepultura, bem como de laços familiares ou outros entre o requerente e a pessoa falecida;»

O Acordo não especifica se o referido documento oficial deve ser emitido pelas autoridades do país onde se realiza a cerimónia fúnebre ou do país de residência da pessoa que deseja estar presente. Deve aceitar-se que as autoridades competentes de ambos os países podem emitir esse tipo de documento oficial.

É necessário apresentar o referido documento oficial comprovativo da existência e conservação da sepultura, bem como de laços familiares ou outros entre o requerente e a pessoa falecida.

Em conformidade com a Declaração da Comunidade Europeia relativa à emissão de vistos de curta duração para pessoas que visitam cemitérios militares e civis, que acompanha o Acordo, em princípio, os vistos de curta duração para pessoas que visitam cemitérios militares e civis são emitidos por um período máximo de 14 dias.

«m) Para as pessoas em visita por motivos de saúde e seus acompanhantes:

- um documento oficial do estabelecimento de saúde comprovativo da necessidade de cuidados médicos nesse estabelecimento, da necessidade de acompanhamento e a prova de meios de subsistência suficientes para pagar o tratamento médico;»

É necessário apresentar o documento oficial do estabelecimento de saúde comprovativo da necessidade de cuidados médicos nesse estabelecimento e a prova de meios de subsistência suficientes para pagar o tratamento médico, bem como a confirmação de que é necessário acompanhamento.

«n) Para os representantes de organizações da sociedade civil que viajam para efeitos de formação, seminários e conferências, incluindo no âmbito de programas de intercâmbio:

- um pedido por escrito da organização anfitriã, uma confirmação de que o interessado representa a organização da sociedade civil e a certidão do registo de constituição dessa organização emitida pela autoridade pública competente nos termos da legislação nacional;»

O documento comprovativo do registo na Ucrânia de uma organização da sociedade civil é uma carta emitida pelo Serviço Nacional dos Registos da Ucrânia com base em informações do Registo das Associações Públicas.

«o) Para os profissionais que participam em exposições, conferências, simpósios, seminários internacionais ou outros eventos semelhantes realizados no território dos Estados-Membros:

- um pedido por escrito da organização anfitriã confirmando que o interessado participa no evento;

p) Para os representantes das comunidades religiosas:

- um pedido por escrito de uma comunidade religiosa registada na Ucrânia, que indique a finalidade, a duração e a frequência das viagens;»

O documento comprovativo da inscrição na Ucrânia de uma comunidade religiosa é um extrato do Registo Nacional Unificado das pessoas coletivas e dos empresários em nome individual, com informações sobre a organização e forma jurídica da entidade que é uma comunidade religiosa.

«q) Para os participantes em programas oficiais de cooperação transfronteiriça da União Europeia, nomeadamente no contexto do Instrumento Europeu de Vizinhança e Parceria (IEVP):

- um pedido por escrito da organização anfitriã.»

Importante: o Acordo não cria quaisquer novas regras de responsabilidade para as pessoas singulares ou coletivas que emitem os pedidos escritos. As legislações nacionais e da UE respetivas aplicam-se em caso de emissão de falsos pedidos.

2.2.2. Emissão de vistos de entradas múltiplas.

Nos casos em que o requerente de visto necessite de viajar frequente ou regularmente no território dos Estados-Membros, deve ser emitido um visto de curta duração para entradas múltiplas, desde que a duração total de tais visitas não exceda 90 dias em cada período de 180 dias.

O artigo 5.º, n.º 1, do Acordo estabelece que:

«1. As missões diplomáticas e postos consulares dos Estados-Membros devem emitir vistos de entradas múltiplas válidos por cinco anos às seguintes categorias de pessoas:

- a) Membros dos Governos e dos Parlamentos nacionais e regionais, membros dos Tribunais Constitucional e Supremo e procuradores nacionais e regionais e seus adjuntos que, no exercício das suas funções, não estejam isentos da obrigação de visto por força do presente Acordo;

- b) Membros permanentes de delegações oficiais que, na sequência de um convite oficial dirigido à Ucrânia, participem regularmente em reuniões, consultas, negociações ou programas de intercâmbio, bem como em eventos realizados no território dos Estados-Membros por organizações intergovernamentais;
- c) Cônjuges e filhos (incluindo filhos adotados) com idade inferior a 21 anos ou que estão a cargo, bem como pais (incluindo tutores) em visita a cidadãos da Ucrânia que residam legalmente no território dos Estados-Membros ou a cidadãos da União Europeia que residam no território do Estado-Membro de que são nacionais;
- d) Empresários e representantes de organizações empresariais que se deslocam regularmente aos Estados-Membros;
- e) Jornalistas e equipa técnica que os acompanha a título profissional.

Em derrogação ao primeiro parágrafo, sempre que a necessidade ou intenção de viajar com frequência ou regularidade se limitar manifestamente a um período mais curto, a validade do visto de entradas múltiplas deve corresponder a esse período, nomeadamente se:

- no caso das pessoas referidas na alínea a), a duração do seu mandato,
- no caso das pessoas referidas na alínea b), a validade do seu estatuto de membro permanente de uma delegação oficial,
- no caso das pessoas referidas na alínea c), a validade da autorização de residência de cidadãos da Ucrânia que residam legalmente na União Europeia,
- no caso das pessoas referidas na alínea d), a validade do estatuto de representante de uma organização empresarial ou do seu contrato de trabalho,
- no caso das pessoas referidas na alínea e), a validade do seu contrato de trabalho

for inferior a cinco anos.».

Para essas categorias de pessoas, tendo em conta a sua situação profissional ou o vínculo familiar com um cidadão da Ucrânia que resida legalmente no território dos Estados-Membros ou com um cidadão da União Europeia que resida no território do Estado-Membro de que é nacional, justifica-se, em princípio, a emissão vistos de entradas múltiplas com um período de validade de cinco anos. Na versão inicial do Acordo, a expressão «válidos até cinco anos» deixava uma margem discricionária aos consulados para decidirem sobre o período de validade do visto, estabelecendo apenas a sua duração máxima. Nos termos do Acordo modificativo, essa margem discricionária desapareceu com a nova redação «válidos por cinco anos», especificando que, se o requerente preencher todos os requisitos do artigo 5.º, n.º 1, do Acordo, «as missões diplomáticas e postos consulares dos Estados-Membros devem emitir vistos de entradas múltiplas válidos por cinco anos».

Para as pessoas abrangidas pelo artigo 5.º, n.º 1, alínea a), do Acordo, deve ser comprovada a sua situação profissional e a duração do mandato.

Essa disposição não se aplica às pessoas abrangidas pelo artigo 5.º, n.º 1, alínea a) do Acordo, que estejam isentas da obrigação de visto pelo presente Acordo, ou seja, se forem titulares de passaportes diplomáticos ou de passaportes de serviço biométricos.

Para as pessoas abrangidas pelo artigo 5.º, n.º 1, alínea b) do Acordo, deve ser comprovado o seu estatuto de membro permanente da delegação e a necessidade de participar regularmente em reuniões, consultas, negociações ou programas de intercâmbio.

Para as pessoas abrangidas pelo artigo 5.º, n.º 1, alínea c) do Acordo, deve ser comprovada a legalidade da residência da pessoa que convida (ver ponto II.2.2.1).

Para as pessoas abrangidas pelo artigo 5.º, n.º 1, alíneas d) e e) do Acordo, deve ser comprovada a sua situação profissional e a duração das suas atividades.

O artigo 5.º, n.º 2, do Acordo estabelece que:

«2. As missões diplomáticas e os postos consulares dos Estados-Membros devem emitir vistos de entradas múltiplas válidos por um ano às seguintes categorias de pessoas, desde que no ano anterior tenham obtido pelo menos um visto e o tenham utilizado em conformidade com a legislação em matéria de entrada e residência do Estado visitado:

- a) Condutores que efetuam serviços de transporte internacional de mercadorias e de passageiros para o território dos Estados-Membros em veículos registados na Ucrânia;

- b) Pessoal de carruagem, de carruagens frigoríficas e de locomotivas de comboios internacionais que circulem no território dos Estados-Membros;
- c) Participantes em atividades científicas, culturais e artísticas, incluindo programas de intercâmbio universitário ou outros, que se deslocam regularmente ao território dos Estados-Membros;
- d) Participantes em eventos desportivos internacionais e seus acompanhantes a título profissional;
- e) Participantes em programas de intercâmbio oficiais organizados por cidades geminadas e outras entidades municipais;
- f) Representantes de organizações da sociedade civil que se desloquem regularmente aos Estados-Membros para efeitos de formação, seminários e conferências, incluindo no âmbito de programas de intercâmbio;
- g) Participantes em programas oficiais de cooperação transfronteiriça da União Europeia, nomeadamente no contexto do Instrumento Europeu de Vizinhaça e Parceria (IEVP);
- h) Estudantes, incluindo de cursos de pós-graduação, que realizem regularmente viagens para efeitos de estudo ou de formação, nomeadamente no âmbito de programas de intercâmbio;
- i) Representantes das comunidades religiosas;
- j) Profissionais que participem em exposições, conferências, simpósios ou seminários internacionais ou outros eventos semelhantes realizados no território dos Estados-Membros;
- k) Pessoas que tenham de fazer visitas periódicas por motivos de saúde e seus acompanhantes.

Em derrogação ao primeiro parágrafo, sempre que a necessidade ou a intenção de viajar com frequência ou regularidade se limitar manifestamente a um período mais curto, a validade do visto de entradas múltiplas deve corresponder a esse período.».

Na versão inicial do Acordo, a expressão «válidos até um ano» deixava uma margem discricionária aos consulados para decidirem sobre o período de validade do visto, estabelecendo apenas a sua duração máxima. Nos termos do Acordo modificativo, essa margem discricionária desapareceu com a nova redação «válidos por um ano», especificando que, se o requerente preencher todos os requisitos do artigo 5.º, n.º 2 do Acordo, «as missões diplomáticas e os postos consulares dos Estados-Membros devem emitir vistos de entradas múltiplas válidos por um ano». Deve notar-se que serão emitidos vistos de entradas múltiplas válidos por um ano para as categorias acima referidas desde que no ano anterior (12 meses), o requerente de visto tenha obtido pelo menos um visto Schengen, que utilizou em conformidade com a legislação em matéria de entrada e estada no(s) Estado(s) visitado(s) (por exemplo, a pessoa não tenha ultrapassado o prazo da estada autorizada) e se tiver razões para solicitar um visto de entradas múltiplas. O visto Schengen obtido durante o ano anterior pode ter sido emitido por um Estado Schengen diferente do que recebeu o novo pedido de visto. Nos casos em que não se justifica a emissão de um visto válido por um ano (por exemplo, se a duração do programa de intercâmbio for inferior a um ano ou se a pessoa não necessita de viajar frequente ou regularmente durante um ano inteiro), a validade do visto será inferior a um ano, desde que estejam preenchidas as outras condições para a emissão do visto.

O artigo 5.º, n.ºs 3 e 4, do Acordo estabelece que:

«3. As missões diplomáticas e os postos consulares dos Estados-Membros devem emitir vistos de entradas múltiplas válidos entre, no mínimo, dois e, no máximo, cinco anos, às categorias de pessoas referidas no n.º 2 do presente artigo, desde que nos dois anos anteriores tenham utilizado o visto de entradas múltiplas de um ano de acordo com a legislação relativa à entrada e estadia do Estado visitado, salvo se a necessidade ou a intenção de viajar com frequência ou regularidade se limitar manifestamente a um período mais curto, caso em que a validade do visto de entradas múltiplas deve corresponder a esse período.

4. A duração total de estada no território dos Estados-Membros das pessoas referidas nos n.ºs 1 a 3 não pode ser superior a 90 dias em cada período de 180 dias.».

Os vistos de entradas múltiplas válidos entre dois e cinco anos serão emitidos para as categorias mencionadas no artigo 5.º, n.º 2 do Acordo, desde que nos dois anos anteriores tenham utilizado um visto de entradas múltiplas de um ano de acordo com a legislação relativa à entrada e estada no território do(s) Estado(s) visitado(s) e desde que a necessidade de viajar com frequência ou regularidade não seja manifestamente limitada a um período mais curto. Deve notar-se que só será emitido um visto válido entre dois e cinco anos se o requerente tiver recebido dois vistos com validade de um ano — e não menos — durante os dois anos anteriores, e se os tiver utilizado em conformidade com a legislação de entrada e estada no território do(s) Estado(s) visitado(s). As missões diplomáticas e os postos consulares dos Estados-Membros decidem, com base na avaliação de cada pedido de visto, o período de validade desses vistos — entre dois e cinco anos.

Quanto aos critérios previstos no artigo 5.º, n.º 2 do Acordo, «desde que [...] existam motivos para solicitar um visto de entradas múltiplas» e no artigo 5.º, n.º 3 do Acordo, «desde que [...] continuem a ser válidos os motivos para solicitar um visto de entradas múltiplas», aplicam-se os critérios previstos no artigo 24.º, n.º 2, alínea a), do Código de Vistos para a emissão desse tipo de vistos, ou seja, a pessoa necessita de viajar frequentemente para um ou vários Estados-Membros, por exemplo, por motivos profissionais.

Não existe qualquer obrigação de emitir um visto de entradas múltiplas se o requerente não tiver utilizado um visto anterior. No entanto, tal visto pode ser emitido se a não utilização do visto anterior se deveu a circunstâncias independentes da vontade do requerente, por exemplo, uma baixa por doença prolongada de um condutor de camião.

No que diz respeito aos documentos justificativos da finalidade da viagem para a emissão de vistos de entradas múltiplas para as categorias de pessoas referidas no artigo 5.º do Acordo, ver ponto II.2.2.1.

2.2.3. Titulares de passaportes diplomáticos e passaportes de serviço.

O artigo 10.º do Acordo estabelece que:

- «1. Os cidadãos da Ucrânia, titulares de passaportes diplomáticos válidos, podem entrar, sair e transitar pelo território dos Estados-Membros sem obrigação de visto.
2. Os cidadãos da Ucrânia, titulares de passaportes de serviço biométricos válidos, podem entrar e sair do território dos Estados-Membros e transitar no mesmo sem obrigação de visto.
3. As pessoas mencionadas nos n.ºs 1 e 2 podem permanecer no território dos Estados-Membros por um período máximo de 90 dias em cada período de 180 dias.».

Os acordos ou convénios bilaterais em vigor que prevejam a isenção da obrigação de visto para os titulares de passaportes de serviço não biométricos continuam a ser aplicáveis, salvo denúncia ou suspensão (ver ponto 1.6).

O destacamento de diplomatas nos Estados-Membros não é regulado pelo Acordo, aplicando-se o procedimento de acreditação habitual.

III. ESTATÍSTICAS

A fim de permitir ao Comité Misto assegurar um controlo eficaz da sua aplicação, as missões diplomáticas e postos consulares dos Estados-Membros devem enviar semestralmente à Comissão estatísticas, sempre que possível repartidas por mês, em especial sobre os seguintes elementos:

- Tipos de vistos emitidos para as diferentes categorias de pessoas abrangidas pelo Acordo;
 - Número de recusas de visto para as diferentes categorias de pessoas abrangidas pelo Acordo;
 - Percentagem de requerentes convocados para uma entrevista pessoal por categoria de pessoas;
 - Vistos de entradas múltiplas válidos por cinco anos emitidos a cidadãos ucranianos (por país);
 - Percentagem de vistos emitidos gratuitamente às diferentes categorias de pessoas abrangidas pelo Acordo.
-

DECISÃO (PESC) 2015/439 DO CONSELHO**de 16 de março de 2015****que prorroga o mandato do Representante Especial da União Europeia para o Sael**

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 33.º e o artigo 31.º, n.º 2,

Tendo em conta a proposta da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 18 de março de 2013, o Conselho adotou a Decisão 2013/133/PESC ⁽¹⁾ que nomeia Michel Dominique REVEYRAND — DE MENTHON Representante Especial da União Europeia (REUE) para o Sael. O mandato do REUE foi prorrogado pela Decisão 2014/130/PESC do Conselho ⁽²⁾ e caduca em 28 de fevereiro de 2015.
- (2) O mandato do REUE deverá ser prorrogado por um novo período de oito meses.
- (3) O REUE cumprirá o seu mandato no contexto de uma situação que poderá vir a deteriorar-se e obstar à consecução dos objetivos da ação externa da União, enunciados no artigo 21.º do Tratado,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Representante Especial da União Europeia

1. O mandato de Michel Dominique REVEYRAND — DE MENTHON como REUE para o Sael é prorrogado até 31 de outubro de 2015. O mandato do REUE pode cessar antes dessa data, se o Conselho assim o decidir, por recomendação do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança (AR).
2. Para os efeitos do mandato do REUE, o Sael abrange o foco principal da Estratégia da UE para a Segurança e o Desenvolvimento do Sael («Estratégia»), a saber, o Burquina Faso, o Chade, o Mali, a Mauritânia e o Níger. Quanto às questões com implicações regionais mais vastas, o REUE colabora, conforme adequado, com outros países e com entidades regionais ou internacionais fora do Sael, situados também na África Ocidental e no Golfo da Guiné.
3. Tendo em vista a necessidade de uma abordagem regional dos desafios interligados que a região enfrenta, o REUE para o Sael trabalha em consulta estreita com outros/as REUE, incluindo o REUE para a região do Sul do Mediterrâneo, o REUE para os Direitos Humanos e o REUE junto da União Africana.

Artigo 2.º

Objetivos políticos

1. O mandato do REUE baseia-se no objetivo político da União relativamente ao Sael de contribuir ativamente para os esforços regionais e internacionais no sentido de alcançar paz, segurança e desenvolvimento duradouros na região. O REUE deve igualmente procurar aumentar a qualidade, a intensidade e o impacto do envolvimento multifacetado da União no Sael.
2. O REUE contribui para desenvolver e executar a abordagem da União, abrangendo todos os aspetos da ação da União, em especial nos domínios político, da segurança e do desenvolvimento, incluindo a Estratégia, e contribui também para coordenar todos os instrumentos relevantes para as ações da União.
3. É inicialmente dada prioridade ao Mali e às dimensões regionais do conflito nesse país.

⁽¹⁾ Decisão 2013/133/PESC do Conselho, de 18 de março de 2013, que nomeia o Representante Especial da União Europeia para o Sael (JO L 75 de 19.3.2013, p. 29).

⁽²⁾ Decisão 2014/130/PESC do Conselho, de 10 de março de 2014, que prorroga o mandato do Representante Especial da União Europeia para o Sael (JO L 71 de 12.3.2014, p. 14).

4. Quanto ao Mali, os objetivos políticos da UE visam, através da utilização coordenada e eficaz de todos os seus instrumentos, promover o regresso do Mali e do seu povo a um caminho de paz, reconciliação, segurança e desenvolvimento. Deve ser também dada a devida atenção ao Burquina Faso e ao Níger, em particular na perspetiva das eleições nesses países.

Artigo 3.º

Mandato

1. Para alcançar os objetivos políticos da União relativos ao Sael, o REUE tem por mandato:
 - a) Contribuir ativamente para a aplicação, coordenação e desenvolvimento da abordagem global da União em relação à crise regional, com base na sua Estratégia, com vista a reforçar a coerência e a eficácia globais das atividades da União no Sael, em especial no Mali;
 - b) Colaborar com todas as partes interessadas na região, governos, autoridades regionais, organizações regionais e internacionais, sociedade civil e diásporas, tendo em vista impulsionar os objetivos da União e contribuir para uma melhor compreensão do papel da União no Sael;
 - c) Representar a União nas instâncias regionais e internacionais relevantes, incluindo o grupo de apoio e acompanhamento da situação no Mali, e assegurar a visibilidade do apoio prestado pela União em matéria de gestão de crises e de prevenção de conflitos, incluindo a missão militar da União Europeia que tem em vista contribuir para a formação das Forças Armadas do Mali (EUTM Mali) e a missão PCSD da União Europeia no Níger (EUCAP SAEL Níger);
 - d) Manter uma estreita cooperação com as Nações Unidas, em particular com o Representante Especial do Secretário-Geral para a África Ocidental e com o Representante Especial do Secretário-Geral para o Mali, com a União Africana (UA), em especial com o Alto Representante da UA para o Mali e para o Sael, com a Comunidade Económica dos Estados da África Ocidental (CEDEAO) e com outros intervenientes nacionais, regionais e internacionais, incluindo outros Enviados Especiais para o Sael, bem como outros organismos relevantes para a zona do Magrebe;
 - e) Acompanhar de perto a dimensão regional e transfronteiras da crise, nomeadamente o terrorismo, o crime organizado, o contrabando de armas, o tráfico de pessoas, o tráfico de droga, os fluxos de refugiados e os fluxos migratórios, bem como os fluxos financeiros com eles relacionados; e contribuir, em estreita cooperação com o Coordenador da Luta contra o Terrorismo da UE, para o desenvolvimento da Estratégia Antiterrorista da UE;
 - f) Manter contactos regulares de alto nível com os países que, na região, são afetados pelo terrorismo e pelo crime internacional, a fim de assegurar uma abordagem coerente e global e de garantir o papel essencial da União nos esforços internacionais para combater o terrorismo e o crime internacional. Tal compreende o apoio ativo da União na criação de capacidades regionais no setor da segurança e também a garantia de que as causas profundas do terrorismo e do crime internacional no Sael são objeto de tratamento adequado;
 - g) Seguir de perto as consequências políticas e em matéria de segurança resultantes das crises humanitárias na região;
 - h) No que toca ao Mali, contribuir para os esforços regionais e internacionais destinados a facilitar a resolução da crise no Mali, em particular o pleno regresso à normalidade constitucional e à governabilidade em todo o território e um diálogo nacional credível e inclusivo visando uma resolução sustentável dos conflitos políticos;
 - i) Promover a criação de instituições, a reforma do setor da segurança e a promoção a longo prazo da paz e da reconciliação no Mali;
 - j) Contribuir para a aplicação na região da política da União em matéria de direitos humanos, em cooperação com o REUE para os Direitos Humanos, nomeadamente as Diretrizes da UE sobre os direitos humanos, em especial as Diretrizes da UE sobre as Crianças e os Conflitos Armados, bem como sobre a violência contra as mulheres e as jovens e o combate contra todas as formas de discriminação de que são vítimas, e da política da União sobre as Mulheres, a Paz e a Segurança, nomeadamente acompanhando a evolução da situação e dando informações, assim como formulando recomendações, a este respeito, e manter contactos regulares com as autoridades relevantes do Mali e da região, o gabinete do Procurador do Tribunal Penal Internacional, o gabinete do Alto-Comissário para os Direitos Humanos e defensores e observadores em matéria de direitos humanos na região;
 - k) Acompanhar e apresentar relatórios sobre o cumprimento das resoluções pertinentes do Conselho de Segurança das Nações Unidas (CSNU), nomeadamente as Resoluções 2056 (2012), 2071 (2012), 2085 (2012) e 2100 (2013) do CSNU.
2. Para efeitos do cumprimento do seu mandato, o REUE deve, nomeadamente:
 - a) Prestar aconselhamento e facultar informações sobre a definição das posições da União nas instâncias regionais e internacionais, conforme adequado, a fim de promover e reforçar proativamente a abordagem global por parte da em relação à crise no Sael;
 - b) Manter uma panorâmica geral das atividades da União e cooperar estreitamente com as delegações da União relevantes.

*Artigo 4.º***Execução do mandato**

1. O REUE é responsável pela execução do mandato, atuando sob a autoridade do AR.
2. O Comité Político e de Segurança (CPS) mantém uma relação privilegiada com o REUE, sendo o seu principal ponto de contacto com o Conselho. O CPS faculta orientação estratégica e direção política ao REUE no âmbito do seu mandato, sem prejuízo das responsabilidades do AR.
3. O REUE trabalha em estreita coordenação com o Serviço Europeu para a Ação Externa (SEAE) e os seus serviços competentes, em especial com o Coordenador para o Sael.

*Artigo 5.º***Financiamento**

1. O montante de referência financeira destinado a cobrir as despesas relativas ao mandato do REUE no período compreendido entre 1 de março de 2015 e 31 de outubro de 2015 é de 900 000 EUR.
2. As despesas são geridas de acordo com os procedimentos e as regras aplicáveis ao orçamento geral da União.
3. A gestão das despesas fica subordinada a um contrato entre o REUE e a Comissão. O REUE responde perante a Comissão por todas as despesas.

*Artigo 6.º***Constituição e composição da equipa**

1. Nos limites do seu mandato e dos correspondentes meios financeiros disponibilizados, o REUE é responsável pela constituição da sua equipa. A equipa deve dispor de conhecimentos especializados sobre questões específicas de política e segurança, em função das necessidades do mandato. O REUE informa prontamente o Conselho e a Comissão da composição da equipa.
2. Os Estados-Membros, as instituições da União e o SEAE podem propor o destacamento de pessoal para trabalhar com o REUE. A remuneração do pessoal destacado para trabalhar com o REUE fica a cargo do Estado-Membro ou da instituição da União em causa, ou do SEAE. Podem igualmente ser adstritos ao REUE peritos destacados pelos Estados-Membros para as instituições da União ou para o SEAE. O pessoal internacional contratado deve ter a nacionalidade de um dos Estados-Membros.
3. Todo o pessoal destacado permanece sob a autoridade administrativa do Estado-Membro de origem, da instituição da União de origem ou do SEAE, desempenhando as suas funções e agindo no interesse do mandato do REUE.
4. Os membros do pessoal que trabalha com o REUE ficam instalados nos serviços do SEAE ou nas delegações da União pertinentes, a fim de assegurarem a coerência das respetivas atividades.

*Artigo 7.º***Privilégios e imunidades do REUE e do seu pessoal**

Os privilégios, imunidades e outras garantias necessárias à realização e ao bom funcionamento da missão do REUE e dos membros do seu pessoal são estabelecidos de comum acordo com os países anfitriões, conforme adequado. Os Estados-Membros e o SEAE prestam todo o apoio necessário para o efeito.

*Artigo 8.º***Segurança das informações classificadas da UE**

O REUE e os membros da sua equipa devem respeitar os princípios e normas mínimas de segurança estabelecidos pela Decisão 2013/488/UE do Conselho ⁽¹⁾.

⁽¹⁾ Decisão 2013/488/UE do Conselho, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 274 de 15.10.2013, p. 1).

*Artigo 9.º***Acesso às informações e apoio logístico**

1. Os Estados-Membros, a Comissão, o SEAE e o Secretariado-Geral do Conselho asseguram que o REUE tenha acesso a todas as informações pertinentes.
2. As delegações da União e/ou os Estados-Membros, conforme adequado, prestam apoio logístico na região.

*Artigo 10.º***Segurança**

De acordo com a política da União em matéria de segurança do pessoal destacado no exterior da União, com funções operacionais, ao abrigo do Título V do Tratado, o REUE toma todas as medidas exequíveis, dentro do razoável, em conformidade com o seu mandato e com base na situação de segurança na zona geográfica sob a sua responsabilidade, para garantir a segurança de todo o pessoal sob a sua autoridade direta, nomeadamente:

- a) Define um plano de segurança específico, com base nas orientações do SEAE, incluindo medidas físicas, organizativas e processuais de segurança específicas, que se aplique à gestão das entradas do pessoal na zona geográfica e das deslocações deste no seu interior em condições de segurança, bem como à gestão dos incidentes de segurança, e que inclua um plano de emergência e de evacuação da missão;
- b) Assegura que todo o pessoal destacado no exterior da União se encontre coberto por um seguro de alto risco adequado às condições vigentes na zona geográfica;
- c) Assegura que a todos os membros da equipa destacados no exterior da União, incluindo o pessoal contratado no local, seja ministrada, antes ou aquando da sua chegada à zona geográfica, formação adequada em segurança com base no grau de risco atribuído a essa zona;
- d) Assegura a execução de todas as recomendações aprovadas de comum acordo na sequência de avaliações periódicas da situação de segurança e apresenta ao Conselho, ao AR e à Comissão relatórios escritos sobre essa execução e sobre outras questões de segurança no âmbito dos relatórios intercalares e do relatório sobre a execução do mandato.

*Artigo 11.º***Apresentação de relatórios**

1. O REUE apresenta periodicamente relatórios ao AR e ao CPS. Sempre que necessário, o REUE informa também os grupos de trabalho do Conselho. Os relatórios periódicos são distribuídos através da rede COREU. O REUE pode apresentar relatórios ao Conselho dos Negócios Estrangeiros. Nos termos do artigo 36.º do Tratado, o REUE pode ser associado à informação do Parlamento Europeu.
2. O REUE apresenta relatórios sobre a melhor forma de levar por diante as iniciativas da União, tal como o contributo desta para as reformas, incluindo os aspetos políticos dos projetos da União relevantes em matéria de desenvolvimento, em coordenação com as delegações da União na região.

*Artigo 12.º***Coordenação com outros intervenientes da União**

1. No âmbito da Estratégia o REUE contribui para a unidade, a coerência e a eficácia da ação política e diplomática da União e ajuda a assegurar que todos os instrumentos da União e as medidas dos Estados-Membros são mobilizados de forma coerente para alcançar os objetivos políticos da União.
2. As atividades do REUE são coordenadas com as das delegações da União e da Comissão, assim como com as de outros REUE que atuem na região. O REUE informa periodicamente as missões dos Estados-Membros e as delegações da União na região.
3. É mantida in loco uma ligação estreita com os chefes das delegações da União e os chefes de missão dos Estados-Membros. O REUE, em estreita coordenação com as delegações da União pertinentes, faculta orientações políticas, a nível local, aos chefes de missão da EUCAP SAEL Níger e da EUCAP SAEL Mali e ao Comandante da Missão da EUTM Mali. O REUE, o Comandante da Missão da EUTM Mali e o Comandante da Operação Civil da EUCAP SAEL Níger e da EUCAP SAEL Mali consultam-se na medida do necessário.

*Artigo 13.º***Reapreciação**

A execução da presente decisão e a sua coerência com outros contributos da União na região são periodicamente reapreciadas. O REUE apresenta ao Conselho, ao AR e à Comissão um relatório circunstanciado sobre a execução do mandato até ao final de agosto de 2015.

*Artigo 14.º***Entrada em vigor**

A presente decisão entra em vigor na data da sua adoção.

A presente decisão é aplicável a partir de 1 de março de 2015.

Feito em Bruxelas, em 16 de março de 2015.

Pelo Conselho

A Presidente

F. MOGHERINI

DECISÃO (PESC) 2015/440 DO CONSELHO
de 16 de março de 2015
que prorroga o mandato do Representante Especial da União Europeia para o Corno de África

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 33.º e o artigo 31.º, n.º 2,

Tendo em conta a proposta da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 8 de dezembro de 2011, o Conselho adotou a Decisão 2011/819/PESC ⁽¹⁾ que nomeia Alexander RONDOS Representante Especial da União Europeia (REUE) para o Corno de África. O mandato do REUE caduca em 28 de fevereiro de 2015.
- (2) O mandato do REUE deverá ser prorrogado até 31 de outubro de 2015.
- (3) O REUE cumprirá o seu mandato no contexto de uma situação que poderá vir a deteriorar-se e obstar à consecução dos objetivos da ação externa da União, enunciados no artigo 21.º do Tratado,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Representante Especial da União Europeia

O mandato de Alexander Rondos como REUE para o Corno de África é prorrogado até 31 de outubro de 2015. O Conselho pode decidir que o mandato do REUE cesse antes dessa data, com base numa avaliação do Comité Político e de Segurança (CPS) e sob proposta do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança (AR).

Para efeitos do mandato do REUE, entende-se que o Corno de África inclui a República do Jibuti, o Estado da Eritreia, a República Federal Democrática da Etiópia, a República do Quênia, a República Federal da Somália, a República do Sudão, a República do Sudão do Sul e a República do Uganda. Quanto às questões com implicações regionais mais vastas, o REUE colabora, se oportuno, com países e entidades regionais fora do Corno de África.

Artigo 2.º

Objetivos políticos

1. O mandato do REUE baseia-se nos objetivos políticos da União em relação ao Corno de África, tal como constam no seu quadro estratégico adotado em 14 de novembro de 2011 e em conclusões pertinentes do Conselho, a saber, contribuir ativamente para os esforços envidados a nível regional e internacional para alcançar a coexistência pacífica e a paz duradoura, a segurança e o desenvolvimento nos países da região e entre eles. O REUE deve igualmente procurar aumentar a qualidade, a intensidade, o impacto e a visibilidade do envolvimento multifacetado da União no Corno de África.
2. Os objetivos políticos incluem nomeadamente:
 - a) A continuação da estabilização na Somália, em especial do ponto de vista de uma dimensão regional;
 - b) A coexistência pacífica entre o Sudão e o Sudão do Sul como dois Estados viáveis e prósperos, dotados de estruturas políticas sólidas e responsáveis;
 - c) A resolução dos atuais conflitos e prevenção de conflitos potenciais nos países da região ou entre eles;
 - d) Apoio à cooperação regional no domínio político, económico e da segurança.

⁽¹⁾ Decisão 2011/819/PESC do Conselho, de 8 de dezembro de 2011, que nomeia o Representante Especial da União Europeia para o Corno de África (JO L 327 de 9.12.2011, p. 62).

Artigo 3.º

Mandato

1. Para alcançar os objetivos políticos da União relativos ao Corno de África, o REUE tem por mandato:
 - a) Colaborar com todas as partes interessadas na região, governos, autoridades regionais, organizações internacionais e regionais, sociedade civil e diásporas, tendo em vista promover os objetivos da União, e contribuir para um melhor conhecimento do papel da União na região;
 - b) Representar a União nas instâncias internacionais relevantes, conforme adequado, e assegurar a visibilidade do apoio por esta prestado no domínio da gestão de crises, bem como da resolução e prevenção de conflitos;
 - c) Incentivar e apoiar a cooperação os domínios político e da segurança e a integração económica efetivas na região através da parceria da União com a União Africana (UA) e as organizações regionais, nomeadamente a Autoridade Intergovernamental para o Desenvolvimento (IGAD);
 - d) Seguir a evolução política e contribuir para o desenvolvimento da política da União na região, nomeadamente no que respeita à Somália, Sudão, Sudão do Sul, à questão da fronteira Etiópia-Eritreia e à implementação do Acordo de Argel, à Iniciativa para a Bacia do Nilo e a outros problemas da região com impacto na sua segurança, estabilidade e prosperidade;
 - e) No que respeita à Somália, e trabalhando em estreita coordenação com o Enviado Especial da UE para a Somália e com os parceiros regionais e internacionais relevantes, incluindo o Representante Especial do Secretário-Geral das Nações Unidas para a Somália e a UA, contribuir ativamente para as ações e iniciativas conducentes a uma maior estabilização e a um regime de pós-transição para a Somália, com destaque para a promoção de uma abordagem internacional coordenada e coerente em relação à Somália, construindo boas relações de vizinhança e apoiando o desenvolvimento do setor da segurança na Somália, nomeadamente através da missão militar da União Europeia que tem em vista contribuir para a formação das Forças de Segurança da Somália (EUTM Somália), a força naval liderada pela União Europeia (EUNAVFOR Atalanta), a Missão da União Europeia sobre a Capacidade Regional Marítima no Corno de África (EUCAP NESTOR) e do apoio continuado da União à Missão da União Africana na Somália (AMISOM), e trabalhar em estreita colaboração com os Estados-Membros;
 - f) No que diz respeito ao Sudão e ao Sudão do Sul, e trabalhando em estreita coordenação com os respetivos chefes das delegações da União, contribuir para a coerência e eficácia da política da União para o Sudão e o Sudão do Sul e apoiar a coexistência pacífica entre estes dois países, nomeadamente através da implementação dos Acordos de Addis Abeba e da resolução das questões pendentes na sequência do Acordo de Paz Global, incluindo a questão de Abyei, soluções políticas para os atuais conflitos, em especial no Darfur, no Kordofan do Sul e no Nilo Azul, o reforço das instituições no Sudão do Sul e a reconciliação nacional. A este respeito, o REUE contribuirá para uma abordagem internacional coerente em estreita cooperação com a UA e em especial com o Painel de Implementação de Alto Nível para o Sudão da UA (AUHIP), as Nações Unidas e outros intervenientes regionais e internacionais importantes;
 - g) Acompanhar os desafios transfronteiriços que afetam o Corno de África, nomeadamente o terrorismo, a radicalização, a segurança marítima e a pirataria, a criminalidade organizada, o contrabando de armas, os fluxos de refugiados e os fluxos migratórios e as eventuais consequências políticas e de segurança das crises humanitárias;
 - h) Promover o acesso humanitário a toda a região;
 - i) Contribuir para a aplicação da Decisão 2011/168/PESC do Conselho ⁽¹⁾ e da política da União em matéria de direitos humanos em cooperação com o REUE para os Direitos Humanos, incluindo as Diretrizes da UE nessa matéria, em especial as Diretrizes da UE sobre as crianças e os conflitos armados, bem como as Diretrizes da UE sobre a violência contra as mulheres e as raparigas e o combate a todas as formas de discriminação de que são vítimas, e da política da União no que diz respeito à Resolução 1325 (2000) do Conselho de Segurança das Nações Unidas em prol das mulheres, da paz e da segurança, nomeadamente acompanhando o evoluir da situação, dando informações e formulando recomendações a este respeito.
2. Para efeitos do cumprimento do mandato, o REUE deve, nomeadamente:
 - a) Prestar aconselhamento e facultar informações sobre a definição das posições da União nas instâncias internacionais, conforme adequado, a fim de promover proativamente a abordagem política global da União em relação ao Corno de África;
 - b) Manter-se a par de todas as atividades da União.

⁽¹⁾ Decisão 2011/168/PESC do Conselho, de 21 de março de 2011, sobre o Tribunal Penal Internacional e que revoga a Posição Comum 2003/444/PESC (JO L 76 de 22.3.2011, p. 56).

*Artigo 4.º***Execução do mandato**

1. O REUE é responsável pela execução do mandato, agindo sob a autoridade do AR.
2. O CPS mantém uma relação privilegiada com o REUE, sendo o seu principal ponto de contacto com o Conselho. O CPS faculta orientação estratégica e direção política ao REUE no âmbito do mandato, sem prejuízo das competências do AR.
3. O REUE trabalha em estreita coordenação com o Serviço Europeu para a Ação Externa (SEAE) e com os seus serviços competentes, com as delegações da União na região e com a Comissão.

*Artigo 5.º***Financiamento**

1. O montante de referência financeira destinado a cobrir as despesas relativas ao mandato do REUE no período compreendido entre 1 de março de 2015 e 31 de outubro de 2015 é de 1 770 000 EUR.
2. As despesas são geridas de acordo com os procedimentos e as regras aplicáveis ao orçamento geral da União.
3. A gestão das despesas fica subordinada a um contrato entre o REUE e a Comissão. O REUE responde perante a Comissão por todas as despesas.

*Artigo 6.º***Constituição e composição da equipa**

1. Nos limites do seu mandato e dos correspondentes meios financeiros disponibilizados, o REUE é responsável pela constituição da sua equipa. A equipa deve dispor de conhecimentos especializados sobre questões específicas de política e segurança, em função das necessidades do mandato. O REUE informa pronta e regularmente o Conselho e a Comissão da composição da sua equipa.
2. Os Estados-Membros, as instituições da União e o SEAE podem propor o destacamento de pessoal para trabalhar com o REUE. A remuneração do pessoal destacado fica a cargo, respetivamente, do Estado-Membro, da instituição da União em causa ou do SEAE. Podem igualmente ser adstritos ao REUE peritos destacados pelos Estados-Membros para as instituições da União ou para o SEAE. O pessoal internacional contratado deve ter a nacionalidade de um dos Estados-Membros.
3. Todo o pessoal destacado fica sob a autoridade administrativa do Estado-Membro de origem, da instituição da União de origem ou do SEAE, desempenhando as suas funções e agindo no interesse do mandato do REUE.
4. Os membros do pessoal que trabalha com o REUE ficam instalados nos serviços do SEAE ou nas delegações da União relevantes, a fim de assegurarem a coerência das respetivas atividades.

*Artigo 7.º***Privilégios e imunidades do REUE e do seu pessoal**

Os privilégios, imunidades e outras garantias necessárias à realização e ao bom funcionamento da missão do REUE e do seu pessoal são estabelecidos de comum acordo com os países anfitriões, conforme adequado. Os Estados-Membros e o SEAE prestam todo o apoio necessário para o efeito.

*Artigo 8.º***Segurança das informações classificadas da UE**

O REUE e os membros da sua equipa devem respeitar os princípios e normas mínimas de segurança estabelecidos pela Decisão 2013/488/UE do Conselho ⁽¹⁾.

⁽¹⁾ Decisão 2013/488/UE do Conselho, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 274 de 15.10.2013, p. 1).

Artigo 9.º**Acesso às informações e apoio logístico**

1. Os Estados-Membros, a Comissão, o SEAE e o Secretariado-Geral do Conselho asseguram que o REUE tenha acesso a todas as informações pertinentes.
2. As delegações da União na região e os Estados-Membros, conforme adequado, prestam apoio logístico na região.

Artigo 10.º**Segurança**

De acordo com a política da União em matéria de segurança do pessoal destacado no exterior da União, com funções operacionais, ao abrigo do Título V do Tratado, o REUE toma todas as medidas exequíveis, dentro do razoável, em conformidade com o seu mandato e com a situação de segurança na zona geográfica sob a sua responsabilidade, para garantir a segurança de todo o pessoal sob a sua autoridade direta, nomeadamente:

- a) Definem um plano de segurança específico da sua missão, com base nas orientações do SEAE, incluindo medidas físicas, organizativas e processuais de segurança específicas da missão, que se aplique à gestão das entradas do pessoal na zona geográfica e das deslocações deste no seu interior em condições de segurança, bem como à gestão dos incidentes de segurança, e que inclua um plano de emergência e um plano de evacuação da missão;
- b) Assegura que todo o pessoal destacado no exterior da União se encontre coberto por um seguro de alto risco adequado às condições vigentes na zona da missão;
- c) Assegura que a todos os membros da sua equipa destacados no exterior da União, incluindo o pessoal contratado no local, seja ministrada, antes ou aquando da sua chegada à zona da missão, formação adequada em segurança com base no grau de risco atribuído à zona da missão pelo SEAE;
- d) Assegura a execução de todas as recomendações aprovadas de comum acordo na sequência de avaliações periódicas da situação de segurança e apresenta ao Conselho, ao AR e à Comissão relatórios escritos sobre essa execução e sobre outras questões de segurança no âmbito dos relatórios intercalares e sobre a execução do mandato.

Artigo 11.º**Apresentação de relatórios**

1. O REUE apresenta periodicamente relatórios orais e escritos ao AR e ao CPS. Sempre que necessário, o REUE informa também os grupos de trabalho do Conselho. Os relatórios periódicos são distribuídos através da rede COREU. O REUE pode apresentar relatórios ao Conselho dos Negócios Estrangeiros. Nos termos do artigo 36.º do Tratado, o REUE pode ser associado à informação do Parlamento Europeu.
2. O REUE apresenta relatórios sobre a melhor forma de levar por diante as iniciativas da União, tal como o contributo desta para as reformas, incluindo sobre os aspetos políticos dos projetos da União relevantes em matéria de desenvolvimento, em coordenação com as delegações da União na região.

Artigo 12.º**Coordenação**

1. O REUE contribui para a unidade, a coerência e a eficácia das ações da União e ajuda a assegurar que todos os instrumentos da União e as medidas dos Estados-Membros são mobilizados de forma coerente para alcançar os objetivos políticos da União. As atividades do REUE são coordenadas com as das delegações da União e da Comissão. O REUE informa periodicamente as missões dos Estados-Membros e as delegações da União na região.
2. É mantida *in loco* uma ligação estreita com os chefes das delegações da União e os chefes das missões dos Estados-Membros. Estes envidam todos os esforços para apoiar o REUE na execução do mandato. O REUE, em estreita coordenação com as delegações da União pertinentes, faculta orientações políticas, a nível local, ao Comandante da Força EUNAVFOR Atalanta, ao Comandante da Missão EUTM Somália e ao Chefe de Missão da EUCAP NESTOR. O REUE, os comandantes das operações da UE e o Comandante da Operação Civil consultam-se na medida do necessário.

3. O REUE trabalha em estreita cooperação com as autoridades dos países envolvidos, as Nações Unidas, a UA, a IGAD e outros intervenientes nacionais, regionais e internacionais e também com a sociedade civil da região.

Artigo 13.º

Reapreciação

A execução da presente decisão e a sua coerência com outros contributos da União na região são periodicamente reapreciadas. O REUE apresenta ao Conselho, ao AR e à Comissão um relatório circunstanciado sobre a execução do mandato até 31 de agosto de 2015.

Artigo 14.º

Entrada em vigor

A presente decisão entra em vigor na data da sua adoção.

A presente decisão é aplicável a partir de 1 de março de 2015.

Feito em Bruxelas, em 16 de março de 2015.

Pelo Conselho

A Presidente

F. MOGHERINI

DECISÃO (PESC) 2015/441 DO CONSELHO**de 16 de março de 2015****que altera e prorroga a Decisão 2010/96/PESC, relativa a uma missão militar da União Europeia que tem em vista contribuir para a formação das Forças de Segurança da Somália**

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 42.º, n.º 4, e o artigo 43.º, n.º 2,

Tendo em conta a proposta da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 15 de fevereiro de 2010, o Conselho adotou a Decisão 2010/96/PESC ⁽¹⁾. O mandato da missão militar da UE termina em 31 de março de 2015.
- (2) A Conferência de Bruxelas sobre a Somália, que teve lugar a 16 de setembro de 2013, esteve na base da elaboração do Pacto sobre a Somália e desencadeou um mecanismo de coordenação e de apropriação por parte da Somália graças à ação do grupo de trabalho «Novo Pacto» para a Somália.
- (3) Durante a reunião internacional coorganizada pelo Reino Unido e pela Somália, que teve lugar em Londres a 18 de setembro de 2014, o Governo Federal traçou as grandes linhas a seguir pelo Ministério da Defesa com vista ao desenvolvimento do Exército Nacional da Somália até 2019 e definiu as suas necessidades imediatas.
- (4) Na sequência da Revisão Estratégica de outubro de 2014, o mandato da missão militar da UE deverá ser prorrogado até 31 de dezembro de 2016.
- (5) Nos termos do artigo 5.º do Protocolo N.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na elaboração nem na execução de decisões e ações da União com implicações em matéria de defesa. A Dinamarca não participa na execução da presente decisão, não contribuindo, por conseguinte, para o financiamento desta missão.
- (6) O mandato da missão militar da UE deverá ser novamente prorrogado e adaptado,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

A Decisão 2010/96/PESC é alterada do seguinte modo:

- 1) No artigo 1.º, o n.º 2 passa a ter a seguinte redação:

«2. Tendo em vista a consecução dos objetivos estabelecidos no n.º 1, a missão militar da UE é projetada na Somália a fim de, por um lado, contribuir para o reforço das capacidades institucionais no setor da defesa graças à prestação de aconselhamento estratégico e, por outro, prestar apoio direto ao Exército Nacional da Somália através de formação, aconselhamento e enquadramento. A missão militar da UE fica também pronta a prestar apoio, dentro dos seus meios e capacidades, a outros intervenientes da União na execução dos respetivos mandatos no domínio da segurança e da defesa na Somália.».

- 2) O artigo 3.º passa a ter a seguinte redação:

«Artigo 3.º

Designação do Quartel-General da Missão

1. O Quartel-General da Missão fica localizado no aeroporto internacional de Mogadixo, em Mogadixo. Desempenha as funções de Quartel-General de Operações e de Quartel-General da Força.
2. O Quartel-General da Missão inclui um gabinete de ligação e de apoio em Nairobi e uma célula de apoio em Bruxelas.».

⁽¹⁾ Decisão 2010/96/PESC do Conselho, de 15 de fevereiro de 2010, relativa a uma missão militar da União Europeia que tem em vista contribuir para a formação das Forças de Segurança da Somália (JO L 44 de 19.2.2010, p. 16).

3) No artigo 7.º, o n.º 4 passa a ter a seguinte redação:

«4. A missão militar da UE atua, na medida dos seus meios e capacidades, em estreita cooperação com outros intervenientes internacionais na região, em particular as Nações Unidas e a AMISOM, em consonância com os requisitos acordados pelo Governo Federal da Somália.»

4) No artigo 10.º, é inserido o seguinte número:

«5. O montante de referência financeira para os custos comuns da missão militar da UE durante o período compreendido entre 1 de abril de 2015 e 31 de dezembro de 2016 é de 17 507 399 EUR. A percentagem do montante de referência a que se refere o artigo 25.º, n.º 1, do ATHENA é fixada em 30 % e a percentagem para autorizações a que se refere o artigo 32.º, n.º 3, do ATHENA é fixada em 90 %.»

5) É inserido o seguinte artigo:

«Artigo 10.º-B

Célula de projetos

1. A missão militar da UE dispõe de uma célula de projetos para a definição e execução de projetos, a financiar pelos Estados-Membros ou por Estados terceiros que sejam consentâneos com os objetivos da missão e contribuam para a realização do seu mandato.

2. Sob reserva do n.º 3, o Comandante da Missão da UE fica autorizado a recorrer a contribuições financeiras dos Estados-Membros ou de Estados terceiros para executar projetos identificados como complemento coerente das demais ações da missão militar da UE. Nesse caso, o Comandante da Missão da UE celebra com esses Estados convênios que regulem, nomeadamente, os procedimentos específicos para a resposta às queixas apresentadas por terceiros por prejuízos sofridos em resultado de atos ou omissões do Comandante da Missão da UE na utilização dos fundos disponibilizados por esses Estados.

Em caso algum podem os Estados contribuintes invocar a responsabilidade da União ou do AR por atos ou omissões do Comandante da Missão da UE na utilização dos fundos disponibilizados pelos referidos Estados.

3. O CPS dá o seu acordo à aceitação de uma contribuição financeira de Estados terceiros para a célula de projetos.»

6) O artigo 11.º é alterado do seguinte modo:

a) No n.º 1, o trecho introdutório passa a ter a seguinte redação: «O AR fica autorizado a comunicar aos Estados terceiros associados à presente decisão, quando adequado e em função das necessidades da Missão, informações e documentos classificados da UE que sejam elaborados para efeitos da Missão, nos termos da Decisão 2013/488/UE do Conselho (*):

(*) Decisão 2013/488/UE do Conselho, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 274 de 15.10.2013, p. 1).»;

b) Nos n.ºs 2 e 3, a referência à «Decisão 2011/292/UE» é substituída pela referência à «Decisão 2013/488/UE do Conselho».

7) No artigo 12.º, os n.ºs 2 e 3 passam a ter a seguinte redação:

«2. O mandato da missão militar da UE cessa em 31 de dezembro de 2016.

3. A presente decisão é revogada a partir da data de encerramento do Quartel-General da UE, do gabinete de ligação e apoio em Nairobi e da célula de apoio em Bruxelas, de acordo com o planeamento aprovado para o termo da missão militar da UE e sem prejuízo dos procedimentos estabelecidos no mecanismo ATHENA relativamente à auditoria e à apresentação das contas da missão militar da UE.»

Artigo 2.º

A presente decisão entra em vigor na data da sua adoção.

A presente decisão é aplicável a partir de 1 de abril de 2015.

Feito em Bruxelas, em 16 de março de 2015.

Pelo Conselho

A Presidente

F. MOGHERINI

DECISÃO (PESC) 2015/442 DO CONSELHO**de 16 de março de 2015****que lança a Missão de Aconselhamento Militar PCSD da União Europeia na República Centro-Africana (EUMAM RCA) e que altera a Decisão (PESC) 2015/78**

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 42.º, n.º 4, e o artigo 43.º, n.º 2,

Tendo em conta a Decisão (PESC) 2015/78 do Conselho, de 19 de janeiro de 2015, relativa a uma Missão de Aconselhamento Militar PCSD da União Europeia na República Centro-Africana (EUMAM RCA) ⁽¹⁾, nomeadamente o artigo 4.º,

Tendo em conta a proposta da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 19 de janeiro de 2015, o Conselho adotou a Decisão (PESC) 2015/78.
- (2) Em 9 de fevereiro de 2015, o Conselho aprovou as Regras de Empenhamento da EUMAM RCA.
- (3) Em 6 de março de 2015, o Conselho aprovou o Plano de Missão da EUMAM RCA.
- (4) Em 11 de março de 2015, o Comité Político e de Segurança congratulou-se com a carta do Comandante de Missão relativa à recomendação de ser lançada a EUMAM RCA e ao calendário previsto para ser declarada a Capacidade Operacional Inicial da EUMAM RCA.
- (5) A EUMAM RCA deverá ser lançada em 16 de março de 2015.
- (6) Nos termos do artigo 5.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na elaboração nem na execução de decisões e ações da União com implicações em matéria de defesa. Consequentemente, a Dinamarca não participa na execução da presente decisão, pelo que não participa no financiamento da presente missão,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

A Missão de Aconselhamento Militar PCSD da União Europeia na República Centro-Africana («EUMAM RCA») é lançada em 16 de março de 2015.

Artigo 2.º

O Comandante de Missão da UE da EUMAM RCA fica autorizado, com efeitos imediatos, a dar início à execução da missão.

Artigo 3.º

No artigo 4.º da Decisão (PESC) 2015/78, o n.º 2 passa a ter a seguinte redação:

- «2. A EUMAM RCA é lançada por uma decisão do Conselho na data recomendada pelo Comandante de Missão, após a aprovação do Plano da Missão e, se necessário, de Regras de Empenhamento adicionais.».

⁽¹⁾ JO L 13 de 20.1.2015, p. 8.

Artigo 4.º

A presente decisão entra em vigor no dia da sua adoção.

Feito em Bruxelas, em 16 de março de 2015.

Pelo Conselho
A Presidente
F. MOGHERINI

DECISÃO (UE, Euratom) 2015/443 DA COMISSÃO**de 13 de março de 2015****relativa à segurança na Comissão**

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 249.º,

Tendo em conta o Tratado que institui a Comunidade Europeia da Energia Atómica,

Tendo em conta o Protocolo n.º 7 relativo aos Privilégios e Imunidades da União Europeia anexo aos Tratados, nomeadamente o artigo 18.º,

Considerando o seguinte:

- (1) O objetivo de segurança na Comissão é permitir a esta instituição funcionar num ambiente seguro e protegido através do estabelecimento de uma abordagem coerente e integrada no que diz respeito à sua segurança, oferecendo níveis adequados de proteção de pessoas, bens e informações que sejam proporcionais aos riscos identificados, e garantindo uma execução eficiente e atempada da segurança.
- (2) A Comissão, à semelhança de outros organismos internacionais, enfrenta ameaças e desafios importantes no domínio da segurança, em especial no que se refere ao terrorismo, aos ciberataques e à espionagem política e comercial.
- (3) A Comissão Europeia celebrou acordos em matéria de segurança para as suas localizações principais com os governos da Bélgica, do Luxemburgo e de Itália ⁽¹⁾. Estes instrumentos confirmam que a Comissão é responsável pela sua segurança.
- (4) A fim de assegurar a segurança de pessoas, bens e informações, a Comissão pode precisar de tomar medidas em domínios protegidos pelos direitos fundamentais, conforme consagrados na Carta dos Direitos Fundamentais e na Convenção Europeia dos Direitos do Homem, tal como reconhecidos pelo Tribunal de Justiça da União Europeia.
- (5) Por conseguinte, importa que essas medidas sejam justificadas pela importância dos interesses que visam proteger, sejam proporcionadas e garantam o pleno respeito dos direitos fundamentais, em especial dos direitos à vida privada e à proteção de dados.
- (6) No âmbito de um sistema empenhado no Estado de direito e no respeito dos direitos fundamentais, a Comissão tem de envidar todos os esforços para obter um nível de segurança apropriado para o seu pessoal, bens e informações que assegure o bom desempenho das suas funções, sem limitar os direitos fundamentais além do estritamente necessário.
- (7) A segurança na Comissão baseia-se nos princípios da legalidade, da transparência, da proporcionalidade e da responsabilização.
- (8) O pessoal mandatado para tomar medidas de segurança não deve ser prejudicado pelas suas ações, a menos que tenha agido fora do âmbito do seu mandato ou em violação da lei; em consequência, a presente decisão será considerada a este respeito como uma ordem de serviço na aceção do Estatuto dos Funcionários.
- (9) A Comissão deve adotar medidas apropriadas que promovam e reforcem a sua cultura de segurança, garantindo uma execução mais eficiente da segurança, melhorando a governação da segurança, intensificando as redes e a cooperação com as autoridades competentes aos níveis internacional, europeu e nacional, e melhorando o acompanhamento e o controlo da aplicação de medidas de segurança.
- (10) A criação do Serviço Europeu para a Ação Externa (SEAE) enquanto órgão da União Europeia funcionalmente autónomo teve um impacto significativo nos interesses de segurança da Comissão, exigindo assim que as normas e os procedimentos de cooperação relativos à proteção e à segurança sejam estabelecidos pelo SEAE e pela Comissão, em especial no que respeita ao cumprimento do dever de diligência da Comissão para o seu pessoal nas delegações da União.

⁽¹⁾ Cf. os seguintes acordos: *Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité*, de 31 de dezembro de 2004, *Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois*, de 20 de janeiro de 2007, e *Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerca nucleari di competenza generale*, de 22 de julho de 1959.

- (11) A execução da política de segurança da Comissão deve ser coerente com outros procedimentos internos que possam implicar elementos de segurança, em particular com a gestão da continuidade das atividades (que visa preservar as funções críticas da Comissão em caso de perturbação operacional) e o processo ARGUS para a coordenação de crises multisectoriais.
- (12) Não obstante as medidas em vigor no momento da adoção da presente decisão e notificadas à Autoridade Europeia para a Proteção de Dados ⁽¹⁾, todas as medidas da mesma que impliquem o tratamento de dados pessoais ficam sujeitas a regras de execução nos termos do artigo 21.º, as quais devem estabelecer garantias adequadas aos titulares dos dados.
- (13) Por conseguinte, é necessário que a Comissão reveja, atualize e consolide a atual regulamentação relativa à segurança na Comissão.
- (14) A Decisão(94) 2129 da Comissão ⁽²⁾ deve, assim, ser revogada,

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

DISPOSIÇÕES GERAIS

Artigo 1.º

Definições

Para efeitos da presente decisão, são aplicáveis as seguintes definições:

- 1) «Bens», todos os bens móveis e imóveis e todos os haveres da Comissão;
- 2) «Serviço da Comissão», uma direção-geral ou um serviço da Comissão, ou um gabinete de um membro da Comissão;
- 3) «Sistema de comunicação e informação» ou «SCI», todos os sistemas que permitam o manuseamento de informações em formato eletrónico, incluindo todos os meios necessários ao seu funcionamento, bem como as infraestruturas, a organização, o pessoal e os recursos de informação;
- 4) «Controlo dos riscos», todas as medidas de segurança razoavelmente suscetíveis de controlar efetivamente um risco de segurança através da sua prevenção, atenuação, anulação ou transferência;
- 5) «Situação de crise», uma circunstância, acontecimento, incidente ou emergência (ou uma sucessão ou combinação deles) que represente uma ameaça grave ou imediata à segurança na Comissão, independentemente da sua origem;
- 6) «Dados», informações em formato que permita a sua comunicação, registo ou tratamento;
- 7) «Membro da Comissão responsável pela segurança», um membro da Comissão que detém autoridade sobre a Direção-Geral dos Recursos Humanos e da Segurança;
- 8) «Dados pessoais», dados pessoais na aceção do artigo 2.º, alínea a), do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho ⁽³⁾;
- 9) «Instalações», todos os imóveis ou bens e haveres equiparados da Comissão;
- 10) «Prevenção de riscos», medidas de segurança suscetíveis de prevenir, atrasar ou impedir um risco de segurança;
- 11) «Risco de segurança», a combinação do nível de ameaça, do nível de vulnerabilidade e do possível impacto de um dado evento;
- 12) «Segurança na Comissão», a segurança de pessoas, bens e informações na Comissão, em particular a integridade física de pessoas e bens, a integridade, a confidencialidade e a disponibilidade das informações e dos sistemas de comunicação e informação, bem como o desempenho sem entraves das funções da Comissão;

⁽¹⁾ DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

⁽²⁾ Decisão C(94) 2129 da Comissão, de 8 de setembro de 1994, sobre as funções do Serviço de Segurança.

⁽³⁾ Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

- 13) «Medida de segurança», todas as medidas tomadas em conformidade com a presente decisão para fins de controlo de riscos de segurança;
- 14) «Estatuto», o Estatuto dos Funcionários da União Europeia, estabelecido pelo Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho ⁽¹⁾ e respetivas alterações;
- 15) «Ameaça à segurança», um acontecimento ou agente que, na ausência de reação ou controlo, seja razoavelmente suscetível de prejudicar a segurança;
- 16) «Ameaça imediata à segurança», uma ameaça à segurança que ocorra sem aviso prévio ou com um aviso prévio extremamente curto;
- 17) «Ameaça grave à segurança», uma ameaça à segurança razoavelmente suscetível de provocar mortes, ferimentos ou danos graves, prejuízos materiais importantes, comprometimentos de informações altamente sensíveis, bem como perturbações dos sistemas informáticos ou das capacidades operacionais essenciais da Comissão;
- 18) «Vulnerabilidade», insuficiência de qualquer natureza razoavelmente suscetível de prejudicar a segurança na Comissão, quando potenciada por uma ou mais ameaças.

Artigo 2.º

Objeto

1. A presente decisão estabelece os objetivos, os princípios de base, a organização e as responsabilidades relativas à segurança na Comissão.
2. A presente decisão é aplicável a todos os serviços e em todas as instalações da Comissão. O pessoal da Comissão que trabalha nas delegações da União está sujeito às regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa ⁽²⁾.
3. Sem prejuízo de indicações específicas relativas a determinados grupos de pessoal, a presente decisão é aplicável aos membros da Comissão, ao pessoal da Comissão abrangido pelo âmbito de aplicação do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União, aos peritos nacionais destacados na Comissão (PND), aos prestadores de serviços e seu pessoal, aos estagiários e a todas as pessoas que tenham acesso aos edifícios ou a outros bens da Comissão, ou a informações manuseadas pela Comissão.
4. As disposições da presente decisão não prejudicam a Decisão 2002/47/CE, CECA, Euratom, da Comissão ⁽³⁾, a Decisão 2004/563/CE, CECA, Euratom, da Comissão ⁽⁴⁾, a Decisão C (2006) 1623 ⁽⁵⁾ da Comissão e a Decisão C (2006) 3602 da Comissão ⁽⁶⁾.

CAPÍTULO 2

PRINCÍPIOS

Artigo 3.º

Princípios da segurança na Comissão

1. Ao executar a presente decisão, a Comissão deve respeitar os Tratados e, em especial, a Carta dos Direitos Fundamentais e o Protocolo n.º 7 relativo aos Privilégios e Imunidades da União Europeia, os instrumentos referidos no considerando 2, as regras de direito nacional aplicáveis, bem como os termos da presente decisão. Se necessário, devem ser emitidas indicações de segurança na aceção do artigo 21.º, n.º 2, fornecendo orientações a este respeito.
2. A segurança na Comissão baseia-se nos princípios da legalidade, da transparência, da proporcionalidade e da responsabilização.
3. O princípio da legalidade indica a necessidade de executar a presente decisão no estrito respeito do seu quadro jurídico, bem como a necessidade de respeitar os seus requisitos legais.

⁽¹⁾ Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho, de 29 de fevereiro de 1968, que fixa o Estatuto dos Funcionários das Comunidades Europeias assim como o Regime aplicável aos outros agentes destas Comunidades, e institui medidas especiais temporariamente aplicáveis aos funcionários da Comissão (Regime aplicável aos outros agentes) (JO L 56 de 4.3.1968, p. 1).

⁽²⁾ Decisão da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança (2013/C 190/01), de 19 de abril de 2013, relativa às regras de segurança aplicáveis ao Serviço Europeu para a Ação Externa (JO C 190 de 29.6.2013, p. 1).

⁽³⁾ Decisão 2002/47/CE, CECA, Euratom, da Comissão, de 23 de janeiro de 2002, que altera o seu regulamento interno (JO L 21 de 24.1.2002, p. 23), anexando-lhe as disposições sobre gestão de documentos.

⁽⁴⁾ Decisão 2004/563/CE, Euratom da Comissão, de 7 de julho de 2004, que altera o seu Regulamento Interno (JO L 251 de 27.7.2004, p. 9), anexando-lhe as disposições relativas aos documentos eletrónicos e digitalizados.

⁽⁵⁾ C (2006) 1623, de 21 de abril de 2006, que estabelece uma política harmonizada em matéria de saúde e segurança no trabalho para todo o pessoal da Comissão Europeia.

⁽⁶⁾ C (2006) 3602, de 16 de agosto de 2006, relativa à segurança dos sistemas de informação utilizados pelos serviços da Comissão.

4. Todas as medidas de segurança devem ser tomadas abertamente, a menos que tal seja suscetível de comprometer o seu efeito. Os destinatários das medidas de segurança devem ser previamente informados da fundamentação e do impacto das mesmas, a menos que tal seja suscetível de comprometer o seu efeito. Nesse caso, os destinatários devem ser informados depois de cessar o risco de comprometer o efeito das medidas de segurança.
5. Os serviços da Comissão devem garantir que as questões de segurança são tidas em conta no início da elaboração e da execução de políticas, decisões, programas, projetos e atividades da Comissão pelos quais sejam responsáveis. Para o efeito, devem envolver na fase mais precoce da sua preparação a Direção-Geral dos Recursos Humanos e da Segurança em geral, e o Diretor da Segurança das Informações da Comissão no que respeita aos sistemas informáticos.
6. Quando apropriado, a Comissão procura cooperar com as autoridades competentes do Estado anfitrião ou de outros Estados-Membros e, quando tal for exequível, com outras instituições, agências ou organismos da UE, levando em consideração as medidas tomadas ou previstas pelas referidas autoridades para fazer face ao risco de segurança em causa.

Artigo 4.º

Obrigações de cumprimento

1. É obrigatório cumprir a presente decisão e as suas regras de execução, bem como as medidas de segurança e as instruções dadas pelo pessoal mandatado.
2. O incumprimento das regras de segurança está sujeito a sanções disciplinares nos termos dos Tratados e do Estatuto, bem como a sanções contratuais e/ou ação judicial ao abrigo da legislação e regulamentação nacionais.

CAPÍTULO 3

GARANTIR A SEGURANÇA

Artigo 5.º

Pessoal mandatado

1. Apenas podem ser atribuídas a pessoal autorizado, com base num mandato nominativo conferido pelo Diretor-Geral dos Recursos Humanos e da Segurança e tendo em conta as suas funções atuais, as competências para tomar uma ou várias das seguintes medidas:
 - (1) Ser portador de armas pessoais;
 - (2) Conduzir inquéritos de segurança, conforme referido no artigo 13.º;
 - (3) Tomar as medidas de segurança indicadas no artigo 12.º, conforme especificado no mandato.
2. Os mandatos referidos no n.º 1 são conferidos por um período que não ultrapasse a duração do cargo ou função da pessoa em causa no âmbito do qual lhe foi conferido o mandato, e em conformidade com as disposições aplicáveis indicadas no artigo 3.º, n.º 1.
3. No que respeita ao pessoal mandatado, a presente decisão constitui uma ordem de serviço na aceção do artigo 21.º do Estatuto.

Artigo 6.º

Disposições gerais sobre as medidas de segurança

1. Ao tomar medidas de segurança, a Comissão deve, em especial, assegurar, tanto quanto for razoavelmente possível, que:
 - a) Só procura apoio ou assistência do Estado em causa se esse Estado for um Estado-Membro da União Europeia ou, não sendo o caso, se for parte na Convenção Europeia dos Direitos do Homem, ou ainda se garantir direitos que sejam no mínimo equivalentes aos direitos garantidos nessa convenção.
 - b) Só pode transferir informações sobre uma pessoa a destinatários, que não sejam das instituições e órgãos comunitários, que não estejam sujeitos à legislação nacional adotada nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho ⁽¹⁾, em conformidade com o artigo 9.º do Regulamento (CE) n.º 45/2001.

⁽¹⁾ Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

- c) Caso uma pessoa constitua uma ameaça à segurança, as medidas de segurança devem ser dirigidas contra essa pessoa, que pode estar sujeita a suportar os custos incorridos. Essas medidas de segurança só podem ser dirigidas contra outras pessoas se uma ameaça imediata ou grave à segurança tiver de ser controlada e se estiverem preenchidas as seguintes condições:
- a) As medidas previstas contra a pessoa que coloque uma ameaça à segurança não podem ser tomadas ou não é provável que sejam eficazes;
 - b) A Comissão não pode controlar a ameaça à segurança com as suas próprias medidas, ou não pode fazê-lo atempadamente;
 - c) A medida não constitui um perigo desproporcionado para a outra pessoa e os seus direitos.
2. A Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança deve elaborar uma síntese das medidas de segurança passíveis de exigir uma decisão de um juiz, em conformidade com a legislação e regulamentação dos Estados-Membros que acolham instalações da Comissão.
3. A Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança pode recorrer a contratantes para que desempenhem, sob a sua direção e supervisão, funções relacionadas com a segurança.

Artigo 7.º

Medidas de segurança relativas às pessoas

1. É prestado um nível adequado de proteção das pessoas nas instalações da Comissão, que tenha em conta os requisitos de segurança e proteção.
2. Em caso de risco grave de segurança, a Direção-Geral dos Recursos Humanos e da Segurança deve assegurar a proteção pessoal dos membros da Comissão ou de outros agentes, caso uma avaliação da ameaça tenha indicado que essa proteção é necessária para garantir a sua segurança.
3. Em caso de risco grave de segurança, a Comissão pode ordenar a evacuação das suas instalações.
4. As vítimas de acidentes ou de ataques ocorridos nas instalações da Comissão devem receber assistência.
5. Para fins de prevenção e controlo dos riscos de segurança, o pessoal mandatado pode proceder à verificação dos antecedentes das pessoas abrangidas pelo âmbito de aplicação da presente decisão, a fim de determinar se facultar a essas pessoas o acesso a instalações ou informações da Comissão coloca uma ameaça à segurança. Para o efeito, e em conformidade com o Regulamento (CE) n.º 45/2001 e as disposições a que se refere o artigo 3.º, n.º 1, o pessoal mandatado pode:
 - a) Utilizar todas as fontes de informação de que dispõe a Comissão, tendo em conta a fiabilidade das mesmas;
 - b) Ter acesso aos ficheiros ou aos dados do pessoal que a Comissão detém em relação às pessoas que emprega ou pretende empregar ou, quando devidamente justificado, ao pessoal contratado.

Artigo 8.º

Medidas de segurança relativas à segurança física e aos bens

1. A segurança dos bens é assegurada mediante a aplicação de medidas físicas e técnicas de proteção que sejam apropriadas e dos procedimentos correspondentes (a seguir designados por «segurança física»), criando um sistema com vários níveis.
2. A fim de proteger as pessoas, bens ou informações na Comissão, podem ser adotadas medidas nos termos do presente artigo.
3. A segurança física tem os seguintes objetivos:
 - prevenir atos de violência contra os membros da Comissão ou as pessoas abrangidas pelo âmbito de aplicação da presente decisão;
 - prevenir a espionagem e as escutas clandestinas de informações sensíveis ou classificadas;
 - prevenir roubos, atos de vandalismo, sabotagem e outras ações violentas destinadas a danificar ou a destruir edifícios e bens da Comissão;

- permitir investigações e inquéritos de incidentes de segurança, verificando nomeadamente ficheiros de relatório de controlo de acesso e saída, gravações de TVCF (televisão em circuito fechado), gravações de chamadas telefónicas e dados semelhantes referidos no artigo 22.º, n.º 2, bem como outras fontes de informação.
4. A segurança física inclui:
- uma política de acesso aplicável a todas as pessoas ou veículos que solicitem acesso às instalações da Comissão, incluindo aos parques de estacionamento;
 - um sistema de controlo dos acessos que inclua guardas, equipamento técnico, medidas técnicas, sistemas de informação ou uma combinação de todos estes elementos.
5. Para assegurar a segurança física, podem ser tomadas as seguintes medidas:
- registar entradas e saídas dos edifícios da Comissão por parte de pessoas, veículos, mercadorias e equipamentos;
 - efetuar controlos de identidade nas suas instalações;
 - inspecionar veículos, mercadorias e equipamentos com meios visuais ou técnicos;
 - impedir o acesso não autorizado às instalações da Comissão a pessoas, veículos e mercadorias.

Artigo 9.º

Medidas de segurança relativas às informações

1. A segurança das informações abrange todas as informações manuseadas pela Comissão.
2. A segurança das informações, independentemente do formato destas, deve equilibrar a transparência, a proporcionalidade, a responsabilização e a eficiência com a necessidade de proteger as informações de acessos, utilizações, divulgações, alterações ou destruições não autorizados.
3. A segurança das informações destina-se a proteger a sua confidencialidade, integridade e disponibilidade.
4. Por conseguinte, devem ser aplicados procedimentos de gestão de riscos para classificar os ativos de informação e desenvolver medidas, procedimentos e normas proporcionais no âmbito da segurança, incluindo medidas de atenuação.
5. Estes princípios gerais subjacentes à segurança das informações devem ser aplicados, em especial, no que se refere a:
 - a) «Informações Classificadas da União Europeia» (a seguir designadas por «ICUE»), ou seja, todas as informações ou material designados por uma classificação de segurança da UE, cuja divulgação não autorizada é passível de causar prejuízos de diversos níveis aos interesses da União Europeia ou de um ou vários Estados-Membros;
 - b) «Informações sensíveis não classificadas», ou seja, informações ou elementos que a Comissão tem de proteger por causa das obrigações jurídicas estabelecidas nos Tratados ou em atos adotados para a sua execução, e/ou por causa da sensibilidade dessas informações ou elementos. As informações sensíveis não classificadas incluem, entre outras, informações ou elementos abrangidos pelo segredo profissional a que se refere o artigo 339.º do TFUE, informações abrangidas pelos interesses protegidos pelo artigo 4.º do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho⁽¹⁾ lido em conjugação com a jurisprudência pertinente do Tribunal de Justiça da União Europeia, ou dados pessoais abrangidos pelo âmbito de aplicação do Regulamento (CE) n.º 45/2001.
6. As informações sensíveis não classificadas estão sujeitas a regras relativas ao seu manuseamento e armazenamento. Essas informações só são divulgadas às pessoas que têm uma «necessidade de conhecer». Quando necessário para a proteção eficaz da sua confidencialidade, essas informações devem ser identificadas por uma marca de segurança e as correspondentes instruções de manuseamento devem ser aprovadas pelo Diretor-Geral dos Recursos Humanos e da Segurança. Quando manuseadas ou armazenadas em sistemas de comunicação e informação, essas informações devem também ser protegidas em conformidade com a Decisão (2006) 3602, as suas regras de execução e as normas correspondentes.
7. As pessoas responsáveis por comprometer ou perder informações ICUE ou informações sensíveis não classificadas, que estejam identificadas como tal nas regras relativas ao seu manuseamento e armazenamento, estão sujeitas a sanções disciplinares nos termos do Estatuto, sem prejuízo de outras eventuais ações judiciais ou penais propostas pelas autoridades nacionais competentes dos Estados-Membros em conformidade com a legislação e regulamentação nacionais, e das vias de recurso contratuais.

⁽¹⁾ Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

*Artigo 10.º***Medidas de segurança relativas aos sistemas de comunicação e informação**

1. Todos os sistemas de comunicação e informação («SCI») utilizados pela Comissão devem respeitar a política de segurança dos sistemas de informação da Comissão definida na Decisão C(2006) 3602, nas suas regras de execução e nas normas de segurança correspondentes.
2. Os serviços da Comissão que detenham, giram ou operem SCI só autorizam o seu acesso a outras instituições, agências, organismos da União ou a outras organizações se estes puderem razoavelmente garantir que os seus sistemas informáticos estão protegidos a um nível equivalente ao da política de segurança dos sistemas de informação da Comissão definida na Decisão C(2006) 3602, nas suas regras de execução e nas normas de segurança correspondentes. A Comissão verifica esse cumprimento e, em caso de incumprimento grave ou continuado, tem o direito de proibir o acesso a esses SCI.

*Artigo 11.º***Análise forense relativa à cibersegurança**

A Direção-Geral dos Recursos Humanos e da Segurança é particularmente responsável por efetuar análises técnicas forenses em cooperação com os serviços competentes da Comissão, em apoio dos inquéritos de segurança referidos no artigo 13.º, relacionados com contraespionagem, fuga de dados, ciberataques e segurança dos sistemas de informação.

*Artigo 12.º***Medidas de segurança relativas às pessoas e aos objetos**

1. A fim de garantir a segurança na Comissão e para prevenir e controlar riscos, o pessoal mandatado nos termos do artigo 5.º pode, em conformidade com os princípios estabelecidos no artigo 3.º, tomar, entre outras, uma ou várias das seguintes medidas de segurança:
 - a) Conservação de cenas e de provas, incluindo ficheiros de relatório de controlo de acesso e saída, imagens de TVCF, em caso de incidentes ou comportamentos suscetíveis de conduzir a processos administrativos, disciplinares, cíveis ou penais;
 - b) Medidas limitadas respeitantes às pessoas que representem uma ameaça para a segurança, incluindo ordenar a pessoas que abandonem as instalações da Comissão, acompanhar pessoas à saída de instalações da Comissão e proibir pessoas de aceder às instalações da Comissão por um período determinado de acordo com os critérios a definir nas regras de execução;
 - c) Medidas limitadas relativas aos objetos que representem uma ameaça para a segurança, incluindo a remoção, a apreensão e a eliminação de objetos;
 - d) Buscas nas instalações da Comissão, incluindo em escritórios situados nessas instalações;
 - e) Buscas em SCI e equipamentos, dados de tráfego de telefones e telecomunicações, ficheiros de registo, contas de utilizador, etc.;
 - f) Outras medidas de segurança específicas com efeitos semelhantes, a fim de prevenir ou controlar riscos de segurança, em especial no âmbito dos direitos da Comissão enquanto locadora ou enquanto empregadora, em conformidade com a legislação nacional aplicável.
2. Em circunstâncias excecionais, o pessoal mandatado da Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança, em conformidade com o artigo 5.º, pode tomar todas as medidas urgentes necessárias, no estrito cumprimento dos princípios estabelecidos no artigo 3.º. O mais depressa possível após tomar essas medidas, esse pessoal deve informar o diretor da Direção da Segurança (que deve obter o mandato adequado do Diretor-Geral dos Recursos Humanos e da Segurança confirmando essas medidas e autorizando eventuais medidas necessárias) e, quando apropriado, deve assegurar a ligação com as autoridades nacionais competentes.
3. As medidas de segurança nos termos do presente artigo são documentadas no momento em que são tomadas ou, em caso de risco imediato ou de situação de crise, num prazo razoável após serem tomadas. Neste caso, a documentação deve incluir também os elementos em se baseou a avaliação relativa à existência de um risco imediato ou de uma situação de crise. A documentação pode ser sucinta, mas deve ser constituída de modo a permitir à pessoa sujeita à medida de segurança exercer os seus direitos de defesa e de proteção de dados pessoais, em conformidade com o Regulamento (CE) n.º 45/2001, e um controlo da legalidade da medida. As informações sobre medidas de segurança específicas dirigidas a funcionários não devem constar do seu processo individual.

4. Ao tomar medidas de segurança nos termos da alínea b), a Comissão garante ainda que seja dada à pessoa em causa a possibilidade de contactar um advogado ou alguém da sua confiança, e que essa pessoa seja informada do direito de recorrer à Autoridade Europeia para a Proteção de Dados.

Artigo 13.º

Inquéritos

1. Sem prejuízo do artigo 86.º e do anexo IX do Estatuto, ou de eventuais convénios especiais entre a Comissão e o SEAE, como o convénio especial assinado em 28 de maio de 2014 entre a Direção-Geral dos Recursos Humanos e da Segurança da Comissão Europeia e o Serviço Europeu para a Ação Externa sobre o dever de solicitude para com o pessoal da Comissão em serviço nas delegações da União, os inquéritos de segurança podem ser conduzidos:

- a) Em caso de incidentes que afetem a segurança na Comissão, incluindo suspeitas de infrações penais;
- b) Em caso de potenciais fugas, manuseamentos indevidos ou comprometimentos de informações sensíveis não classificadas, de informações classificadas da UE ou de informações classificadas Euratom;
- c) No âmbito da contrainformação e do antiterrorismo;
- d) Em caso de incidentes informáticos graves.

2. A decisão de conduzir inquéritos de segurança é tomada pelo Diretor-Geral dos Recursos Humanos e da Segurança, que será igualmente o destinatário dos relatórios de inquérito.

3. Os inquéritos de segurança são conduzidos apenas pelos funcionários responsáveis da Direção-Geral dos Recursos Humanos e da Segurança, devidamente mandatados em conformidade com o artigo 5.º.

4. O pessoal mandatado exerce com independência a competência para conduzir inquéritos de segurança nos termos do mandato e dispõe das competências enumeradas no artigo 12.º.

5. O pessoal mandatado com competência para conduzir inquéritos de segurança pode recolher informações de todas as fontes disponíveis relacionadas com as infrações administrativas ou penais cometidas nas instalações da Comissão, ou que envolvam as pessoas referidas no artigo 2.º, n.º 3, na qualidade de vítimas ou de autores dessas infrações.

6. Quando apropriado, a Direção-Geral dos Recursos Humanos e da Segurança informa as autoridades competentes do Estado-Membro anfitrião ou de outro Estado-Membro em causa, sobretudo se o inquérito apurou indícios de que foi cometido um crime. Neste contexto, a referida direção-geral pode, quando apropriado ou exigido, prestar apoio às autoridades do Estado-Membro anfitrião ou de outro Estado-Membro em causa.

7. Em caso de incidente informático grave, a Direção-Geral da Informática deve colaborar estreitamente com a Direção-Geral dos Recursos Humanos e da Segurança para prestar apoio em todas as questões técnicas. A Direção-Geral dos Recursos Humanos e da Segurança decide, em colaboração com a Direção-Geral da Informática, qual o momento adequado para informar as autoridades competentes do país anfitrião ou de outro Estado-Membro em causa. No que se refere ao apoio a outras instituições e agências da UE que possam ser afetadas, serão utilizados os serviços de coordenação de incidentes da Equipa de Resposta a Emergências Informáticas para as instituições, organismos e agências da UE (CERT-UE).

8. Os inquéritos de segurança devem ser documentados.

Artigo 14.º

Delimitação de competências no que respeita aos inquéritos de segurança e a outros tipos de investigação

1. Quando a Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança conduz os inquéritos de segurança a que se refere o artigo 13.º, e esses inquéritos caiam no âmbito de competências do Organismo Europeu de Luta Antifraude (OLAF) ou do Serviço de Averiguação e Disciplina da Comissão (IDOC), assegura imediatamente a ligação com esses organismos, tendo em vista, sobretudo, não comprometer medidas tomadas posteriormente pelo OLAF ou o IDOC. Quando apropriado, a Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança convida o OLAF ou o IDOC a participar nas investigações.

2. Os inquéritos de segurança referidos no artigo 13.º não prejudicam as competências do OLAF ou do IDOC estabelecidas nas regras que regem esses organismos. A Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança pode ser solicitada a prestar assistência técnica aos inquéritos abertos pelo OLAF ou o IDOC.

3. A Direção da Segurança da Direção-Geral dos Recursos Humanos e da Segurança pode ser solicitada a prestar assistência aos agentes do OLAF quando estes acedam a instalações da Comissão em conformidade com os artigos 3.º, n.º 5, e 4.º, n.º 4, do Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho ⁽¹⁾, a fim de

⁽¹⁾ Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho, de 11 de setembro de 2013, relativo aos inquéritos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF) e que revoga o Regulamento (CE) n.º 1073/1999 do Parlamento Europeu e do Conselho e o Regulamento (Euratom) n.º 1074/1999 do Conselho (JO L 248 de 18.9.2013, p. 1).

facilitar o desempenho das suas funções. A Direção da Segurança informa de tais pedidos de assistência o Secretário-Geral e o Diretor-Geral da Direção-Geral dos Recursos Humanos e da Segurança ou, caso a investigação se efetue em instalações da Comissão ocupadas pelos seus membros ou pelo Secretário-Geral, o Presidente da Comissão e o Comissário responsável pelos Recursos Humanos.

4. Sem prejuízo do artigo 22.º-A do Estatuto, quando um processo caia no âmbito de competências da Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança e também do IDOC, a Direção de Segurança, no relatório ao Diretor-Geral dos Recursos Humanos em conformidade com o artigo 13.º, pronuncia-se o mais cedo possível sobre a existência ou não de motivos que justifiquem submeter a questão ao IDOC. Em particular, considera-se esta fase atingida quando a ameaça imediata à segurança tenha cessado. Cabe ao Diretor-Geral dos Recursos Humanos e da Segurança decidir sobre a questão.

5. Quando um processo caia no âmbito de competências da Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança e do OLAF, a Direção de Segurança deve comunicar imediatamente tal facto ao Diretor-Geral dos Recursos Humanos e da Segurança e informar o Diretor-Geral do OLAF o mais brevemente possível. Em particular, considera-se esta fase atingida quando a ameaça imediata à segurança tenha cessado.

Artigo 15.º

Inspecções de segurança

1. A Direção-Geral dos Recursos Humanos e da Segurança efetua inspecções de segurança a fim de verificar o cumprimento da presente decisão e das suas regras de execução pelos serviços da Comissão e por particulares, e de formular recomendações quando necessário.

2. Quando apropriado, a Direção-Geral dos Recursos Humanos e da Segurança procede a inspecções de segurança, ao acompanhamento da segurança ou a visitas de avaliação para verificar se a segurança do pessoal, dos bens e das informações da Comissão da responsabilidade de outras instituições, agências ou organismos da União, de Estados-Membros, de Estados terceiros ou de organizações internacionais, é devidamente protegida em conformidade com regras, regulamentações e normas de segurança pelo menos equivalentes às da Comissão. Quando apropriado e num espírito de boa cooperação entre administrações, essas inspecções de segurança incluem também inspecções efetuadas no contexto do intercâmbio de informações classificadas com outras instituições, organismos e agências da União, com Estados-Membros ou com Estados terceiros ou organizações internacionais.

3. Este artigo é aplicado, com as devidas adaptações, ao pessoal da Comissão nas delegações da União, sem prejuízo de eventuais convénios especiais entre a Comissão e o SEAE, como o convénio especial assinado em 28 de maio de 2014 entre a Direção-Geral dos Recursos Humanos e da Segurança da Comissão Europeia e o Serviço Europeu para a Ação Externa sobre o dever de solicitude para com o pessoal da Comissão em serviço nas delegações da União.

Artigo 16.º

Estados de alerta e gestão de situações de crise

1. A Direção-Geral dos Recursos Humanos e da Segurança é responsável por aplicar medidas apropriadas para estados de alerta, em antecipação ou em reação a ameaças e incidentes que afetem a segurança na Comissão, e pelas medidas necessárias à gestão de situações de crise.

2. As medidas de estados de alerta referidas no n.º 1 devem ser proporcionais ao nível da ameaça à segurança. Os níveis de estados de alerta são definidos em estreita cooperação com os serviços competentes de outras instituições, agências e organismos da União, e do Estado-Membro ou Estados-Membros que acolhem instalações da Comissão.

3. A Direção-Geral dos Recursos Humanos e da Segurança é o ponto de contacto para os estados de alerta e a gestão de situações de crise.

CAPÍTULO 4

ORGANIZAÇÃO

Artigo 17.º

Responsabilidades gerais dos serviços da Comissão

1. As responsabilidades da Comissão referidas na presente decisão são exercidas pela Direção-Geral dos Recursos Humanos e da Segurança, sob a autoridade e a responsabilidade do membro da Comissão responsável pela segurança.

2. As disposições específicas no que respeita à cibersegurança estão definidas na Decisão (2006) 3602.
3. As responsabilidades pela execução da presente decisão e das suas regras de execução, bem como pelo seu cumprimento diário, podem ser delegadas a outros serviços da Comissão sempre que uma execução descentralizada da segurança ofereça ganhos significativos em termos de eficiência, recursos ou poupança de tempo, por exemplo devido à localização geográfica dos serviços em causa.
4. Nos casos em que se aplique o n.º 3, a Direção-Geral dos Recursos Humanos e da Segurança, e, quando apropriado, o Diretor-Geral da Informática, devem celebrar acordos com serviços específicos da Comissão que definam claramente as funções e as responsabilidades pela execução e o acompanhamento das políticas de segurança.

Artigo 18.º

Direção-Geral dos Recursos Humanos e da Segurança

1. A Direção-Geral dos Recursos Humanos e da Segurança é particularmente responsável por:
 - (1) desenvolver a política de segurança, as regras de execução e as indicações de segurança da Comissão;
 - (2) recolher informações, tendo em vista avaliar ameaças e riscos de segurança e sobre todas as questões que possam afetar a segurança na Comissão;
 - (3) fornecer contravigilância eletrónica e proteção a todas as localizações da Comissão, tendo na devida conta avaliações de ameaças e provas de atividades não autorizadas contra os interesses da Comissão;
 - (4) oferecer serviços de emergência 24 horas por dia, sete dias por semana, aos serviços e pessoal da Comissão, para todas as questões relacionadas com proteção e segurança;
 - (5) aplicar medidas de segurança destinadas a atenuar riscos de segurança e a desenvolver e manter SCI apropriados para cobrir as suas necessidades operacionais, em especial nos domínios do controlo do acesso físico, da gestão das autorizações de segurança e do manuseamento das informações sensíveis e classificadas da UE;
 - (6) sensibilizar, organizar treinos e simulações, e dar formações e aconselhamento sobre todas as questões relacionadas com a segurança na Comissão, tendo em vista promover uma cultura de segurança e criar uma reserva de pessoal devidamente treinado em questões de segurança.
2. Sem prejuízo das competências e responsabilidades de outros serviços da Comissão, a Direção-Geral dos Recursos Humanos e da Segurança assegura a ligação externa relativamente:
 - (1) aos serviços de segurança das outras instituições, agências e organismos da União, sobre questões relacionadas com a segurança de pessoas, bens e informações na Comissão;
 - (2) aos serviços de segurança, de informações e de avaliação de ameaças, incluindo autoridades nacionais de segurança, dos Estados-Membros, de países terceiros e de organizações e organismos internacionais, sobre questões que afetem a segurança de pessoas, bens e informações na Comissão;
 - (3) à polícia e outros serviços de emergência, sobre todas as questões de rotina e de emergência que afetem a segurança da Comissão;
 - (4) às autoridades de segurança de outras instituições, agências e organismos da UE, dos Estados-Membros e de países terceiros no domínio da resposta a ciberataques com potencial impacto ao nível da segurança na Comissão;
 - (5) à receção, avaliação e distribuição de informações sobre as ameaças colocadas por atividades terroristas e de espionagem que afetem a segurança na Comissão;
 - (6) às questões relacionadas com informações classificadas, conforme especificadas na Decisão (UE, Euratom) 2015/444 da Comissão ⁽¹⁾.
3. A Direção-Geral dos Recursos Humanos e da Segurança é responsável pela transmissão segura de informações, incluindo a transmissão de dados pessoais, realizada nos termos do presente artigo.

Artigo 19.º

Grupo de peritos de segurança da Comissão (ComSEG)

É criado um grupo de peritos de segurança da Comissão com o mandato de, quando apropriado, aconselhar a Comissão sobre questões relacionadas com a sua política de segurança interna e, mais especificamente, sobre a proteção de informações classificadas da UE.

⁽¹⁾ Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (ver página 53 do presente Jornal Oficial).

Artigo 20.º

Responsáveis locais de segurança (LSO)

1. Cada serviço da Comissão ou gabinete nomeia um responsável local de segurança (LSO), que será o principal ponto de contacto entre esse serviço e a Direção-Geral dos Recursos Humanos e da Segurança para todas as questões relacionadas com a segurança na Comissão. Quando apropriado, podem ser nomeados um ou mais LSO adjuntos. Os LSO são funcionários ou agentes temporários.
2. Na qualidade de principal ponto de contacto para as questões de segurança nos diferentes serviços da Comissão ou gabinetes, o LSO deve, a intervalos regulares, comunicar à Direção-Geral dos Recursos Humanos e da Segurança e aos seus superiores hierárquicos as questões de segurança que envolvam o seu serviço da Comissão, e sobre eventuais incidentes de segurança sem demora, incluindo aqueles em que as ICUE ou as informações sensíveis não classificadas possam ter sido comprometidas.
3. Nas questões relacionadas com a segurança dos sistemas de comunicação e informação, o LSO assegura a ligação com o responsável local da segurança informática (LISO) do seu serviço da Comissão, cujas funções e responsabilidades estão estabelecidas na Decisão C(2006) 3602.
4. Devem contribuir para o desenvolvimento de atividades de formação e de sensibilização no âmbito da segurança, respondendo às necessidades específicas do pessoal, dos contratantes e de outras pessoas que trabalhem sob a autoridade do seu serviço da Comissão.
5. Em caso de risco grave ou imediato de segurança ou em caso de emergência, podem ser atribuídas funções específicas aos LSO mediante pedido da Direção-Geral dos Recursos Humanos e da Segurança. O Diretor-Geral ou o Diretor dos Recursos Humanos da Direção-Geral de cada LSO deve ser informado dessas funções específicas pela Direção-Geral dos Recursos Humanos e da Segurança.
6. As responsabilidades dos LSO são exercidas sem prejuízo das funções e responsabilidades atribuídas aos responsáveis locais da segurança informática (LISO), aos gestores da saúde e segurança, aos responsáveis do controlo do registo (RCO), ou de outras funções que impliquem responsabilidades relacionadas com a segurança ou a proteção. Os LSO devem estabelecer uma ligação com esses responsáveis, a fim de garantir uma abordagem coerente de segurança e um fluxo de informações eficiente sobre matérias relacionadas com a segurança na Comissão.
7. Os LSO têm acesso direto ao seu diretor-geral ou ao seu chefe de serviço e, simultaneamente, informam a sua hierarquia direta. Devem ser titulares de uma autorização de segurança para acesso a ICUE, pelo menos até ao nível SECRET UE/EU SECRET.
8. A fim de promover o intercâmbio de informações e boas práticas, a Direção-Geral dos Recursos Humanos e da Segurança, deve organizar, pelo menos duas vezes por ano, uma conferência de LSO. A presença dos LSO nestas conferências é obrigatória.

CAPÍTULO 5

EXECUÇÃO

Artigo 21.º

Regras de execução e indicações de segurança

1. Conforme for necessário, a adoção das regras de execução da presente decisão será objeto de uma outra decisão de delegação de poderes da Comissão a favor do membro da Comissão responsável pelas questões de segurança, no pleno respeito do regulamento interno.
2. Após a delegação de poderes na sequência dessa decisão da Comissão, o membro da Comissão responsável pelas questões de segurança pode elaborar indicações de segurança que definam orientações e boas práticas, no âmbito de aplicação da presente decisão e das suas regras de execução.
3. A Comissão pode, através de uma decisão de delegação separada, delegar as funções referidas no n.º 1 e no n.º 2 do presente artigo ao Diretor-Geral dos Recursos Humanos e da Segurança, em plena conformidade com o regulamento interno.

CAPÍTULO 6

DISPOSIÇÕES DIVERSAS E FINAIS*Artigo 22.º***Tratamento de dados pessoais**

1. A Comissão efetua o tratamento de dados pessoais necessário para executar a presente decisão em conformidade com o Regulamento (CE) n.º 45/2001.
2. Não obstante as medidas em vigor no momento da adoção da presente decisão e notificadas à Autoridade Europeia para a Proteção de Dados ⁽¹⁾, todas as medidas da presente decisão que impliquem o tratamento de dados pessoais (como os dados relacionados com relatórios de controlo de acesso e saída, gravações de TVCF, gravações de chamadas telefónicas para serviços de permanência ou centrais telefónicas e dados semelhantes), necessário por razões de segurança ou em reação a crises, estão sujeitas a regras de execução em conformidade com o artigo 21.º, que devem estabelecer garantias adequadas aos titulares dos dados.
3. O Diretor-Geral da Direção-Geral dos Recursos Humanos e da Segurança é responsável pela segurança dos tratamentos de dados pessoais efetuados no âmbito da presente decisão.
4. Essas regras de execução e procedimentos são adotados após consulta ao responsável pela proteção de dados e à Autoridade Europeia para a Proteção de Dados, em conformidade com o Regulamento (CE) n.º 45/2001.

*Artigo 23.º***Transparência**

A presente decisão e as suas regras de execução devem ser levadas ao conhecimento do pessoal da Comissão e de todas as pessoas a quem se aplicam.

*Artigo 24.º***Revogação de decisões anteriores**

É revogada a Decisão (94) 2129.

*Artigo 25.º***Entrada em vigor**

A presente decisão entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 13 de março de 2015.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

⁽¹⁾ DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

DECISÃO (UE, Euratom) 2015/444 DA COMISSÃO**de 13 de março de 2015****relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE**

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 249.º,

Tendo em conta o Tratado que institui a Comunidade Europeia da Energia Atómica, nomeadamente o artigo 106.º,

Tendo em conta o Protocolo n.º 7 relativo aos Privilégios e Imunidades da União Europeia, anexo aos Tratados, nomeadamente o artigo 18.º,

Considerando o seguinte:

- (1) As regras de segurança da Comissão relativas à proteção das informações classificadas da União Europeia (ICUE) precisam de ser revistas e atualizadas, tendo em conta as evoluções registadas a nível institucional, organizativo, operacional e tecnológico.
- (2) A Comissão Europeia estabeleceu acordos em matéria de segurança para as suas localizações principais, juntamente com os Governos da Bélgica, Luxemburgo e Itália ⁽¹⁾.
- (3) A Comissão, o Conselho e o Serviço Europeu para a Ação Externa estão empenhados em aplicar normas de segurança equivalentes para proteger as ICUE.
- (4) É importante que, sempre que possível, o Parlamento Europeu e as outras instituições, agências, organismos ou serviços da União Europeia sejam associados aos princípios, normas e regras de proteção das informações classificadas que são necessários para proteger os interesses da União e dos seus Estados-Membros.
- (5) Os riscos a que as ICUE estão expostas são geridos como um processo. Esse processo tem por objetivo determinar os riscos de segurança conhecidos, definir as medidas de segurança destinadas a reduzir esses riscos para um nível aceitável em conformidade com os princípios básicos e as normas mínimas estabelecidos na presente decisão e aplicar tais medidas de acordo com o conceito de defesa em profundidade. A eficácia dessas medidas é objeto de avaliação contínua.
- (6) Na Comissão, a segurança física que visa proteger informações classificadas consiste na aplicação de medidas físicas e técnicas de proteção destinadas a impedir o acesso não autorizado a ICUE.
- (7) A gestão das ICUE consiste na aplicação de medidas administrativas de controlo destas informações ao longo do seu ciclo de vida que visam complementar as medidas previstas nos capítulos 2, 3 e 5 da presente decisão e contribuir assim para dissuadir e detetar a perda ou o comprometimento deliberados ou acidentais de informações e para recuperar essas informações em caso de perda ou comprometimento. Estas medidas dizem respeito, nomeadamente, à produção, armazenamento, registo, cópia, tradução, desgradação, desclassificação, transporte e destruição de ICUE e complementam as regras gerais sobre gestão de documentos da Comissão (Decisões 2002/47/CE, CECA, Euratom ⁽²⁾ e 2004/563/CE, Euratom ⁽³⁾).

⁽¹⁾ Cf. «Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité», de 31 de dezembro de 2004, «Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois», de 20 de janeiro de 2007, e «Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale», de 22 de julho de 1959.

⁽²⁾ Decisão 2002/47/CE, CECA, Euratom da Comissão, de 23 de janeiro de 2002, que altera o seu regulamento interno (JO L 21 de 24.1.2002, p. 23).

⁽³⁾ Decisão 2004/563/CE, Euratom da Comissão, de 7 de julho de 2004, que altera o seu Regulamento Interno (JO L 251 de 27.7.2004, p. 9).

- (8) O disposto na presente decisão não prejudica:
- a) o Regulamento (Euratom) n.º 3 ⁽¹⁾;
 - b) o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho ⁽²⁾;
 - c) o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho ⁽³⁾;
 - d) o Regulamento (CEE, Euratom) n.º 354/83 do Conselho ⁽⁴⁾,

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

PRINCÍPIOS BÁSICOS E NORMAS MÍNIMAS

Artigo 1.º

Definições

Para efeitos da presente decisão, entende-se por:

- 1) «Serviço da Comissão»: qualquer direção-geral ou serviço da Comissão, ou qualquer gabinete de um membro da Comissão;
- 2) «Material criptográfico»: algoritmos criptográficos, módulos criptográficos de *hardware* e *software*, e produtos que incluam regras de aplicação e documentação conexas e material de cifragem;
- 3) «Desclassificação»: a eliminação de qualquer classificação de segurança;
- 4) «Defesa em profundidade»: a aplicação de uma série de medidas de segurança organizadas em múltiplos estratos de defesa;
- 5) «Documento»: uma informação registada, independentemente da sua forma física ou das suas características;
- 6) «Desgradação»: uma redução do nível de classificação de segurança;
- 7) «Manuseamento de ICUE»: todas as ações a que as ICUE possam ser sujeitas ao longo do seu ciclo de vida. Compreende a sua produção, registo, tratamento, transporte, desgradação, desclassificação e destruição. Em relação aos sistemas de comunicação e informação (SCI), compreende igualmente a sua recolha, visualização, transmissão e armazenamento;
- 8) «Detentor»: pessoa devidamente autorizada com necessidade comprovada de tomar conhecimento, que está na posse de ICUE e é consequentemente responsável pela sua proteção;
- 9) «Regras de execução»: qualquer conjunto de regras ou indicações de segurança adotado em conformidade com o capítulo 5 da Decisão (UE, Euratom) 2015/443 da Comissão ⁽⁵⁾;
- 10) «Material»: qualquer meio, suporte de dados ou peça de maquinaria ou equipamento, já fabricado ou em fase de fabrico;
- 11) «Entidade de origem»: a instituição, agência ou organismo da União, Estado-Membro, Estado terceiro ou organização internacional sob cuja autoridade tenham sido produzidas e/ou introduzidas nas estruturas da União informações classificadas;
- 12) «Instalações»: todos os imóveis ou bens e haveres equiparados da Comissão;

⁽¹⁾ Regulamento (Euratom) n.º 3, de 31 de julho de 1958, que aplica o artigo 24.º do Tratado que institui a Comunidade Europeia da Energia Atómica (JO L 17 de 6.10.1958, p. 406/58).

⁽²⁾ Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

⁽³⁾ Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

⁽⁴⁾ Regulamento (CEE, Euratom) n.º 354/83 do Conselho, de 1 de fevereiro de 1983, relativo à abertura ao público dos arquivos históricos da Comunidade Económica Europeia e da Comunidade Europeia da Energia Atómica (JO L 43 de 15.2.1983, p. 1).

⁽⁵⁾ Decisão (UE, Euratom) 2015/443 da Comissão, de 13 de março de 2015, relativa à segurança na Comissão (ver página 41 do presente Jornal Oficial).

- 13) «Processo de gestão do risco de segurança»: todo o processo de identificação, controlo e minimização de acontecimentos indeterminados que possam afetar a segurança de determinada organização ou qualquer um dos sistemas por ela utilizados. Este processo abarca todas as atividades relacionadas com o risco, designadamente a avaliação, tratamento, aceitação e comunicação;
- 14) «Estatuto»: o Estatuto dos Funcionários da União Europeia e o Regime Aplicável aos Outros Agentes da União Europeia, estabelecidos no Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho ⁽¹⁾;
- 15) «Ameaça»: causa potencial de um incidente indesejável que pode resultar em danos para uma organização ou para qualquer um dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque;
- 16) «Vulnerabilidade»: insuficiência de qualquer natureza suscetível de ser potenciada por uma ou mais ameaças. A vulnerabilidade pode consistir numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, exaustividade ou coerência, podendo ser de natureza técnica, processual, material, organizativa ou operacional.

Artigo 2.º

Objeto e âmbito de aplicação

1. A presente decisão estabelece os princípios básicos e as normas mínimas de segurança aplicáveis à proteção das ICUE.
2. A presente decisão é aplicável a todos os serviços e em todas as instalações da Comissão.
3. Sem prejuízo de quaisquer indicações específicas relativas a determinados grupos de pessoal, a presente decisão é aplicável aos membros da Comissão, ao pessoal da Comissão abrangido pelo âmbito de aplicação do Estatuto dos Funcionários da União Europeia e pelo Regime Aplicável aos Outros Agentes da União, aos peritos nacionais destacados (PND) na Comissão, aos prestadores de serviços e seu pessoal, aos estagiários e a qualquer pessoa com acesso aos edifícios ou outros bens da Comissão ou a informações tratadas pela Comissão.
4. As disposições da presente decisão não prejudicam a Decisão 2002/47/CE, CECA, Euratom nem a Decisão 2004/563/CE, Euratom.

Artigo 3.º

Definição de ICUE, classificações e marcas de segurança

1. Entende-se por «informações classificadas da União Europeia» (ICUE) quaisquer informações ou material designado por uma classificação de segurança da UE cuja divulgação não autorizada possa causar prejuízos de vária ordem aos interesses da União Europeia ou de um ou mais Estados-Membros.
2. As ICUE são classificadas num dos seguintes níveis:
 - a) TRÈS SECRET UE/EU TOP SECRET: informações e material cuja divulgação não autorizada possa prejudicar de forma excepcionalmente grave os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
 - b) SECRET UE/EU SECRET: informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
 - c) CONFIDENTIEL UE/EU CONFIDENTIAL: informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
 - d) RESTREINT UE/EU RESTRICTED: informações e material cuja divulgação não autorizada possa ser desfavorável aos interesses da União Europeia ou de um ou mais Estados-Membros.
3. As ICUE devem ostentar uma marca de classificação de segurança em conformidade com o n.º 2. Podem ostentar marcas adicionais, que não sejam marcas de classificação, mas que se destinem a designar o domínio de atividade a que se referem, identificar a entidade de origem, limitar a distribuição, restringir a utilização ou indicar a comunicabilidade.

⁽¹⁾ Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho, de 29 de fevereiro de 1968, que fixa o Estatuto dos Funcionários das Comunidades Europeias assim como o Regime aplicável aos outros agentes destas Comunidades, e institui medidas especiais temporariamente aplicáveis aos funcionários da Comissão (Regime aplicável aos outros agentes) (JO L 56 de 4.3.1968, p. 1).

*Artigo 4.º***Gestão das classificações**

1. Cada membro da Comissão ou serviço da Comissão deve garantir que as ICUE que produz sejam devidamente classificadas e claramente identificadas como ICUE e mantenham o seu nível de classificação apenas durante o tempo necessário.
2. Sem prejuízo do disposto no artigo 26.º, as ICUE não podem ser desgraduadas nem desclassificadas e nenhuma das marcas de classificação de segurança a que se refere o artigo 3.º, n.º 2, pode ser alterada ou suprimida sem o consentimento prévio, por escrito, da entidade de origem.
3. Se for caso disso, são adotadas regras de execução sobre o manuseamento das ICUE, incluindo um guia prático de classificação, em conformidade com o artigo 60.º.

*Artigo 5.º***Proteção das informações classificadas**

1. As ICUE devem ser protegidas em conformidade com a presente decisão e com as suas regras de execução.
2. Segundo as regras previstas no capítulo 4, incumbe ao detentor de quaisquer ICUE a responsabilidade pela sua proteção, em conformidade com a presente decisão e as suas regras de execução.
3. Quando os Estados-Membros introduzirem nas estruturas ou redes da Comissão informações classificadas que ostentem uma marca de classificação de segurança nacional, a Comissão deve proteger essas informações em conformidade com os requisitos aplicáveis às ICUE de nível equivalente, como estabelecido na tabela de equivalências das classificações de segurança constante do anexo I.
4. Um agregado de ICUE pode justificar um nível de proteção correspondente a uma classificação mais elevada do que a de cada um dos seus componentes.

*Artigo 6.º***Gestão dos riscos de segurança**

1. As medidas de segurança destinadas a proteger as ICUE ao longo do seu ciclo de vida devem ser proporcionais, em particular, à classificação de segurança, à forma e ao volume das informações ou do material, à localização e construção das instalações que albergam as ICUE e à avaliação local da ameaça de atos mal-intencionados e/ou atividades criminosas, nomeadamente de espionagem, sabotagem e terrorismo.
2. Os planos de emergência devem ter em conta a necessidade de proteger as ICUE em situações de emergência, a fim de evitar o acesso ou a divulgação não autorizados ou a perda de integridade ou disponibilidade.
3. Os planos de continuidade das atividades de todos os serviços devem incluir medidas de prevenção e recuperação destinadas a minimizar o impacto de quaisquer falhas ou incidentes graves sobre o manuseamento e armazenamento das ICUE.

*Artigo 7.º***Execução da presente decisão**

1. Se necessário, são adotadas regras de execução para completar ou apoiar a presente decisão, em conformidade com o artigo 60.º.
2. Os serviços da Comissão devem tomar todas as medidas necessárias sob a sua responsabilidade para assegurar que, no manuseamento ou armazenamento de ICUE ou de quaisquer outras informações classificadas, são aplicadas a presente decisão e as regras de execução pertinentes.
3. As medidas de segurança adotadas em aplicação da presente decisão devem ser conformes com os princípios de segurança na Comissão previstos no artigo 3.º da Decisão (UE, Euratom) 2015/443.

4. O diretor-geral dos Recursos Humanos e da Segurança deve criar a Autoridade de Segurança da Comissão na Direção-Geral dos Recursos Humanos e da Segurança. A Autoridade de Segurança da Comissão terá as responsabilidades que lhe são atribuídas pela presente decisão e pelas suas regras de execução.

5. Em cada serviço da Comissão, o responsável local de segurança (LSO), tal como referido no artigo 20.º da Decisão (UE, Euratom) 2015/443, tem as seguintes responsabilidades gerais em matéria de proteção das ICUE em conformidade com a presente decisão, em estreita colaboração com a Direção-Geral dos Recursos Humanos e da Segurança:

- a) gerir os pedidos de autorizações de segurança do pessoal;
- b) contribuir para ações de formação e de sensibilização em matéria de segurança;
- c) supervisionar o responsável do controlo do registo (RCO) do serviço;
- d) apresentar informações sobre quebras de segurança e comprometimento de ICUE;
- e) possuir duplicados das chaves e um registo escrito de cada combinação;
- f) assumir outras tarefas relacionadas com a proteção das ICUE ou definidas pelas regras de execução.

Artigo 8.º

Quebras de segurança e comprometimento de ICUE

1. As quebras de segurança resultam de atos ou omissões de uma pessoa que são contrários às regras de segurança estabelecidas na presente decisão e nas suas regras de execução.

2. O comprometimento de ICUE ocorre quando, em consequência de uma quebra de segurança, estas são, no todo ou em parte, divulgadas a pessoas não autorizadas.

3. As quebras de segurança de que haja conhecimento ou suspeita devem ser imediatamente comunicadas à Autoridade de Segurança da Comissão.

4. Quando haja conhecimento ou motivos razoáveis para presumir que houve comprometimento ou perda de ICUE, deve ser realizado um inquérito de segurança em conformidade com o artigo 13.º da Decisão (UE, Euratom) 2015/443.

5. Devem ser tomadas todas as medidas necessárias para:

- a) informar a entidade de origem;
- b) garantir que o caso seja investigado por elementos do pessoal não diretamente envolvidos na quebra de segurança, a fim de determinar os factos ocorridos;
- c) avaliar os danos eventualmente causados aos interesses da União ou dos Estados-Membros;
- d) tomar as medidas adequadas para impedir novas ocorrências; e
- e) notificar as autoridades competentes das medidas que tiverem sido tomadas.

6. O responsável pela violação das regras de segurança estabelecidas na presente decisão é passível de ação disciplinar, em conformidade com o disposto no Estatuto do Pessoal. O responsável pelo comprometimento ou pela perda de ICUE é passível de ação disciplinar e/ou judicial, em conformidade com as disposições legislativas e regulamentares aplicáveis.

CAPÍTULO 2

SEGURANÇA DO PESSOAL

Artigo 9.º

Definições

Para efeitos do presente capítulo, entende-se por:

- 1) «Autorização de acesso a ICUE»: uma decisão da Autoridade de Segurança da Comissão tomada com base na garantia dada por uma autoridade competente de um Estado-Membro de que pode ser facultado acesso a ICUE a um funcionário ou outro agente da Comissão, ou perito nacional destacado, até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, depois de comprovada a necessidade de essa pessoa tomar conhecimento de tais informações e tendo a mesma sido devidamente informada das responsabilidades que lhe incumbem; diz-se da pessoa nestas condições que «possui autorização de segurança».

- 2) «Autorização de segurança do pessoal»: aplicação de medidas destinadas a garantir que o acesso às ICUE só seja concedido a quem:
 - a) tenha necessidade de tomar conhecimento das informações,
 - b) possua a autorização de segurança para o nível adequado, se for caso disso; e
 - c) tenha sido informado das responsabilidades que lhe incumbem.
- 3) «Credenciação de Segurança do Pessoal» (CSP): declaração de uma autoridade competente de um Estado-Membro, feita depois de concluída uma investigação de segurança conduzida pelas autoridades competentes de um Estado-Membro, pela qual se atesta que uma dada pessoa pode aceder a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), e até determinada data, depois de comprovada a necessidade de essa pessoa tomar conhecimento de tais informações e tendo a mesma sido devidamente informada das responsabilidades que lhe incumbem;
- 4) «Certificado de Credenciação de Segurança do Pessoal» (CCSP): certificado emitido por uma autoridade competente pelo qual se atesta que uma dada pessoa possui uma credenciação de segurança válida ou uma autorização de segurança emitida pela Autoridade de Segurança da Comissão que indica o nível de ICUE a que a pessoa pode aceder (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de validade da credenciação ou autorização de segurança pertinente e a data de caducidade do próprio certificado;
- 5) «Investigação de Segurança»: procedimentos de investigação conduzidos pela autoridade competente de um Estado-Membro, em conformidade com as disposições legislativas e regulamentares nacionais, a fim de obter a garantia de que não há conhecimento de circunstâncias desfavoráveis que impeçam uma dada pessoa de obter uma credenciação de segurança até um determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior).

Artigo 10.º

Princípios básicos

1. O acesso a ICUE só pode ser concedido às pessoas depois de:
 - 1) ter ficado comprovada a sua necessidade de tomar conhecimento de tais informações;
 - 2) terem sido informadas das regras de segurança aplicáveis à proteção das ICUE e das normas e diretrizes de segurança pertinentes e terem reconhecido as suas responsabilidades no que respeita à proteção dessas informações;
 - 3) no caso de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, possuírem a autorização de segurança para o nível adequado ou outra autorização devidamente emitida, em virtude das funções que exercem, em conformidade com as disposições legislativas e regulamentares nacionais.
2. Todas as pessoas que, no exercício das suas funções, possam ter de aceder a ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior devem receber a autorização de segurança para o nível adequado antes de lhes ser facultado o acesso às referidas ICUE. A pessoa em causa deve consentir por escrito ser submetida ao procedimento de credenciação de segurança do pessoal. Se não o fizer, a pessoa não pode ser afetada a um cargo, função ou tarefa que implique o acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior.
3. Devem ser definidos procedimentos de credenciação de segurança do pessoal que permitam verificar se determinada pessoa pode ter acesso a ICUE, tendo em conta a sua lealdade, idoneidade e fiabilidade.
4. A lealdade, idoneidade e fiabilidade de uma dada pessoa para efeitos de atribuição de uma credenciação de segurança para acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são determinadas mediante uma investigação de segurança conduzida pelas autoridades competentes de um Estado-Membro em conformidade com as respetivas disposições legislativas e regulamentares nacionais.
5. A Autoridade de Segurança da Comissão é a única autoridade responsável pela ligação com as Autoridades Nacionais de Segurança (ANS) ou outras autoridades nacionais competentes relativamente a todas as questões de credenciação de segurança. Todos os contactos entre os serviços da Comissão e o seu pessoal e as ANS e outras autoridades competentes devem ser realizados através da Autoridade de Segurança da Comissão.

Artigo 11.º

Procedimento de autorização de segurança

1. Cada diretor-geral ou chefe de serviço da Comissão identifica os lugares no seu serviço cujos titulares precisam de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior para desempenhar as suas funções e que, consequentemente, precisam de receber uma autorização de segurança.

2. Logo que se saiba que uma pessoa vai ser nomeada para funções que exijam acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, o LSO do serviço da Comissão em questão deve informar a Autoridade de Segurança da Comissão, que transmite à pessoa em causa o questionário de credenciação de segurança emitido pela ANS do Estado-Membro de que seja nacional a pessoa nomeada como membro do pessoal das instituições europeias. A pessoa em causa deve dar o seu consentimento por escrito antes de ser submetida ao procedimento de credenciação de segurança e devolver o questionário preenchido o mais rapidamente possível à Autoridade de Segurança da Comissão.
3. A Autoridade de Segurança da Comissão envia o questionário de segurança do pessoal preenchido à ANS do Estado-Membro de que é nacional a pessoa nomeada como membro do pessoal das instituições europeias, solicitando a realização de uma investigação de segurança para o nível de ICUE às quais a pessoa deverá ter acesso.
4. Se a Autoridade de Segurança da Comissão tomar conhecimento de informações relevantes para a investigação de segurança a respeito de alguém que tenha solicitado uma credenciação de segurança, informa desse facto a ANS competente, em conformidade com as regras e regulamentações pertinentes.
5. Após a conclusão da investigação de segurança, e o mais rapidamente possível após ter sido notificada pela ANS competente da sua avaliação global dos resultados dessa investigação, a Autoridade de Segurança da Comissão:
 - a) se da investigação de segurança resultar a garantia de que não há conhecimento de fatores desfavoráveis que ponham em causa a lealdade, a idoneidade e a fiabilidade da pessoa, pode conceder à pessoa em causa uma autorização de acesso a ICUE até ao nível adequado e até uma data por ela especificada, por um período máximo de cinco anos;
 - b) se da investigação de segurança não resultar tal garantia, em conformidade com as regras e regulamentações aplicáveis, notifica do facto a pessoa em causa, que pode pedir para ser ouvida pela referida Autoridade. A Autoridade de Segurança da Comissão pode solicitar à ANS competente quaisquer outros esclarecimentos que esta possa prestar em conformidade com as respetivas disposições legislativas e regulamentares nacionais. Se os resultados da investigação de segurança se confirmarem, não é emitida uma autorização de acesso a ICUE.
6. A investigação de segurança, juntamente com os resultados obtidos, fica sujeita às disposições legislativas e regulamentares pertinentes em vigor no Estado-Membro em questão, incluindo em matéria de recurso. As decisões tomadas pela Autoridade de Segurança da Comissão são suscetíveis de recurso em conformidade com o Estatuto do Pessoal.
7. A Comissão aceita uma autorização de acesso a ICUE que seja concedida por qualquer outra instituição, organismo ou agência da União, desde que se mantenha válida. A autorização abrange quaisquer funções que a pessoa em causa venha a desempenhar na Comissão. A instituição, organismo ou agência da União no qual a pessoa assume funções informa a ANS competente da mudança de empregador.
8. Se o período de serviço da pessoa não tiver começado no prazo de 12 meses a contar da notificação dos resultados da investigação de segurança à Autoridade de Segurança da Comissão, ou se houver uma interrupção de 12 meses no serviço durante a qual a pessoa não exerceu funções na Comissão ou em qualquer outra instituição, organismo ou agência da União ou na administração de um Estado-Membro, a Autoridade de Segurança da Comissão remete a questão para a ANS competente, para confirmação de que a credenciação de segurança continua a ser válida e pertinente.
9. Se a Autoridade de Segurança da Comissão tomar conhecimento de informações a respeito da existência de qualquer risco para a segurança colocado por uma pessoa que disponha de uma autorização de segurança válida, informa desse facto a ANS competente, em conformidade com as regras e regulamentações pertinentes.
10. Se uma ANS comunicar à Autoridade de Segurança da Comissão que retirou a uma pessoa que possua uma autorização válida para acesso a ICUE a garantia que lhe fora dada em conformidade com o n.º 5, alínea a), a Autoridade de Segurança da Comissão pode solicitar à ANS quaisquer esclarecimentos que esta possa prestar em conformidade com as respetivas disposições legislativas e regulamentares nacionais. Se as informações desfavoráveis forem confirmadas pela ANS competente, a autorização de segurança deve ser retirada e a pessoa em causa excluída do acesso às ICUE e afastada de funções em que esse acesso seja possível ou a pessoa possa prejudicar a segurança.
11. A decisão de retirar ou suspender uma autorização de acesso a ICUE a qualquer pessoa abrangida pelo âmbito de aplicação da presente decisão e, se for caso disso, as razões que motivaram essa decisão são notificadas à pessoa em causa, que pode pedir para ser ouvida pela Autoridade de Segurança da Comissão. As informações prestadas pela ANS ficam sujeitas às disposições legislativas e regulamentares pertinentes em vigor no Estado-Membro em questão. As decisões tomadas neste contexto pela Autoridade de Segurança da Comissão são suscetíveis de recurso, em conformidade com o Estatuto do Pessoal.

12. Os serviços da Comissão devem certificar-se de que, antes de assumirem funções, os peritos nacionais destacados para um cargo que exija uma autorização de segurança para aceder a ICUE apresentam à Autoridade de Segurança da Comissão uma CSP válida ou um Certificado de Credenciação de Segurança do Pessoal (CCSP), em conformidade com as disposições legislativas e regulamentares nacionais. Com base nestes documentos, a Autoridade de Segurança da Comissão concede uma autorização de segurança para aceder a ICUE até ao nível equivalente ao referido na credenciação de segurança nacional, com uma validade máxima equivalente ao período da afetação.

Acesso a ICUE por pessoas devidamente autorizadas em virtude das funções que exercem

13. Os membros da Comissão, que têm acesso às ICUE em virtude das funções que exercem com base no Tratado, são informados acerca das suas obrigações de segurança no que respeita à proteção das ICUE.

Registos das credenciações de segurança e das autorizações de segurança

14. Os registos das credenciações e autorizações de segurança concedidas com vista ao acesso a ICUE devem ser mantidos pela Autoridade de Segurança da Comissão, em conformidade com a presente decisão. Esses registos devem especificar, pelo menos, o nível das ICUE a que a pessoa pode ter acesso, a data de emissão da credenciação de segurança e o seu período de validade.

15. A Autoridade de Segurança da Comissão pode emitir um CCSP indicando o nível de ICUE a que a pessoa pode ter acesso (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), o período de validade da autorização pertinente para efeitos de acesso a ICUE ou a data de expiração do próprio certificado.

Renovação das autorizações de segurança

16. Depois da primeira atribuição de uma autorização de segurança, e desde que a pessoa em causa tenha prestado ininterruptamente serviço na Comissão Europeia ou noutra instituição, organismo ou agência da União e continue a precisar de ter acesso a ICUE, a autorização de segurança para aceder a ICUE deve ser revista, para efeitos de renovação, regra geral, de cinco em cinco anos a contar da data da notificação dos resultados da última investigação de segurança que lhe tenha servido de base.

17. A Autoridade de Segurança da Comissão pode prorrogar o prazo de validade da autorização de segurança existente por um período de, no máximo, 12 meses, se não tiver sido recebida qualquer informação desfavorável da ANS ou de outra autoridade nacional competente no prazo de dois meses a contar da data de transmissão do pedido de renovação e do correspondente questionário de credenciação de segurança. Se, decorrido este período de 12 meses, a ANS em causa ou outra autoridade nacional competente não tiver notificado o seu parecer à Autoridade de Segurança da Comissão, a pessoa em causa é afetada a funções que não exijam uma autorização de segurança.

Artigo 12.º

Sessões de informação sobre as autorizações de segurança

1. Após terem participado na sessão de informação sobre as autorizações de segurança organizada pela Autoridade de Segurança da Comissão, as pessoas a quem tenha sido atribuída uma autorização de segurança devem confirmar por escrito que compreenderam as obrigações a que estão sujeitas no que respeita à proteção das ICUE e as consequências do comprometimento de ICUE. A Autoridade de Segurança da Comissão deve conservar um registo dessas declarações escritas.

2. As pessoas autorizadas a aceder a ICUE ou que precisem de manusear ICUE devem ser inicialmente sensibilizadas e periodicamente informadas das ameaças existentes para a segurança e comunicar imediatamente à Autoridade de Segurança da Comissão qualquer atitude ou atividade que considerem suspeita ou pouco habitual.

3. As pessoas que deixarem de exercer funções que exijam acesso a ICUE são informadas de que devem continuar a proteger as ICUE e, se necessário, confirmar por escrito essa sua obrigação.

Artigo 13.º

Autorizações de segurança temporárias

1. Em circunstâncias excecionais devidamente justificadas pelo interesse do serviço e na pendência da conclusão de uma investigação de segurança exaustiva, a Autoridade de Segurança da Comissão, após consulta da ANS do Estado-Membro de nacionalidade do interessado e sob reserva dos resultados da verificação inicial de que não há conhecimento de informações pertinentes desfavoráveis, pode conceder à pessoa em causa uma autorização temporária de acesso a ICUE para uma função específica, sem prejuízo das disposições relativas à renovação das credenciações de segurança. Essas autorizações temporárias de acesso a ICUE são válidas por um período único não superior a seis meses e não permitem o acesso a informações com classificação TRÈS SECRET UE/EU TOP SECRET.

2. Após terem assistido à sessão de informação em conformidade com o artigo 12.º, n.º 1, todas as pessoas a quem tenha sido concedida uma autorização temporária devem confirmar por escrito que compreenderam as obrigações a que estão sujeitas no que respeita à proteção das ICUE e as consequências do comprometimento de ICUE. A Autoridade de Segurança da Comissão deve conservar um registo dessas declarações escritas.

Artigo 14.º

Participação em reuniões classificadas organizadas pela Comissão

1. Os serviços da Comissão responsáveis pela organização de reuniões nas quais sejam discutidas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior informam, através do seu LSO ou do organizador da reunião, a Autoridade de Segurança da Comissão com bastante antecedência das datas, horários, locais e participantes nessas reuniões.

2. Sem prejuízo do disposto no artigo 11.º, n.º 13, as pessoas designadas para participar em reuniões organizadas pela Comissão nas quais sejam discutidas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior só o poderão fazer depois de confirmado o seu estatuto de credenciação de segurança ou de autorização de segurança. O acesso a estas reuniões deve ser recusado às pessoas que não tenham apresentado à Autoridade de Segurança da Comissão um CCSP ou outra prova de credenciação de segurança, bem como aos participantes da Comissão que não possuam uma autorização de segurança.

3. Antes de organizar uma reunião classificada, o responsável pela organização da reunião ou o LSO do serviço da Comissão que organiza a reunião solicita aos participantes externos que apresentem à Autoridade de Segurança da Comissão um CCSP ou outra prova da credenciação de segurança. A Autoridade de Segurança da Comissão informa o LSO ou o organizador da reunião do CCSP ou outra prova de CSP que tiver recebido. Quando aplicável, pode ser usada uma lista consolidada de nomes que forneça a prova de credenciação de segurança pertinente.

4. Se a Autoridade de Segurança da Comissão for informada pelas autoridades competentes de que foi retirada uma CSP a uma pessoa cujas funções requerem a participação em reuniões organizadas pela Comissão, deve notificar do facto o LSO do serviço da Comissão responsável pela organização da reunião.

Artigo 15.º

Acesso potencial a ICUE

Os estafetas, guardas e escoltas devem possuir a autorização de segurança para o nível adequado ou ser sujeitos a uma investigação adequada em conformidade com as disposições legislativas e regulamentares nacionais, ser informados dos procedimentos de segurança aplicáveis à proteção das ICUE e alertados para o seu dever de proteção das informações que lhes forem confiadas.

CAPÍTULO 3

SEGURANÇA FÍSICA DESTINADA A PROTEGER INFORMAÇÕES CLASSIFICADAS

Artigo 16.º

Princípios básicos

1. Devem ser concebidas medidas de segurança física que permitam impedir a entrada sub-reptícia ou forçada de intrusos, dissuadir, impedir e detetar ações não autorizadas e permitir uma diferenciação do pessoal no que se refere ao acesso a ICUE, segundo o princípio da necessidade de tomar conhecimento de tais informações. Essas medidas devem ser determinadas com base num processo de gestão do risco, em conformidade com a presente decisão e as suas regras de execução.

2. Em especial, devem ser concebidas medidas de segurança física para impedir o acesso não autorizado a ICUE:

- a) assegurando que as ICUE sejam manuseadas e armazenadas de forma adequada;
- b) permitindo a diferenciação do pessoal no que se refere ao acesso a ICUE com base na sua necessidade de tomar conhecimento de tais informações e, se for caso disso, na respetiva autorização de segurança;
- c) dissuadindo, impedindo e detetando ações não autorizadas; e
- d) impedindo ou retardando a entrada sub-reptícia ou forçada de intrusos.

3. Devem ser aplicadas medidas de segurança física em todas as instalações, edifícios, gabinetes, salas e outras zonas onde sejam manuseadas ou armazenadas ICUE, nomeadamente nas zonas em que se encontrem sistemas de comunicação e de informação, tal como referidos no capítulo 5.
4. As zonas onde sejam armazenadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior devem ser instituídas como Zonas de Segurança, em conformidade com o presente capítulo, e acreditadas pela Autoridade de Segurança da Comissão.
5. Só devem ser utilizados equipamentos ou dispositivos aprovados pela Autoridade de Segurança da Comissão para proteger as ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou superior.

Artigo 17.º

Requisitos e medidas de segurança física

1. As medidas de segurança física são selecionadas com base numa avaliação de risco feita pela Autoridade de Segurança da Comissão, sempre que adequado em consulta com outros serviços da Comissão, outras instituições, agências ou organismos da União e/ou as autoridades competentes dos Estados-Membros. A Comissão aplica um processo de gestão de risco à proteção das ICUE nas suas instalações, a fim de assegurar que seja concedido um nível de proteção física proporcional ao risco avaliado. No processo de gestão de risco devem ser tidos em conta todos os fatores pertinentes, nomeadamente:
 - a) o nível de classificação das ICUE;
 - b) a forma e o volume das ICUE, tendo em conta que as grandes quantidades ou acervos de ICUE podem justificar a aplicação de medidas de proteção mais rigorosas;
 - c) a envolvente e a estrutura dos edifícios ou zonas que albergam as ICUE; e
 - d) a avaliação da ameaça proveniente de serviços de informações que tenham por alvo a União, as suas instituições, organismos ou agências, ou os Estados-Membros, de atos de sabotagem ou de terrorismo, bem como de outras atividades subversivas ou criminosas.
2. A Autoridade de Segurança da Comissão, aplicando o conceito de defesa em profundidade, determina qual a combinação adequada de medidas de segurança física a implementar. Para o efeito, elabora normas e critérios mínimos de segurança, definidos nas regras de execução.
3. A Autoridade de Segurança da Comissão é autorizada a efetuar buscas nas entradas e saídas, que funcionam como elemento dissuasor da introdução não autorizada de material ou da saída não autorizada de ICUE das instalações ou edifícios.
4. Quando houver risco de olhares indiscretos sobre ICUE, mesmo que acidentalmente, os serviços da Comissão em causa devem tomar as medidas adequadas, tal como definidas pela Autoridade de Segurança da Comissão, para neutralizar esse risco.
5. Na fase de planeamento e conceção de novas instalações, devem ser definidos os requisitos de segurança física e as respetivas especificações funcionais, com o consentimento da Autoridade de Segurança da Comissão. Nas instalações já existentes, os requisitos de segurança física devem ser aplicados em conformidade com as normas e critérios mínimos previstos nas regras de execução.

Artigo 18.º

Equipamento para a proteção física das ICUE

1. São estabelecidos dois tipos de zonas fisicamente protegidas, para assegurar a proteção física das ICUE:
 - a) Zonas Administrativas; e
 - b) Zonas de Segurança (incluindo as Zonas Tecnicamente Seguras).
2. A Autoridade de Acreditação de Segurança da Comissão determina que uma dada zona preenche os requisitos para ser designada Zona Administrativa, Zona de Segurança ou Zona Tecnicamente Segura.
3. No caso das Zonas Administrativas:
 - a) é estabelecido um perímetro visivelmente definido que permita o controlo de pessoas e, se possível, de veículos;
 - b) só podem ter acesso sem escolta as pessoas devidamente autorizadas pela Autoridade de Segurança da Comissão ou por qualquer outra autoridade competente; e
 - c) quaisquer outras pessoas devem ser permanentemente escoltadas ou sujeitas a controlos equivalentes.

4. No caso das Zonas de Segurança:

- a) é estabelecido um perímetro visivelmente definido, em que qualquer entrada ou saída é controlada através de um sistema de livre-trânsito ou de reconhecimento de pessoas;
- b) só podem ter acesso sem escolta as pessoas com a devida credenciação de segurança e especificamente autorizadas a entrar nessa zona por terem necessidade de tomar conhecimento das ICUE em causa;
- c) quaisquer outras pessoas devem ser permanentemente escoltadas ou sujeitas a controlos equivalentes.

5. Nos casos em que a entrada numa Zona de Segurança represente, para todos os efeitos práticos, um acesso direto às informações classificadas que nela se encontrem, aplicam-se ainda os seguintes requisitos:

- a) deve haver uma indicação clara do nível de classificação de segurança mais elevado das informações normalmente conservadas nessa zona;
- b) todos os visitantes devem pedir uma autorização específica para entrar nessa zona, ser permanentemente escoltados e possuir a devida credenciação de segurança, a menos que sejam tomadas medidas para assegurar que não seja possível ter acesso às ICUE.

6. As Zonas de Segurança protegidas contra escutas são designadas Zonas Tecnicamente Seguras. A estas zonas aplicam-se ainda os seguintes requisitos:

- a) devem ser equipadas com um sistema de deteção de intrusos (IDS), fechadas à chave quando não estiverem ocupadas e guardadas quando ocupadas. Todas as chaves devem ser geridas em conformidade com o artigo 20.º;
- b) são sujeitas a controlo todas as pessoas ou material que nelas penetrem;
- c) são sujeitas a inspeção física e/ou técnica regular pela Autoridade de Segurança da Comissão. Essa inspeção deve ser igualmente efetuada na sequência de qualquer entrada não autorizada ou de suspeitas dessa possibilidade; e
- d) são desprovidas de dispositivos não autorizados, como linhas de comunicação, telefones ou outros aparelhos de comunicação, bem como equipamento elétrico ou eletrónico.

7. Não obstante o disposto no n.º 6, alínea d), e em circunstâncias em que a ameaça para as ICUE seja considerada elevada, qualquer tipo de aparelho de comunicações e equipamento elétrico ou eletrónico deve ser inspecionado pela Autoridade de Segurança da Comissão antes de ser utilizado em zonas onde decorram reuniões ou se trabalhe com informações com classificação SECRET UE/EU SECRET ou superior, por forma a garantir que nenhuma informação inteligível seja transmitida por esse equipamento, ilícita ou inadvertidamente, para fora do perímetro da Zona de Segurança.

8. As Zonas de Segurança que não estejam ocupadas por pessoal em serviço 24 horas por dia são, se necessário, inspecionadas no final das horas normais de serviço e a intervalos aleatórios fora dessas horas, a menos que esteja instalado um IDS.

9. Podem ser criadas temporariamente Zonas de Segurança e Zonas Tecnicamente Seguras no interior de uma determinada Zona Administrativa com vista à realização de uma reunião classificada ou qualquer outro fim semelhante.

10. O LSO do serviço da Comissão em questão estabelece procedimentos operacionais de segurança (SecOP) para cada Zona de Segurança sob a sua responsabilidade que estipulem, em conformidade com as disposições da presente decisão e das suas regras de execução:

- a) o nível das ICUE que podem ser manuseadas ou armazenadas nessa zona;
- b) as medidas de vigilância e de proteção a manter;
- c) as pessoas autorizadas a aceder sem escolta à zona por terem necessidade de tomar conhecimento das ICUE em causa e possuírem a devida autorização de segurança;
- d) se necessário, os procedimentos respeitantes a escoltas ou à proteção das ICUE, quando se autorize o acesso de outras pessoas a essa zona;
- e) quaisquer outras medidas e procedimentos pertinentes.

11. Devem ser construídas casas-fortes dentro das Zonas de Segurança. As paredes, o chão, os tetos, as janelas e as portas com sistema de fecho devem ser aprovados pela Autoridade de Segurança da Comissão e beneficiar de proteção equivalente à de um contentor de segurança aprovado para o armazenamento de ICUE com o mesmo nível de classificação.

Artigo 19.º

Medidas de proteção física para o manuseamento e armazenamento de ICUE

1. As ICUE com classificação RESTREINT UE/EU RESTRICTED podem ser manuseadas:
 - a) em Zonas de Segurança;
 - b) em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas; ou
 - c) fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas as transporte nas condições estabelecidas no artigo 31.º e se tenha comprometido a respeitar as medidas de compensação estabelecidas nas regras de execução, a fim de assegurar que as ICUE fiquem protegidas do acesso por parte de pessoas não autorizadas.
2. As ICUE com classificação RESTREINT UE/EU RESTRICTED devem ser armazenadas em mobiliário de escritório apropriado e fechado à chave, numa Zona Administrativa ou numa Zona de Segurança. As referidas ICUE podem ser temporariamente armazenadas fora de Zonas Administrativas ou de Zonas de Segurança, desde que o detentor das informações classificadas se tenha comprometido a respeitar as medidas de compensação estabelecidas nas regras de execução.
3. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET podem ser manuseadas:
 - a) em Zonas de Segurança;
 - b) em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas; ou
 - c) fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas:
 - i) se tenha comprometido a respeitar as medidas de compensação estabelecidas nas regras de execução, a fim de assegurar que as ICUE fiquem protegidas do acesso por parte de pessoas não autorizadas;
 - ii) mantenha as ICUE permanentemente sob o seu controlo pessoal; e
 - iii) no caso de documentos em suporte papel, tenha informado desse facto o registo competente.
4. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser armazenadas em Zonas de Segurança, dentro de um contentor de segurança ou de uma casa-forte.
5. As ICUE com classificação TRÈS SECRET UE/EU TOP SECRET devem ser manuseadas em Zonas de Segurança, criadas e mantidas pela Autoridade de Segurança da Comissão, e acreditadas a esse nível pela Autoridade de Acreditação de Segurança da Comissão.
6. As ICUE com classificação TRÈS SECRET UE/EU TOP SECRET devem ser armazenadas em Zonas de Segurança e acreditadas a esse nível pela Autoridade de Acreditação de Segurança da Comissão, numa das seguintes condições:
 - a) num contentor de segurança, em conformidade com o estabelecido no artigo 18.º, com pelo menos um dos seguintes controlos suplementares:
 - 1) proteção ou verificação permanente por pessoal de segurança ou de serviço com credenciação de segurança;
 - 2) um IDS aprovado, em combinação com pessoal de segurança incumbido das situações de emergência;ou
 - b) numa casa-forte com IDS, em combinação com pessoal de segurança incumbido das situações de emergência.

Artigo 20.º

Controlo das chaves e combinações de fechaduras de segredo utilizadas para proteção das ICUE

1. Nas regras de execução devem ser estabelecidos procedimentos para a gestão das chaves e das combinações das fechaduras de segredo dos gabinetes, salas, casas-fortes e contentores de segurança, em conformidade com o artigo 60.º. Tais procedimentos destinam-se a assegurar a proteção contra o acesso não autorizado.
2. As combinações devem ser memorizadas pelo menor número possível de pessoas que precisem de as conhecer. As combinações dos contentores de segurança e das casas-fortes em que sejam conservadas ICUE devem ser mudadas:
 - a) aquando da receção de um novo contentor;
 - b) sempre que mude o pessoal que conhece a combinação;
 - c) sempre que haja conhecimento ou suspeita de comprometimento;
 - d) sempre que uma fechadura tenha sido objeto de manutenção ou reparação; e
 - e) pelo menos de 12 em 12 meses.

CAPÍTULO 4

GESTÃO DAS INFORMAÇÕES CLASSIFICADAS DA UE

Artigo 21.º

Princípios básicos

1. Todos os documentos com ICUE são geridos em conformidade com a política da Comissão em matéria de gestão de documentos, pelo que devem ser registados, arquivados, conservados e, por fim, eliminados ou transferidos, integralmente ou por amostragem, para os arquivos históricos, em conformidade com a lista comum de conservação de dossiês da Comissão Europeia.
2. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são registadas, para fins de segurança, antes da distribuição e no momento da receção. As informações com classificação TRÈS SECRET UE/EU TOP SECRET devem ser inscritas em registos próprios.
3. Na Comissão, deve ser estabelecido um sistema de registo de ICUE, em conformidade com o disposto no artigo 27.º.
4. Os serviços e instalações da Comissão onde se proceda ao manuseamento ou armazenamento de ICUE devem ser inspecionados periodicamente pela Autoridade de Segurança da Comissão.
5. As ICUE são transmitidas entre diferentes serviços e instalações fora do perímetro das zonas fisicamente protegidas, de acordo com as regras a seguir enunciadas:
 - a) as ICUE são, regra geral, transmitidas por meios eletrónicos protegidos por produtos criptográficos aprovados em conformidade com o capítulo 5;
 - b) se não forem utilizados os meios referidos na alínea a), as ICUE são transportadas:
 - i) em suporte eletrónico (chaves USB, CD, discos rígidos) protegido por produtos criptográficos aprovados em conformidade com o capítulo 5; ou
 - ii) em todos os demais casos, nas condições estipuladas nas regras de execução.

Artigo 22.º

Classificações e marcas

1. As informações são classificadas se precisarem de proteção em virtude da sua confidencialidade, em conformidade com o artigo 3.º, n.º 1.
2. A entidade de origem das ICUE é responsável pela determinação do nível de classificação de segurança, em conformidade com as regras de execução pertinentes e as orientações e normas em matéria de classificação, bem como pela divulgação inicial das informações.
3. O nível de classificação das ICUE é determinado em conformidade com o artigo 3.º, n.º 2, e com as regras de execução pertinentes.
4. A classificação de segurança deve ser clara e corretamente indicada, independentemente de as ICUE serem apresentadas em papel, oralmente, eletronicamente ou por outro meio.
5. Cada uma das partes de um determinado documento (páginas, parágrafos, secções, anexos, apêndices, adendas e elementos apensos) pode exigir classificações diferentes, devendo ostentar a marca correspondente, inclusivamente quando for armazenada em suporte eletrónico.
6. A classificação geral de um documento ou dossiê deve ser pelo menos tão elevada como a da parte desse documento classificada ao nível mais elevado. Quando forem coligidas informações provenientes de várias fontes, o produto final é analisado para determinar o seu nível geral de classificação de segurança, uma vez que pode justificar uma classificação mais elevada do que a das partes que o compõem.
7. Na medida do possível, os documentos que contenham partes com níveis de classificação diferentes devem ser estruturados de forma a que as partes com um nível de classificação diferente possam ser facilmente identificadas e, se necessário, separadas.
8. A classificação de uma carta ou nota de envio deve ser tão elevada como a mais alta classificação dos seus anexos. A entidade de origem deve indicar claramente em que nível é classificada a carta ou nota quando separada dos anexos, utilizando uma marca adequada, por exemplo:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sem anexo(s) RESTREINT UE/EU RESTRICTED

Artigo 23.º

Marcas

Para além de uma das marcas de classificação de segurança previstas no artigo 3.º, n.º 2, as ICUE podem ostentar outras marcas, tais como:

- a) um identificador para designar a entidade de origem;
- b) eventuais advertências, códigos ou acrónimos que especifiquem o domínio de atividade a que o documento diz respeito, uma distribuição especial baseada na necessidade de ter conhecimento ou restrições de utilização;
- c) marcas relativas à comunicabilidade;
- d) se for caso disso, a data ou o acontecimento específico após os quais podem ser desgraduadas ou desclassificadas.

Artigo 24.º

Marcas de classificação abreviadas

1. Para indicar o nível de classificação de certos parágrafos de determinado texto, podem ser utilizadas marcas de classificação sob a forma de abreviaturas normalizadas. As abreviaturas não substituem as marcas de classificação por extenso.
2. Nos documentos classificados da UE, para indicar o nível de classificação de secções ou blocos do texto com menos de uma página, podem ser utilizadas as seguintes abreviaturas normalizadas:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Artigo 25.º

Produção de ICUE

1. Ao produzir um documento classificado da UE:
 - a) todas as páginas são marcadas de forma clara com o nível de classificação;
 - b) todas as páginas são numeradas;
 - c) o documento ostenta um número de registo e o assunto, que não constituem por si só informação classificada, a menos que estejam marcados como tal;
 - d) o documento é datado;
 - e) os documentos com classificação SECRET UE/EU SECRET ou superior que devam ser distribuídos em vários exemplares ostentam um número de exemplar em todas as páginas.
2. Quando não for possível aplicar o disposto no n.º 1 às ICUE, devem ser tomadas outras medidas adequadas, em conformidade com as regras de execução.

Artigo 26.º

Desgradação e desclassificação de ICUE

1. Aquando da produção de ICUE, a entidade de origem indica, sempre que possível, se as mesmas podem ser desgraduadas ou desclassificadas em determinada data ou após um dado acontecimento.
2. Cada serviço da Comissão deve analisar regularmente as ICUE de que seja a entidade de origem, a fim de apurar se o respetivo nível de classificação continua a ser aplicável. As regras de execução devem estabelecer um sistema para proceder, pelo menos de cinco em cinco anos, à reanálise do nível de classificação das ICUE registadas produzidas pela Comissão. Essa reanálise não é necessária se a entidade de origem tiver indicado à partida que as informações serão automaticamente desgraduadas ou desclassificadas e se nelas tiver sido aposta a marca correspondente.

3. As informações com classificação RESTREINT UE/EU RESTRICTED com origem na Comissão são consideradas automaticamente desclassificadas após trinta anos, em conformidade com o Regulamento (CEE, Euratom) n.º 354/83, com a redação que lhe foi dada pelo Regulamento (CE, Euratom) n.º 1700/2003 do Conselho ⁽¹⁾.

Artigo 27.º

Sistema de registo de ICUE na Comissão

1. Sem prejuízo do disposto no artigo 52.º, n.º 5, em cada serviço da Comissão onde sejam tratadas ou armazenadas ICUE ao nível CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET, deve ser identificado um responsável local pelo registo de ICUE para assegurar que estas informações sejam manuseadas em conformidade com a presente decisão.
2. O registo de ICUE gerido pelo Secretariado-Geral é o registo central de ICUE da Comissão. Serve de:
 - registo local de ICUE do Secretariado-Geral da Comissão,
 - registo de ICUE dos gabinetes dos membros da Comissão, exceto se estes dispuserem de um registo local de ICUE designado,
 - registo de ICUE das direções-gerais ou serviços que não dispõem de um registo local de ICUE,
 - principal ponto de entrada e de saída de todas as informações com classificação RESTREINT UE/EU RESTRICTED e superior, incluindo SECRET UE/EU SECRET, trocadas entre a Comissão e os seus serviços e os Estados terceiros e as organizações internacionais, bem como, quando tal estiver previsto em disposições específicas, outras instituições, agências e organismos da União.
3. Na Comissão, é designado pela Autoridade de Segurança da Comissão um registo que atuará como autoridade central de receção e envio de informações com classificação TRÈS SECRET UE/EU TOP SECRET. Se necessário, podem ser designados registos dependentes do registo central, a fim de manusear essas informações para efeitos de registo.
4. Os registos dependentes não podem comunicar documentos com classificação TRÈS SECRET UE/EU TOP SECRET diretamente a outros registos dependentes adstritos ao mesmo registo central TRÈS SECRET UE/EU TOP SECRET nem ao exterior sem a aprovação expressa deste último, concedida por escrito.
5. Os registos de ICUE devem ser estabelecidos como Zonas de Segurança, tal como definidas no capítulo 3, e acreditados pela Autoridade de Acreditação de Segurança (AAS) da Comissão.

Artigo 28.º

Responsável do controlo do registo

1. Cada registo de ICUE é gerido por um responsável do controlo do registo (RCO).
2. O RCO deve ter a credenciação de segurança adequada.
3. O RCO é sujeito à supervisão do LSO no serviço da Comissão em questão, se estiver em causa a aplicação das disposições relativas ao manuseamento de documentos que contenham ICUE e o cumprimento das regras de segurança, normas e orientações pertinentes.
4. No âmbito da responsabilidade pela gestão do registo de ICUE que lhe foi atribuída, o RCO assume as seguintes tarefas gerais, em conformidade com a presente decisão e com as regras de execução, normas e orientações pertinentes:
 - gerir as operações relativas ao registo, preservação, reprodução, tradução, transmissão, expedição e destruição ou transferência de ICUE para o serviço dos arquivos históricos,
 - verificar periodicamente a necessidade de manter a classificação das informações,
 - desempenhar quaisquer outras tarefas relacionadas com a proteção das ICUE definidas nas regras de execução.

Artigo 29.º

Registo de ICUE para efeitos de segurança

1. Para efeitos da presente decisão, entende-se por «registo para efeitos de segurança» («registo») a aplicação de procedimentos que registem o ciclo de vida das ICUE, incluindo a sua divulgação.

⁽¹⁾ Regulamento (CE, Euratom) n.º 1700/2003 do Conselho, de 22 de setembro de 2003, que altera o Regulamento (CEE, Euratom) n.º 354/83 relativo à abertura ao público dos arquivos históricos da Comunidade Económica Europeia e da Comunidade Europeia da Energia Atómica (JO L 243 de 27.9.2003, p. 1).

2. Todas as informações ou material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e superior são inscritos em registos próprios aquando da sua receção ou envio de uma entidade organizativa.
3. Quando as ICUE forem manuseadas ou armazenadas recorrendo a sistemas de comunicação e informação (SCI), estes podem executar os procedimentos de registo recorrendo aos seus próprios processos.
4. As regras de execução estabelecem disposições mais pormenorizadas relativas ao registo de ICUE para efeitos de segurança.

Artigo 30.º

Cópia e tradução de documentos classificados da UE

1. Os documentos com classificação TRÈS SECRET UE/EU TOP SECRET não podem ser copiados nem traduzidos sem o consentimento prévio, por escrito, da entidade de origem.
2. Os documentos com classificação SECRET UE/EU SECRET ou inferior podem ser copiados ou traduzidos por ordem do detentor, se a respetiva entidade de origem não tiver imposto restrições à sua cópia ou tradução.
3. As medidas de segurança aplicáveis ao documento original são igualmente aplicáveis às respetivas cópias e traduções.

Artigo 31.º

Transporte de ICUE

1. As ICUE devem ser transportadas de forma a protegê-las da divulgação não autorizada durante o seu transporte.
2. O transporte de ICUE fica sujeito às medidas de proteção, que devem:
 - ser proporcionais ao nível de classificação das ICUE transportadas, e
 - ser adaptadas às condições específicas do seu transporte, em especial consoante as ICUE forem transportadas:
 - no interior de um edifício ou bloco de edifícios da Comissão,
 - entre edifícios da Comissão situados no mesmo Estado-Membro,
 - dentro do território da União,
 - do território da União para o território de um Estado terceiro, e
 - ser adaptadas à natureza e à forma das ICUE.
3. Estas medidas de proteção devem ser estabelecidas pormenorizadamente nas regras de execução, ou, no caso dos projetos e programas referidos no artigo 42.º, como parte integrante das instruções de segurança do programa ou projeto (ISP) pertinentes.
4. As regras de execução ou ISP devem incluir disposições proporcionais ao nível das ICUE no que diz respeito:
 - ao tipo de transporte, como o transporte em mão própria, em mala diplomática, por serviços de estafetas militares, pelos serviços postais ou por serviços comerciais de estafeta;
 - à embalagem das ICUE,
 - às contramedidas técnicas para as ICUE transportadas por meios electrónicos,
 - a qualquer outra medida processual, física ou eletrónica,
 - aos procedimentos de registo,
 - ao recurso a pessoal de segurança autorizado.
5. Quando as ICUE forem transportadas por meios electrónicos, e não obstante o disposto no artigo 21.º, n.º 5, as medidas de proteção estabelecidas nas regras de execução pertinentes podem ser complementadas pelas contramedidas técnicas adequadas aprovadas pela Autoridade de Segurança da Comissão, a fim de minimizar o risco de perda ou comprometimento.

*Artigo 32.º***Destruição de ICUE**

1. Os documentos classificados da UE que deixem de ser necessários podem ser destruídos, tendo em conta a regulamentação em matéria de arquivos e as regras e regulamentações da Comissão em matéria de gestão e arquivo de documentos, em especial a lista comum de conservação a nível da Comissão.
2. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são destruídas pelo RCO do registo responsável pelas ICUE por ordem do detentor ou de uma autoridade competente. O RCO atualiza os livros de registo e outras informações de registo em conformidade.
3. A destruição dos documentos com classificação SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET é efetuada pelo RCO na presença de uma testemunha, que deve possuir uma credenciação pelo menos equivalente ao nível de classificação dos documentos a destruir.
4. O funcionário do registo e a testemunha, sempre que a presença desta última seja exigida, assinam um certificado de destruição, que é arquivado no registo. O RCO do registo responsável pelas ICUE conserva os certificados de destruição dos documentos com classificação TRÈS SECRET UE/EU TOP SECRET durante um período mínimo de dez anos e os dos documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET durante um período mínimo de cinco anos.
5. Os documentos classificados, incluindo os documentos com classificação RESTREINT UE/EU RESTRICTED, são destruídos por métodos definidos nas regras de execução e que respeitem as normas da UE pertinentes ou normas equivalentes.
6. A destruição dos suportes informáticos de ICUE é efetuada em conformidade com os procedimentos estabelecidos nas regras de execução.

*Artigo 33.º***Destruição de ICUE em situações de emergência**

1. Os serviços da Comissão que detêm ICUE devem elaborar, com base nas condições locais, planos para a salvaguarda do material classificado da UE em situações de crise, incluindo, se necessário, a destruição de emergência e planos de evacuação. Esses serviços devem publicar as instruções consideradas necessárias para impedir que as ICUE possam chegar às mãos de pessoas não autorizadas.
2. As disposições para a salvaguarda e/ou destruição de material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET numa situação de crise não devem prejudicar, em caso algum, a salvaguarda ou a destruição de material com classificação TRÈS SECRET UE/EU TOP SECRET (incluindo o equipamento de cifragem), cujo tratamento deve ter prioridade sobre todas as outras tarefas.
3. Em caso de emergência, se houver um risco iminente de divulgação não autorizada, as ICUE devem ser destruídas pelo seu detentor de modo a não poderem ser reconstituídas integral ou parcialmente. A entidade e o registo de origem devem ser informados da destruição de emergência das ICUE registadas.
4. As regras de execução devem estabelecer disposições mais pormenorizadas sobre a destruição de ICUE.

CAPÍTULO 5

PROTEÇÃO DAS INFORMAÇÕES CLASSIFICADAS DA UE NOS SISTEMAS DE COMUNICAÇÃO E INFORMAÇÃO (SCI)*Artigo 34.º***Princípios básicos da garantia da informação**

1. A garantia da informação (GI) no domínio dos sistemas de comunicação e informação consiste na confiança de que esses sistemas protegem as informações neles manuseadas e funcionam como devem, quando for necessário, sob o controlo de utilizadores legítimos.

2. Uma garantia da informação eficaz deve assegurar níveis adequados de:

Autenticidade: a garantia de que a informação é genuína e provém de fonte fidedigna;

Disponibilidade: a propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada;

Confidencialidade: a propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas ou segundo processos não autorizados;

Integridade: a propriedade de salvaguardar o carácter exato e completo dos ativos e da informação;

Não rejeição: a capacidade de provar que um ato ou acontecimento teve lugar, de modo a que esse acontecimento ou ato não possa ser subseqüentemente negado.

3. A GI baseia-se num processo de gestão de risco.

Artigo 35.º

Definições

Para efeitos do presente capítulo, entende-se por:

- a) «Acreditação»: a autorização e aprovação formal concedidas a um sistema de comunicação e informação pela Autoridade de Acreditação de Segurança (AAS) para tratar ICUE no seu ambiente operacional, após a validação formal do plano de segurança e a sua correta aplicação;
- b) «Processo de acreditação»: as medidas e tarefas necessárias exigidas antes da acreditação pela Autoridade de Acreditação de Segurança. Estas medidas e tarefas devem ser especificadas numa norma do processo de acreditação;
- c) «Sistema de comunicação e informação (SCI)»: qualquer sistema que permita o manuseamento de informações em formato eletrónico. Um sistema de comunicação e informação compreende todos os meios necessários ao seu funcionamento, designadamente a infraestrutura, a organização, o pessoal e os recursos em matéria de informação;
- d) «Risco residual»: o risco que permanece após terem sido aplicadas medidas de segurança, dado que não é possível neutralizar todas as ameaças nem eliminar todas as vulnerabilidades;
- e) «Risco»: a possibilidade de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos. Mede-se pela combinação da probabilidade de as ameaças ocorrerem e do respetivo impacto;
- f) «Aceitação do risco»: decisão de aceitar a persistência de um risco residual após o tratamento do risco;
- g) «Avaliação do risco»: identificação das ameaças e vulnerabilidades e realização da análise de risco conexa, ou seja, a análise da probabilidade e do impacto;
- h) «Comunicação do risco»: consciencialização dos grupos de utilizadores de SCI para os riscos, informação das autoridades de aprovação quanto a esses riscos e comunicação dos mesmos às autoridades operacionais;
- i) «Tratamento do risco»: atenuação, eliminação, redução (mediante uma combinação adequada de medidas técnicas, materiais, organizativas e processuais), transferência ou acompanhamento do risco.

Artigo 36.º

Manuseamento de ICUE pelos SCI

1. Os SCI devem manusear as ICUE em conformidade com o conceito de GI.

2. Para os SCI que manuseiam ICUE, a conformidade com a política de segurança dos sistemas de informação da Comissão, tal como referida na Decisão C(2006) 3602 ⁽¹⁾ da Comissão, implica que:

- a) a abordagem «planear-efetuar-verificar-atuar» deve ser aplicada à implementação da política de segurança dos sistemas de informação durante todo o ciclo de vida do sistema de informação;
- b) as necessidades de segurança devem ser identificadas através de uma avaliação do impacto sobre as atividades;
- c) o sistema de informação e os dados nele contidos devem ser objeto de uma classificação formal dos ativos;

⁽¹⁾ Decisão C(2006) 3602, de 16 de agosto de 2006, relativa à segurança dos sistemas de informação utilizados pela Comissão Europeia.

- d) devem ser implementadas todas as medidas de segurança obrigatórias, tal como determinadas pela política de segurança dos sistemas de informação;
 - e) deve ser aplicado um processo de gestão de risco, que consiste nas seguintes etapas: identificação das ameaças e vulnerabilidades, avaliação do risco, tratamento do risco, aceitação do risco e comunicação do risco;
 - f) deve ser definido, executado, verificado e reexaminado um plano de segurança que inclua a política de segurança e os procedimentos operacionais de segurança.
3. Todo o pessoal envolvido na conceção, desenvolvimento, ensaio, exploração, gestão ou utilização de SCI que manuseiem ICUE deve notificar à AAS todas as potenciais lacunas de segurança, incidentes, violações da segurança ou comprometimentos suscetíveis de ter impacto sobre a proteção do SCI e/ou as ICUE nele contidas.
4. Quando a proteção das ICUE for assegurada por produtos criptográficos, estes devem ser aprovados de acordo com o seguinte procedimento:
- a) é dada preferência aos produtos que tiverem sido aprovados pelo Conselho ou pelo Secretário-Geral do Conselho, na qualidade de Autoridade de Aprovação Criptográfica do Conselho, por recomendação do grupo de peritos de segurança da Comissão;
 - b) quando tal se justifique por razões operacionais específicas, a Autoridade de Aprovação Criptográfica da Comissão (AAC) pode, por recomendação do grupo de peritos de segurança da Comissão, dispensar os requisitos previstos na alínea a) e conceder uma aprovação provisória para um período específico.
5. Durante a transmissão, tratamento e armazenamento de ICUE por via eletrónica, devem ser utilizados produtos criptográficos aprovados. Não obstante este requisito, podem ser aplicados procedimentos específicos, em situações de emergência ou em configurações técnicas específicas, após aprovação pela AAC.
6. São aplicadas medidas de segurança para proteger os SCI que manuseiem informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior contra o risco de comprometimento de tais informações devido a emanações eletromagnéticas não intencionais («medidas de segurança TEMPEST»). Essas medidas de segurança devem ser proporcionais ao risco de exploração e ao nível de classificação das informações.
7. A Autoridade de Segurança da Comissão assume as seguintes funções:
- Autoridade de GI (AGI),
 - Autoridade de Acreditação de Segurança (AAS),
 - Autoridade TEMPEST (AT),
 - Autoridade de Aprovação Criptográfica (AAC),
 - Autoridade de Distribuição Criptográfica (ADC).
8. A Autoridade de Segurança da Comissão deve designar, para cada sistema, a Autoridade Operacional de GI.
9. As responsabilidades inerentes às funções descritas nos n.ºs 7 e 8 são definidas nas regras de execução.

Artigo 37.º

Acreditação dos SCI que manuseiam ICUE

1. Todos os SCI que manuseiam ICUE devem ser objeto de um processo de acreditação, com base nos princípios da garantia da informação, cujo nível de pormenor deve ser proporcional ao nível de proteção exigido.
2. O processo de acreditação inclui a validação formal, pela AAS da Comissão, do plano de segurança para o SCI em causa, de modo a obter a garantia de que:
- a) o processo de gestão de risco referido no artigo 36.º, n.º 2, foi corretamente executado;
 - b) o proprietário do sistema aceitou conscientemente o risco residual; e
 - c) foi alcançado um nível de proteção suficiente do SCI e das ICUE nele manuseadas, em conformidade com a presente decisão.

3. A AAS da Comissão emite uma declaração de acreditação que determina o nível máximo de classificação das ICUE que podem ser manuseadas pelo SCI, bem como as respetivas modalidades e condições de execução. Tal não prejudica as tarefas confiadas ao Comité de Acreditação de Segurança definido no artigo 11.º do Regulamento (UE) n.º 512/2014 do Parlamento Europeu e do Conselho ⁽¹⁾.
4. Um Comité Conjunto de Acreditação de Segurança (CAS) é responsável pela acreditação dos SCI da Comissão que envolvam várias partes. O Comité Conjunto é composto por um representante da AAS de cada parte interessada e presidido por um representante da AAS da Comissão.
5. O processo de acreditação consiste numa série de tarefas a executar pelas partes envolvidas. A responsabilidade pela preparação dos processos e da documentação de acreditação cabe inteiramente ao proprietário do SCI.
6. A acreditação é da responsabilidade da AAS da Comissão, que, a qualquer momento durante o ciclo de vida do SCI, tem o direito de:
 - a) exigir a aplicação de um processo de acreditação;
 - b) realizar uma auditoria ou inspeção do SCI;
 - c) sempre que as condições de funcionamento deixem de estar preenchidas, exigir a definição e aplicação efetiva de um plano de melhoria da segurança, num calendário bem definido, retirando eventualmente a autorização de funcionamento do SCI até as condições de funcionamento voltarem a estar reunidas.
7. O processo de acreditação é estabelecido numa norma sobre o processo de acreditação dos SCI que manuseiam ICUE, que deve ser adotada em conformidade com o artigo 10.º, n.º 3, da Decisão C(2006) 3602.

Artigo 38.º

Circunstâncias de emergência

1. Não obstante o disposto no presente capítulo, os procedimentos específicos a seguir descritos podem ser aplicados numa emergência, nomeadamente em situações de crise iminente ou real, de conflito ou de guerra, ou em circunstâncias operacionais excecionais.
2. As ICUE podem ser transmitidas através de produtos criptográficos aprovados para um nível de classificação inferior, ou sem cifragem, com o consentimento da autoridade competente, se o prejuízo causado por um atraso for claramente mais grave do que o decorrente da eventual divulgação do material classificado, e se:
 - a) o remetente e o destinatário não dispuserem do dispositivo de cifragem necessário; e
 - b) o material classificado não puder ser enviado a tempo por outros meios.
3. As informações classificadas transmitidas nas circunstâncias referidas no n.º 1 não podem ostentar marcas nem indicações que as distingam de informações não classificadas ou de informações que possam ser protegidas por produtos de cifragem disponíveis. Os destinatários devem ser imediatamente notificados, por outros meios, do nível de classificação das informações.
4. Subsequentemente deve ser apresentado um relatório à autoridade competente e ao grupo de peritos de segurança da Comissão.

CAPÍTULO 6

SEGURANÇA INDUSTRIAL

Artigo 39.º

Princípios básicos

1. Entende-se por «segurança industrial» a aplicação de medidas destinadas a garantir a proteção das ICUE:
 - a) no âmbito de contratos classificados, pelos:
 - i) candidatos ou proponentes durante o concurso e o procedimento de adjudicação do contrato;
 - ii) contratantes ou subcontratantes durante a vigência dos contratos classificados;

⁽¹⁾ Regulamento (UE) n.º 512/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, que altera o Regulamento (CE) n.º 912/2010 que cria a Agência do GNSS Europeu (JO L 150 de 20.5.2014, p. 72).

- b) no âmbito de convenções de subvenção classificadas, pelos:
 - i) requerentes durante os procedimentos de concessão de subvenções;
 - ii) beneficiários durante a vigência das convenções de subvenção classificadas.
- 2. Estes contratos ou convenções de subvenção não podem envolver informações com classificação TRÈS SECRET UE/ /EU TOP SECRET.
- 3. Salvo indicação em contrário, as disposições do presente capítulo referentes a contratos classificados ou contratantes são igualmente aplicáveis a subcontratos classificados ou subcontratantes.

Artigo 40.º

Definições

Para efeitos do presente capítulo, entende-se por:

- a) «Contrato classificado»: um contrato-quadro ou contrato, tal como referido no Regulamento (CE, Euratom) n.º 1605/2002 do Conselho ⁽¹⁾, celebrado pela Comissão ou um dos seus serviços com um contratante para o fornecimento de bens móveis ou imóveis, a execução de obras ou a prestação de serviços, cuja execução exija ou implique a produção, tratamento ou armazenamento de ICUE;
- b) «Subcontrato classificado»: um contrato celebrado entre um contratante da Comissão ou de um dos seus serviços e outro contratante (ou seja, o subcontratante) para o fornecimento de bens móveis ou imóveis, a realização de obras ou a prestação de serviços, cuja execução exija ou implique a produção, tratamento ou armazenamento de ICUE;
- c) «Convenção de subvenção classificada»: um acordo nos termos do qual a Comissão concede uma subvenção, como referida na parte I, título VI, do Regulamento (CE, Euratom) n.º 1605/2002, cuja execução exija ou implique a produção, tratamento ou armazenamento de ICUE;
- d) «Autoridade de Segurança Designada» (ASD): autoridade responsável perante a Autoridade Nacional de Segurança (ANS) de um Estado-Membro que está encarregada de comunicar às entidades industriais ou outras a política nacional em todas as matérias relacionadas com a segurança industrial e de facultar orientação e prestar assistência na sua implementação. As funções de ASD podem ser desempenhadas pela ANS ou por qualquer outra autoridade competente.

Artigo 41.º

Procedimento aplicável aos contratos classificados ou às convenções de subvenção classificadas

- 1. Ao adjudicar contratos classificados ou ao conceder subvenções classificadas, cada serviço da Comissão, na qualidade de autoridade contratante, deve garantir a referência ou integração no contrato das normas mínimas de segurança industrial estabelecidas no presente capítulo, bem como o seu cumprimento.
- 2. Para efeitos do n.º 1, os serviços competentes da Comissão devem solicitar o parecer da Direção-Geral dos Recursos Humanos e da Segurança, nomeadamente da Direção da Segurança, e garantir que os modelos de contratos e subcontratos e os modelos de convenções de subvenção incluem disposições que relembram os princípios básicos e as normas mínimas aplicáveis à proteção das ICUE a respeitar pelos contratantes e subcontratantes e pelos beneficiários de subvenções, respetivamente.
- 3. A Comissão trabalha em estreita cooperação com as ANS, as ASD ou quaisquer outras autoridades competentes dos Estados-Membros em causa.
- 4. Sempre que uma autoridade contratante tencione lançar um procedimento com vista à celebração de um contrato classificado ou de uma convenção de subvenção classificada, deve solicitar o parecer da Autoridade de Segurança da Comissão sobre o caráter e os elementos classificados do procedimento, em todas as suas fases.
- 5. Após consulta do grupo de peritos de segurança da Comissão, devem ser estabelecidos nas regras de execução em matéria de segurança industrial os modelos de contratos e subcontratos classificados, de convenções de subvenção classificadas, de anúncios de contrato, as orientações sobre as circunstâncias em que é necessária uma Credenciação de Segurança da Empresa (CSE), as instruções de segurança do programa ou projeto (ISP), as Cláusulas Adicionais de Segurança (CAS), as visitas, a transmissão e transporte de ICUE no âmbito de contratos classificados ou de convenções de subvenção classificadas.

⁽¹⁾ Regulamento (CE, Euratom) n.º 1605/2002 do Conselho, de 25 de junho de 2002, que institui o Regulamento Financeiro aplicável ao orçamento geral das Comunidades Europeias (JO L 248 de 16.9.2002, p. 1).

6. A Comissão pode celebrar contratos classificados ou convenções de subvenção classificadas no âmbito dos quais sejam confiadas tarefas, que envolvam ou impliquem o acesso a ICUE ou o seu manuseamento ou armazenamento, a operadores económicos registados num Estado-Membro ou num Estado terceiro com o qual tenha sido celebrado um acordo ou um convénio administrativo, em conformidade com o capítulo 7 da presente decisão.

Artigo 42.º

Elementos de segurança num contrato classificado ou numa convenção de subvenção classificada

1. Os contratos classificados e as convenções de subvenção classificadas devem incluir os seguintes elementos de segurança:

Instruções de Segurança do Programa ou Projeto

- a) «Instruções de Segurança do Programa ou Projeto» (ISP): lista de procedimentos de segurança que são aplicados a um programa ou projeto específico a fim de normalizar os procedimentos de segurança. As ISP podem ser revistas em qualquer fase do programa ou projeto;
- b) a Direção-Geral dos Recursos Humanos e da Segurança elabora ISP genéricas. Os serviços da Comissão responsáveis pelos programas ou projetos que impliquem o manuseamento ou armazenamento de ICUE podem, se for caso disso, elaborar ISP específicas, baseadas nas ISP genéricas;
- c) são elaboradas ISP específicas, em especial para os programas e projetos caracterizados pelo seu grande alcance, dimensão ou complexidade ou pela multiplicidade e/ou diversidade dos contratantes, beneficiários e outros parceiros e interessados, por exemplo no que respeita ao seu estatuto jurídico. As ISP específicas devem ser elaboradas pelo(s) serviço(s) da Comissão que gere(m) o programa ou projeto, em estreita colaboração com a Direção-Geral dos Recursos Humanos e da Segurança;
- d) a Direção-Geral dos Recursos Humanos e da Segurança submete à apreciação do grupo de peritos de segurança da Comissão tanto as ISP genéricas como as específicas.

Cláusulas Adicionais de Segurança

- a) «Cláusula Adicional de Segurança» (CAS): condições contratuais especiais emitidas pela autoridade contratante que fazem parte integrante de um contrato classificado que implica o acesso a ICUE ou a sua produção, e nas quais são identificados os requisitos de segurança e as partes do contrato que exigem proteção de segurança;
 - b) os requisitos de segurança específicos de determinado contrato são descritos numa CAS. Esta CAS compreende, sempre que necessário, o Guia da Classificação de Segurança (GCS) e faz parte integrante do contrato ou subcontrato classificado ou da convenção de subvenção classificada;
 - c) a CAS contém disposições que exigem que o contratante ou o beneficiário cumpram as normas mínimas estabelecidas na presente decisão. A autoridade contratante deve certificar-se de que o CAS determina que o incumprimento dessas normas mínimas pode constituir motivo suficiente para a denúncia do contrato ou da convenção de subvenção.
2. Tanto as ISP como a CAS devem conter um GCS como elemento de segurança obrigatório:
- a) «Guia da Classificação de Segurança» (GCS): um documento que descreve as partes classificadas do programa, projeto, contrato ou convenção de subvenção, especificando os níveis da classificação de segurança aplicáveis. O GCS pode ser alargado durante a vigência do programa, projeto, contrato ou convenção de subvenção e as informações podem ser reclassificadas ou desgraduadas; quando existe um GCS, este faz parte integrante das CAS.
 - b) antes de abrir concursos ou de adjudicar contratos classificados, o serviço da Comissão determina, enquanto autoridade contratante, qual a classificação de segurança de todas as informações a fornecer aos candidatos e proponentes ou contratantes, bem como de todas as informações a produzir pelos contratantes. Para o efeito, elabora um GCS para ser utilizado na execução do contrato, em conformidade com a presente decisão e as suas regras de execução, após consulta da Autoridade de Segurança da Comissão.

- c) para determinar qual a classificação de segurança das várias partes de um contrato classificado, são aplicáveis os seguintes princípios:
- i) na elaboração do GCS, o serviço da Comissão, enquanto autoridade contratante, tem em consideração todos os aspetos de segurança pertinentes, nomeadamente a classificação de segurança atribuída às informações fornecidas e aprovadas pela respetiva entidade de origem para utilização no âmbito do contrato;
 - ii) o nível global de classificação do contrato não pode ser inferior à classificação mais elevada de qualquer das suas partes; e
 - iii) se necessário, a autoridade contratante contacta, através da Autoridade de Segurança da Comissão, as ANS, ASD ou quaisquer outras autoridades de segurança competentes dos Estados-Membros quando houver alguma alteração à classificação das informações produzidas pelos contratantes ou a estas fornecidas na execução de um contrato e quando pretender fazer alterações ao GCS.

Artigo 43.º

Acesso a ICUE por parte do pessoal dos contratantes e dos beneficiários

A autoridade contratante ou que concede a subvenção deve assegurar que o contrato classificado ou a convenção de subvenção classificada contenha disposições que determinem que o acesso a ICUE só deve ser concedido ao pessoal de um contratante, subcontratante ou beneficiário que, para a execução do contrato, subcontrato ou convenção de subvenção classificado, solicitar tal acesso se:

- a) a pessoa possuir uma autorização de segurança para o nível adequado ou outra autorização devidamente emitida em que tenha ficado comprovada a sua necessidade de tomar conhecimento das informações;
- b) a pessoa tiver sido informada das regras de segurança aplicáveis à proteção das ICUE e tiver reconhecido as suas responsabilidades no que respeita à proteção dessas informações;
- c) a pessoa possuir uma credenciação de segurança ao nível adequado para informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET emitida pela respetiva ANS, ASD ou qualquer outra autoridade competente.

Artigo 44.º

Credenciação de Segurança da Empresa

1. «Credenciação de Segurança da Empresa» (CSE): decisão administrativa, emitida por uma ANS, ASD ou qualquer outra autoridade de segurança competente, de que, do ponto de vista da segurança, determinada empresa está apta a garantir um nível adequado de proteção das ICUE com determinado nível de classificação de segurança.
2. Uma CSE concedida pela ANS, ASD ou qualquer outra autoridade de segurança competente de um Estado-Membro para indicar, em conformidade com as disposições legislativas e regulamentares nacionais, que um operador económico está em condições de proteger as ICUE ao nível de classificação adequado (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET) dentro das respetivas instalações deve ser apresentada à Autoridade de Segurança da Comissão que, por sua vez, a transmite ao serviço da Comissão, na qualidade de autoridade contratante ou que concede a subvenção, antes de poder ser facultado acesso a ICUE a um candidato, proponente ou contratante, ou a um requerente ou beneficiário de uma subvenção.
3. Se necessário, a autoridade contratante informa, através da Autoridade de Segurança da Comissão, a ANS, ASD, ou qualquer outra autoridade de segurança competente, de que é necessária uma CSE para a execução do contrato. É exigida uma CSE ou uma CSP quando tiverem de ser fornecidas ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET durante o procedimento de adjudicação do contrato ou de concessão da subvenção.
4. A autoridade contratante ou que concede a subvenção não adjudica um contrato classificado nem celebra uma convenção de subvenção com o proponente ou participante preferido antes de ter recebido, da ANS, ASD ou qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante em causa esteja registado, confirmação de que, sendo exigível, foi emitida a CSE adequada.
5. Quando a Autoridade de Segurança da Comissão tiver sido notificada pela ANS, a ASD ou qualquer outra autoridade de segurança competente que tenha emitido uma CSE de qualquer alteração que afete a CSE, deve informar o serviço da Comissão, na qualidade de autoridade contratante ou que concede a subvenção. No caso da subcontratação, é informada em conformidade a ANS, a ASD ou qualquer outra autoridade de segurança competente.

6. A retirada de uma CSE pela ANS, a ASD ou qualquer outra autoridade de segurança competente constitui motivo suficiente para que a autoridade contratante ou que concede a subvenção ponha termo a um contrato classificado ou exclua do procedimento concorrencial um candidato, proponente ou requerente de subvenção. Deve ser incluída uma disposição para o efeito nos modelos de contrato e nas convenções de subvenção.

Artigo 45.º

Disposições a incluir nos contratos classificados e nas convenções de subvenção classificadas

1. Quando forem fornecidas ICUE a um candidato, proponente ou requerente de subvenção durante o procedimento de contratação, o anúncio de concurso ou o convite à apresentação de propostas deve conter uma disposição que obrigue o candidato, proponente ou requerente de subvenção que não chegue a apresentar uma proposta ou não seja selecionado a devolver todos os documentos classificados num prazo determinado.
2. A autoridade contratante ou que concede a subvenção deve notificar, através da Autoridade de Segurança da Comissão, a ANS, ASD ou qualquer outra autoridade de segurança competente de que foi adjudicado um contrato classificado ou celebrada uma convenção de subvenção classificada, bem como os dados relevantes, como o nome do(s) contratante(s) ou dos beneficiários, a duração do contrato e o nível máximo de classificação.
3. Quando tais contratos ou convenções de subvenção chegarem ao termo, a autoridade contratante ou que concede a subvenção deve notificar imediatamente do facto, através da Autoridade de Segurança da Comissão, a ANS, a ASD ou qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou o beneficiário da subvenção esteja registado.
4. No termo do contrato classificado ou da convenção de subvenção classificada, ou da participação de um beneficiário de uma subvenção, o contratante ou o beneficiário da subvenção deve, regra geral, restituir à autoridade contratante ou que concede a subvenção quaisquer ICUE que se encontrem na sua posse.
5. São estabelecidas na CAS disposições específicas referentes à eliminação das ICUE durante a fase de execução ou após o termo do contrato classificado ou da convenção de subvenção classificada.
6. Quando o contratante ou beneficiário de uma subvenção for autorizado a conservar ICUE após o termo de um contrato classificado ou de uma convenção de subvenção classificada, as normas mínimas estabelecidas na presente decisão devem continuar a ser cumpridas e a confidencialidade das ICUE protegida pelo contratante ou beneficiário de uma subvenção.

Artigo 46.º

Disposições específicas a incluir nos contratos classificados

1. As condições para a proteção das ICUE ao abrigo das quais os contratantes podem subcontratar devem ser definidas no anúncio de concurso e no contrato classificado.
2. Antes de procederem à subcontratação de qualquer parte de um contrato classificado, os contratantes devem obter a autorização da autoridade contratante. Nenhum subcontrato que implique o acesso a ICUE pode ser adjudicado a subcontratantes registados num país terceiro, exceto se existir um quadro regulamentar para a segurança das informações, como previsto no capítulo 7.
3. O contratante é responsável por garantir que todas as atividades de subcontratação respeitam as normas mínimas estabelecidas na presente decisão e não pode fornecer ICUE a nenhum subcontratante sem o prévio consentimento escrito da autoridade contratante.
4. A Comissão é considerada a entidade de origem das ICUE produzidas ou manuseadas pelo contratante, sendo os direitos que lhe incumbem exercidos pela autoridade contratante.

Artigo 47.º

Visitas associadas a contratos classificados

1. Quando o pessoal da Comissão ou de quaisquer contratantes ou beneficiários de subvenções precise de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações uns dos outros para a execução de um contrato classificado ou de uma convenção de subvenção classificada, são organizadas visitas, em ligação com as ANS, ASD ou quaisquer outras autoridades de segurança competentes a que o assunto diga respeito. A Autoridade de Segurança da Comissão deve ser informada dessas visitas. Todavia, no contexto de determinados programas ou projetos, as ANS, ASD, ou quaisquer outras autoridades de segurança competentes podem também aprovar um procedimento segundo o qual as visitas dessa natureza podem ser organizadas diretamente.

2. Para aceder às ICUE relacionadas com o contrato classificado, todos os visitantes devem possuir a devida credenciação de segurança e ter «necessidade de tomar conhecimento» dessas informações.
3. Apenas será concedido aos visitantes acesso às ICUE relacionadas com a finalidade da visita.
4. As regras de execução estabelecem disposições mais pormenorizadas.
5. É obrigatório o cumprimento das disposições relativas às visitas relacionadas com contratos classificados, estabelecidas na presente decisão e nas regras de execução referidas no n.º 4.

Artigo 48.º

Transmissão e transporte de ICUE associados a contratos classificados ou convenções de subvenção classificadas

1. Para efeitos de transmissão de ICUE por meios eletrónicos, são aplicáveis as disposições pertinentes do capítulo 5 da presente decisão.
2. Para efeitos de transporte de ICUE, são aplicáveis as disposições pertinentes do capítulo 4 da presente decisão e das suas regras de execução, em conformidade com as disposições legislativas e regulamentares nacionais.
3. Para o transporte de material classificado como mercadoria, são aplicados os seguintes princípios aquando da determinação dos mecanismos de segurança:
 - a) deve ser garantida a segurança em todas as fases do transporte, desde o ponto de origem até ao destino final;
 - b) o grau de proteção atribuído a uma remessa é determinado pelo nível de classificação mais elevado do material nela contido;
 - c) antes de qualquer transporte transnacional de material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o expedidor elabora um plano de transporte, que deve ser aprovado pela ANS, ASD ou qualquer outra autoridade de segurança competente;
 - d) na medida do possível, os transportes devem ser diretos e efetuados tão rapidamente quanto as circunstâncias o permitam;
 - e) sempre que possível, os itinerários apenas devem atravessar o território de Estados-Membros. Só devem atravessar Estados terceiros quando tal for autorizado pelas ANS, ASD ou quaisquer outras autoridades de segurança competentes dos Estados do expedidor e do destinatário.

Artigo 49.º

Transferência de ICUE para contratantes ou beneficiários de subvenções estabelecidos em Estados terceiros

A transferência de ICUE para contratantes ou beneficiários de subvenções estabelecidos em Estados terceiros deve ser feita em conformidade com as medidas de segurança acordadas entre a Autoridade de Segurança da Comissão, o serviço da Comissão, enquanto autoridade contratante ou que concede a subvenção, e a ANS, ASD ou outra autoridade de segurança competente do país terceiro em que o contratante ou beneficiário de subvenção se encontre registado.

Artigo 50.º

Manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED no contexto de contratos classificados ou de convenções de subvenção classificadas

1. A proteção das informações com classificação RESTREINT UE/EU RESTRICTED manuseadas ou armazenadas no âmbito de contratos classificados ou convenções de subvenção classificadas baseia-se nos princípios da proporcionalidade e da relação custo-eficácia.
2. Não são necessárias CSE ou CSP no contexto de contratos classificados ou convenções de subvenção classificadas que impliquem o manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED.
3. Quando um contrato ou convenção de subvenção implique o manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED num SCI explorado por um contratante ou beneficiário de subvenção, a autoridade contratante ou que concede a subvenção assegura, após consulta da Autoridade de Segurança da Comissão, que o contrato ou convenção de subvenção especifique os requisitos técnicos e administrativos necessários à acreditação ou aprovação do SCI que sejam proporcionais ao risco avaliado, tendo em conta todos os fatores pertinentes. O alcance da acreditação ou aprovação do SCI é acordado entre a Autoridade de Segurança da Comissão e a ANS ou ASD competente.

CAPÍTULO 7

INTERCÂMBIO DE INFORMAÇÕES CLASSIFICADAS COM OUTRAS INSTITUIÇÕES, AGÊNCIAS, ORGANISMOS E SERVIÇOS DA UNIÃO, COM OS ESTADOS-MEMBROS E COM ESTADOS TERCEIROS E ORGANIZAÇÕES INTERNACIONAIS*Artigo 51.º***Princípios básicos**

1. Caso a Comissão ou um dos seus serviços determine que existe a necessidade de proceder ao intercâmbio de ICUE com outra instituição, agência, organismo ou serviço da União, ou com um Estado terceiro ou uma organização internacional, são dados os passos necessários para estabelecer um quadro jurídico ou administrativo adequado para o efeito, que podem incluir acordos de segurança das informações ou convénios administrativos, celebrados em conformidade com a regulamentação pertinente.
2. Sem prejuízo do disposto no artigo 57.º, as ICUE só podem ser objeto de intercâmbio com outra instituição, agência, organismo ou serviço da União, ou com um Estado terceiro ou organização internacional, se estiver em vigor esse quadro jurídico ou administrativo adequado e se houver garantias suficientes de que a instituição, agência, organismo ou serviço da União, ou o Estado terceiro ou organização internacional em causa aplica princípios básicos e normas mínimas de proteção das informações classificadas equivalentes.

*Artigo 52.º***Intercâmbio de ICUE com outras instituições, agências, organismos e serviços da União**

1. Antes de celebrar um convénio administrativo para o intercâmbio de ICUE com outra instituição, agência, órgão ou serviço da União, a Comissão deve certificar-se de que a instituição, agência, organismo ou serviço da União em causa:
 - a) dispõe de um quadro regulamentar para a proteção das ICUE que estabeleça princípios básicos e normas mínimas equivalentes aos estabelecidos na presente decisão e nas suas regras de execução;
 - b) aplica normas de segurança e orientações relativas à segurança do pessoal, à segurança física, à gestão das ICUE e à segurança dos sistemas de comunicação e informação (SCI) que garantam um nível de proteção das ICUE equivalente ao alcançado na Comissão.
 - c) marca as informações classificadas que produz como ICUE.
2. A Direção-Geral dos Recursos Humanos e da Segurança, em estreita cooperação com outros serviços competentes da Comissão, é o serviço responsável na Comissão pela celebração de convénios administrativos para o intercâmbio de ICUE com outras instituições, agências, organismos ou serviços da União.
3. Regra geral, os convénios administrativos assumem a forma de troca de cartas, assinadas pelo Diretor-Geral dos Recursos Humanos e da Segurança, em nome da Comissão.
4. Antes de celebrar um convénio administrativo sobre o intercâmbio de ICUE, a Autoridade de Segurança da Comissão efetua uma visita de avaliação destinada a avaliar o quadro regulamentar para a proteção das ICUE e a determinar a eficácia das medidas de proteção das ICUE aplicadas. O convénio administrativo só entra em vigor e só se procede ao intercâmbio de ICUE se o resultado desta visita for satisfatório e se as recomendações feitas após a visita tiverem sido respeitadas. Deve ser efetuado um acompanhamento regular das visitas de avaliação a fim de verificar se o convénio administrativo é respeitado e se as medidas de segurança em vigor continuam a respeitar os princípios de base e as normas mínimas acordadas.
5. Na Comissão, o registo de ICUE gerido pelo Secretariado-Geral deve, regra geral, ser o principal ponto de entrada e de saída para os intercâmbios de informações classificadas com outra instituição, agência, organismo ou serviço da União. Se, no entanto, por razões de segurança, organizativas ou operacionais for mais adequado para proteger as ICUE, determinados registos locais de ICUE estabelecidos nos serviços da Comissão em conformidade com a presente decisão e com as suas regras de execução devem funcionar como ponto de entrada e de saída das informações classificadas relativas a matérias da competência dos serviços em causa.
6. O grupo de peritos de segurança da Comissão deve ser informado do processo de celebração de convénios administrativos, em conformidade com o n.º 2.

Artigo 53.º

Intercâmbio de ICUE com os Estados-Membros

1. As ICUE podem ser objeto de intercâmbio e comunicadas aos Estados-Membros, desde que estes protejam essas informações em conformidade com os requisitos aplicáveis às informações classificadas que ostentam uma classificação de segurança nacional de nível equivalente, de acordo com a tabela de equivalências das classificações de segurança constante do anexo I.
2. Quando os Estados-Membros introduzem nas estruturas ou redes da União Europeia informações classificadas que ostentem uma marca de classificação de segurança nacional, a Comissão deve proteger essas informações em conformidade com os requisitos aplicáveis às ICUE de nível equivalente, de acordo com a tabela de equivalências das classificações de segurança constante do anexo I.

Artigo 54.º

Intercâmbio de ICUE com Estados terceiros e organizações internacionais

1. Caso a Comissão determine que existe a necessidade, a longo prazo, de proceder ao intercâmbio de informações classificadas com Estados terceiros ou organizações internacionais, são dados os passos necessários para estabelecer um quadro jurídico ou administrativo adequado para o efeito, que podem incluir acordos de segurança das informações ou convénios administrativos, celebrados em conformidade com a regulamentação pertinente.
2. Os acordos de segurança das informações e os convénios administrativos referidos no n.º 1 devem conter disposições destinadas a assegurar que, ao receberem ICUE, os Estados terceiros e as organizações internacionais concedem a essas informações uma proteção que seja adequada ao respetivo nível de classificação e obedeça a normas mínimas equivalentes às estabelecidas na presente decisão.
3. A Comissão pode celebrar convénios administrativos em conformidade com o artigo 56.º quando o nível de classificação das ICUE não seja, regra geral, superior a RESTREINT UE/EU RESTRICTED.
4. Os convénios administrativos para o intercâmbio de informações classificadas referidos no n.º 3 devem conter disposições destinadas a assegurar que, ao receberem ICUE, os Estados terceiros ou organizações internacionais concedam a essas informações uma proteção que seja adequada ao respetivo nível de classificação e obedeça a normas mínimas equivalentes às estabelecidas na presente decisão. O grupo de peritos de segurança da Comissão deve ser consultado relativamente à celebração de acordos de segurança das informações ou de convénios administrativos.
5. A decisão de comunicar ICUE emanadas da Comissão a um Estado terceiro ou organização internacional é tomada, caso a caso, pelo serviço da Comissão, enquanto entidade de origem dessas ICUE na Comissão, em função da natureza e do teor dessas informações, da necessidade do destinatário de tomar conhecimento das mesmas e das vantagens que daí advenham para a União. Se as informações classificadas cuja comunicação se pretende, ou o material de referência que possam conter, não emanarem da Comissão, o serviço da Comissão que detém essas informações classificadas deve solicitar à entidade de origem que dê, por escrito, o consentimento prévio para a sua comunicação. Se não for possível determinar a entidade de origem, o serviço da Comissão que detém essas informações classificadas assume a responsabilidade em seu lugar, após consulta do grupo de peritos de segurança da Comissão.

Artigo 55.º

Acordos de segurança das informações

1. Os acordos de segurança das informações com Estados terceiros ou organizações internacionais são celebrados em conformidade com o artigo 218.º do TFUE.
2. Os acordos de segurança das informações devem:
 - a) estabelecer os princípios básicos e as normas mínimas aplicáveis ao intercâmbio de informações classificadas entre a União e os Estados terceiros ou organizações internacionais;
 - b) prever modalidades técnicas de execução a acordar entre as autoridades de segurança competentes das instituições e organismos pertinentes da União e a autoridade de segurança competente do Estado terceiro ou organização internacional em questão. Essas modalidades devem ter em conta o nível de proteção previsto nas regras, estruturas e procedimentos de segurança existentes no Estado terceiro ou organização internacional em causa;
 - c) estabelecer que, antes de se proceder ao intercâmbio de informações classificadas ao abrigo do acordo, deve determinar-se que a parte destinatária está em condições de proteger e salvaguardar adequadamente as informações classificadas que lhe forem comunicadas.

3. A Comissão consulta, quando for definida nos termos do artigo 51.º, n.º 1, uma necessidade de intercâmbio de informações classificadas, o Serviço Europeu para a Ação Externa, o Secretariado-Geral do Conselho e outras instituições e organismos da União, conforme adequado, a fim de avaliar se deve ser apresentada uma recomendação nos termos do artigo 218.º, n.º 3 do TFUE.
4. Não podem ser trocadas ICUE por meios eletrónicos, a não ser que tal se encontre expressamente previsto no acordo de segurança das informações ou nas modalidades técnicas de execução.
5. Na Comissão, o registo de ICUE gerido pelo Secretariado-Geral deve, regra geral, ser o principal ponto de entrada e de saída para os intercâmbios de informações classificadas com Estados terceiros e organizações internacionais. Se, no entanto, por razões de segurança, organizativas ou operacionais for mais adequado para proteger as ICUE, determinados registos locais de ICUE estabelecidos nos serviços da Comissão em conformidade com a presente decisão e com as suas regras de execução devem funcionar como ponto de entrada e de saída das informações classificadas relativas a matérias da competência dos serviços em causa.
6. A fim de avaliar a eficácia das regras, estruturas e procedimentos de segurança existentes no Estado terceiro ou organização internacional em questão, a Comissão participa em visitas de avaliação, em colaboração com outras instituições, agências ou organismos da União, e de comum acordo com o Estado terceiro ou organização internacional em questão. Essas visitas de avaliação devem avaliar:
 - a) o quadro regulamentar aplicável à proteção das informações classificadas;
 - b) quaisquer características específicas da política de segurança e a forma como se encontra organizada a segurança no Estado terceiro ou organização internacional que possam ser determinantes para o nível de classificação das informações suscetíveis de intercâmbio;
 - c) as medidas e os procedimentos de segurança efetivamente aplicados; e
 - d) os procedimentos de credenciação de segurança para o nível de ICUE a comunicar.

Artigo 56.º

Convénios administrativos

1. Quando exista, a longo prazo, no contexto de um quadro político ou jurídico da União, necessidade de proceder ao intercâmbio de informações com classificação, regra geral, não superior a RESTREINT UE/EU RESTRICTED com um Estado terceiro ou organização internacional, e a Autoridade de Segurança da Comissão, após consulta do grupo de peritos de segurança, tenha determinado, em especial, que a outra parte interessada não dispõe de um sistema de segurança suficientemente desenvolvido para que seja possível celebrar um acordo de segurança das informações, a Comissão pode decidir celebrar um convénio administrativo com as autoridades competentes do Estado terceiro ou organização internacional em questão.
2. Regra geral, estes convénios administrativos assumem a forma de troca de cartas.
3. É efetuada uma visita de avaliação antes da celebração do convénio. O grupo de peritos de segurança da Comissão deve ser informado dos resultados da visita de avaliação. Se houver razões de carácter excecional para o intercâmbio urgente de informações classificadas, as ICUE podem ser comunicadas, desde que sejam envidados todos os esforços para a realização de uma visita de avaliação o mais rapidamente possível.
4. Não podem ser trocadas ICUE por meios eletrónicos, a não ser que tal se encontre expressamente previsto no convénio administrativo.

Artigo 57.º

Comunicação *ad hoc* de ICUE a título excecional

1. Se não estiver em vigor qualquer acordo de segurança das informações ou convénio administrativo, e se a Comissão ou um dos seus serviços constatar a necessidade excecional, no contexto de um quadro político ou jurídico da União, de comunicar ICUE a um Estado terceiro ou organização internacional, a Autoridade de Segurança da Comissão deve, na medida do possível, verificar junto das autoridades de segurança do Estado terceiro ou organização internacional em questão se as respetivas regras, estruturas e procedimentos de segurança são capazes de garantir que as ICUE que lhes forem comunicadas serão protegidas segundo normas não menos rigorosas do que as estabelecidas na presente decisão.
2. A decisão de comunicar as ICUE ao Estado terceiro ou organização internacional em questão deve ser tomada pela Comissão, após consulta do grupo de peritos de segurança da Comissão, com base numa proposta apresentada pelo membro da Comissão responsável pelas questões de segurança.

3. Na sequência da decisão da Comissão de comunicar ICUE e sob reserva do consentimento prévio por escrito da entidade de origem, incluindo as entidades de origem do material de referência que as informações possam conter, o serviço competente da Comissão transmite as informações em causa, que devem ostentar uma marca relativa à comunicabilidade indicando o Estado terceiro ou organização internacional a que as ICUE foram comunicadas. Antes da comunicação ou no momento em que esta é efetuada, a parte terceira em questão deve assumir o compromisso, por escrito, de proteger as ICUE que receber em conformidade com os princípios básicos e as normas mínimas estabelecidos na presente decisão.

CAPÍTULO 8

DISPOSIÇÕES FINAIS

Artigo 58.º

Substituição de anteriores decisões

A presente decisão revoga e substitui a Decisão 2001/844/CE, CECA, Euratom da Comissão ⁽¹⁾.

Artigo 59.º

Informações classificadas produzidas antes da entrada em vigor da presente decisão

1. Todas as ICUE classificadas em conformidade com a Decisão 2001/844/CE, CECA, Euratom devem continuar a ser protegidas em conformidade com as disposições pertinentes da presente decisão.
2. Todas as informações classificadas na posse da Comissão na data em que a Decisão 2001/844/CE, CECA, Euratom entrou em vigor, com exceção das informações classificadas da Euratom devem:
 - a) se tiverem sido produzidas pela Comissão, continuar a ser subsidiariamente consideradas como tendo sido reclassificadas RESTREINT UE, a não ser que o seu autor tivesse decidido atribuir-lhes outra classificação até 31 de janeiro de 2002 e tivesse informado todos os destinatários do documento em causa;
 - b) se tiverem sido produzidas por autores exteriores à Comissão, conservar a sua classificação inicial e, por conseguinte, ser tratadas como ICUE de nível equivalente, a não ser que os seus autores concordem com a desclassificação ou desgradação das informações.

Artigo 60.º

Regras de execução e indicações de segurança

1. Quando necessário, a adoção das regras de execução da presente decisão deve ser objeto de uma decisão separada de delegação de poderes da Comissão em favor do membro da Comissão responsável pelas questões de segurança, em plena conformidade com o regulamento interno.
2. Após ter sido habilitado na sequência da referida decisão da Comissão, o membro da Comissão responsável pelas questões de segurança pode elaborar indicações de segurança que definam orientações de segurança e boas práticas abrangidas pelo âmbito de aplicação da presente decisão e das suas regras de execução.
3. A Comissão pode delegar as tarefas referidas nos n.ºs 1 e 2 no Diretor-Geral dos Recursos Humanos e da Segurança por meio de uma decisão de delegação separada, em plena conformidade com o regulamento interno.

Artigo 61.º

Entrada em vigor

A presente decisão entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 13 de março de 2015.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

⁽¹⁾ Decisão 2001/844/CE, CECA, Euratom da Comissão, de 29 de novembro de 2001, que altera o seu Regulamento Interno (JO L 317 de 3.12.2001, p. 1).

ANEXO I

EQUIVALÊNCIA DAS CLASSIFICAÇÕES DE SEGURANÇA

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Bélgica	Très Secret (Loi 11.12.1998) Zeër Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Ver nota <i>infra</i> ⁽¹⁾
Bulgária	Строго секретно	Секретно	Поверително	За служебно ползване
República Checa	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dinamarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Alemanha	Streng geheim	Geheim	VS (?) — Vertraulich	VS — Nur für den Dienstgebrauch
Estónia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grécia	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Espanha	Secreto	Reservado	Confidencial	Difusión Limitada
França	Très Secret Défense	Secret Défense	Confidentiel Défense	Ver nota abaixo ⁽²⁾
Croácia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Itália	Segretissimo	Segreto	Riservatissimo	Riservato
Chipre	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Letónia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituânia	Visiškai slapiai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungria	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Países Baixos	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Áustria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polónia	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roménia	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Eslovénia	Strogo tajno	Tajno	Zaupno	Interno
Eslováquia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlândia	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suécia ⁽⁴⁾	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Reino Unido	UK TOP SECRET	UK SECRET	Sem equivalente ⁽⁵⁾	UK OFFICIAL — SENSITIVE

⁽¹⁾ «Diffusion Restreinte/Beperkte Verspreiding» não é uma classificação de segurança na Bélgica. A Bélgica manuseia e protege as informações «RESTREINT UE/EU RESTRICTED» de modo não menos rigoroso do que as normas e procedimentos descritos nas regras de segurança do Conselho da União Europeia.

⁽²⁾ Alemanha: VS = Verschlusssache.

⁽³⁾ A França não utiliza a classificação «RESTREINT» no seu sistema nacional. A França manuseia e protege as informações «RESTREINT UE/EU RESTRICTED» de modo não menos rigoroso do que as normas e procedimentos descritos nas regras de segurança do Conselho da União Europeia.

⁽⁴⁾ Suécia: as marcas de classificação de segurança indicadas na linha de cima são utilizadas pelas autoridades de defesa, e as indicadas na linha de baixo são utilizadas por outras autoridades.

⁽⁵⁾ O Reino Unido manuseia e protege as ICUE com classificação «CONFIDENTIEL UE/EU CONFIDENTIAL» de acordo com os requisitos de proteção de segurança correspondentes a «UK SECRET».

ANEXO II

LISTA DE ABREVIATURAS

Acrónimo	Significado
AC	Autoridade Criptográfica
AAC	Autoridade de Aprovação Criptográfica
CCTV	Televisão em circuito fechado
ADC	Autoridade de Distribuição Criptográfica
SCI	Sistemas de comunicação e de informação em que sejam manuseadas ICUE
ASD	Autoridade de Segurança Designada
ICUE	Informações classificadas da UE
CSE	Credenciação de Segurança de Empresa
GI	Garantia da informação
AGI	Autoridade de garantia da informação
IDS	Sistema de deteção de intrusos
TI	Tecnologias da informação
LSO	Responsável local de segurança
ANS	Autoridade Nacional de Segurança
CSP	Credenciação de Segurança do Pessoal
CCSP	Certificado de Credenciação de Segurança do Pessoal
ISP	Instruções de Segurança do Programa/Projeto
RCO	Responsável do Controlo do Registo
AAS	Autoridade de Acreditação de Segurança
CAS	Cláusulas Adicionais de Segurança
GCS	Guia da Classificação de Segurança
SecOP	Procedimentos Operacionais de Segurança
AT	Autoridade TEMPEST
TFUE	Tratado sobre o Funcionamento da União Europeia

ANEXO III

LISTA DAS AUTORIDADES NACIONAIS DE SEGURANÇA

BÉLGICA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et
Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. Secretariado: +32 25014542
Fax +32 25014596
Endereço eletrónico: nvo-ans@diplobel.fed.be

BULGÁRIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sófia
Tel. +359 29333600
Fax +359 29873750
Endereço eletrónico: dksi@government.bg
Sítio web: www.dksi.bg

REPÚBLICA CHECA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praga 56
Tel. +420 257283335
Fax +420 257283110
Endereço eletrónico: czech.nsa@nbu.cz
Sítio web: www.nbu.cz

DINAMARCA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Fax +45 33430190
Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Fax: +45 33931320

ALEMANHA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlim
Tel. +49 30186810
Fax +49 30186811441
Endereço eletrónico: oesIII3@bmi.bund.de

ESTÓNIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Fax +372 7170213
Endereço eletrónico: nsa@mod.gov.ee

GRÉCIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΤ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612
Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Tel. +30 2106572045,
+30 2106572009
Fax +30 2106536279, +30 2106577612
ESPANHA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +34 913725000
Fax +34 913725808
Endereço eletrónico: nsa-sp@areatec.com

FRANÇA

Secrétariat général de la défense et de la sécurité nationale

Sous-direction Protection du secret (SGDSN/PSD)

51 Boulevard de la Tour-Maubourg

75700 Paris 07 SP

Tel. +33 171758177

Fax + 33 171758200

Ministry of Defence

Minister's Military Staff

National Security Authority (NSA)

4 Emanuel Roidi street

1432 Nicósia

Tel. +357 22807569, +357 22807643,

+357 22807764

Fax +357 22302351

Endereço eletrónico: cynsa@mod.gov.cy

CROÁCIA

Office of the National Security Council

Croatian NSA

Jurjevska 34

10000 Zagreb

Tel. +385 14681222

Fax + 385 14686049

Sítio web: www.uvns.hr

LETÓNIA

Autoridade Nacional de Segurança

Constitution Protection Bureau of the Republic of Latvia

P.O.Box 286

LV-1001 Riga

Tel. +371 67025418

Fax +371 67025454

Endereço eletrónico: ndi@sab.gov.lv

IRLANDA

National Security Authority

Department of Foreign Affairs

76-78 Harcourt Street

Dublin 2

Tel. +353 14780822

Fax +353 14082959

LITUÂNIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)

Gedimino 40/1

LT-01110 Vilnius

Tel. +370 706 66701, +370 706 66702

Fax +370 706 66700

Endereço eletrónico: nsa@vsd.lt

ITÁLIA

Presidenza del Consiglio dei Ministri

D.I.S. — U.C.Se.

Via di Santa Susanna, 15

00187 Roma

Tel. +39 0661174266

Fax +39 064885273

LUXEMBURGO

Autorité nationale de Sécurité

Boîte postale 2379

1023 Luxembourg

Tel. +352 24782210 central, + 352 24782253 direto

Fax +352 24782243

CHIPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Υπουργείο Άμυνας

Λεωφόρος Εμμανουήλ Ροΐδη 4

1432 Λευκωσία, Κύπρος

Τηλέφωνο: +357 22807569, +357 22807643,

+357 22807764

Τηλεομοιότυπο: +357 22302351

HUNGRIA

Nemzeti Biztonsági Felügyelet

(National Security Authority of Hungary)

H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel. +36 (1) 7952303

Fax +36 (1) 7950344

Endereço postal:

H-1357 Budapest, PO Box 2

Endereço eletrónico: nbf@nbf.hu

Sítio web: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Fax +356 25695321

1300-342 Lisboa
Tel. +351 213031710
Fax +351 213031711

PAÍSES BAIXOS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Fax +31 703187522

ROMÉLIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucureste
Tel. +40 212245830
Fax +40 212240714
Endereço eletrónico: nsa.romania@nsa.ro
Sítio web: www.orniss.ro

ÁUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Viena
Tel. +43 1531152594
Fax: +43 1531152615
Endereço eletrónico: ISK@bka.gv.at

ESLOVÉNIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Fax +386 14781399
Endereço eletrónico: gp.uvtp@gov.si

POLÓNIA

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
Fax +48 22 58 57 443
Endereço eletrónico: nsa@abw.gov.pl
Sítio web: www.abw.gov.pl

ESLOVÁQUIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax +421 263824005
Sítio web: www.nbusr.sk

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69

FINLÂNDIA

Autoridade Nacional de Segurança
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. +358 16055890
Fax +358 916055140
Endereço eletrónico: NSA@formin.fi

SUÉCIA

Utrikesdepartementet

(Ministry for Foreign Affairs)

SSSB

S-103 39 Stockholm

Tel. +46 84051000

Fax +46 87231176

Endereço eletrónico: ud-nsa@foreign.ministry.se

REINO UNIDO

UK National Security Authority

Room 335, 3rd Floor

70 Whitehall

London

SW1A 2AS

Tel. 1: +44 2072765649

Tel. 2: +44 2072765497

Fax +44 2072765651

Endereço eletrónico: UK-NSA@cabinet-office.x.gsi.gov.uk

ISSN 1977-0774 (edição eletrónica)
ISSN 1725-2601 (edição em papel)



Serviço das Publicações da União Europeia
2985 Luxemburgo
LUXEMBURGO

PT