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, desgraduação, 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 conexa 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) «Desgraduação»: 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, desgraduação, 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 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 excecionalmente 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

Desgraduação 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 eletrónicos, 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 subsequentemente 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 refletem 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) seviço(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 estes 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 desgraduação 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) Zeer 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 *infra* (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 (2) — 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 (3)
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 slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungria	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Países Baixos	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Áustria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polónia	Ściśle 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
ΣΤΓ 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

CROÁCIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel. +385 14681222
Fax + 385 14686049
Sítio *web*: www.uvns.hr

IRLANDA

National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax +353 14082959

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

CHIPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

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

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

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

LUXEMBURGO

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 central, + 352 24782253 direto
Fax +352 24782243

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

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

ÁUSTRIA

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

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

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Fax +351 213031711

ROMÉNIA

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

ESLOVÉNIA

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

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

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