

## II

(Actos não legislativos)

## DECISÕES

## DECISÃO DO CONSELHO

de 31 de Março de 2011

relativa às regras de segurança aplicáveis à protecção das informações classificadas da UE

(2011/292/UE)

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o n.º 3 do artigo 240.º,

Tendo em conta a Decisão 2009/937/UE do Conselho, de 1 de Dezembro de 2009, que aprova o Regulamento Interno do Conselho <sup>(1)</sup>, nomeadamente o artigo 24.º,

Considerando o seguinte:

- (1) A fim de desenvolver actividades do Conselho em todas as áreas que exijam o manuseamento de informações classificadas, é necessário criar um sistema geral de segurança para protecção dessas informações que abranja o Conselho, o seu Secretariado-Geral e os Estados-Membros.
- (2) O disposto na presente decisão deverá aplicar-se sempre que o Conselho, as suas instâncias preparatórias e o Secretariado-Geral do Conselho (SGC) manuseiem informações classificadas da UE (ICUE).
- (3) Nos termos das disposições legislativas e regulamentares nacionais e na medida do necessário para assegurar o funcionamento do Conselho, os Estados-Membros deverão respeitar a presente decisão sempre que as autoridades competentes, o pessoal ou os contratantes respectivos manuseiem ICUE, de forma a que cada um possa estar certo de que é concedido um nível de protecção equivalente às mesmas.
- (4) O Conselho e a Comissão estão empenhados em aplicar normas de segurança equivalentes para protecção das ICUE.
- (5) O Conselho sublinha a importância de associar, quando tal se justifique, o Parlamento Europeu e as outras instituições, agências, organismos ou serviços da UE aos

princípios, normas e regras de protecção das informações classificadas que são necessários para proteger os interesses da União e seus Estados-Membros.

- (6) As agências e os organismos da UE instituídos ao abrigo do Capítulo 2 do Título V do Tratado da União Europeia, Europol e Eurojust aplicam, na respectiva organização interna, os princípios básicos e as normas mínimas estabelecidos na presente decisão para protecção das ICUE, tal como previsto nos actos que os instituem.
- (7) As operações de gestão de crises estabelecidas ao abrigo do Capítulo 2 do Título V do TUE e o respectivo pessoal aplicam as regras de segurança aprovadas pelo Conselho para protecção das ICUE.
- (8) Os Representantes Especiais da UE e os membros das respectivas equipas aplicam as regras de segurança aprovadas pelo Conselho para protecção das ICUE.
- (9) A presente decisão é aprovada sem prejuízo dos artigos 15.º e 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e dos instrumentos que lhes dão execução.
- (10) A presente decisão é aprovada sem prejuízo das práticas seguidas nos Estados-Membros em matéria de informação dos Parlamentos nacionais acerca das actividades da União,

APROVOU A PRESENTE DECISÃO:

Artigo 1.º

**Objecto, âmbito de aplicação e definições**

1. A presente decisão estabelece os princípios básicos e as normas mínimas de segurança aplicáveis à protecção das ICUE.

<sup>(1)</sup> JO L 325 de 11.12.2009, p. 35.

2. Esses princípios básicos e normas mínimas são aplicáveis ao Conselho e ao SGC e devem ser respeitados pelos Estados-Membros, nos termos das respectivas disposições legislativas e regulamentares nacionais, de forma a que cada um possa estar certo de que é concedido um nível de protecção equivalente às ICUE.

3. Para efeitos da presente decisão, são aplicáveis as definições estabelecidas no Apêndice A.

#### Artigo 2.º

##### **Definição de ICUE, classificações e marcas de segurança**

1. Entende-se por «informações classificadas da UE» (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 serão classificadas num dos seguintes níveis:

- a) TRÈS SECRET UE/EU TOP SECRET: informações e material cuja divulgação não autorizada possa prejudicar de forma excepcionalmente grave os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
- b) SECRET UE/EU SECRET: informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
- c) CONFIDENTIEL UE/EU CONFIDENTIAL: informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou mais Estados-Membros;
- d) RESTREINT UE/EU RESTRICTED: informações e material cuja divulgação não autorizada possa ser desfavorável aos interesses da União Europeia ou de um ou mais Estados-Membros.

3. As ICUE ostentam uma marca de classificação de segurança nos termos do disposto no n.º 2, podendo além disso ostentar marcas que designem o domínio de actividade a que se referem, identifiquem a entidade de origem, limitem a distribuição, restrinjam a utilização ou indiquem a comunicabilidade.

#### Artigo 3.º

##### **Gestão das classificações**

1. As autoridades competentes garantem que as ICUE sejam devidamente classificadas e claramente identificadas como informações classificadas, e mantenham o seu nível de classificação durante o tempo necessário.

2. As ICUE não podem ser desgraduadas nem desclassificadas e nenhuma das marcas a que se refere o artigo 2.º, n.º 3, pode ser alterada ou suprimida sem o consentimento prévio, por escrito, da entidade de origem.

3. O Conselho aprova uma política de segurança para a produção de ICUE, que compreende um guia prático de classificação.

#### Artigo 4.º

##### **Protecção das informações classificadas**

1. As ICUE são protegidas nos termos da presente decisão.

2. Cabe ao detentor de quaisquer ICUE a responsabilidade pela sua protecção nos termos da presente decisão.

3. Quando os Estados-Membros introduzirem nas estruturas ou redes da União Europeia informações classificadas que ostentem uma marca de classificação de segurança nacional, o Conselho e o SGC protegem essas informações nos termos dos requisitos aplicáveis às ICUE de nível equivalente, de acordo com a tabela de equivalências das classificações de segurança constante do Apêndice B.

4. As grandes quantidades ou o acervo de ICUE podem justificar um nível de protecção correspondente a uma classificação mais elevada.

#### Artigo 5.º

##### **Gestão dos riscos de segurança**

1. Os riscos a que as ICUE estão expostas são sujeitos a um processo de gestão. Esse processo terá por objectivo determinar os riscos de segurança conhecidos, definir as medidas de segurança destinadas a reduzir esses riscos para um nível aceitável nos termos dos princípios básicos e normas mínimas estabelecidos na presente decisão e aplicar tais medidas de acordo com o conceito de defesa em profundidade como definido no Apêndice A. A eficácia das medidas será sujeita a avaliação contínua.

2. As medidas de segurança para protecção das ICUE ao longo do seu ciclo de vida devem ser proporcionais, designadamente, 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 actos mal-intencionados e/ou actividades criminosas, nomeadamente de espionagem, sabotagem e terrorismo.

3. Os planos de emergência têm 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.

4. Os planos de continuidade das actividades incluem medidas de prevenção e recuperação destinadas a minimizar o impacto de quaisquer falhas ou incidentes graves sobre o manuseamento e armazenamento das ICUE.

**Artigo 6.º****Execução da presente decisão**

1. Se necessário, o Conselho, por recomendação do Comité de Segurança, aprovará políticas de segurança que estabeleçam medidas de execução da presente decisão.

2. O Comité de Segurança pode definir, ao seu nível, diretrizes de segurança para apoio ou complemento da presente decisão e das políticas de segurança aprovadas pelo Conselho.

**Artigo 7.º****Requisitos de segurança do pessoal**

1. A segurança do pessoal consiste na aplicação de medidas que se destinam a garantir que o acesso às ICUE só seja concedido a quem:

- tenha necessidade de tomar conhecimento,
- possua a credenciação de segurança para o nível adequado, consoante as necessidades, e
- tenha sido informado das responsabilidades que lhe cabem.

2. São definidos procedimentos de credenciação de segurança do pessoal que permitam verificar se determinada pessoa pode ter acesso a ICUE, tendo em conta as suas lealdade, idoneidade e fiabilidade.

3. Todo o pessoal do SGC que, no exercício das suas funções, possa ter de aceder a ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior deve receber a credenciação de segurança para o nível adequado antes de lhe ser facultado o acesso às referidas ICUE. No Anexo I é estabelecido o procedimento de credenciação de segurança do pessoal aplicável aos funcionários e outros agentes do SGC.

4. O pessoal dos Estados-Membros a que se refere o artigo 14.º, n.º 3, que, no exercício das suas funções, possa ter de aceder a ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior deve possuir a credenciação de segurança para o nível adequado ou outra autorização devidamente emitida em virtude das funções que exerce, nos termos das disposições legislativas e regulamentares nacionais antes de lhe ser facultado o acesso às referidas ICUE.

5. Antes de lhes ser facultado o acesso a ICUE e, posteriormente, a intervalos regulares, todas as pessoas são informadas das suas responsabilidades no que respeita à protecção das ICUE nos termos da presente decisão e reconhecem essas mesmas responsabilidades.

6. As regras de execução do presente artigo são estabelecidas no Anexo I.

**Artigo 8.º****Segurança física**

1. A segurança física consiste na aplicação de medidas físicas e técnicas de protecção destinadas a impedir o acesso não autorizado a ICUE.

2. São concebidas medidas de segurança física que permitam impedir a entrada sub-reptícia ou forçada de intrusos, dissuadir, impedir e detectar acções 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 são determinadas com base num processo de gestão de risco.

3. São aplicadas medidas de segurança física em todas as instalações, edifícios, gabinetes, salas e outras zonas onde sejam manuseadas ou armazenadas ICUE, nomeadamente zonas em que se encontrem sistemas de comunicação e de informação, tal como definidos no artigo 10.º, n.º 2.

4. As zonas onde sejam armazenadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são instituídas como zonas de segurança, nos termos do Anexo II, e aprovadas pela autoridade de segurança competente.

5. Só são utilizados equipamentos ou dispositivos aprovados para proteger as ICUE de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou superior.

6. As regras de execução do presente artigo são estabelecidas no Anexo II.

**Artigo 9.º****Gestão das informações classificadas**

1. A gestão das informações classificadas consiste na aplicação de medidas administrativas de controlo das ICUE ao longo do seu ciclo de vida que visam complementar as medidas previstas nos artigos 7.º, 8.º e 10.º e contribuir, deste modo, para dissuadir e detectar 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, registo, cópia, tradução, transporte e destruição de ICUE.

2. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são registadas, para fins de segurança, antes da distribuição e no momento da recepção. Para o efeito, as autoridades competentes do SGC e dos Estados-Membros criam um sistema de registo. As informações com classificação TRÈS SECRET UE/EU TOP SECRET são inscritas em registos próprios.

3. Os serviços e instalações onde se proceda ao manuseamento ou armazenamento de ICUE são periodicamente inspecionados pela autoridade de segurança competente.

4. A 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 electrónicos protegidos por produtos criptográficos aprovados nos termos do artigo 10.º, n.º 6;
- b) Se não se utilizarem os meios referidos na alínea a), as ICUE são transportadas:
  - i) em suporte electrónico (chaves USB, CD, discos rígidos) protegido por produtos criptográficos aprovados nos termos do artigo 10.º, n.º 6,
  - ii) ou, em todos os demais casos, nas condições estipuladas pela autoridade de segurança competente, de acordo com as medidas de protecção pertinentes estabelecidas no Anexo III.

5. As regras de execução do presente artigo são estabelecidas no Anexo III.

#### Artigo 10.º

#### Protecção das ICUE manuseadas nos sistemas de comunicação e informação

1. A garantia da informação (GI) no domínio dos sistemas de comunicação e informação consiste na confiança em que esses sistemas protegem as informações neles manuseadas e funcionam como for necessário, quando for necessário, sob o controlo de utilizadores legítimos. Uma GI eficaz deve assegurar níveis adequados de confidencialidade, integridade, disponibilidade, não rejeição e autenticidade. A GI baseia-se num processo de gestão de risco.

2. Um sistema de comunicação e informação consiste num sistema que permita o manuseamento automatizado de informações. Um sistema de comunicação e informação compreende todos os activos necessários ao seu funcionamento, designadamente infra-estrutura, organização, pessoal e recursos em matéria de informação. A presente decisão é aplicável aos sistemas de comunicação e de informação em que sejam manuseadas ICUE (SCI).

3. As ICUE são manuseadas pelos SCI de acordo com o conceito de GI.

4. Todos os SCI são submetidos a um processo de acreditação. A acreditação visa obter a garantia de que foram tomadas todas as medidas de segurança adequadas e de que foi alcançado um nível suficiente de protecção das ICUE e do próprio SCI, nos termos da presente decisão. A declaração de acreditação determina o nível máximo de classificação das informações que podem ser manuseadas pelo SCI e os termos e condições correspondentes.

5. Os SCI em que sejam manuseadas informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior são protegidos de forma a impedir o comprometimento das informações devido a emanações electromagnéticas não intencionais («medidas de segurança TEMPEST»).

6. Quando a protecção das ICUE for assegurada por produtos criptográficos, estes são aprovados de acordo com o seguinte procedimento:

- a) A confidencialidade das informações com classificação SECRET UE/EU SECRET ou superior é protegida por produtos criptográficos aprovados pelo Conselho, na qualidade de Autoridade de Aprovação Criptográfica (AAC), por recomendação do Comité de Segurança;
- b) A confidencialidade das informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou RESTREINT UE/EU RESTRICTED é protegida por produtos criptográficos aprovados pelo Secretário-Geral do Conselho (a seguir designado por «Secretário-Geral»), na qualidade de AAC, por recomendação do Comité de Segurança.

Não obstante o disposto na alínea b), as ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou RESTREINT UE/EU RESTRICTED podem ser protegidas dentro dos sistemas nacionais dos Estados-Membros por produtos criptográficos aprovados pelas AAC dos próprios Estados-Membros.

7. Durante a transmissão de ICUE por via electrónica, são utilizados produtos criptográficos aprovados. Não obstante este requisito, podem ser aplicados procedimentos específicos, em circunstâncias de emergência ou configurações técnicas específicas, nos termos do Anexo IV.

8. As autoridades competentes do SGC e dos Estados-Membros, respectivamente, criarão as seguintes funções em matéria de GI:

- a) Autoridade de GI (AGI);
- b) Autoridade TEMPEST (AT);
- c) Autoridade de Aprovação Criptográfica (AAC);
- d) Autoridade de Distribuição Criptográfica (ADC).

9. Para cada sistema, as autoridades competentes do SGC e dos Estados-Membros, respectivamente, criarão as seguintes entidades:

- a) Autoridade de Acreditação de Segurança (AAS);
- b) Uma Autoridade Operacional de GI.

10. As regras de execução do presente artigo são estabelecidas no Anexo IV.

*Artigo 11.º***Segurança industrial**

1. Entende-se por «segurança industrial» a aplicação de medidas destinadas a garantir a protecção das ICUE pelos contratantes ou subcontratantes no âmbito das negociações pré-contratuais e durante a vigência dos contratos classificados. Estes contratos não devem envolver o acesso a informações com classificação TRÈS SECRET UE/EU TOP SECRET.

2. O SGC pode confiar tarefas que envolvam ou impliquem o acesso a ICUE ou o seu manuseamento ou armazenamento a entidades industriais ou outras registadas num Estado-Membro ou num Estado terceiro que tenha celebrado um acordo ou um convénio administrativo nos termos do artigo 12.º, n.º 2, alíneas a) ou b).

3. Ao adjudicar contratos classificados a entidades industriais ou outras, o SGC, na qualidade de entidade adjudicante, garante o cumprimento das normas mínimas de segurança industrial estabelecidas na presente decisão, às quais o contrato fará referência.

4. As Autoridades Nacionais de Segurança (ANS), as Autoridades de Segurança Designadas (ASD) ou quaisquer outras autoridades competentes dos Estados-Membros garantem, na medida em que as disposições legislativas e regulamentares nacionais o permitirem, que os contratantes e subcontratantes registados nos respectivos territórios tomem todas as medidas adequadas para proteger as ICUE no âmbito das negociações pré-contratuais ou da execução dos contratos classificados.

5. As ANS, ASD ou quaisquer outras autoridades competentes dos Estados-Membros garantem, nos termos das disposições legislativas e regulamentares nacionais, que os contratantes ou subcontratantes registados nos respectivos Estados-Membros que participem na execução de contratos ou subcontratos que exijam acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dentro das suas próprias instalações, seja na execução do contrato, seja na fase pré-contratual, possuam uma Credenciação de Segurança de Empresa (CSE) para o nível de classificação adequado.

6. É concedida ao pessoal do contratante ou subcontratante que tenha de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET para a execução de contratos classificados uma Certificação de Segurança do Pessoal (CSP), emitida pela respectiva ANS, ASD ou por qualquer outra autoridade de segurança competente nos termos das disposições legislativas e regulamentares nacionais e das normas mínimas estabelecidas no Anexo I.

7. As regras de execução do presente artigo são estabelecidas no Anexo V.

*Artigo 12.º***Intercâmbio de informações classificadas com Estados terceiros e organizações internacionais**

1. Quando o Conselho determinar que é necessário proceder ao intercâmbio de ICUE com um Estado terceiro ou uma organização internacional, é estabelecido um quadro adequado para esse efeito.

2. Para estabelecer esse quadro e definir regras recíprocas em matéria de protecção das informações classificadas trocadas,

a) O Conselho celebra acordos sobre os procedimentos de segurança para o intercâmbio e a protecção de informações classificadas (a seguir designados por «acordos de segurança das informações»); ou

b) O Secretário-Geral pode celebrar convénios administrativos nos termos do ponto 17 do Anexo VI sempre que o nível de classificação das ICUE a comunicar não seja, regra geral, superior a RESTREINT UE/EU RESTRICTED.

3. Os acordos de segurança das informações ou os convénios administrativos a que se refere o n.º 2 contêm disposições destinadas a assegurar que, ao receberem ICUE, os Estados terceiros e as organizações internacionais concedam a essas informações uma protecção que seja adequada ao respectivo nível de classificação e obedeça a normas mínimas não menos rigorosas do que as estabelecidas na presente decisão.

4. A decisão de comunicar ICUE emanadas do Conselho a um Estado terceiro ou organização internacional é tomada caso a caso pelo Conselho, em função da natureza e do teor dessas informações, da necessidade que o destinatário tenha de tomar conhecimento das mesmas, e das vantagens que daí advenham para a UE. Se as informações classificadas cuja comunicação se pretende não emanarem do Conselho, o SGC solicita à entidade de origem que dê, por escrito, o consentimento prévio para a sua comunicação. Se não for possível identificar a entidade de origem, o Conselho assume a responsabilidade em seu lugar.

5. São organizadas visitas de avaliação para avaliar a eficácia das medidas de segurança aplicadas num Estado terceiro ou organização internacional para protecção das ICUE facultadas ou trocadas.

6. As regras de execução do presente artigo são estabelecidas no Anexo VI.

*Artigo 13.º***Quebras de segurança e comprometimento de ICUE**

1. As quebras de segurança resultam de actos ou omissões de uma pessoa que são contrários às regras de segurança estabelecidas na presente decisão.

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 competente.

4. Sempre que haja conhecimento ou motivos razoáveis para presumir que houve comprometimento ou perda de ICUE, a autoridade de segurança competente toma todas as medidas adequadas, nos termos das disposições legislativas e regulamentares pertinentes, para:

- a) Informar a entidade de origem;
- b) Garantir que o caso seja investigado por elementos do pessoal não directamente envolvidos na quebra de segurança, a fim de determinar os factos ocorridos;
- c) Avaliar os danos eventualmente causados aos interesses da UE 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.

5. Quem for responsável pela violação das regras de segurança estabelecidas na presente decisão pode ser passível de acção disciplinar nos termos das disposições regulamentares aplicáveis. Quem for responsável pelo comprometimento ou pela perda de ICUE é passível de acção disciplinar e/ou judicial nos termos das disposições legislativas e regulamentares aplicáveis.

#### Artigo 14.º

##### Responsabilidade pela execução

1. O Conselho toma todas as medidas necessárias para assegurar a coerência global da aplicação da presente decisão.

2. O Secretário-Geral toma todas as medidas necessárias para assegurar que, no manuseamento ou armazenamento de ICUE ou de quaisquer outras informações classificadas, a presente decisão é cumprida pelos funcionários e outros agentes do SGC, pelo pessoal destacado para o SGC e pelas entidades a que o SGC tenha adjudicado contratos, tanto nas instalações utilizadas pelo Conselho como no interior do SGC, incluindo os seus gabinetes de ligação em países terceiros.

3. Os Estados-Membros tomam todas as medidas necessárias, nos termos das respectivas disposições legislativas e regulamentares nacionais, para assegurar que, quando forem manuseadas ou armazenadas informações confidenciais da UE, a presente decisão é respeitada:

- a) Pelo pessoal das Representações Permanentes dos Estados-Membros junto da União Europeia, bem como pelos delegados nacionais que participem em reuniões do Conselho ou das suas instâncias preparatórias, ou que tomem parte noutras actividades do Conselho;

- b) Por outros elementos do pessoal das administrações nacionais dos Estados-Membros, incluindo o pessoal destacado para essas administrações, quer exerçam a sua actividade no território do respectivo Estado-Membro, quer no estrangeiro;

- c) Por quaisquer outras pessoas nos Estados-Membros que, em virtude das funções que exercem, estejam devidamente autorizadas a aceder às ICUE; e

- d) Pelas entidades a que os Estados-Membros tenham adjudicado contratos, quer no território dos Estados-Membros, quer no estrangeiro.

#### Artigo 15.º

##### Organização da segurança no Conselho

1. No âmbito da sua missão de assegurar a coerência global da aplicação da presente decisão, o Conselho aprova:

- a) Os acordos a que se refere o artigo 12.º, n.º 2, alínea a);

- b) As decisões que autorizem a comunicação de ICUE a Estados terceiros e organizações internacionais;

- c) Um programa anual de inspecções, proposto pelo Secretário-Geral e recomendado pelo Comité de Segurança, para a realização de inspecções aos serviços e instalações dos Estados-Membros e às agências e organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol e Eurojust, bem como de visitas de avaliação a Estados terceiros e organizações internacionais a fim de avaliar a eficácia das medidas aplicadas para protecção das ICUE; e

- d) Políticas de segurança, tal como previsto no artigo 6.º, n.º 1.

2. O Secretário-Geral é a Autoridade de Segurança do SGC, cabendo-lhe nessa qualidade:

- a) Executar a política de segurança do Conselho e proceder regularmente à sua reapreciação;

- b) Estabelecer a coordenação com as ANS dos Estados-Membros em todas as questões de segurança relacionadas com a protecção das informações classificadas relevantes para as actividades do Conselho;

- c) Conceder a CSP UE aos funcionários e outros agentes do SGC, nos termos do artigo 7.º, n.º 3, antes de lhes ser facultado o acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior;

- d) Se necessário, ordenar a investigação de casos concretos ou de suspeitas de comprometimento ou perda de informações classificadas detidas pelo Conselho ou emanadas do Conselho, e solicitar às autoridades de segurança competentes que prestem assistência nessas investigações;

- e) Proceder à inspecção periódica dos mecanismos de segurança destinados a proteger as informações classificadas nas instalações do SGC;
- f) Proceder à inspecção periódica dos mecanismos de segurança destinados a proteger as ICUE nas agências e nos organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol, Eurojust, bem como nas operações de gestão de crises estabelecidas ao abrigo do Capítulo 2 do TUE e junto dos Representantes Especiais da UE (REUE) e membros das respectivas equipas;
- g) Proceder, em conjunto e de comum acordo com a ANS competente, à inspecção periódica dos mecanismos de segurança destinados a proteger as ICUE nos serviços e instalações dos Estados-Membros;
- h) Coordenar as medidas de segurança com as autoridades competentes dos Estados-Membros responsáveis pela protecção das informações classificadas e, se necessário, com Estados terceiros ou organizações internacionais, no que respeita, designadamente, à natureza das ameaças à segurança das ICUE e aos meios de protecção contra essas ameaças;
- i) Celebrar os convénios administrativos a que se refere o artigo 12.º, n.º 2, alínea b); e
- j) Proceder a visitas de avaliação iniciais e periódicas a Estados terceiros e organizações internacionais, a fim de avaliar a eficácia das medidas aplicadas para protecção das ICUE facultadas ou trocadas.

O Gabinete de Segurança do SGC está à disposição do Secretário-Geral para o assistir no desempenho destas funções.

3. Para efeitos da execução do artigo 14.º, n.º 3, cabe aos Estados-Membros:

- a) Designar uma ANS responsável pelos mecanismos de segurança destinados a proteger as ICUE, de modo a que:
- i) as ICUE detidas por qualquer serviço, organismo ou agência nacional, público ou privado, quer dentro, quer fora do país, sejam protegidas nos termos da presente decisão,
- ii) os mecanismos de segurança destinados a proteger as ICUE sejam periodicamente inspeccionados,
- iii) todas as pessoas empregadas pelas administrações nacionais ou por um contratante a quem seja facultado o acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL, ou superior, possuam a credenciação de segurança adequada ou outra autorização

devidamente emitida, em virtude das funções que exercem, nos termos das disposições legislativas e regulamentares nacionais,

- iv) sejam criados os programas de segurança necessários para minimizar o risco de perda ou comprometimento das ICUE,
- v) as questões de segurança relacionadas com a protecção das ICUE sejam tratadas em coordenação com as outras autoridades nacionais competentes, nomeadamente aquelas a que se refere a presente decisão, e
- vi) seja dada resposta aos pedidos de credenciação de segurança adequada apresentados pelas agências e organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol, Eurojust, bem como pelas operações de gestão de crises estabelecidas ao abrigo do Capítulo 2 do Título V do TUE e pelos REUE e respectivas equipas.

A lista das ANS consta do Apêndice C;

- b) Assegurar que as suas autoridades competentes prestem informações e aconselhamento ao respectivo Governo, e através dele ao Conselho, sobre a natureza das ameaças à segurança das ICUE e os meios de as proteger dessas ameaças.

#### Artigo 16.º

#### Comité de Segurança

1. É criado um Comité de Segurança, que fica incumbido de analisar e avaliar todas as questões de segurança abrangidas pela presente decisão e de dirigir recomendações ao Conselho, consoante as necessidades.

2. O Comité de Segurança será composto por representantes das ANS dos Estados-Membros, nele participando um representante da Comissão e do Serviço Europeu para a Acção Externa. Será presidido pelo Secretário-Geral ou pelo delegado que este designar. Reunir-se-á conforme as instruções do Conselho, ou a pedido do Secretário-Geral ou de uma ANS.

Os representantes das agências e organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol e Eurojust podem ser convidados a participar nas reuniões quando forem tratadas questões que lhes digam respeito.

3. O Comité de Segurança organiza as suas actividades de forma a poder formular recomendações sobre domínios de segurança específicos. O Comité cria uma subformação especializada para as questões de GI, para além de outras subformações especializadas, consoante as necessidades. O Comité define os mandatos dessas subformações especializadas, as quais lhe apresentam relatórios das suas actividades e, se necessário, eventuais recomendações a dirigir ao Conselho.

*Artigo 17.º***Substituição de anteriores decisões**

1. A presente decisão revoga e substitui a Decisão 2001/264/CE do Conselho, de 19 de Março de 2001, que aprova as regras de segurança do Conselho <sup>(1)</sup>.

2. Todas as ICUE classificadas nos termos da Decisão 2001/264/CE continuam a ser protegidas nos termos das disposições pertinentes da presente decisão.

*Artigo 18.º***Entrada em vigor**

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

Feito em Bruxelas, em 31 de Março de 2011.

*Pelo Conselho*  
O Presidente  
VÖLNER P.

---

<sup>(1)</sup> JO L 101 de 11.4.2001, p. 1.

## ANEXOS

## ANEXO I

Requisitos de segurança do pessoal

## ANEXO II

Segurança física

## ANEXO III

Gestão das informações classificadas

## ANEXO IV

Protecção das ICUE manuseadas em SCI

## ANEXO V

Segurança industrial

## ANEXO VI

Intercâmbio de informações classificadas com Estados terceiros e organizações internacionais

---

## ANEXO I

**REQUISITOS DE SEGURANÇA DO PESSOAL****I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 7.º. Nele se definem não só os critérios a ter em conta para determinar se, com base nas suas lealdade, idoneidade e fiabilidade, uma dada pessoa pode ser autorizada a ter acesso a ICUE, mas também os procedimentos administrativos e de investigação a seguir para esse efeito.
2. Em todo o texto do presente anexo, e exceptuando os casos de relevância da distinção, a expressão «Credenciação de Segurança do Pessoal» corresponde a uma credenciação nacional de segurança do pessoal (CSP nacional) e/ou a uma credenciação UE de segurança do pessoal (CSP UE), de acordo com a definição dada no Apêndice A.

**II. AUTORIZAÇÃO DE ACESSO ÀS ICUE**

3. Ninguém pode ser autorizado a ter acesso a informações da UE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior sem que:
  - a) Tenha ficado comprovada a sua necessidade de tomar conhecimento de tais informações;
  - b) Lhe tenha sido conferida a CSP para o nível adequado ou outra autorização devidamente emitida em virtude das funções que exerce nos termos das disposições legislativas e regulamentares nacionais; e
  - c) Tenha sido informado das regras e procedimentos de segurança aplicáveis à protecção das ICUE e tenha reconhecido as suas responsabilidades no que respeita à protecção dessas informações.
4. Os Estados-Membros e o SGC identificarão os cargos que, nas respectivas estruturas, precisam de ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior e para os quais é, por esse motivo, exigida uma CSP para o nível adequado.

**III. REQUISITOS DA CREDENCIAÇÃO DE SEGURANÇA DO PESSOAL**

5. Depois de terem recebido um pedido devidamente autorizado, as ANS ou outras autoridades nacionais competentes serão responsáveis por assegurar que sejam realizadas investigações de segurança a respeito dos respectivos cidadãos que precisem de ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior. As normas de investigação respeitarão as disposições legislativas e regulamentares nacionais.
6. Se a pessoa residir no território de outro Estado-Membro ou de um Estado terceiro, as autoridades nacionais competentes solicitarão assistência à autoridade competente do Estado de residência, nos termos das disposições legislativas e regulamentares nacionais. Os Estados-Membros prestar-se-ão mutuamente assistência na condução das investigações de segurança, nos termos das disposições legislativas e regulamentares nacionais.
7. Quando as disposições legislativas e regulamentares nacionais o permitirem, as ANS ou outras autoridades nacionais competentes podem realizar investigações a respeito de cidadãos de outros países que precisem de ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior. As normas de investigação respeitarão as disposições legislativas e regulamentares nacionais.

**Critérios da investigação de segurança**

8. A lealdade, a idoneidade e a fiabilidade de uma dada pessoa para efeitos de concessão de uma CSP para acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior serão determinadas por meio de uma investigação de segurança. A autoridade nacional competente procederá a uma avaliação global baseada nos resultados da investigação de segurança. Nenhum resultado desfavorável constituirá, por si só, razão para recusar a CSP. Os principais critérios a usar para esse efeito deverão consistir nomeadamente em ponderar, na medida em que tal seja possível à luz das disposições legislativas e regulamentares nacionais, se a pessoa:
  - a) Cometeu ou tentou cometer, conspirou com alguém ou auxiliou alguém a cometer algum acto de espionagem, terrorismo, sabotagem, traição ou sedição;
  - b) Está ou esteve associada a espíões, terroristas, sabotadores, ou a indivíduos razoavelmente suspeitos de o ser, ou associada a representantes de organizações ou Estados estrangeiros, incluindo serviços de informações estrangeiros, que possam ameaçar a segurança da UE e/ou dos Estados-Membros, a menos que tais associações tenham sido autorizadas no cumprimento de funções oficiais;

- c) É ou foi membro de alguma organização que vise, por meios violentos, subversivos ou outros meios ilegais, nomeadamente, derrubar o Governo ou alterar a ordem constitucional, a forma de governo ou as políticas governamentais de um Estado-Membro;
  - d) É, ou foi, apoiante de alguma organização descrita na alínea c), ou está, ou esteve, estreitamente associada a membros de tais organizações;
  - e) Reteve, ocultou, deturpou ou falseou deliberadamente informações importantes, especialmente em matéria de segurança, ou mentiu deliberadamente ao preencher um questionário de segurança do pessoal ou durante uma entrevista para efeitos de segurança;
  - f) Foi condenada por uma ou várias infracções penais;
  - g) Tem um historial de dependência do álcool, de consumo de drogas ilegais e/ou de abuso de drogas legais;
  - h) Tem, ou teve, uma conduta que possa suscitar o risco de vulnerabilidade à chantagem ou a pressões;
  - i) Demonstrou, por actos ou palavras, falta de honestidade, lealdade, fiabilidade ou idoneidade;
  - j) Infringiu de forma grave ou reiterada as regulamentações de segurança, ou tentou, ou conseguiu, realizar actividades não autorizadas no domínio dos sistemas de comunicação e informação;
  - k) Pode estar sujeita a pressões (por exemplo, possuindo uma ou mais nacionalidades extra UE ou por intermédio de familiares ou pessoas próximas potencialmente vulneráveis em relação a serviços de informações estrangeiros, grupos terroristas ou outras organizações ou indivíduos com actividades subversivas, cujos interesses possam ameaçar os interesses de segurança da UE e/ou dos Estados-Membros).
9. Se necessário, e nos termos das disposições legislativas e regulamentares nacionais, também podem considerar-se pertinentes no quadro da investigação de segurança os antecedentes médicos e financeiros da pessoa.
10. Se necessário, e nos termos das disposições legislativas e regulamentares nacionais, também podem considerar-se pertinentes no quadro da investigação de segurança o carácter, a conduta e a situação de um cônjuge, coabitante ou familiar próximo da pessoa.

#### **Requisitos de investigação para acesso a ICUE**

##### *Primeira atribuição da CSP*

11. A CSP inicial para acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET basear-se-á numa investigação de segurança que abranja pelo menos os últimos cinco anos, ou o período compreendido entre os 18 anos de idade e o momento presente, consoante o período mais curto, consistindo, nomeadamente, no seguinte:
- a) Preenchimento de um questionário nacional de segurança do pessoal para o nível de ICUE a que o elemento do pessoal poderá ter necessidade de aceder; uma vez preenchido, o questionário será enviado à autoridade de segurança competente;
  - b) Controlo de identidade/cidadania/nacionalidade – Será verificada a data de nascimento, a naturalidade, bem como a identidade. Será determinada a cidadania e/ou a nacionalidade, passada e presente; tal inclui a avaliação de qualquer vulnerabilidade a pressões por parte de fontes estrangeiras, devido por exemplo a uma residência ou associação anteriores; e
  - c) Controlo dos registos nacionais e locais – Será feita uma verificação nos registos nacionais de segurança e nos registos criminais centrais, caso estes existam, e/ou noutros registos governamentais e policiais equivalentes. Serão verificados os registos dos serviços de polícia competentes nos locais onde a pessoa tenha residido ou trabalhado.
12. A CSP inicial para acesso a informações com classificação TRÈS SECRET UE/EU TOP SECRET basear-se-á numa investigação de segurança que abranja pelo menos os últimos dez anos, ou o período compreendido entre os 18 anos de idade e o momento presente, consoante o período mais curto. No caso de serem realizadas entrevistas conforme estabelecido na alínea e), as investigações abrangerão pelo menos os últimos sete anos, ou o período compreendido entre os 18 anos de idade e o momento presente, consoante o período mais curto. Além dos critérios indicados no ponto 8 acima, serão investigados, na medida em que tal seja possível à luz das disposições legislativas e regulamentares nacionais, os elementos que adiante se enumeram antes de ser concedida a CSP TRÈS SECRET UE/EU TOP SECRET; esses elementos poderão ser também investigados antes de ser concedida uma CSP CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, quando as disposições legislativas e regulamentares nacionais o exigirem:
- a) Situação financeira – Serão pedidas informações sobre a situação financeira a fim de avaliar qualquer vulnerabilidade a pressões nacionais ou estrangeiras em virtude de sérias dificuldades financeiras, ou para descobrir qualquer enriquecimento inexplicado;

- b) Educação – Serão pedidas informações para verificar o percurso seguido em escolas, universidades e outros estabelecimentos de ensino frequentados desde os 18 anos de idade, ou durante um período considerado apropriado pela autoridade investigadora;
  - c) Emprego – Serão pedidas informações sobre o actual e os anteriores empregos, fazendo referência a fontes como registos de emprego, relatórios de desempenho ou eficiência, e a entidades patronais ou supervisores;
  - d) Serviço militar – Se for caso disso, será verificado o serviço nas forças armadas e o tipo de desquite; e
  - e) Entrevistas – Quando previstas e admissíveis nos termos da legislação nacional, serão efectuadas uma ou mais entrevistas. Serão também realizadas entrevistas com outras pessoas que estejam em posição de fazer uma avaliação imparcial dos antecedentes, actividades, lealdade, idoneidade e fiabilidade da pessoa em causa. No caso de ser prática nacional pedir referências à pessoa investigada, as pessoas que derem essas referências serão entrevistadas, a menos que haja boas razões para não o fazer.
13. Se necessário, e nos termos das disposições legislativas e regulamentares nacionais, poderão ser efectuadas investigações adicionais para aprofundar todas as informações pertinentes de que se disponha sobre a pessoa, bem como para corroborar ou refutar as informações desfavoráveis.

#### *Renovação das CSP*

14. Depois da primeira atribuição da CSP, e desde que a pessoa em causa tenha prestado ininterruptamente serviço numa administração nacional ou no SGC e continue a precisar de ter acesso a ICUE, a CSP será revista, para efeitos de renovação, a intervalos não superiores a cinco anos para uma credenciação TRÈS SECRET UE/EU TOP SECRET e a dez anos para credenciações SECRET UE/EU SECRET e CONFIDENTIEL UE/EU CONFIDENTIAL, com efeitos a partir da data da notificação dos resultados da última investigação de segurança que lhes tenha servido de base. Todas as investigações de segurança com vista à renovação da CSP abrangerão o período decorrido desde a última investigação.
15. Para a renovação das CSP, serão investigados os elementos descritos nos pontos 11 e 12.
16. Os pedidos de renovação serão feitos em tempo útil, tendo em conta o período necessário para efectuar as investigações de segurança. Não obstante, se a ANS ou qualquer outra autoridade nacional competente tiver recebido o pedido de renovação e o correspondente questionário de segurança do pessoal antes do termo de validade da CSP, e a necessária investigação de segurança ainda não tiver sido concluída, a autoridade nacional competente poderá prorrogar a validade da CSP existente por um período de, no máximo, 12 meses, se tal for admissível nos termos das disposições legislativas e regulamentares nacionais. Se, findo este período de 12 meses, a investigação de segurança ainda não estiver concluída, a pessoa em causa será afectada a funções que não exijam CSP.

#### *Procedimento de concessão de CSP no SGC*

17. No que respeita aos funcionários e outros agentes do SGC, a Autoridade de Segurança do SGC enviará o questionário de segurança do pessoal, preenchido, à ANS do Estado-Membro de nacionalidade da pessoa, solicitando que seja levada a cabo uma investigação de segurança para o nível de ICUE às quais a pessoa deverá ter acesso.
18. Se o SGC tomar conhecimento de informações relevantes para a investigação de segurança a respeito de alguém que tenha solicitado uma CSP UE, o SGC informará desse facto a ANS competente, nos termos das regras e regulamentações pertinentes.
19. Concluída a investigação de segurança, a ANS competente comunicará à Autoridade de Segurança do SGC os resultados dessa investigação, utilizando para o efeito a minuta estipulada pelo Comité de Segurança.
- a) Se da investigação de segurança se concluir que não há garantidamente conhecimento de factores desfavoráveis que ponham em dúvida a lealdade, a idoneidade e a fiabilidade da pessoa, a Autoridade do SGC Investida do Poder de Nomeação pode conceder à pessoa em questão uma CSP UE e autorizá-la a ter acesso a ICUE até ao nível adequado e até determinada data;
  - b) Se da investigação de segurança se não concluir pela existência dessa garantia, a Autoridade do SGC Investida do Poder de Nomeação notificará do facto a pessoa em causa, que poderá pedir para ser ouvida pela referida Autoridade. A Autoridade Investida do Poder de Nomeação poderá pedir à ANS competente quaisquer outros esclarecimentos que esta possa prestar nos termos das respectivas disposições legislativas e regulamentares nacionais. Se as conclusões se confirmarem, não será concedida a CSP UE.

20. A investigação de segurança, bem como os resultados obtidos ficarão sujeitos às disposições legislativas e regulamentares pertinentes em vigor no Estado-Membro em questão, incluindo em matéria de recurso. As decisões tomadas pela Autoridade do SGC Investida do Poder de Nomeação são passíveis de recurso nos termos do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União Europeia, previstos no Regulamento (CEE, Euratom, CECA) n.º 259/68 <sup>(1)</sup> (a seguir designado «Estatuto e Regime aplicável»).
21. A garantia em que se basear a CSP UE, desde que se mantenha válida, abrangerá quaisquer funções que a pessoa em causa venha a desempenhar no SGC ou na Comissão.
22. 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 do SGC Investida do Poder de Nomeação, ou se houver uma interrupção de 12 meses no serviço durante a qual a pessoa não exerça funções no SGC ou na administração de um Estado-Membro, os referidos resultados serão remetidos à ANS competente, para confirmação de que continuam a ser válidos e pertinentes.
23. Se o SGC tomar conhecimento de informações a respeito da existência de qualquer risco para a segurança que provenha de alguém que tenha uma CSP UE válida, o SGC informará desse facto a ANS competente, nos termos das regras e regulamentações pertinentes. Quando a ANS comunicar ao SGC que retirou a alguém que possua uma CSP UE válida a garantia que lhe fora dada nos termos do ponto 19, alínea a), a Autoridade do SGC Investida do Poder de Nomeação pode pedir à ANS quaisquer esclarecimentos que esta possa prestar nos termos das respectivas disposições legislativas e regulamentares nacionais. Se as informações desfavoráveis forem confirmadas, a CSP UE será retirada e a pessoa em causa será excluída do acesso à ICUE e afastada de funções no âmbito das quais esse acesso seja possível ou a pessoa possa prejudicar a segurança.
24. A decisão de retirar a CSP UE a um funcionário ou agente do SGC e, se necessário, as razões que a motivaram serão notificadas à pessoa em causa, que pode pedir para ser ouvida pela Autoridade Investida do Poder de Nomeação. As informações prestadas pela ANS ficarão sujeitas às disposições legislativas e regulamentares pertinentes em vigor no Estado-Membro em questão, incluindo em matéria de recurso. As decisões tomadas pela Autoridade do SGC Investida do Poder de Nomeação são passíveis de recurso nos termos do Estatuto e do Regime Aplicável.
25. Antes de assumirem funções, os peritos nacionais destacados para um lugar no SGC que exija uma CSP UE deverão apresentar à Autoridade de Segurança do SGC uma CSP nacional válida para efeitos de acesso a ICUE.

#### *Registos de CSP*

26. Os Estados-Membros e o SGC manterão, respectivamente, registos das CSP nacionais e das CSP UE conferidas para efeitos de acesso a ICUE. Esses registos especificarão, pelo menos, o nível das ICUE a que a pessoa pode ter acesso (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de concessão e o período de validade da CSP.
27. A autoridade de segurança competente poderá emitir um Certificado de Credenciação de Segurança do Pessoal (CCSP), indicando o nível de ICUE a que a pessoa pode ter acesso (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), o período de validade da CSP nacional para efeitos de acesso a ICUE ou da CSP UE e o prazo de validade do próprio certificado.

#### **Isenção do requisito de Credenciação de Segurança do Pessoal**

28. O acesso a ICUE por parte de pessoas devidamente autorizadas nos Estados-Membros em virtude das funções que exercem será determinado nos termos das disposições legislativas e regulamentares nacionais; essas pessoas serão informadas das suas obrigações de segurança no que respeita à protecção das ICUE.

#### **IV. EDUCAÇÃO E SENSIBILIZAÇÃO PARA A SEGURANÇA**

29. Todas as pessoas a quem tenha sido conferida uma CSP confirmarão por escrito que compreenderam as obrigações a que estão sujeitas no que respeita à protecção das ICUE e as consequências do comprometimento de ICUE. Os Estados-Membros e o SGC, consoante o caso, conservarão um registo dessas declarações escritas.
30. Todas as pessoas autorizadas a aceder a ICUE ou que precisem de manusear ICUE serão inicialmente sensibilizadas e periodicamente informadas das ameaças existentes para a segurança e deverão comunicar imediatamente às autoridades de segurança competentes qualquer atitude ou actividade que considerem suspeita ou pouco habitual.
31. Quem deixar de exercer funções que exijam acesso a ICUE será informado de que deverá continuar a salvaguardar as ICUE e, se necessário, confirmará por escrito essa sua obrigação.

<sup>(1)</sup> JO L 56 de 4.3.1968, p. 1.

## V. CIRCUNSTÂNCIAS EXCEPCIONAIS

32. Quando as disposições legislativas e regulamentares nacionais o permitirem, a CSP concedida por uma autoridade nacional competente de um Estado-Membro para acesso a informações classificadas nacionais pode, temporariamente, até à concessão de uma CSP nacional para acesso a ICUE, permitir que funcionários nacionais tenham acesso a ICUE até ao nível equivalente, como se indica na tabela de equivalências que figura no Apêndice B, se esse acesso temporário for do interesse da UE. Quando as disposições legislativas e regulamentares nacionais não permitam esse acesso temporário às ICUE, as ANS informarão desse facto o Comité de Segurança.
33. Por motivos de urgência devidamente justificados pelo interesse do serviço e enquanto se aguarda a conclusão de uma investigação de segurança exaustiva, a Autoridade do SGC Investida do Poder de Nomeação, após consulta à ANS do Estado-Membro de nacionalidade do interessado e sob reserva dos resultados da verificação inicial de que não há conhecimento de informações desfavoráveis, pode conceder aos funcionários e outros agentes do SGC uma autorização temporária de acesso a ICUE para uma função concreta. Essas autorizações temporárias terão uma validade não superior a seis meses e não permitirão o acesso a informações com classificação TRÈS SECRET UE/EU TOP SECRET. Todas as pessoas a quem tenha sido concedida uma autorização temporária confirmarão por escrito que compreenderam as obrigações a que estão sujeitas no que respeita à protecção das ICUE e as consequências do comprometimento de ICUE. O SGC conservará um registo dessas declarações escritas.
34. Quando devam ser atribuídas a alguém funções que exijam uma CSP de nível superior ao que a pessoa possui, a atribuição pode ser feita a título temporário, desde que:
- a) A necessidade urgente de acesso a ICUE de nível superior seja justificada, por escrito, pelo superior hierárquico da pessoa em causa;
  - b) O acesso seja limitado a ICUE específicas de apoio às funções exercidas;
  - c) A pessoa em causa possua uma CSP nacional ou CSP UE válida;
  - d) Tenham sido iniciados os trâmites necessários para obter autorização para o nível de acesso exigido para essas funções;
  - e) A autoridade competente tenha feito verificações satisfatórias das quais se tenha concluído que a pessoa em causa não infringiu as regras de segurança de forma grave nem reiterada;
  - f) A atribuição de funções à pessoa em causa seja aprovada pela autoridade competente; e
  - g) A excepção, incluindo uma descrição das informações para as quais tenha sido aprovado o acesso, seja averbada no registo responsável ou num registo que dele dependa.
35. O procedimento acima descrito será utilizado para um único acesso a ICUE de nível superior àquele para o qual tenha sido concedida credenciação de segurança à pessoa em causa. Não se recorrerá repetidamente a este procedimento.
36. Em circunstâncias muito excepcionais, como sejam as missões em ambiente hostil ou os períodos de crescente tensão internacional, quando as medidas de emergência o exijam, nomeadamente para salvar vidas humanas, os Estados-Membros e o Secretário-Geral poderão conceder, por escrito, acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET a pessoas que não possuam a necessária CSP, desde que tal autorização seja absolutamente necessária e não haja dúvidas razoáveis quanto à lealdade, à idoneidade e à fiabilidade da pessoa em causa. Será conservado registo desta autorização, com a descrição das informações para as quais tenha sido aprovado acesso.
37. No caso de informações com classificação TRÈS SECRET UE/EU TOP SECRET, este acesso de emergência será limitado aos nacionais da UE que tenham sido autorizados a aceder ao equivalente nacional do nível TRÈS SECRET UE/EU TOP SECRET ou às informações com classificação SECRET UE/EU SECRET.
38. O Comité de Segurança será informado dos casos em que se recorra ao procedimento descrito nos pontos 36 e 37.
39. Quando as disposições legislativas e regulamentares nacionais dos Estados-Membros prevejam regras mais rigorosas a respeito de autorizações temporárias, atribuição temporária de funções, acesso único ou acesso de emergência a informações classificadas, os procedimentos previstos na presente secção serão aplicados apenas dentro dos limites definidos nas referidas disposições legislativas e regulamentares nacionais.
40. Será anualmente apresentado ao Comité de Segurança um relatório sobre o recurso aos procedimentos estabelecidos na presente secção.

## VI. PARTICIPAÇÃO EM REUNIÕES DO CONSELHO

41. Sob reserva do ponto 28, as pessoas que devam participar em reuniões do Conselho ou das suas instâncias preparatórias em que sejam discutidas informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior só poderão fazê-lo depois de confirmado o seu estatuto de CSP. No caso dos delegados, o CCSP, ou outra prova de CSP, será enviado pelas autoridades nacionais competentes ao Gabinete de Segurança do SGC ou, a título excepcional, apresentado pelo próprio delegado. Se necessário, poderá ser usada uma lista consolidada de nomes, com a indicação da prova de CSP relevante.
42. Se, por razões de segurança, for retirada a CSP nacional para efeitos de acesso a ICUE de alguém cuja presença em reuniões do Conselho ou das suas instâncias preparatórias seja necessária em virtude das funções que exerce, a autoridade competente informará do facto o SGC.

## VII. ACESSO POTENCIAL A ICUE

43. Quem for recrutado para trabalhar em circunstâncias em que possa ter acesso a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior ficará sujeito aos procedimentos de credenciação de segurança adequados ou será permanentemente escoltado.
  44. Os estafetas, guardas e escoltas devem possuir a credenciação de segurança para o nível adequado ou ser de outro modo sujeitos a uma investigação adequada nos termos das disposições legislativas e regulamentares nacionais, ser informados dos procedimentos de segurança aplicáveis à protecção das ICUE e alertados para o seu dever de protecção das informações que lhes forem confiadas.
-

## ANEXO II

## SEGURANÇA FÍSICA

## I. INTRODUÇÃO

1. O presente anexo estabelece as regras de execução do artigo 8.º. Nele se definem os requisitos mínimos para a protecção física de instalações, edifícios, gabinetes, salas e outras zonas em que sejam manuseadas e armazenadas ICUE, e, nomeadamente, zonas que alberguem SCI.
2. Serão concebidas medidas de segurança física para impedir o acesso não autorizado a ICUE:
  - a) Assegurando que as ICUE sejam devidamente manuseadas e armazenadas;
  - 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 respectiva credenciação de segurança;
  - c) Dissuadindo, impedindo e detectando acções não autorizadas; e
  - d) Impedindo ou retardando a entrada sub-reptícia ou forçada de intrusos.

## II. REQUISITOS E MEDIDAS DE SEGURANÇA FÍSICA

3. As medidas de segurança física serão seleccionadas com base na avaliação de risco feita pelas autoridades competentes. Tanto o SGC como os Estados-Membros aplicarão um processo de gestão de risco à protecção das ICUE nas suas instalações, por forma a assegurar que seja concedido um nível de protecção física proporcional ao risco avaliado. No processo de gestão de risco serão tidos em conta todos os factores 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 protecção mais rigorosas;
  - c) A envolvente e a estrutura dos edifícios ou zonas que albergam as ICUE; e
  - d) A avaliação da ameaça representada pelos serviços de informações que tenham por alvo a UE ou os Estados-Membros, pelos actos de sabotagem ou de terrorismo, bem como por outras actividades subversivas ou criminosas.
4. A autoridade de segurança competente determinará, aplicando o conceito de defesa em profundidade, qual a combinação adequada de medidas de segurança física a implementar, que pode ser constituída por uma ou mais das que a seguir se enunciam:
  - a) Perímetro: barreira física que resguarda os limites de uma zona que precisa de ser protegida;
  - b) Sistemas de detecção de intrusos (IDS): podem ser utilizados IDS para aumentar o nível de segurança proporcionado pelo perímetro ou para substituir ou apoiar o pessoal de segurança em salas e edifícios;
  - c) Controlo do acesso: o controlo do acesso poderá ser exercido em relação a um local, a um edifício ou edifícios de determinado local, ou a zonas ou salas de um edifício. O controlo poderá ser exercido por processos electrónicos ou electromecânicos, efectuado pelo pessoal de segurança e/ou por um rececionista, ou por quaisquer outros meios físicos;
  - d) Pessoal de segurança: poderá nomeadamente recorrer-se a pessoal de segurança devidamente formado, supervisionado e, se necessário, com a devida credenciação de segurança para dissuadir todos aqueles que planeiem uma intrusão dissimulada;
  - e) Televisão em circuito fechado (CCTV): o pessoal de segurança poderá utilizar um sistema de CCTV para verificar incidentes e alarmes de IDS em locais de grandes dimensões ou nos perímetros;
  - f) Luzes de segurança: poderão ser utilizadas luzes de segurança para dissuadir os potenciais intrusos e proporcionar a iluminação necessária para uma vigilância efectiva, efectuada quer directamente pelo pessoal de segurança, quer indirectamente através de um sistema de CCTV; e
  - g) Quaisquer outras medidas físicas adequadas que sejam concebidas para dissuadir ou detectar o acesso não autorizado ou evitar que as ICUE se percam ou sejam danificadas.

5. A autoridade competente pode ser autorizada a efectuar buscas nas entradas e saídas, que funcionarão como elemento dissuasor da introdução não autorizada de material ou da saída não autorizada de ICUE das instalações ou edifícios.
6. Quando houver risco de olhares indiscretos sobre ICUE, mesmo que acidentalmente, serão tomadas as medidas necessárias para neutralizar esse risco.
7. Na fase de planeamento e concepção de novas instalações, deverão ser definidos os requisitos de segurança física e as respectivas especificações funcionais. Em instalações já existentes, os requisitos de segurança física serão aplicados em toda a medida do possível.

### III. EQUIPAMENTO PARA A PROTECÇÃO FÍSICA DAS ICUE

8. Aquando da aquisição de equipamento (por exemplo, contentores de segurança, máquinas trituradoras, fechaduras de porta, sistemas electrónicos de controlo de acesso, sistemas de detecção de intrusos, sistemas de alarme) para protecção física das ICUE, a autoridade de segurança competente certificar-se-á de que o equipamento satisfaz as normas técnicas e os requisitos mínimos aprovados.
9. As especificações técnicas do equipamento a utilizar na protecção física das ICUE serão estabelecidas em directrizes de segurança aprovadas pelo Comité de Segurança.
10. Os sistemas de segurança serão regularmente sujeitos a inspecção e o equipamento será objecto de manutenção regular. Nos trabalhos de manutenção serão tidos em conta os resultados das inspecções, a fim de garantir que o equipamento continue a funcionar nas melhores condições.
11. Em cada inspecção será reavaliada a eficácia de cada medida de segurança e do sistema de segurança em geral.

### IV. ZONAS FISICAMENTE PROTEGIDAS

12. Serão estabelecidos dois tipos de zonas fisicamente protegidas, ou os seus equivalentes nacionais, para assegurar a protecção física das ICUE:
  - a) Zonas Administrativas; e
  - b) Zonas de Segurança (incluindo as Zonas Tecnicamente Seguras).

Na presente decisão, todas as referências às Zonas Administrativas e Zonas de Segurança, incluindo as Zonas Tecnicamente Seguras, devem ser igualmente entendidas como referências aos seus equivalentes nacionais.

13. A autoridade de segurança competente determinará que uma dada zona preenche os requisitos para ser designada Zona Administrativa, Zona de Segurança ou Zona Tecnicamente Segura.
14. No caso das Zonas Administrativas:
  - a) Será estabelecido um perímetro visivelmente definido que permita o controlo de pessoas e, se possível, de veículos;
  - b) Só poderão ter acesso sem escolta as pessoas devidamente autorizadas pela autoridade competente; e
  - c) Quaisquer outras pessoas serão permanentemente escoltadas ou sujeitas a controlos equivalentes.
15. No caso das Zonas de Segurança:
  - a) Será estabelecido um perímetro visivelmente definido, em que qualquer entrada ou saída será controlada por meio de um sistema de livre-trânsito ou de reconhecimento de pessoas;
  - b) Só poderão 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 serão permanentemente escoltadas ou sujeitas a controlos equivalentes.

16. Nos casos em que a entrada numa Zona de Segurança represente, para todos os efeitos práticos, um acesso directo 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 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,
  17. As Zonas de Segurança a proteger contra escutas serão designadas Zonas Tecnicamente Seguras. A estas zonas aplicam-se ainda os seguintes requisitos:
    - a) Serão equipadas com sistemas de detecção de intrusos (IDS), fechadas à chave quando não estiverem ocupadas e guardadas quando ocupadas. Todas as chaves serão controladas de acordo com a Secção VI;
    - b) Serão sujeitas a controlo todas as pessoas ou material que nelas penetrem;
    - c) Serão sujeitas a inspeção física e/ou técnica regular, consoante o que a autoridade de segurança competente exigir. Essa inspeção será igualmente efectuada na sequência de qualquer entrada não autorizada ou de suspeitas dessa possibilidade; e
    - d) Serão desprovidas de dispositivos não autorizados como linhas de comunicação, telefones ou outros aparelhos de comunicação, bem como equipamento eléctrico ou electrónico.
  18. Não obstante o disposto na alínea d) do ponto 17, e em circunstâncias em que a ameaça seja considerada elevada, qualquer tipo de aparelho de comunicações e equipamento eléctrico ou electrónico será inspeccionado pela autoridade de segurança competente antes de ser utilizado em zonas onde decorram reuniões ou se trabalhe com informações com classificação SECRET UE/EU SECRET e 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.
  19. As Zonas de Segurança que não estejam ocupadas por pessoal em serviço 24 horas por dia serão, se necessário, inspeccionadas no final das horas normais de serviço e a intervalos aleatórios fora dessas horas, a menos que esteja instalado um sistema de detecção de intrusos.
  20. Poderão ser temporariamente criadas Zonas de Segurança e Zonas Tecnicamente Seguras no interior de determinada Zona Administrativa para a realização de uma reunião classificada ou para qualquer outro fim semelhante.
  21. Para cada Zona de Segurança serão estabelecidos procedimentos operacionais de segurança que estipulem:
    - a) O nível das ICUE que podem ser manuseadas ou armazenadas nessa zona;
    - b) As medidas de vigilância e de protecção 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 credenciação de segurança;
    - d) Se necessário, os procedimentos respeitantes a escoltas ou à protecção das ICUE quando se autorize o acesso de outras pessoas a essa zona;
    - e) Quaisquer outras medidas e procedimentos relevantes.
  22. Serão construídas casas-fortes dentro das Zonas de Segurança. As paredes, o chão, os tectos, as janelas e as portas com sistema de fecho serão aprovados pela autoridade de segurança competente e beneficiarão de protecção equivalente à de um contentor de segurança aprovado para armazenamento de ICUE com o mesmo nível de classificação.
- V. MEDIDAS DE PROTECÇÃO FÍSICA PARA O MANUSEAMENTO E ARMAZENAMENTO DE ICUE
23. 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 nos pontos 28 a 40 do Anexo III e se tenha comprometido a respeitar as medidas de compensação estabelecidas nas instruções emitidas pela autoridade de segurança competente, a fim de assegurar que as ICUE fiquem protegidas do acesso por parte de pessoas não autorizadas.

24. As ICUE com classificação RESTREINT UE/EU RESTRICTED devem ser armazenadas em mobiliário de escritório apropriado e fechado à chave, numa Zona Administrativa ou Zona de Segurança. As referidas ICUE poderão ser temporariamente armazenadas fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas se tenha comprometido a respeitar as medidas de compensação estabelecidas nas instruções emitidas pela autoridade de segurança competente.
25. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET podem ser manuseadas:
- Em Zonas de Segurança;
  - Em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas; ou
  - Fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor das informações classificadas:
    - as transporte nas condições estabelecidas nos pontos 28 a 40 do Anexo III,
    - se tenha comprometido a respeitar as medidas de compensação estabelecidas nas instruções emitidas pela autoridade de segurança competente, a fim de assegurar que as ICUE fiquem protegidas do acesso por parte de pessoas não autorizadas,
    - mantenha as ICUE permanentemente sob o seu controlo pessoal, e
    - no caso de documentos em suporte papel, tenha informado desse facto o registo competente.
26. As ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET serão armazenadas em Zonas de Segurança, dentro de um contentor de segurança ou de uma casa-forte.
27. As ICUE com classificação TRÈS SECRET UE/EU TOP SECRET serão manuseadas em Zonas de Segurança.
28. As ICUE com classificação TRÈS SECRET UE/EU TOP SECRET serão armazenadas em Zonas de Segurança, numa das seguintes condições:
- Num contentor de segurança, de acordo com o estabelecido no ponto 8, com um ou vários dos seguintes controlos suplementares:
    - protecção ou verificação permanente por pessoal de segurança ou de serviço com credenciação de segurança,
    - um IDS aprovado, conjugado com pessoal de segurança incumbido das situações de emergência;
- ou
- Numa casa-forte com IDS, conjugada com pessoal de segurança incumbido das situações de emergência.
29. As regras a que deve obedecer o transporte de ICUE fora das zonas fisicamente protegidas são estabelecidas no Anexo III.
- VI. CONTROLO DAS CHAVES E COMBINAÇÕES DE FECHADURAS DE SEGREGO UTILIZADAS PARA PROTECÇÃO DAS ICUE
30. A autoridade de segurança competente definirá procedimentos para a gestão das chaves e das combinações das fechaduras de segredo dos gabinetes, salas, casas-fortes e contentores de segurança. Tais procedimentos deverão assegurar a protecção contra o acesso não autorizado.
31. As combinações deverão 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 deverão ser mudadas:
- Sempre que mude o pessoal que conhece a combinação;
  - Sempre que haja conhecimento ou suspeita de comprometimento;
  - Sempre que uma fechadura tenha sido objecto de manutenção ou reparação; e
  - Pelo menos de 12 em 12 meses.
-

## ANEXO III

**GESTÃO DAS INFORMAÇÕES CLASSIFICADAS****I. INTRODUÇÃO**

1. O presente anexo estabelece as regras de execução do artigo 9.º. Nele se definem as medidas administrativas de controlo das ICUE ao longo do seu ciclo de vida que visam contribuir para dissuadir e detectar a perda ou comprometimento deliberados ou acidentais de informações e para recuperar essas informações em caso de perda ou comprometimento.

**II. GESTÃO DAS CLASSIFICAÇÕES****Classificações e marcas**

2. As informações serão classificadas se precisarem de protecção em virtude da sua confidencialidade.
3. A entidade de origem das ICUE será responsável pela determinação do nível de classificação de segurança, nos termos das directrizes de classificação relevantes, e pela divulgação inicial das informações.
4. O nível de classificação das ICUE será determinado nos termos do artigo 2.º, n.º 2, e mediante remissão para a política de segurança a aprovar nos termos do artigo 3.º, n.º 3.
5. A classificação de segurança deverá ser clara e correctamente indicada, independentemente do suporte em que a ICUE seja apresentada: papel, oral, electrónico ou outro.
6. Cada uma das partes de um determinado documento (páginas, parágrafos, secções, anexos, apêndices, adendas e elementos apensos) poderá exigir classificações diferentes, devendo ostentar a marca correspondente, inclusivamente quando for armazenado em suporte electrónico.
7. A classificação geral de um documento ou dossiê deverá ser pelo menos tão elevada quanto a da parte desse documento classificada ao nível mais elevado. Quando forem coligidas informações provenientes de várias fontes, o produto final será analisado para determinar o seu nível geral de classificação de segurança, uma vez que poderá justificar uma classificação mais elevada que a das partes que o compõem.
8. Na medida do possível, os documentos que contenham partes com níveis de classificação diferentes serão estruturados de forma a que as partes com um nível de classificação diferente possam ser facilmente identificadas e, se necessário, destacadas.
9. A classificação de uma carta ou nota de envio deverá ser tão elevada quanto a mais alta classificação dos seus anexos. A entidade de origem deverá indicar claramente a que nível é classificada a carta ou nota quando destacada dos anexos, para o que deverá utilizar uma marca adequada, por exemplo:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sem anexo(s) RESTREINT UE/EU RESTRICTED

**Marcas**

10. Para além de uma das marcas de classificação previstas no artigo 2.º, n.º 2, as ICUE poderão 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 actividade 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.

**Marcas de classificação abreviadas**

11. Para indicar o nível de classificação de certos parágrafos de determinado texto, podem ser utilizadas marcas de classificação sob forma de abreviaturas normalizadas. As abreviaturas não substituem as marcas de classificação por extenso.

12. Nos documentos classificados da UE, podem ser utilizadas, para indicar o nível de classificação de secções ou blocos do texto com menos de uma página, 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

#### **Produção de ICUE**

13. Ao produzir um documento classificado da UE:
- Todas as páginas serão marcadas de forma clara com o nível de classificação;
  - Todas as páginas serão numeradas;
  - O documento ostentará um número de referência e o assunto, que não constituem por si só informação classificada, a menos que estejam marcados como tal;
  - O documento será datado;
  - Os documentos com classificação SECRET UE/EU SECRET ou superior que devam ser distribuídos em vários exemplares ostentarão um número de exemplar em todas as páginas.
14. Quando não for possível aplicar o disposto no ponto 13 às ICUE, deverão ser tomadas outras medidas adequadas nos termos das directrizes de segurança a estabelecer ao abrigo do artigo 6.º, n.º 2.

#### **Desgradação e desclassificação de ICUE**

15. Aquando da produção de ICUE, a entidade de origem indicará, sempre que possível, especialmente se se tratar de informações com classificação RESTREINT UE/EU RESTRICTED, se estas podem ser desgraduadas ou desclassificadas em determinada data ou após um dado acontecimento.
16. O SGC analisará regularmente as ICUE que se encontrem na sua posse, a fim de apurar se o respectivo nível de classificação continua a ser aplicável. O SGC estabelecerá um sistema para proceder, pelo menos de cinco em cinco anos, à reanálise do nível de classificação das ICUE registadas que tiver produzido. Essa reanálise não será 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.

### **III. REGISTO DE ICUE PARA EFEITOS DE SEGURANÇA**

17. Será designado um registo responsável para cada entidade orgânica do SGC e das administrações nacionais dos Estados-Membros em que sejam manuseadas ICUE para assegurar que as informações classificadas da UE sejam manuseadas nos termos da presente decisão. Os registos serão considerados Zonas de Segurança, tal como definidas no Anexo II.
18. Para efeitos da presente decisão, entende-se por «registo para efeitos de segurança» (a seguir designado por «registo») a aplicação de procedimentos que registem o ciclo de vida do material, incluindo a sua divulgação e destruição.
19. Todo o material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e superior será inscrito em registos próprios à entrada e à saída de uma entidade orgânica.
20. O Registo Central do SGC registará todas as informações classificadas comunicadas pelo Conselho e pelo SGC a Estados terceiros e organizações internacionais, bem como todas as informações classificadas recebidas de Estados terceiros e organizações internacionais.
21. Os SCI podem executar os procedimentos de registo recorrendo aos seus próprios processos.
22. O Conselho aprovará uma política de segurança aplicável ao registo de ICUE para efeitos de segurança.

**Registos de informações com classificação TRÈS SECRET UE/EU TOP SECRET**

23. Será designado nos Estados-Membros e no SGC um registo que actuará como autoridade central de recepção e envio de informações com classificação TRÈS SECRET UE/EU TOP SECRET. Se necessário, poderão ser designados registos dependentes do registo central, a fim de manusear essas informações para efeitos de registo.
24. Os registos dependentes não poderão enviar documentos com classificação TRÈS SECRET UE/EU TOP SECRET directamente 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.

**IV. CÓPIA E TRADUÇÃO DE DOCUMENTOS CLASSIFICADOS DA UE**

25. Os documentos com classificação TRÈS SECRET UE/EU TOP SECRET não serão copiados nem traduzidos sem o consentimento prévio da entidade de origem, dado por escrito.
26. Os documentos com classificação SECRET UE/EU SECRET ou inferior poderão ser copiados ou traduzidos por ordem do detentor se a respectiva entidade de origem não tiver imposto restrições à sua cópia ou tradução.
27. As medidas de segurança aplicáveis ao documento original serão igualmente aplicáveis às respectivas cópias e traduções.

**V. TRANSPORTE DE ICUE**

28. O transporte de ICUE fica sujeito às medidas de protecção estabelecidas nos pontos 30 a 40. Quando as ICUE forem transportadas por meios electrónicos, e não obstante o artigo 9.º, n.º 4, as medidas de protecção a seguir estabelecidas poderão ser complementadas pelas contramedidas técnicas adequadas que a autoridade de segurança competente determinar, a fim de minimizar o risco de perda ou comprometimento.
29. As autoridades de segurança competentes do SGC e dos Estados-Membros emitirão instruções para o transporte de ICUE, nos termos da presente decisão.

**No interior de um edifício ou bloco de edifícios**

30. As ICUE transportadas dentro de um edifício ou bloco de edifícios deverão ser cobertas para evitar que o seu conteúdo possa ser visto.
31. No interior de um edifício ou bloco de edifícios, as informações com classificação TRÈS SECRET UE/EU TOP SECRET deverão ser transportadas num envelope de segurança que ostente apenas o nome do destinatário.

**Dentro do território da União Europeia**

32. As ICUE transportadas entre edifícios ou instalações dentro do território da União Europeia devem ser acondicionadas de forma que as proteja da divulgação não autorizada.
33. O transporte de informações com classificação até SECRET UE/EU SECRET dentro do território da União Europeia será efectuado por um dos seguintes meios:
  - a) Estafeta militar, correio oficial ou mala diplomática, consoante o caso;
  - b) Transporte por mão própria, desde que:
    - i) as ICUE não saiam das mãos do portador, a menos que se encontrem armazenadas nos termos dos requisitos estabelecidos no Anexo II,
    - ii) as ICUE não sejam abertas pelo caminho nem lidas em locais públicos,
    - iii) as pessoas em causa sejam informadas das suas responsabilidades em matéria de segurança,
    - iv) as pessoas em causa recebam, se necessário, um certificado de estafeta;
  - c) Serviços postais ou serviços comerciais de estafeta, desde que:
    - i) sejam aprovados pela ANS competente, nos termos das disposições legislativas e regulamentares nacionais,
    - ii) apliquem medidas de protecção adequadas nos termos dos requisitos mínimos a estabelecer nas directrizes de segurança ao abrigo do artigo 6.º, n.º 2.

Em caso de transporte de um Estado-Membro para outro, o disposto na alínea c) fica limitado a informações com classificação até CONFIDENTIEL UE/EU CONFIDENTIAL.

34. O material classificado CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET (por exemplo, equipamento ou maquinaria) que não possa ser transportado pelos meios a que se refere o ponto 33 será transportado como mercadoria por transportadoras comerciais nos termos do Anexo V.
35. O transporte de informações com classificação TRÈS SECRET UE/EU TOP SECRET entre edifícios ou instalações dentro do território da União Europeia será efectuado por estafeta militar, correio oficial ou mala diplomática, consoante o caso.

#### **Do território da União Europeia para o território de um Estado terceiro**

36. As ICUE transportadas do território da União Europeia para o território de um Estado terceiro devem ser acondicionadas de forma que as proteja da divulgação não autorizada.
37. O transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET do território da União Europeia para o território de um Estado terceiro será efectuado por um dos seguintes meios:
  - a) Estafeta militar ou mala diplomática;
  - b) Transporte por mão própria, desde que:
    - i) o volume ostente um selo oficial ou esteja acondicionado de modo a indicar que se trata de remessa oficial que não deverá ser sujeita a inspecção aduaneira ou de segurança,
    - ii) as pessoas em causa possuam um certificado de estafeta que identifique o volume e as autorize a transportá-lo,
    - iii) as ICUE não saiam das mãos do portador, a menos que se encontrem armazenadas nos termos dos requisitos estabelecidos no Anexo II,
    - iv) as ICUE não sejam abertas pelo caminho nem lidas em locais públicos, e
    - v) as pessoas em causa sejam informadas das suas responsabilidades em matéria de segurança.

38. O transporte de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET comunicadas pela UE a um Estado terceiro ou organização internacional deverá cumprir as disposições relevantes ao abrigo de um acordo de segurança das informações ou de um convénio administrativo nos termos do artigo 12.º, n.º 2, alíneas a) ou b).

39. As informações com classificação RESTREINT UE/EU RESTRICTED podem também ser transportadas por serviços postais ou serviços comerciais de estafeta.

40. O transporte de informações com classificação TRÈS SECRET UE/EU TOP SECRET do território da União Europeia para o território de um Estado terceiro será efectuado por estafeta militar ou mala diplomática.

#### **VI. DESTRUIÇÃO DE ICUE**

41. Os documentos classificados da UE que deixem de ser necessários podem ser destruídos, sem prejuízo das regras e regulamentações pertinentes em matéria de arquivo.
42. Os documentos que devam ser registados nos termos do artigo 9.º, n.º 2 serão destruídos pelo registo responsável por ordem do detentor ou de uma autoridade competente. Os livros de registos e outras informações a registar serão actualizados em conformidade.
43. A destruição dos documentos com classificação SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET será efectuada na presença de uma testemunha, que possuirá uma credenciação equivalente, pelo menos, ao nível de classificação dos documentos a destruir.
44. O funcionário do registo e a testemunha, sempre que a presença desta última seja exigida, assinarão um certificado de destruição, que será arquivado no registo. O registo conservará os certificados de destruição dos documentos 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.
45. Os documentos classificados, incluindo os documentos com classificação RESTREINT UE/EU RESTRICTED, serão destruídos por métodos que respeitem as normas EU relevantes ou normas equivalentes ou que tenham sido aprovados pelos Estados-Membros nos termos das normas técnicas nacionais, de modo a impedir a sua reconstrução total ou parcial.

46. A destruição dos suportes informáticos de ICUE será efectuada nos termos do ponto 36 do Anexo IV.
- VII. INSPECÇÕES E VISITAS DE AVALIAÇÃO
47. O termo «inspecção» a seguir utilizado designa
- Qualquer inspecção efectuada nos termos do artigo 9.º, n.º 3, e do artigo 15.º, n.º 2, alíneas e), f) e g); ou
  - Qualquer visita de avaliação efectuada nos termos do artigo 12.º, n.º 5, a fim de avaliar a eficácia das medidas aplicadas para protecção das ICUE.
48. Serão efectuadas inspecções para, nomeadamente:
- Garantir o respeito das normas mínimas aplicáveis à protecção de ICUE estabelecidas na presente decisão;
  - Realçar a importância da segurança e de uma gestão de risco eficaz nas entidades inspeccionadas;
  - Recomendar contramedidas destinadas a atenuar as consequências específicas da perda de confidencialidade, integridade ou disponibilidade de informações classificadas; e
  - Reforçar os programas que as autoridades de segurança tenham em curso em matéria de educação e sensibilização para a segurança.
49. Antes do final de cada ano civil, o Conselho aprovará o programa de inspecções para o ano seguinte, previsto na alínea c) do artigo 15.º, n.º 1. As datas concretas de cada inspecção serão determinadas de comum acordo com a agência ou organismo da UE, o Estado-Membro, o Estado terceiro ou a organização internacional em questão.

#### **Realização de inspecções**

50. Serão efectuadas inspecções para controlar as regras, regulamentações e procedimentos pertinentes da entidade inspeccionada e verificar se as suas práticas cumprem as normas mínimas e os princípios básicos estabelecidos na presente decisão e nas disposições que regem o intercâmbio de informações classificadas com essa mesma entidade.
51. As inspecções serão efectuadas em duas fases. Se necessário, antes da inspecção propriamente dita será organizada uma reunião preparatória com a entidade inspeccionada. Após essa reunião preparatória, a equipa de inspecção definirá, de comum acordo com a entidade inspeccionada, um programa de inspecção pormenorizado que abranja todas as áreas da segurança. A equipa de inspecção terá acesso a todos os locais em que sejam manuseadas ICUE, designadamente registos e pontos de presença de SCI.
52. As inspecções às administrações nacionais dos Estados-Membros serão efectuadas sob a responsabilidade de uma equipa conjunta do SGC e da Comissão, em plena cooperação com os funcionários da entidade inspeccionada.
53. As inspecções às administrações nacionais dos Estados terceiros e organizações internacionais serão efectuadas sob a responsabilidade de uma equipa conjunta do SGC e da Comissão, em plena cooperação com os funcionários do Estado terceiro ou organização internacional inspeccionada.
54. As inspecções às agências e organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol e Eurojust serão efectuadas pelo Gabinete de Segurança do SGC, assistido por peritos da ANS em cujo território a agência ou organismo esteja localizado. A Direcção de Segurança da Comissão Europeia (DSCE) pode ser associada à inspecção caso proceda a intercâmbios regulares de ICUE com a agência ou organismo em causa.
55. Para as inspecções às agências e organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol e Eurojust, bem como a Estados terceiros e organizações internacionais, serão solicitados a assistência e o contributo de peritos da ANS, segundo regras de pormenor a aprovar pelo Comité de Segurança.

#### **Relatórios de inspecção**

56. No final da inspecção, serão apresentadas à entidade inspeccionada as principais conclusões e recomendações. Em seguida, será elaborado um relatório de inspecção, sob a responsabilidade da Autoridade de Segurança do SGC (Gabinete de Segurança). Caso tenham sido propostas medidas correctivas e formuladas recomendações, devem constar do relatório os elementos necessários para corroborar as conclusões tiradas. O relatório será enviado à autoridade competente da entidade inspeccionada.

57. No caso das inspeções efectuadas às administrações nacionais dos Estados-Membros:
- a) O projecto de relatório de inspecção será remetido à ANS interessada para verificar se está factualmente correcto e se não contém informações com classificação superior a RESTREINT UE/EU RESTRICTED;
  - b) A menos que a ANS interessada do Estado-Membro solicite que a distribuição geral seja suspensa, os relatórios de inspecção serão facultados aos membros do Comité de Segurança e à DSCE; será atribuída ao relatório a classificação RESTREINT UE/EU RESTRICTED.
- Será elaborado, sob a responsabilidade da Autoridade de Segurança do SGC (Gabinete de Segurança), um relatório periódico destacando os ensinamentos recolhidos das inspeções efectuadas nos Estados-Membros durante um período determinado, relatório esse que será analisado pelo Comité de Segurança.
58. No caso das visitas de avaliação efectuadas a Estados terceiros e organizações internacionais, o relatório será distribuído ao Comité de Segurança e à DSCE. O relatório terá, no mínimo, a classificação RESTREINT UE/EU RESTRICTED. As eventuais medidas correctivas serão verificadas durante uma visita posterior e comunicadas ao Comité de Segurança.
59. No caso das inspeções efectuadas às agências e organismos da UE criados ao abrigo do Capítulo 2 do Título V do TUE, Europol e Eurojust, serão distribuídos relatórios de inspecção aos membros do Comité de Segurança e à DSCE. O projecto de relatório de inspecção será remetido à agência ou organismo interessado para verificar se está factualmente correcto e se não contém informações com classificação superior a RESTREINT UE/EU RESTRICTED. As eventuais medidas correctivas serão verificadas durante uma visita posterior e comunicadas ao Comité de Segurança.
60. A Autoridade de Segurança do SGC efectuará inspeções regulares às entidades orgânicas do SGC para os efeitos previstos no ponto 48.

#### **Lista de controlo**

61. A Autoridade de Segurança do SGC (Gabinete de Segurança) elaborará e actualizará uma lista de controlo dos pontos a verificar durante as inspeções. A referida lista de controlo será remetida ao Comité de Segurança.
62. As informações necessárias para completar a lista de controlo serão obtidas, nomeadamente durante a inspecção, junto dos serviços de gestão da segurança da entidade inspeccionada. Uma vez completada com as respostas pormenorizadas, a lista de controlo será classificada de comum acordo com a entidade inspeccionada. Esta lista não fará parte do relatório de inspecção.
-

## ANEXO IV

## PROTECÇÃO DAS ICUE MANUSEADAS EM SCI

## I. INTRODUÇÃO

1. O presente anexo estabelece as regras de execução do artigo 10.º.
2. Para a segurança e o correcto funcionamento das operações em SCI, são essenciais as seguintes propriedades e conceitos de GI:

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 exacto e completo da informação e dos activos;

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

## II. PRINCÍPIOS DA GARANTIA DA INFORMAÇÃO

3. As disposições adiante estabelecidas constituirão a base da segurança dos SCI em que sejam manuseadas ICUE. Serão definidos nas políticas e directrizes de segurança em matéria de GI requisitos de pormenor para a execução das presentes disposições.

**Gestão dos riscos de segurança**

4. A gestão dos riscos de segurança constituirá parte integrante da definição, desenvolvimento, exploração e manutenção do SCI. A gestão de risco (avaliação, tratamento, aceitação e comunicação) será conduzida como um processo iterativo em que participem conjuntamente os representantes dos proprietários do sistema, as autoridades de projecto, as autoridades operacionais e as autoridades de aprovação de segurança, seguindo um processo de avaliação dos riscos comprovado, transparente e plenamente compreensível para todos. O alcance do SCI e os seus activos serão claramente definidos logo no início do processo de gestão de risco.
5. As autoridades competentes analisarão as potenciais ameaças ao SCI e farão avaliações rigorosas e actualizadas da ameaça que reflectam o ambiente operacional vigente. Actualizarão constantemente o seu conhecimento das questões relacionadas com as vulnerabilidades e procederão periodicamente à reanálise da avaliação das vulnerabilidades por forma a acompanhar a evolução do ambiente das tecnologias da informação (TI).
6. O objectivo de tratar os riscos de segurança consistirá em aplicar um conjunto de medidas de segurança que resulte num compromisso satisfatório entre os requisitos do utilizador, os custos e o risco de segurança residual.
7. Os requisitos, a escala e o grau de pormenor específicos determinados pela AAS competente para proceder à acreditação de um SCI serão proporcionais ao risco avaliado, tendo em conta todos os factores pertinentes, nomeadamente o nível de classificação das ICUE manuseadas no SCI. A acreditação incluirá uma declaração formal de risco residual e a aceitação do risco residual por uma autoridade responsável.

**Segurança ao longo do ciclo de vida do SCI**

8. Haverá que garantir a segurança ao longo de todo o ciclo de vida do SCI, desde o início até à retirada de serviço.
9. Para cada fase do ciclo de vida, será identificado o papel de cada um dos intervenientes no SCI e a interacção entre eles em termos de segurança do sistema.
10. Os SCI, incluindo as medidas de segurança, de carácter técnico e outras, serão sujeitos a ensaios de segurança durante o processo de acreditação, a fim de assegurar o nível de garantia adequado e de verificar se os sistemas estão correctamente implementados, integrados e configurados.
11. Serão periodicamente efectuadas avaliações, inspecções e análises de segurança durante o funcionamento e a manutenção dos SCI, e quando ocorrerem circunstâncias excepcionais.

12. A documentação de segurança do SCI evoluirá ao longo do seu ciclo de vida enquanto parte integrante do processo de gestão da mudança e da configuração.

#### **Melhores práticas**

13. O SGC e os Estados-Membros cooperarão no desenvolvimento das melhores práticas de protecção das ICUE manuseadas nos SCI. As orientações de melhores práticas apresentarão medidas de segurança de natureza técnica, material, organizativa e processual para os SCI, de comprovada eficácia na luta contra determinadas ameaças e vulnerabilidades.
14. A protecção das ICUE manuseadas nos SCI basear-se-á na experiência adquirida pelas entidades envolvidas na GI, tanto dentro como fora da UE.
15. A divulgação e a subsequente aplicação das melhores práticas ajudarão a atingir um nível de garantia equivalente nos vários SCI que são explorados pelo SGC e pelos Estados-Membros e em que são manuseadas ICUE.

#### **Defesa em profundidade**

16. Para atenuar os riscos que pesam sobre os SCI, será posta em prática uma série de medidas de segurança, de natureza técnica e não técnica, organizadas em múltiplos estratos de defesa, a saber:
- a) *Dissuasão*: medidas de segurança dissuasivas da concretização de planos hostis de ataque ao SCI;
  - b) *Prevenção*: medidas de segurança destinadas a impedir ou bloquear um ataque ao SCI;
  - c) *Deteção*: medidas de segurança destinadas a descobrir a ocorrência de um ataque ao SCI;
  - d) *Resistência*: medidas de segurança destinadas a limitar o impacto do ataque a um conjunto mínimo de informações ou activos do SCI e a prevenir mais danos; e
  - e) *Recuperação*: medidas de segurança destinadas a restabelecer uma situação segura para o SCI.

O grau de rigor destas medidas de segurança será determinado após uma avaliação dos riscos.

17. As autoridades competentes deverão ter capacidade de resposta a incidentes susceptíveis de ultrapassar as fronteiras de uma organização ou de um país, a fim de coordenar as respostas e de partilhar informações sobre esses incidentes e os riscos deles resultantes (capacidades de resposta a emergências informáticas).

#### **Princípio da minimalidade e do menor privilégio**

18. A fim de evitar riscos desnecessários, só serão activadas as funcionalidades, os dispositivos e os serviços essenciais para satisfazer os requisitos operacionais.
19. Para limitar os danos que possam resultar de acidentes, de erros ou da utilização não autorizada dos recursos do SCI, os seus utilizadores e processos automatizados beneficiarão unicamente de acesso, privilégios ou autorizações que forem indispensáveis ao desempenho das suas funções.
20. Os procedimentos de registo cumpridos pelo SCI serão, sempre que necessário, verificados no âmbito do processo de acreditação.

#### **Sensibilização para a Garantia da Informação**

21. A sensibilização para os riscos e para as medidas de segurança disponíveis constitui a primeira linha de defesa da segurança dos sistemas de comunicação e informação. Mais concretamente, todos os elementos do pessoal envolvido no ciclo de vida dos SCI, incluindo os utilizadores, deverão compreender que:
- a) As falhas de segurança podem prejudicar significativamente os sistemas de comunicação e informação;
  - b) A interconexão e a interdependência podem causar prejuízos a terceiros; e
  - c) Cada um tem a sua parte de responsabilidade e deverá prestar contas pela segurança do SCI, em função do papel que desempenha nos sistemas e processos.
22. A fim de assegurar uma boa percepção das responsabilidades em matéria de segurança, os cursos de formação e sensibilização para a GI serão obrigatórios para todo o pessoal envolvido, incluindo os funcionários que ocupem lugares de direcção e os utilizadores dos SCI.

**Avaliação e aprovação de produtos de segurança informática**

23. O necessário grau de confiança nas medidas de segurança, definido como um nível de garantia, será determinado à luz dos resultados do processo de gestão de risco e de acordo com as políticas e directrizes de segurança relevantes.
24. O nível de garantia será verificado mediante a utilização de metodologias e processos reconhecidos internacionalmente ou aprovados a nível nacional, entre os quais se destacam a avaliação, os controlos e as auditorias.
25. Os produtos criptográficos de protecção de ICUE serão avaliados e aprovados por uma Autoridade nacional de Aprovação Criptográfica (AAC) de um Estado-Membro.
26. Antes de a sua aprovação ser recomendada ao Conselho ou ao Secretário-Geral, nos termos do artigo 10.º, n.º 6, os produtos criptográficos deverão ter sido submetidos com êxito a uma segunda avaliação por uma Autoridade de Avaliação Habilitada (AQUA) de um Estado-Membro que não esteja envolvido na concepção nem no fabrico do equipamento. O grau de pormenor exigido na segunda avaliação dependerá do nível de classificação máximo previsto para as ICUE a proteger pelos referidos produtos. O Conselho aprovará uma política de segurança aplicável à avaliação e aprovação de produtos criptográficos.
27. Quando tal se justifique por razões operacionais específicas, o Conselho ou o Secretário-Geral, consoante o caso, podem, por recomendação do Comité de Segurança, dispensar os requisitos previstos nos pontos 25 ou 26 e conceder uma aprovação provisória por um período específico, nos termos do artigo 10.º, n.º 6.
28. A AQUA é uma AAC de um Estado-Membro que tenha sido acreditada com base em critérios definidos pelo Conselho para realizar a segunda avaliação dos produtos criptográficos destinados a proteger as ICUE.
29. O Conselho aprovará uma política de segurança aplicável à qualificação e aprovação de produtos não criptográficos de segurança informática.

**Transmissão dentro de Zonas de Segurança**

30. Não obstante o disposto na presente decisão, quando a transmissão de ICUE se realizar dentro de Zonas de Segurança, poderá ser utilizada a distribuição não cifrada ou a cifragem a um nível inferior, com base nos resultados de um processo de gestão de risco e sob reserva de aprovação da AAS.

**Interconexão segura dos SCI**

31. Para efeitos da presente decisão, entende-se por «interconexão» a conexão directa, unidireccional ou multidireccional, de dois ou mais sistemas informáticos para efeitos de partilha de dados e de outros recursos de informação (por exemplo, comunicação).
32. O SCI tratará qualquer sistema informático com ele interconectado como não fiável e tomará medidas de protecção para controlar o intercâmbio de informações classificadas.
33. Todas as interconexões de SCI com outro sistema informático obedecerão aos seguintes requisitos básicos:
  - a) Os requisitos operacionais ou de actividade dessas interconexões serão determinados e aprovados pelas autoridades competentes;
  - b) A interconexão será submetida a um processo de gestão de risco e de acreditação e deverá ser aprovada pelas AAS competentes; e
  - c) Serão instalados serviços de protecção periférica (*Boundary Protection Services – BPS*) no perímetro de todos os SCI.
34. Não pode haver interconexão entre um SCI acreditado e uma rede desprotegida ou pública, a não ser que o SCI tenha aprovado um BPS instalado para esse efeito entre o SCI e a rede desprotegida ou pública. As medidas de segurança aplicáveis a estas interconexões serão avaliadas pela AGI competente e aprovadas pela AAS competente.

Quando a rede desprotegida ou pública for exclusivamente utilizada como transmissora e os dados forem cifrados por um produto criptográfico aprovado nos termos do artigo 10.º, não se considerará essa conexão como uma interconexão.

35. É proibida a interconexão directa ou em cascata entre SCI acreditados para manusear informações com classificação TRÈS SECRET UE/EU TOP SECRET e redes desprotegidas ou públicas.

**Suportes informáticos**

36. Os suportes informáticos deverão ser destruídos segundo procedimentos aprovados pela autoridade de segurança competente.
37. Os suportes informáticos deverão ser reutilizados, desgraduados ou desclassificados segundo uma política de segurança a estabelecer ao abrigo do artigo 6.º, n.º 1.

**Circunstâncias de emergência**

38. Não obstante o disposto na presente decisão, 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 excepcionais.
39. As ICUE poderão ser transmitidas por meio de produtos criptográficos aprovados para um nível de classificação inferior, ou sem cifragem, mediante 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 ou não possuem nenhum dispositivo de cifragem; e
  - b) O material classificado não puder ser enviado a tempo por outros meios.
40. As informações classificadas transmitidas nas circunstâncias referidas no ponto 38 não ostentarão marcas nem indicações que as distingam de informações não classificadas ou de informações que possam ser protegidas por produtos de cifragem disponíveis. Os destinatários serão imediatamente notificados, por outros meios, do nível de classificação das informações.
41. Em caso de recurso ao disposto no ponto 38, será subsequentemente apresentado um relatório nessa matéria à autoridade competente e ao Comité de Segurança.

**III. FUNÇÕES E AUTORIDADES DE GARANTIA DA INFORMAÇÃO**

42. Serão criadas nos Estados-Membros e no SGC as funções GI a seguir enunciadas. As funções em causa não implicam a existência de entidades orgânicas únicas. Terão mandatos independentes. Contudo, aquelas funções, e as responsabilidades que lhes estão associadas, podem ser combinadas ou integradas na mesma entidade orgânica ou divididas em diferentes entidades orgânicas, desde que sejam evitados quaisquer conflitos internos de interesses ou funções.

**Autoridade de Garantia da Informação**

43. Cabe à AGI:
- a) Definir políticas e directrizes de segurança em matéria de GI e controlar a sua eficácia e pertinência;
  - b) Salvaguardar e administrar as informações técnicas relativas aos produtos criptográficos;
  - c) Garantir que as medidas em matéria de GI seleccionadas para protecção das ICUE estejam em consonância com as políticas que regem as suas elegibilidade e selecção;
  - d) Garantir que os produtos criptográficos sejam seleccionados em conformidade com as políticas que regem as suas elegibilidade e selecção;
  - e) Coordenar a formação e a sensibilização em matéria de GI;
  - f) Consultar o fornecedor do sistema, os intervenientes e os representantes dos utilizadores no domínio da segurança, a respeito das políticas e directrizes de segurança em matéria de GI; e
  - g) Garantir que a subformação do Comité de Segurança especializada para as questões de GI disponha das competências técnicas adequadas.

**Autoridade TEMPEST**

44. A Autoridade TEMPEST (AT) será responsável pela garantia de conformidade dos SCI com as políticas e directrizes TEMPEST. A AT procederá à aprovação de contramedidas TEMPEST aplicáveis a instalações e produtos destinados a proteger as ICUE, no seu ambiente operacional, até um determinado nível de classificação.

**Autoridade de Aprovação Criptográfica**

45. A Autoridade de Aprovação Criptográfica (AAC) será responsável pela garantia de conformidade dos produtos criptográficos com a política nacional ou do Conselho em matéria de cifragem. A AAC procederá à aprovação de um produto criptográfico destinado a proteger as ICUE, no seu ambiente operacional, até um determinado nível de classificação. A AAC será ainda responsável pela avaliação dos produtos criptográficos utilizados nos Estados-Membros.

**Autoridade de Distribuição Criptográfica**

46. Cabe à Autoridade de Distribuição Criptográfica (ADC):
- Gerir e prestar contas pelo material criptográfico da UE;
  - Garantir a aplicação dos procedimentos e a criação dos canais adequados para prestar contas por todo o material criptográfico da UE e proceder ao seu manuseamento, armazenamento e distribuição em condições de segurança; e
  - Assegurar as transferências de material criptográfico da UE para as pessoas singulares ou os serviços que o utilizem e as transferências deles provenientes.

**Autoridade de Acreditação de Segurança**

47. Cabe à Autoridade de Acreditação de Segurança (AAS), relativamente a cada sistema:
- Garantir a conformidade dos SCI com as políticas e directrizes de segurança pertinentes, emitir uma declaração de aprovação dos SCI para o manuseamento de ICUE até um determinado nível de classificação, no seu ambiente operacional, enunciando os termos e condições da acreditação e os critérios segundo os quais é exigida nova aprovação;
  - Definir um processo de acreditação de segurança, nos termos das políticas pertinentes, em que sejam claramente estabelecidas as condições de aprovação dos SCI sob a sua autoridade;
  - Definir uma estratégia de acreditação de segurança em que se estabeleça para o processo de acreditação um grau de pormenor proporcional ao nível de garantia exigido;
  - Analisar e aprovar documentação em matéria de segurança, nomeadamente as declarações de gestão de risco e de risco residual, os requisitos de segurança específicos do sistema (adiante designados por «RSES»), a documentação de verificação da implementação e os procedimentos operacionais de segurança (adiante designados por «POS»), e garantir a conformidade desta documentação com as regras e políticas de segurança do Conselho;
  - Verificar a implementação das medidas de segurança relativamente aos SCI realizando ou promovendo avaliações, inspecções ou controlos de segurança;
  - Definir requisitos de segurança (por exemplo níveis de credenciação do pessoal) para posições sensíveis relativamente aos SCI;
  - Subscrever a selecção dos produtos criptográficos e TEMPEST aprovados que são utilizados para conferir segurança aos SCI;
  - Aprovar a interconexão de um SCI com outro SCI, ou, se for caso disso, participar na aprovação conjunta dessa interconexão; e
  - Consultar o fornecedor do sistema, os intervenientes e os representantes dos utilizadores no domínio da segurança a respeito da gestão de risco, em especial do risco residual, e dos termos e condições da declaração de aprovação.
48. A AAS do SGC será responsável pela acreditação de todos os SCI que operem no âmbito do mandato do SGC.
49. A AAS pertinente de cada Estado-Membro será responsável pela acreditação dos SCI e seus componentes que operem no âmbito do mandato do Estado-Membro.
50. Cabe a um Conselho Conjunto de Acreditação de Segurança proceder à acreditação dos SCI no âmbito dos mandatos respectivos da AAS do SGC e das AAS dos Estados-Membros. O Conselho Conjunto será composto por um representante da AAS de cada Estado-Membro, nele participando um representante da AAS da Comissão Europeia. Serão convidadas a participar nas reuniões outras entidades com nódulos num SCI quando for debatido o sistema em causa.
- O Conselho Conjunto será presidido por um representante da AAS do SGC. Deliberará por consenso dos representantes das AAS das instituições, dos Estados-Membros e de outras entidades com nódulos no SCI. Apresentará periodicamente um relatório de actividades ao Comité de Segurança e notificará-lo-á de todas as declarações de acreditação.

**Autoridade Operacional de Garantia da Informação**

51. Cabe à Autoridade Operacional de GI, relativamente a cada sistema:

- a) Elaborar documentação em matéria de segurança de acordo com as políticas e directrizes na matéria e em especial com os RSES, nomeadamente a declaração de risco residual, os POS e o plano criptográfico no processo de acreditação do SCI;
  - b) Tomar parte na selecção e no ensaio das medidas técnicas de segurança, dispositivos e programas informáticos específicos do sistema, a fim de supervisionar a sua implementação e garantir a segurança da sua instalação, configuração e manutenção, nos termos da documentação de segurança pertinente;
  - c) Participar na selecção de medidas e dispositivos de segurança TEMPEST se os RSES o exigirem e garantir a segurança da sua instalação e manutenção, em colaboração com a AT;
  - d) Acompanhar a implementação e aplicação dos POS e, se necessário, delegar no proprietário do sistema quaisquer responsabilidades em matéria de segurança operacional;
  - e) Gerir e manusear os produtos criptográficos, assegurar a guarda de elementos cifrados e controlados e, se necessário, assegurar a geração de variáveis criptográficas;
  - f) Proceder a revisões das análises de segurança e a ensaios, em especial para a elaboração dos relatórios de risco exigidos pela AAS;
  - g) Organizar acções de formação em matéria de GI específica do SCI;
  - h) Executar e pôr em prática medidas de segurança específicas do SCI.
-

## ANEXO V

**SEGURANÇA INDUSTRIAL**

## I. INTRODUÇÃO

1. O presente anexo estabelece as regras de execução do artigo 11.º. Estabelece as disposições gerais de segurança aplicáveis a entidades industriais ou outras no âmbito das negociações pré-contratuais e durante a vigência dos contratos classificados celebrados pelo SGC.
2. O Conselho aprova uma política em matéria de segurança industrial que estabeleça, nomeadamente, os requisitos detalhados aplicáveis às CSE, às Cláusulas Adicionais de Segurança (CAS), às visitas, à transmissão e ao transporte de ICUE.

## II. ELEMENTOS DE SEGURANÇA DOS CONTRATOS CLASSIFICADOS

**Guia da Classificação de Segurança (GCS)**

3. Antes de abrir concursos públicos ou de celebrar contratos classificados, o SGC determinará, enquanto entidade adjudicante, qual a classificação de segurança de todas as informações a fornecer aos proponentes e contratantes, bem como de todas as informações a produzir pelos contratantes. Para o efeito, o SGC prepara um guia de classificação de segurança (GCS) para ser utilizado na execução do contrato.
4. Para determinar qual a classificação de segurança dos vários elementos de um contrato classificado, serão aplicáveis os seguintes princípios:
  - a) Na elaboração do guia de classificação de segurança, o SGC terá em consideração todos os aspectos de segurança relevantes, nomeadamente a classificação de segurança atribuída às informações fornecidas e aprovadas pela respectiva entidade de origem para utilização no âmbito do contrato;
  - b) O nível global de classificação do contrato não pode ser inferior à classificação mais elevada de qualquer das suas partes; e
  - c) Se necessário, o SGC contacta as ANS/ASD ou quaisquer outras autoridades de segurança competentes dos Estados-Membros quando houver alguma alteração à classificação das informações produzidas pelos contratantes ou a estas fornecidas na execução de um contrato e quando pretender fazer alterações ao guia de classificação de segurança.

**Cláusula Adicional de Segurança (CAS)**

5. Os requisitos de segurança específicos do contrato serão descritos numa CAS. Esta CAS compreenderá, sempre que necessário, o guia de classificação de segurança e fará parte integrante do contrato ou subcontrato.
6. A CAS exigirá que o contratante e/ou subcontratante cumpra as normas mínimas estabelecidas na presente decisão. O incumprimento dessas normas mínimas pode constituir motivo suficiente para a resolução do contrato.

**Instruções de Segurança do Programa/Projecto (ISP)**

7. Em função do âmbito dos programas ou projectos que impliquem acesso, manuseamento ou armazenamento de ICUE, a entidade adjudicante designada para efeitos da gestão do programa ou projecto pode elaborar Instruções específicas de Segurança do Programa/Projecto (ISP). As ISP deverão ser aprovadas pelas ANS/ASD ou por quaisquer outras autoridades de segurança competentes dos Estados-Membros que participem no programa/projecto e podem estabelecer requisitos de segurança adicionais.

## III. CREDENCIAÇÃO DE SEGURANÇA DA EMPRESA (CSE)

8. A CSE será concedida pela ANS ou ASD ou por qualquer outra autoridade de segurança competente de um Estado-Membro, a fim de certificar, nos termos das disposições legislativas e regulamentares nacionais, que determinada entidade industrial ou outra está em condições de proteger as ICUE ao nível de classificação adequado (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET) dentro das respectivas instalações. A CSE será apresentada ao SGC, enquanto entidade adjudicante, antes de as ICUE serem fornecidas ao contratante ou subcontratante ou potencial contratante ou de lhe ser concedido acesso as essas informações.
9. Ao emitir uma CSE, a ANS ou ASD competente deverá, no mínimo:
  - a) Avaliar a integridade da entidade industrial ou outra;
  - b) Avaliar em que medida a propriedade, o controlo ou a potencial exposição a influências indevidas podem ser considerados um risco para a segurança;

- c) Certificar-se de que a entidade industrial ou outra instalou um sistema de segurança que abranja todas as medidas de segurança necessárias à protecção das informações ou material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, nos termos dos requisitos da presente decisão;
- d) Certificar-se de que o estatuto de segurança da administração, dos proprietários e dos empregados que precisem de aceder a informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET foi estabelecido nos termos dos requisitos da presente decisão;
- e) Certificar-se de que a entidade industrial ou outra nomeou um Oficial de Segurança da Empresa, responsável perante a respectiva administração pelo cumprimento das obrigações em matéria de segurança na referida entidade.
10. Se necessário, o SGC, enquanto entidade adjudicante, informará a ANS/ASD competente, ou qualquer outra autoridade de segurança competente, de que é necessária uma CSE para a fase pré-contratual ou para a execução do contrato. Será exigida uma CSE ou uma CSP para a fase pré-contratual quando haja que fornecer ICUE com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET durante o processo de apresentação de propostas.
11. A entidade adjudicante não adjudicará nenhum contrato classificado ao proponente preferido antes de ter recebido, da ANS/ASD ou de qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante esteja registado, confirmação de que, sendo exigível, foi emitida a CSE adequada.
12. A ANS/ASD ou qualquer outra autoridade de segurança competente que tenha emitido a CSE informará o SGC, enquanto entidade adjudicante, de qualquer alteração que afecte a CSE. No caso da subcontratação, será informada em conformidade a ANS/ASD ou qualquer outra autoridade de segurança competente.
13. A retirada da CSE por parte da ANS/ASD ou de qualquer outra autoridade de segurança competente constituirá motivo suficiente para que o SGC, enquanto entidade adjudicante, ponha termo a um contrato classificado ou exclua um dos proponentes do concurso.
- IV. CONTRATOS E SUBCONTRATOS CLASSIFICADOS
14. Quando forem fornecidas ICUE aos proponentes na fase pré-contratual, o aviso de concurso deverá compreender uma disposição que obrigue aqueles que não cheguem a apresentar proposta ou não sejam seleccionados a devolver todos os documentos classificados num prazo determinado.
15. Uma vez adjudicado um contrato ou subcontrato classificado, o SGC, enquanto entidade adjudicante, informará a ANS/ASD ou qualquer outra autoridade de segurança competente do contratante ou subcontratante acerca das disposições de segurança do contrato classificado.
16. Em caso de resolução de contratos desta natureza, o SGC, enquanto entidade adjudicante (e/ou a ANS/ASD ou qualquer outra autoridade de segurança competente, consoante o caso, quando se trate de um subcontrato), informará imediatamente desse facto a ANS/ASD ou qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante esteja registado.
17. No termo do contrato classificado, o contratante ou subcontratante deverá, regra geral, restituir à entidade adjudicante quaisquer ICUE que se encontrem na sua posse.
18. Serão estabelecidas na CAS disposições específicas referentes à eliminação das ICUE durante a fase de execução ou após o termo do contrato.
19. Quando o contratante ou subcontratante for autorizado a conservar ICUE após o termo do contrato, as normas mínimas estabelecidas na presente decisão continuarão a ser cumpridas e a confidencialidade das ICUE protegida pelo contratante ou subcontratante.
20. As condições em que o contratante pode subcontratar serão definidas no concurso e no contrato.
21. Antes de procederem à subcontratação de quaisquer partes de contratos classificados, os contratantes deverão obter autorização do SGC, enquanto entidade adjudicante. Nenhum subcontrato pode ser celebrado com entidades industriais ou outras registadas num Estado que não seja membro da União Europeia e com o qual a União não tenha celebrado nenhum acordo de segurança das informações.

22. É da responsabilidade do contratante garantir que todas as actividades de subcontratação respeitem as normas mínimas estabelecidas na presente decisão, não devendo fornecer ICUE a nenhum subcontratante sem o prévio consentimento escrito da entidade adjudicante.

23. Os direitos de entidade de origem das ICUE que o contratante ou subcontratante tenha produzido ou manuseado serão exercidos pela entidade adjudicante.

#### V. VISITAS ASSOCIADAS A CONTRATOS CLASSIFICADOS

24. Quando o SGC ou quaisquer contratantes ou subcontratantes precisem 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, serão organizadas visitas em ligação com as ANS/ASD ou quaisquer outras autoridades de segurança competentes a que o assunto diga respeito. Todavia, no contexto de determinados projectos, as ANS/ASD podem também aprovar um procedimento segundo o qual as visitas dessa natureza podem ser organizadas directamente.

25. Para aceder às ICUE relacionadas com o contrato do SGC, todos os visitantes devem possuir a devida CSP e ter «necessidade de tomar conhecimento» dessas informações.

26. Apenas será concedido aos visitantes acesso às ICUE relacionadas com a finalidade da visita.

#### VI. TRANSMISSÃO E TRANSPORTE DE ICUE

27. Para efeitos de transmissão de ICUE por meios electrónicos são aplicáveis as disposições pertinentes do artigo 10.º e do Anexo IV.

28. Para efeitos de transporte de ICUE, são aplicáveis as disposições pertinentes do Anexo III, nos termos das disposições legislativas e regulamentares nacionais.

29. Para o transporte como mercadoria de material classificado, serão aplicados os seguintes princípios aquando da determinação dos mecanismos de segurança:

- a) É garantida a segurança em todas as fases do transporte desde o ponto de origem até ao destino final;
- b) O grau de protecção atribuído a uma remessa é determinado pelo nível de classificação mais elevado do material nela contido;
- c) Será obtida uma CSE de nível adequado para as empresas que efectuem o transporte. Nesses casos, o pessoal que manipula a remessa será sujeito a credenciação de segurança, nos termos do Anexo I;
- d) Antes de qualquer transporte transfronteiras de material com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, o expedidor elabora um plano de transporte, que é aprovado pela ANS/ASD em causa ou por qualquer outra autoridade de segurança competente;
- e) Na medida do possível, os transportes serão directos, efectuando-se tão rapidamente quanto as circunstâncias o permitirem;
- f) Sempre que possível, os itinerários apenas devem atravessar o território de Estados-Membros. Só deverão atravessar Estados que não sejam membros da União Europeia quando tal for autorizado pelas ANS/ASD ou por quaisquer outras autoridades de segurança competentes dos Estados do expedidor e do destinatário;

#### VII. TRANSFERÊNCIA DE ICUE PARA CONTRATANTES ESTABELECIDOS EM ESTADOS TERCEIROS

30. A transferência de ICUE para contratantes e subcontratantes estabelecidos em Estados terceiros far-se-á de acordo com as medidas de segurança acordadas entre o SGC, enquanto entidade adjudicante, e a ANS/ASD do Estado terceiro em que o contratante se encontre registado.

#### VIII. MANUSEAMENTO E ARMAZENAMENTO DE INFORMAÇÕES COM CLASSIFICAÇÃO RESTREINT UE/EU RESTRICTED

31. Enquanto entidade adjudicante e com base nas disposições contratuais, assiste ao SGC, em ligação com a ANS/ASD do Estado-Membro, consoante o caso, o direito de efectuar visitas às instalações dos contratantes ou subcontratantes, para verificar se foram tomadas as medidas de segurança necessárias à protecção das ICUE de nível RESTREINT UE/EU RESTRICTED nos termos do contrato.

32. Na medida do necessário ao abrigo das disposições legislativas e regulamentares nacionais, as ANS/ASD ou quaisquer outras autoridades de segurança competentes serão informadas pelo SGC, na qualidade de entidade adjudicante, dos contratos ou subcontratos que envolvam informações com classificação RESTREINT UE/EU RESTRICTED.
  33. Não será necessário que os contratantes ou subcontratantes e respectivo pessoal possuam CSE nem CSP para a execução de contratos celebrados pelo SGC que envolvam informações com classificação RESTREINT UE/EU RESTRICTED.
  34. Não obstante as exigências de CSE ou CSP eventualmente previstas nas disposições legislativas e regulamentares nacionais, o SGC, enquanto entidade adjudicante, analisará as candidaturas apresentadas em concursos para adjudicação de contratos que exijam acesso a informações com classificação RESTREINT UE/EU RESTRICTED.
  35. As condições em que o contratante pode recorrer à subcontratação deverão respeitar o disposto no ponto 21.
  36. Quando um contrato implique o manuseamento de informações com classificação RESTREINT UE/EU RESTRICTED num SCI explorado por um contratante, o SGC, enquanto entidade adjudicante, assegurará que o contrato ou eventual subcontrato especifique requisitos técnicos e administrativos necessários à acreditação do SCI que sejam proporcionais ao risco avaliado, tendo em conta todos os factores pertinentes. O alcance da acreditação do SCI será acordado entre a entidade adjudicante e a ANS/ASD competente.
-

## ANEXO VI

**INTERCÂMBIO DE INFORMAÇÕES CLASSIFICADAS COM ESTADOS TERCEIROS E ORGANIZAÇÕES INTERNACIONAIS**

## I. INTRODUÇÃO

1. O presente anexo estabelece as regras de execução do artigo 12.º.

## II. QUADROS REGULAMENTARES PARA O INTERCÂMBIO DE INFORMAÇÕES CLASSIFICADAS

2. Caso o Conselho determine que existe, a longo prazo, a necessidade de trocar informações classificadas, proceder-se-á à celebração de:

- um acordo de segurança das informações, ou
- um convénio administrativo,

nos termos do artigo 12.º, n.º 2, e das secções III e IV e com base numa recomendação do Comité de Segurança.

3. Em caso de divulgação de ICUE produzidas para efeitos de uma operação PCSD a Estados terceiros ou organizações internacionais que participem na operação, e não existindo nenhum dos quadros referidos no ponto 2, o intercâmbio de ICUE com o Estado terceiro ou organização internacional contribuinte reger-se-á, nos termos da Secção V, por um dos seguintes instrumentos:

- um acordo-quadro de participação,
- um acordo de participação *ad hoc*, ou
- não existindo nenhum dos acordos acima, um convénio administrativo *ad hoc*.

4. Não existindo nenhum dos quadros referidos nos pontos 2 e 3, e caso se decida, a título excepcional, proceder à comunicação *ad hoc* de ICUE a um Estado terceiro ou organização internacional nos termos na Secção VI, ser-lhe-á pedido que garanta, por escrito, que protegerá as ICUE que lhe sejam comunicadas nos termos dos princípios básicos e das normas mínimas estabelecidos na presente decisão.

## III. ACORDOS DE SEGURANÇA DAS INFORMAÇÕES

5. Os acordos de segurança das informações estabelecerão os princípios básicos e as normas mínimas aplicáveis ao intercâmbio de informações classificadas entre a UE e os Estados terceiros e organizações internacionais.
6. Os acordos de segurança das informações deverão prever modalidades técnicas de execução a acordar entre o Gabinete de Segurança do SGC, a DSCE e a autoridade de segurança competente do Estado terceiro ou organização internacional em questão. Essas modalidades terão em conta o nível de protecção previsto nas regras, estruturas e procedimentos de segurança existentes no Estado terceiro ou organização internacional, e serão aprovadas pelo Comité de Segurança.
7. Não serão trocadas ICUE por meios electrónicos, a não ser que tal se encontre expressamente previsto no acordo de segurança das informações ou nas modalidades técnicas de execução.
8. Os acordos de segurança das informações estabelecerão que, antes de se proceder ao intercâmbio de informações classificadas ao abrigo do acordo, o Gabinete de Segurança do SGC e a DSCE determinem de comum acordo que a parte receptora está em condições de proteger e salvaguardar as informações que lhe sejam fornecidas pelas vias adequadas.
9. Quando o Conselho celebrar um acordo de segurança das informações, será designado em cada uma das partes um registo como principal ponto de entrada e saída das informações classificadas que forem trocadas.
10. A fim de avaliar a eficácia das regras, estruturas e procedimentos de segurança existentes no Estado terceiro ou organização internacional em questão, o Gabinete de Segurança do SGC efectuará visitas de avaliação, em conjunto com a DSCE e de comum acordo com o Estado terceiro ou organização internacional em questão. Essas visitas de avaliação serão conduzidas nos termos das disposições relevantes do Anexo III e deverão avaliar:

- a) O quadro regulamentar aplicável à protecção 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 susceptíveis de intercâmbio;
  - c) As medidas e os procedimentos de segurança efectivamente aplicados; e
  - d) Os procedimentos de credenciação de segurança para o nível de ICUE a comunicar.
11. As equipas que efectuarem visitas de avaliação em nome da UE verificarão se as regulamentações e procedimentos de segurança em vigor nos Estados terceiros ou organizações internacionais em questão são adequados para proteger as ICUE de um determinado nível.
  12. As conclusões das visitas serão apresentadas num relatório em que o Comité de Segurança se baseará para determinar o nível máximo das ICUE que podem ser trocadas em suporte material e, se adequado, por via electrónica com a parte terceira interessada, bem como as eventuais condições específicas aplicáveis aos intercâmbios com essa mesma parte terceira.
  13. Envidar-se-ão todos os esforços no sentido de efectuar uma visita completa de avaliação de segurança ao Estado terceiro ou organização internacional em questão antes de o Comité de Segurança aprovar as modalidades de execução, a fim de determinar a natureza e eficácia do sistema de segurança existente. Porém, quanto tal não seja possível, o Gabinete de Segurança do SGC enviará ao Comité de Segurança um relatório tão circunstanciado quanto possível, baseado nas informações de que dispõe, informando o referido Comité das regras de segurança aplicáveis e da forma como a segurança se encontra organizada no Estado terceiro ou organização internacional em questão.
  14. O Comité de Segurança pode determinar que, enquanto não forem analisados os resultados de uma visita de avaliação, não possam ser comunicadas ICUE, ou possam ser comunicadas apenas até um determinado nível de classificação, podendo ainda impor outras condições específicas à comunicação de ICUE ao Estado terceiro ou organização internacional em questão. O Gabinete de Segurança do SGC notificará em conformidade o Estado terceiro ou organização internacional em questão.
  15. De comum acordo com o Estado terceiro ou a organização internacional em questão, o Gabinete de Segurança do SGC efectuará, a intervalos regulares, novas visitas de avaliação, a fim de verificar se as medidas aplicadas continuam a respeitar as normas mínimas acordadas.
  16. Após a entrada em vigor do acordo sobre segurança das informações e o início do intercâmbio de informações classificadas com o Estado terceiro ou organização internacional em questão, o Comité de Segurança pode decidir alterar o nível máximo de ICUE que podem ser trocadas em suporte papel ou por via electrónica, nomeadamente em função dos resultados de qualquer visita de avaliação posteriormente efectuada.

#### IV. CONVÉNIOS ADMINISTRATIVOS

17. Quando exista, a longo prazo, necessidade de proceder ao intercâmbio de informações com uma classificação regra geral não superior a RESTREINT UE/EU RESTRICTED com um Estado terceiro ou organização internacional, e o Comité de Segurança tenha determinado 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, o Secretário-Geral pode, sob reserva da aprovação do Conselho, celebrar um convénio administrativo com as autoridades competentes do Estado terceiro ou organização internacional em questão.
18. Se, por razões operacionais urgentes, houver necessidade de estabelecer rapidamente um quadro regulamentar para o intercâmbio de informações classificadas, o Conselho pode decidir, a título excepcional, que seja celebrado um convénio administrativo para o intercâmbio de informações com uma classificação de nível superior.
19. Regra geral, os convénios administrativos assumirão a forma de troca de cartas.
20. Será efectuada uma visita de avaliação nos termos do ponto 10 e enviado relatório ao Comité de Segurança, que o deverá considerar satisfatório antes de se proceder à comunicação efectiva das ICUE ao Estado terceiro ou organização internacional em questão. Todavia, quando haja razões de carácter excepcional, assinaladas ao Conselho, para o intercâmbio urgente de informações classificadas, as ICUE poderão ser comunicadas, desde que tudo seja feito para que a referida visita de avaliação seja efectuada no mais breve prazo possível.
21. Não serão trocadas ICUE por meios electrónicos, a não ser que tal se encontre expressamente previsto no convénio administrativo.

## V. INTERCÂMBIO DE INFORMAÇÕES CLASSIFICADAS NO ÂMBITO DE OPERAÇÕES PCSD

22. A participação de Estados terceiros e organizações internacionais em operações PCSD rege-se por acordos-quadro de participação. Esses acordos incluirão disposições aplicáveis à comunicação de ICUE produzidas para efeitos de operações PCSD aos Estados terceiros e organizações internacionais contribuintes. O nível máximo de classificação das ICUE que podem ser trocadas deve ser RESTREINT UE/EU RESTRICTED para as operações PCSD civis e CONFIDENTIEL UE/EU CONFIDENTIAL para as operações PCSD militares, salvo disposição em contrário na decisão que estabelecer a operação PCSD em questão.
23. Os acordos de participação *ad hoc* celebrados para uma determinada operação PCSD incluirão disposições aplicáveis à comunicação de ICUE produzidas para efeitos dessa operação aos Estados terceiros ou organizações internacionais contribuintes. O nível máximo de classificação das ICUE que podem ser trocadas deve ser RESTREINT UE/EU RESTRICTED para as operações PCSD civis e CONFIDENTIEL UE/EU CONFIDENTIAL para as operações militares da PCSD militares, salvo disposição em contrário na decisão que estabelecer a operação PCSD em questão.
24. Os convénios administrativos *ad hoc* sobre a participação de um Estado terceiro ou organização internacional numa determinada operação PCSD podem abranger, nomeadamente, a comunicação de ICUE produzidas para efeitos da operação a esse Estado terceiro ou organização internacional. Esses convénios administrativos *ad hoc* serão celebrados nos termos dos pontos 17 e 18 da Secção IV. O nível máximo de classificação das ICUE que podem ser trocadas deve ser RESTREINT UE/EU RESTRICTED para as operações PCSD civis e CONFIDENTIEL UE/EU CONFIDENTIAL para as operações militares da PCSD militares, salvo disposição em contrário na decisão que estabelecer a operação PCSD em questão.
25. A execução das disposições em matéria de comunicação de ICUE no âmbito dos pontos 22, 23 e 24 não requer modalidades de aplicação nem visitas de avaliação prévias.
26. Se o Estado anfitrião em cujo território seja conduzida uma operação PCSD não tiver celebrado nenhum acordo de segurança das informações ou convénio administrativo com a UE para o intercâmbio de informações classificadas, pode ser celebrado um convénio administrativo *ad hoc*, em caso de necessidade operacional específica e imediata. Esta possibilidade deverá ser prevista na decisão que estabelecer a operação PCSD. As ICUE comunicadas nessas circunstâncias limitar-se-ão às produzidas para efeitos da operação PCSD e com classificação não superior a RESTREINT UE/EU RESTRICTED. No âmbito desse convénio administrativo *ad hoc*, o Estado anfitrião comprometer-se-á a proteger as ICUE de acordo com normas mínimas não menos rigorosas do que as estabelecidas na presente decisão.
27. As disposições em matéria de informações classificadas a prever nos acordos-quadro de participação, nos acordos de participação *ad hoc* e nos convénios administrativos *ad hoc* a que se referem os pontos 22 a 24 determinarão que o Estado terceiro ou organização internacional em questão garanta que o pessoal que destacar para a operação protegerá as ICUE nos termos das regras de segurança do Conselho e de outras directrizes emitidas pelas autoridades competentes, nomeadamente a cadeia de comando da operação.
28. Se for posteriormente celebrado um acordo de segurança das informações entre a UE e um Estado terceiro ou organização internacional contribuinte, esse acordo substitui-se a qualquer acordo-quadro de participação, acordo de participação *ad hoc* ou convénio administrativo *ad hoc* no que diz respeito ao intercâmbio e manuseamento de ICUE.
29. Não será permitido o intercâmbio de ICUE por meios electrónicos ao abrigo de acordos-quadro de participação, acordos de participação *ad hoc* ou de convénios administrativos *ad hoc* com Estados terceiros ou organizações internacionais, a não ser que tal se encontre expressamente previsto no acordo ou convénio em causa.
30. As ICUE produzidas para efeitos de uma operação PCSD podem ser divulgadas ao pessoal destacado para a operação por Estados terceiros ou organizações internacionais, nos termos dos pontos 22 a 29. Se o referido pessoal for autorizado a aceder a ICUE nas instalações ou no SCI de uma operação PCSD, devem ser aplicadas medidas (que incluam o registo das ICUE divulgadas) para atenuar o risco de perda ou comprometimento. Tais medidas serão definidas nos documentos de planeamento ou de missão pertinentes.

## VI. COMUNICAÇÃO AD HOC DE ICUE A TÍTULO EXCEPCIONAL

31. Não existindo nenhum dos quadros previstos nas Secções III a V, e constatando o Conselho, ou uma das suas instâncias preparatórias, a necessidade excepcional de comunicar ICUE a um Estado terceiro ou organização internacional, caberá ao SGC:
  - a) Na medida do possível, verificar junto das autoridades de segurança do Estado terceiro ou organização internacional em questão se as respectivas regras, estruturas e procedimentos de segurança são de molde a garantir que as ICUE que lhe sejam comunicadas serão protegidas segundo normas não menos rigorosas do que as estabelecidas na presente decisão;

- b) Solicitar ao Comité de Segurança que, com base nas informações disponíveis, formule uma recomendação sobre a confiança que pode ser depositada nas regras, estruturas e procedimentos de segurança do Estado terceiro ou organização internacional a que as ICUE deverão ser comunicadas.
32. Se o Comité de Segurança formular uma recomendação favorável à comunicação das ICUE, o assunto será remetido ao Comité de Representantes Permanentes (Coreper), que decidirá dessa comunicação.
33. Se a recomendação do Comité de Segurança for desfavorável à divulgação das ICUE:
- a) O Comité Político e de Segurança debaterá o assunto e formulará uma recomendação tendo em vista uma decisão do Coreper, se estiverem em causa matérias relacionadas com a PESC/PCSD;
- b) O Coreper debaterá o assunto e tomará decisão, se estiverem em causa quaisquer outras matérias.
34. Nos casos em que tal se considere adequado, e sob reserva do consentimento prévio da entidade de origem, expresso por escrito, o Coreper pode determinar que as informações classificadas só possam ser comunicadas parcialmente ou depois de desgraduadas ou desclassificadas, ou ainda que as informações a comunicar sejam expurgadas da referência à fonte ou ao nível inicial de classificação UE.
35. Após a decisão de comunicação das ICUE, o SGC procederá ao envio do documento em causa, que ostentará 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 efectuada, a parte terceira em questão deverá assumir o compromisso, por escrito, de proteger as ICUE que receber nos termos dos princípios básicos e das normas mínimas estabelecidos na presente decisão.
- VII. AUTORIDADE PARA A COMUNICAÇÃO DE ICUE A ESTADOS TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS
36. Se existir um dos quadros referidos no ponto 2 para o intercâmbio de informações classificadas com determinado Estado terceiro ou organização internacional, o Conselho decidirá autorizar o Secretário-Geral a comunicar as ICUE, de acordo com o princípio do consentimento da entidade de origem, a esse Estado terceiro ou organização internacional.
37. Se existir um dos quadros referidos no ponto 3 para o intercâmbio de informações classificadas com determinado Estado terceiro ou organização internacional, o Secretário-Geral será autorizado a comunicar as ICUE, nos termos da decisão que estabelece a operação PCSD e de acordo com o princípio do consentimento da entidade de origem.
38. O Secretário-Geral pode delegar essa autorização em altos funcionários do SGC ou noutras pessoas que se encontrem sob a sua autoridade.
-

*Apêndices**Apêndice A*

Definições

*Apêndice B*

Equivalência das classificações de segurança

*Apêndice C*

Lista das Autoridades Nacionais de Segurança (ANS)

*Apêndice D*Lista de abreviaturas

---

## Apêndice A

## DEFINIÇÕES

Para efeitos da presente decisão, entende-se por:

«Acreditação»: processo que conduz a uma declaração formal, emitida pela Autoridade de Acreditação de Segurança (AAS), segundo a qual um dado sistema está aprovado para funcionar com um determinado nível de classificação, num determinado modo de segurança no seu ambiente operacional e a um nível de risco aceitável, com base na premissa de que foi implementado um conjunto aprovado de medidas de segurança de carácter técnico, material, organizativo e processual;

«Activo»: tudo o que é útil para uma organização, para as suas actividades e para a continuidade destas, nomeadamente os recursos de informação que a apoiam no desempenho das suas funções;

«Ameaça»: causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer 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;

«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 de 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;

«Certificado de Credenciação de Segurança do Pessoal» (CCSP): certificado, emitido por uma autoridade competente, pelo qual se atesta que uma dada pessoa possui credenciação de segurança e é detentora de uma CSP nacional ou CSP UE, e se indica o nível de ICUE a que a pessoa pode aceder (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior), a data de validade da CSP em causa e a data de caducidade do próprio certificado;

«Ciclo de vida do SCI»: todo o período de existência do SCI, que compreende as fases da iniciativa, concepção, planeamento, análise dos requisitos, projecto, desenvolvimento, ensaio, implementação, exploração, manutenção e desactivação;

«Cláusula Adicional de Segurança» (CAS): condições contratuais especiais emitidas pela entidade adjudicante 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 ou as partes do contrato que exigem protecção de segurança;

«Contratante»: pessoa singular ou colectiva com capacidade jurídica para celebrar contratos;

«Contrato classificado»: contrato celebrado pelo SGC com um contratante para o fornecimento de bens, a execução de obras ou a prestação de serviços cuja execução exija ou implique o acesso ou a produção de ICUE;

«Credenciação de Segurança da Empresa» (CSE): certificação administrativa, emitida por uma ANS ou ASD, de que, do ponto de vista da segurança, determinada empresa está apta a garantir um nível adequado de protecção das ICUE com determinado nível de classificação de segurança e de que o seu pessoal que precise de aceder a ICUE foi sujeito ao processo de credenciação de segurança correspondente e informado dos requisitos de segurança necessários para aceder às ICUE e garantir a sua protecção;

«Credenciação de Segurança do Pessoal» (CSP): uma das seguintes, ou ambas:

— «Credenciação UE de Segurança do Pessoal» (CSP UE) para acesso a ICUE: autorização dada pela Autoridade do SGC Investida do Poder de Nomeação, tomada nos termos da presente decisão, depois de concluída uma investigação de segurança conduzida pelas autoridades competentes de um Estado-Membro, e 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, desde que tenha sido comprovada a sua «necessidade de tomar conhecimento»; diz-se da pessoa nestas condições que «possui credenciação de segurança»;

— «Credenciação nacional de Segurança do Pessoal» (CSP nacional) para acesso a ICUE: 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, e 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, desde que tenha sido comprovada a sua «necessidade de tomar conhecimento»; diz-se da pessoa nestas condições que «possui credenciação de segurança»;

«Defesa em profundidade»: aplicação de uma série de medidas de segurança organizadas em múltiplos estratos de defesa;

«Desclassificação»: eliminação de qualquer classificação de segurança;

«Desgradação»: redução do nível de classificação de segurança;

«Detentor»: pessoa devidamente autorizada com necessidade comprovada de tomar conhecimento, que está na posse de ICUE e é consequentemente responsável pela sua protecção;

«Documento»: quaisquer informações registadas, independentemente da sua forma ou características materiais;

«Entidade de origem»: instituição, agência ou organismo da UE, Estado-Membro, Estado terceiro ou organização internacional sob cuja autoridade tenham sido produzidas e/ou introduzidas nas estruturas da UE informações classificadas;

«Entidade industrial ou outra»: entidade envolvida no fornecimento de bens, execução de obras ou prestação de serviços. Pode tratar-se de uma entidade industrial, comercial, de serviços, científica, educativa, de investigação ou desenvolvimento, bem como de trabalhador por conta própria;

«Garantia da Informação» – ver artigo 10.º, n.º 1;

«Gestão das informações classificadas» – ver artigo 9.º, n.º 1;

«Guia da Classificação de Segurança» (GCS): documento que descreve as partes do programa ou contrato que são classificadas, com especificação dos níveis de classificação de segurança aplicáveis. O GCS pode ser alargado durante a vigência do programa ou contrato e as informações podem ser reclassificadas ou desgraduadas. Existindo um GCS, este fará parte integrante da CAS;

«Informações classificadas da UE» (ICUE) – ver artigo 2.º, n.º 1;

«Instruções de Segurança do Programa/Projecto» (ISP): lista de procedimentos de segurança que são aplicados a um programa ou projecto específico a fim de normalizar os procedimentos de segurança. As Instruções podem ser revistas em qualquer fase do programa ou projecto;

«Interconexão» – ver Anexo IV, ponto 31;

«Investigação de Segurança»: procedimentos de investigação conduzidos pela autoridade competente de um Estado-Membro, nos termos das respectivas disposições legislativas e regulamentares nacionais, a fim de se certificar que não há conhecimento de circunstâncias desfavoráveis que impeçam uma dada pessoa de obter uma CSP nacional ou CSP UE para acesso a ICUE até determinado nível (CONFIDENTIEL UE/EU CONFIDENTIAL ou superior);

«Manuseamento» de ICUE: todas as actividades a que as ICUE possam eventualmente ser sujeitas ao longo do seu ciclo de vida, que compreende a sua produção, tratamento, transporte, desgradação, desclassificação e destruição. Relativamente ao SCI, compreende ainda a sua recolha, visualização, transmissão e armazenamento;

«Material»: qualquer documento ou peça de maquinaria ou equipamento, já fabricado ou em fase de fabrico;

«Material criptográfico (material cripto)»: algoritmos criptográficos, módulos criptográficos de *hardware* e *software*, e produtos que incluam detalhes de implementação e documentação conexa e material de cifragem;

«Modo de funcionamento de segurança»: definição das condições em que o SCI funciona, com base na classificação das informações manuseadas e nos níveis de credenciação, aprovações formais de acesso, e necessidade de tomar conhecimento dessas informações por parte dos utilizadores do sistema. Existem quatro modos de funcionamento para manusear ou transmitir informações classificadas: modo dedicado, modo elevado, modo compartimentado e modo combinado;

— «Modo dedicado»: modo de funcionamento em que todos os indivíduos com acesso ao SCI estão credenciados para o mais alto nível de classificação das informações manuseadas no SCI e têm uma necessidade comum de tomar conhecimento de todas as informações nele manuseadas,

— «Modo elevado»: modo de funcionamento em que todos os indivíduos com acesso ao SCI estão credenciados para o mais alto nível de classificação das informações manuseadas no SCI, mas nem todos os indivíduos com acesso ao SCI têm uma necessidade comum de tomar conhecimento das informações nele manuseadas; a aprovação do acesso às informações pode ser concedida por uma só pessoa,

— «Modo compartimentado»: modo de funcionamento em que todos os indivíduos com acesso ao SCI estão credenciados para o mais alto nível de classificação das informações manuseadas no SCI, mas nem todos os indivíduos com acesso ao SCI dispõem de uma autorização formal de acesso a todas as informações nele manuseadas; a autorização formal pressupõe uma gestão formal centralizada do controlo de acesso, por oposição ao poder discricionário de concessão de acesso por parte de uma só pessoa,

— «Modo combinado»: modo de funcionamento em que nem todos os indivíduos com acesso ao SCI estão credenciados para o mais alto nível de classificação das informações manuseadas no SCI e NEM TODOS os indivíduos com acesso ao SCI têm uma necessidade comum de tomar conhecimento das informações nele manuseadas;

«Operação PCSD»: operação de gestão militar ou civil de crises conduzida ao abrigo do Capítulo 2 do Título V do TUE;

«Processo de gestão do risco de segurança»: todo o processo de identificação, controlo e minimização de acontecimentos indeterminados que possam afectar a segurança de determinada organização ou qualquer dos sistemas por ela utilizados. Este processo abarca todas as actividades relacionadas com o risco, designadamente avaliação, tratamento, aceitação e comunicação;

«Registo» – ver Anexo III, ponto 18;

«Risco»: 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 respectivos activos corpóreos ou incorpóreos. Mede-se pela combinação entre a probabilidade de as ameaças ocorrerem e o respectivo impacto.

— «Aceitação do risco»: decisão de aceitar a persistência de um risco residual após o tratamento do risco;

— «Avaliação do risco»: identificação das ameaças e vulnerabilidades e realização da análise de risco conexa, ou seja, a análise da probabilidade e do impacto;

— «Comunicação do risco»: consciencializar os grupos de utilizadores de SCI para os riscos, informar as autoridades de aprovação desses riscos e reportá-los às autoridades operacionais;

— «Tratamento do risco»: atenuação, eliminação, redução (mediante uma combinação adequada de medidas técnicas, materiais, organizativas e processuais), transferência ou monitorização do risco;

«Risco residual»: risco que permanece após terem sido aplicadas medidas de segurança, dado que não é possível neutralizar todas as ameaças nem eliminar todas as vulnerabilidades;

«Segurança do pessoal» – ver artigo 7.º, n.º 1;

«Segurança física» – ver artigo 8.º, n.º 1;

«Segurança industrial» – ver artigo 11.º, n.º 1;

«Sistema de comunicação e informação» (SCI) – ver artigo 10.º, n.º 2;

«Subcontrato classificado»: contrato celebrado entre um contratante do SGC e outro contratante (ou seja, o subcontratante) para o fornecimento de bens, a realização de obras ou a prestação de serviços cuja execução exija ou implique o acesso ou a produção de ICUE;

«TEMPEST»: investigação, estudo e controlo das emanações electromagnéticas comprometedoras e medidas destinadas à sua eliminação;

«Vulnerabilidade»: insuficiência, seja de que natureza for, que possa ser explorada 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, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional.

---

## Apêndice B

## EQUIVALÊNCIA DAS CLASSIFICAÇÕES DE SEGURANÇA

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU 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)	<i>Ver nota (1) infra</i>
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	<i>Ver nota (3) infra</i>
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	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Roména	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
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 (*)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Reino Unido	Top Secret	Secret	Confidential	Restricted

(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 marcações de classificação de segurança constantes da linha de cima são utilizadas pelas autoridades de defesa, e as marcações da linha de baixo são utilizadas por outras autoridades.

## Apêndice C

## LISTA DAS AUTORIDADES NACIONAIS DE SEGURANÇA (ANS)

<p><b>BÉLGICA</b>  Autorité nationale de sécurité  SPF Affaires étrangères, Commerce extérieur et Coopération  au Développement  15, rue des Petits Carmes  B-1000 Bruxelles</p> <p>Telefone Secretariado: + 32/2/501 45 42  Fax: + 32/2/501 45 96  E-mail: nvo-ans@diplobel.fed.be</p>	<p><b>DINAMARCA</b>  Politiets Efterretningstjeneste  (Danish Security Intelligence Service)  Klausdalsbrovej 1  DK-2860 Søborg</p> <p>Telefone: + 45/33/14 88 88  Fax: + 45/33/43 01 90</p> <p>Forsvarets Efterretningstjeneste  (Danish Defence Intelligence Service)  Kastellet 30  DK-2100 Copenhagen Ø</p> <p>Telefone: + 45/33/32 55 66  Fax: + 45/33/93 13 20</p>
<p><b>BULGÁRIA</b>  State Commission on Information Security  90 Cherkovna Str.  BG-1505 Sofia</p> <p>Telefone: + 359/2/921 5911  Fax: + 359/2/987 3750  E-mail: dksi@government.bg  Website: www.dksi.bg</p>	<p><b>ALEMANHA</b>  Bundesministerium des Innern  Referat OS III 3  Alt-Moabit 101 D  D-11014 Berlin</p> <p>Telefone: + 49/30/18 681 0  Fax: + 49/30/18 681 1441  E-mail: oesIII3@bmi.bund.de</p>
<p><b>REPÚBLICA CHECA</b>  Národní bezpečnostní úřad  (National Security Authority)  Na Popelce 2/16  CZ-150 06 Praha 56</p> <p>Telefone: + 420/257 28 33 35  Fax: + 420/257 28 31 10  E-mail: czech.nsa@nbu.cz  Website: www.nbu.cz</p>	<p><b>ESTÓNIA</b>  National Security Authority Department  Estonian Ministry of Defence  Sakala 1  EE-15094 Tallinn, Estonia</p> <p>Telefone: +372/7170 113, +372/7170 117  Fax: +372/7170 213  E-mail: nsa@kmin.ee</p>
<p><b>IRLANDA</b>  National Security Authority  Department of Foreign Affairs  76 – 78 Harcourt Street  Dublin 2 Irlanda</p> <p>Telefone: + 353/1/ 478 08 22  Fax: + 353/1/ 408 29 59</p>	<p><b>ESPAÑHA</b>  Autoridad Nacional de Seguridad  Oficina Nacional de Seguridad  Avenida Padre Huidobro s/n  E-28023 Madrid</p> <p>Telefone: + 34/91/372 50 00  Fax: + 34/91/372 58 08  E-mail: nsa-sp@areatec.com</p>
<p><b>GRÉCIA</b>  Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)  Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)  Διεύθυνση Ασφαλείας και Αντιπληροφοριών  ΣΤΓ 1020 –Χολαργός (Αθήνα)  Ελλάδα</p> <p>Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)  + 30/210/657 20 09 (ώρες γραφείου)  Φαξ: + 30/210/653 62 79  + 30/210/657 76 12</p> <p>Hellenic National Defence General Staff (HNDGS)  Military Intelligence Sectoral Directorate  Security Counterintelligence Directorate  GR-STG 1020 Holargos – Athens</p> <p>Telefone: + 30/210/657 20 45  + 30/210/657 20 09  Fax: + 30/210/653 62 79  + 30/210/657 76 12</p>	<p><b>FRANÇA</b>  Secrétariat général de la défense et de la sécurité nationale  Sous-direction Protection du secret (SGDSN/PSD)  51 Boulevard de la Tour-Maubourg  F-75700 Paris 07 SP</p> <p>Telefone: + 33/1/71 75 81 77  Fax: + 33/1/71 75 82 00</p>

<p><b>ΙΤΑΛΙΑ</b>          Presidenza del Consiglio dei Ministri          Autorità Nazionale per la Sicurezza          D.I.S. – U.C.Se.          Via di Santa Susanna, 15          I-00187 Roma</p> <p>Telefono: + 39/06/611 742 66          Fax: + 39/06/488 52 73</p>	<p><b>LETÓNIA</b>          National Security Authority          Constitution Protection Bureau of the Republic of Latvia          P.O.Box 286          LV-1001 Riga</p> <p>Telefono: + 371/6702 54 18          Fax: + 371/6702 54 54          E-mail: ndi@sab.gov.lv</p>
<p><b>CHIPRE</b>          ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ          ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ          Εθνική Αρχή Ασφάλειας (ΕΑΑ)          Υπουργείο Άμυνας          Λεωφόρος Εμμανουήλ Ροΐδη 4          1432 Λευκωσία, Κύπρος</p> <p>Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43,          + 357/22/80 77 64          Τηλεομοιότυπο: + 357/22/30 23 51</p> <p>Ministry of Defence          Minister's Military Staff          National Security Authority (NSA)          4 Emanuel Roidi street          CY-1432 Nicosia</p> <p>Telephone: + 357/22/80 75 69, + 357/22/80 76 43,          +357 /22/80 77 64          Fax: + 357/22/30 23 51          E-mail: cynsa@mod.gov.cy</p>	<p><b>LITUÂNIA</b>          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</p> <p>Telefono: + 370/5/266 32 01,          + 370/5/266 32 02          Fax: + 370/5/266 32 00          E-mail: nsa@vds.lt</p>
<p><b>LUXEMBURGO</b>          Autorité nationale de Sécurité          Boîte postale 2379          L-1023 Luxembourg</p> <p>Telefono: + 352/2478 22 10 central          + 352/2478 22 53 direct          Fax: + 352/2478 22 43</p>	<p><b>PAÍSES BAIXOS</b>          Ministerie van Binnenlandse Zaken en Koninkrijksrelaties          Postbus 20010          NL-2500 EA Den Haag</p> <p>Telefono: + 31/70/320 44 00          Fax: + 31/70/320 07 33</p>
<p><b>HUNGRIA</b>          Nemzeti Biztonsági Felügyelet          (National Security Authority)          P.O. Box 2          HU-1357 Budapest</p> <p>Telefono: + 361/346 96 52          Fax: + 361/346 96 58          E-mail: nbf@nbf.hu          Website: www.nbf.hu</p>	<p>Ministerie van Defensie          Beveiligingsautoriteit          Postbus 20701          NL-2500 ES Den Haag</p> <p>Telefono: + 31/70/318 70 60          Fax: + 31/70/318 75 22</p>
<p><b>MALTA</b>          Ministry of Justice and Home Affairs          P.O. Box 146          MT-Valetta</p> <p>Telefono: + 356/21 24 98 44          Fax: + 356/25 69 53 21</p>	<p><b>ÁUSTRIA</b>          Informationssicherheitskommission          Bundeskanzleramt          Ballhausplatz 2          A-1014 Wien</p> <p>Telefono: + 43/1/531 15 25 94          Fax: + 43/1/531 15 26 15          E-mail: ISK@bka.gv.at</p>

<p><b>POLÓNIA</b>          Agencja Bezpieczeństwa Wewnętrzznego – ABW          (Internal Security Agency)          2A Rakowiecka St.          PL-00-993 Warszawa</p> <p>Telefone: + 48/22/585 73 60          Fax: + 48/22/585 85 09          E-mail: nsa@abw.gov.pl          Website: www.abw.gov.pl</p> <p>Służba Kontrwywiadu Wojskowego          (Military Counter-Intelligence Service)          Classified Information Protection Bureau          Oczki 1          PL-02-007 Warszawa</p> <p>Telefone: + 48/22/684 12 47          Fax: + 48/22/684 10 76          E-mail: skw@skw.gov.pl</p>	<p><b>ROMÉNIA</b>          Oficiul Registrului Național al Informațiilor Secrete de Stat          (Romanian NSA – ORNISS          National Registry Office for Classified Information)          4 Mures Street          RO-012275 Bucharest</p> <p>Telefone: + 40/21/ 224 58 30          Fax: + 40/21/ 224 07 14          E-mail: nsa.romania@nsa.ro          Website: www.orniss.ro</p>
<p><b>PORTUGAL</b>          Presidência do Conselho de Ministros          Autoridade Nacional de Segurança          Rua da Junqueira, 69          P-1300-342 Lisboa</p> <p>Telefone: +351/ 213 031 710          Fax: +351/ 213 031 711</p>	<p><b>ESLOVÉNIA</b>          Urad Vlade RS za varovanje tajnih podatkov          Gregorčičeva 27          SVN-1000 Ljubljana</p> <p>Telefone: + 386/1/478 13 90          Fax: + 386/1/478 13 99</p>
<p><b>ESLOVÁQUIA</b>          Národný bezpečnostný úrad          (National Security Authority)          Budatínska 30          P.O. Box 16          SVK-850 07 Bratislava</p> <p>Telefone: + 421/2/68 69 23 14          Fax: + 421/2/63 82 40 05          Website: www.nbusr.sk</p>	<p><b>SUÉCIA</b>          Utrikesdepartementet          (Ministry for Foreign Affairs)          SSSB          S-103 39 Stockholm</p> <p>Telefone: + 46/8/405 10 00          Fax: + 46/8/723 11 76          E-mail: ud-nsa@foreign.ministry.se</p>
<p><b>FINLÂNDIA</b>          National Security Authority          Ministry for Foreign Affairs          P.O. Box 453          FI-00023 Government</p> <p>Telefone 1: + 358/9/160 56487          Telefone 2: + 358/9/160 56484          Fax: + 358/9/160 55140          E-mail: NSA@formin.fi</p>	<p><b>REINO UNIDO</b>          UK National Security Authority          Room 335, 3rd Floor          70 Whitehall          London          SW1A 2AS</p> <p>Telefone 1: + 44/20/7276 5649          Telefone 2: + 44/20/7276 5497          Fax: + 44/20/7276 5651          E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk</p>

## Apêndice D

## LISTA DE ABREVIATURAS

Acrónimo	Significado
AAC	Autoridade de Aprovação Criptográfica
AAS	Autoridade de Acreditação de Segurança
ADC	Autoridade de Distribuição Criptográfica
AGI	Autoridade de GI
ANS	Autoridade Nacional de Segurança
AQUA	Autoridade de Avaliação Habilitada
ASD	Autoridade de Segurança Designada
AT	Autoridade TEMPEST
BPS	Serviços de protecção periférica
CAS	Cláusulas Adicionais de Segurança
CCSP	Certificado de Credenciação de Segurança do Pessoal
CCTV	Televisão em circuito fechado
Conselho Conjunto	Conselho Conjunto de Acreditação de Segurança
Coreper	Comité dos Representantes Permanentes
CSE	Credenciação de Segurança de Empresa
CSP	Certificação de Segurança do Pessoal
DSCE	Direcção de Segurança da Comissão Europeia
GCS	Guia da Classificação de Segurança
GI	Garantia da informação
ICUE	Informações classificadas da UE
IDS	Sistemas de detecção de intrusos
ISP	Instruções de Segurança do Programa/Projecto
PCSD	Política Comum de Segurança e Defesa
PESC	Política Externa e de Segurança Comum
POS	Procedimentos operacionais de segurança
REUE	Representante Especial da UE
RSES	Requisito de segurança específico do sistema
SCI	Sistemas de comunicação e de informação em que sejam manuseadas ICUE
SGC	Secretariado-Geral do Conselho
TI	Tecnologias da informação