►**B**

DECISÃO DA COMISSÃO

de 29 de Novembro de 2001

que altera o seu Regulamento Interno

[notificada com o número C(2001) 3031]

(2001/844/CE, CECA, Euratom)

(JO L 317 de 3.12.2001, p. 1)

Alterada por:

		Jornal Oficial		
		n.º	página	data
►**M1**	Decisão da Comissão 2005/94/CE, Euratom, de 3 de Fevereiro de 2005	L 31	66	4.2.2005
►**M2**	Decisão da Comissão 2006/70/CE, Euratom, de 31 de Janeiro de 2006	L 34	32	7.2.2006
►**M3**	Decisão da Comissão 2006/548/CE, Euratom, de 2 de Agosto de 2006	L 215	38	5.8.2006

▼B

DECISÃO DA COMISSÃO

de 29 de Novembro de 2001

que altera o seu Regulamento Interno

[notificada com o número C(2001) 3031]

(2001/844/CE, CECA, Euratom)

A COMISSÃO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Europeia, e, nomeadamente, o n.º 2 do seu artigo 218.º,

Tendo em conta o Tratado que institui a Comunidade Europeia do Carvão e do Aço, e, nomeadamente, o seu artigo 16.º,

Tendo em conta o Tratado que institui a Comunidade Europeia da Energia Atómica, e, nomeadamente, o seu artigo 131.º,

Tendo em conta o Tratado da União Europeia, e, nomeadamente, o n.º 1 do seu artigo 28.º e o n.º 1 do seu artigo 41.º,

DECIDE:

Artigo 1.º

As disposições da Comissão em matéria de segurança, cujo texto consta do anexo da presente decisão, são aditadas, como anexo, ao Regulamento Interno da Comissão.

Artigo 2.º

A presente decisão entra em vigor no dia da sua publicação no *Jornal Oficial das Comunidades Europeias*.

A presente decisão é aplicável a partir de1 de Dezembro de 2001.

▼B

ANEXO

DISPOSIÇÕES DA COMISSÃO EM MATÉRIA DE SEGURANÇA

Considerando o seguinte:

(1) A fim de desenvolver as actividades da Comissão em áreas que exigem confidencialidade, é necessário estabelecer um regime geral de segurança aplicável à Comissão, às outras instituições, instâncias, gabinetes e agências estabelecidos por força ou com base no Tratado CE, aos Estados-Membros e a qualquer outro destinatário de informações classificadas da União Europeia, a seguir denominadas «informações classificadas da UE».

(2) A fim de salvaguardar a eficácia do regime de segurança assim estabelecido, a Comissão limitará a comunicação de informações classificadas da UE exclusivamente aos organismos externos que ofereçam garantias de que tomaram todas as medidas necessárias para a aplicação de regras estritamente equivalentes às das presentes disposições.

(3) As presentes disposições são adoptadas sem prejuízo do Regulamento n.º 3, de 31 de Julho de 1958, que aplica o artigo 24.º do Tratado que institui a Comunidade Europeia da Energia Atómica ([1]), do Regulamento (Euratom, CEE) n.º 1588/90 do Conselho, de 11 de Junho de 1990, relativo à transmissão de informações abrangidas pelo segredo estatístico ao Serviço de Estatística das Comunidades Europeias ([2]), e da Decisão C (95) 1510 final da Comissão, de 23 de Novembro de 1995, relativa à protecção dos sistemas de informação.

(4) Com vista a assegurar o bom funcionamento do processo de tomada de decisões a nível da União, o regime de segurança da Comissão baseia-se nos princípios enunciados na Decisão 2001/264/CE do Conselho, de 19 de Março de 2001, que aprova as regras de segurança do Conselho ([3]).

(5) A Comissão sublinha a importância de associar, se for caso disso, as outras instituições às regras e normas de confidencialidade necessárias para proteger os interesses da União e dos seus Estados-Membros.

(6) A Comissão reconhece a necessidade de criar o seu próprio conceito de segurança, tendo em conta todos os elementos relativos à segurança e o carácter específico da Comissão enquanto instituição.

(7) As presentes disposições são adoptadas sem prejuízo do artigo 255.º do Tratado e do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão ([4]).

▼M2

(8) Estas disposições são aplicáveis sem prejuízo do artigo 286.º do Tratado CE e do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados;

▼B

Artigo 1.º

As regras de segurança da Comissão constam do anexo.

Artigo 2.º

1. O Membro da Comissão responsável pelas questões de segurança toma as medidas adequadas para assegurar que, no tratamento das informações classificadas da UE, as regras a que se refere o artigo 1.º sejam cumpridas pelos funcionários e outros agentes da Comissão e pelo pessoal destacado na Comissão, no interior da Comissão e em todas as suas instalações, incluindo as suas representações e gabinetes na União e as suas delegações em países terceiros, e igualmente pelos prestadores de serviços externos à Comissão.

▼M3

Sempre que um contrato ou convenção de subvenção entre a Comissão e um prestador externo de serviços ou beneficiário envolva o tratamento de informações classificadas da UE nas instalações do prestador de serviços ou do beneficiário, as medidas adequadas a tomar pelo referido prestador de serviços ou beneficiário para assegurar o cumprimento das regras a que se refere o artigo 1.º no tratamento das informações classificadas da UE farão parte integrante do contrato ou convenção de subvenção.

([1]) JO n.º 17 de 6.10.1958, p. 406/58.
([2]) JO L 151 de 15.6.1990, p. 1.
([3]) JO L 101 de 11.4.2001, p. 1.
([4]) JO L 145 de 31.5.2001, p. 43.

▼B

2. Os Estados-Membros e as outras instituições, instâncias, gabinetes e agências estabelecidos por força ou com base nos Tratados podem receber informações classificadas da UE desde que velem por que, no tratamento de tais informações, sejam aplicadas, nos seus serviços e instalações, regras estritamente equivalentes às referidas no artigo 1.º, nomeadamente por:

a) Membros das representações permanentes dos Estados-Membros junto da União Europeia, bem como pelos membros das delegações nacionais que participem em reuniões da Comissão ou das suas instâncias ou que participem noutras actividades da Comissão;

b) Outros membros das administrações nacionais dos Estados-Membros que tratem informações classificadas da UE, quer exerçam a sua actividade no território dos Estados-Membros quer no estrangeiro;

c) Prestadores externos de serviços e pessoal destacado que tratem informações classificadas da UE.

Artigo 3.º

Os países terceiros, as organizações internacionais e outras instâncias podem receber informações classificadas da UE desde que velem por que, no tratamento de tais informações, sejam aplicadas regras estritamente equivalentes às referidas no artigo 1.º

Artigo 4.º

Em conformidade com os princípios básicos e normas mínimas de segurança que constam da parte I do anexo, o Membro da Comissão responsável pelas questões de segurança pode tomar medidas nos termos da parte II do anexo.

Artigo 5.º

A partir da data em que for aplicável, a presente decisão substitui:

a) A Decisão C(94) 3282 da Comissão, de 30 de Novembro de 1994, relativa às medidas de segurança aplicáveis às informações classificadas elaboradas ou trocadas no âmbito das actividades da União Europeia;

b) A Decisão C(99) 423 da Comissão, de 25 de Fevereiro de 1999, relativa às modalidades segundo as quais os funcionários e agentes da Comissão Europeia podem ser autorizados a aceder a informações classificadas na posse da Comissão.

Artigo 6.º

A partir da data de aplicação das presentes disposições, todas as informações classificadas mantidas pela Comissão até essa data, com excepção das informações classificadas da Euratom:

a) Se tiverem sido criadas pela Comissão, serão automaticamente consideradas reclassificadas «►**M1** RESTREINT UE ◄», a não ser que os seus autores decidam atribuir-lhes outra classificação até 31 de Janeiro de 2002. Neste caso, os autores informarão todos os destinatários dos documentos em causa;

b) Se tiverem sido criadas por autores exteriores à Comissão, conservarão a sua classificação original e, em consequência, serão tratadas como informações classificadas da UE de nível equivalente, a não ser que os seus autores concordem com a desclassificação ou desgraduação das informações.

▼B

ANEXO

REGRAS DE SEGURANÇA

Índice

▼B

16. CLASSIFICAÇÕES, DESIGNADORES DE SEGURANÇA E MARCAÇÕES

16.1. **Níveis de classificação**

16.2. **Designadores de segurança**

16.3. **Marcações**

16.4. **Aposição da classificação**

16.5. **Aposição de designadores de segurança**

17. GESTÃO DAS CLASSIFICAÇÕES

17.1. **Disposições gerais**

17.2. **Aplicação das classificações**

17.3. **Desgraduação e desclassificação**

18. SEGURANÇA FÍSICA

18.1. **Disposições gerais**

18.2. **Requisitos de segurança**

18.3. **Medidas de segurança física**

18.3.1. *Áreas de segurança*

18.3.2. *Áreas administrativas*

18.3.3. *Controlo das entradas e saídas*

18.3.4. *Rondas*

18.3.5. *Contentores de segurança e casas-fortes*

18.3.6. *Fechaduras*

18.3.7. *Controlo das chaves e dos segredos das fechaduras*

18.3.8. *Dispositivos de detecção de intrusão*

18.3.9. *Equipamento acreditado*

18.3.10. *Protecção física das fotocopiadoras e das telecopiadoras*

18.4. **Protecção contra visão e escuta não-autorizadas**

18.4.1. *Visão não-autorizada*

18.4.2. *Escuta não-autorizada*

18.4.3. *Introdução de equipamento electrónico e de registo*

18.5. **Áreas tecnicamente seguras**

19. REGRAS GERAIS SOBRE O PRINCÍPIO DA NECESSIDADE DE TOMAR CONHECIMENTO E A HABILITAÇÃO EM MATÉRIA DE SEGURANÇA DO PESSOAL DA UNIÃO EUROPEIA

19.1. **Disposições gerais**

19.2. **Regras específicas de acesso a informações com a classificação TRES SECRET UE/EU TOP SECRET**

19.3. **Regras específicas de acesso a informações com a classificação SECRET UE e CONFIDENTIEL UE**

19.4. **Regras específicas de acesso a informações com a classificação RESTREINT UE**

19.5. **Transferências**

▼B

19.6. **Instruções especiais**

20. PROCEDIMENTO DE HABILITAÇÃO EM MATÉRIA DE SEGURANÇA DOS FUNCIONÁRIOS E OUTROS AGENTES DA COMISSÃO

21. ELABORAÇÃO, DISTRIBUIÇÃO, TRANSMISSÃO, HABILITAÇÃO EM MATÉRIA DE SEGURANÇA DO PESSOAL DE TRANSPORTE, CÓPIAS, TRADUÇÕES E EXTRACTOS DE DOCUMENTOS CLASSIFICADOS DA UNIÃO EUROPEIA

21.1. **Elaboração**

21.2. **Distribuição**

21.3. **Transmissão de documentos classificados da União Europeia**

21.3.1. *Embalagem e recibos*

21.3.2. *Transmissão no interior de um edifício ou de um grupo de edifícios*

21.3.3. *Transmissão no interior de um país*

21.3.4. *Transmissão de um Estado para outro*

21.3.5. *Transmissão de documentos com a classificação RESTREINT UE*

21.4. **Habilitação em matéria de segurança do pessoal de transporte**

21.5. **Transmissão electrónica ou por outros meios técnicos**

21.6. **Cópias, traduções e extractos de documentos classificados da União Europeia**

22. REGISTOS, INVENTÁRIOS, VERIFICAÇÕES, ARQUIVAGEM E DESTRUIÇÃO DE INFORMAÇÕES CLASSIFICADAS DA UNIÃO EUROPEIA

22.1. **Registos locais de informações classificados da UE**

22.2. **Registo TRES SECRET UE/EU TOP SECRET**

22.2.1. *Disposições gerais*

22.2.2. *Registo TRES SECRET UE/EU TOP SECRET central*

22.2.3. *Sub-registos TRES SECRET UE/EU TOP SECRET*

22.3. **Inventários e verificações de documentos classificados da União Europeia**

22.4. **Arquivagem de informações classificadas da UE**

22.5. **Destruição de documentos classificados da UE**

22.6. **Destruição em casos de emergência**

23. MEDIDAS DE SEGURANÇA A APLICAR POR OCASIÃO DE REUNIÕES ESPECÍFICAS REALIZADAS FORA DAS INSTALAÇÕES DA COMISSÃO E QUE ENVOLVAM INFORMAÇÃO CLASSIFICADA DA UE

23.1. **Disposições gerais**

23.2. **Responsabilidades**

23.2.1. ▶ **M2** *Direcção de Segurança da Comissão* ◀

23.2.2. *Responsável da Segurança da reunião (MSO)*

23.3 **Medidas de segurança**

23.3.1. *Áreas de segurança*

23.3.2. *Passes*

23.3.3. *Controlo do equipamento fotográfico e de som*

▼B

▼B

▼B

PARTE I: PRINCÍPIOS DE BASE E NORMAS MÍNIMAS DE SEGURANÇA

1. INTRODUÇÃO

As presentes disposições estabelecem os princípios de base e as normas mínimas de segurança que deverão ser respeitadas pela Comissão em todos os seus locais de trabalho e por todos os destinatários de informações classificadas da UE, de modo que a segurança seja salvaguardada e possa ser garantida a existência de uma norma comum de protecção.

2. PRINCÍPIOS GERAIS

A política de segurança da Comissão é parte integrante da sua política geral de gestão interna e baseia-se, portanto, nos princípios que regem a sua política geral.

Esses princípios compreendem a legalidade, a transparência, a responsabilidade e a subsidiariedade (proporcionalidade).

Entende-se por legalidade a necessidade de que a execução das funções de segurança se mantenha estritamente no quadro jurídico, bem como do respeito das exigências legais. Significa, igualmente, que as responsabilidades em matéria de segurança devem assentar em disposições jurídicas apropriadas. Aplicam-se na íntegra as disposições do estatuto dos funcionários, nomeadamente o seu artigo 17.º, sobre a obrigação de discrição em relação às informações da Comissão, e o seu título VI, sobre as medidas disciplinares. Por fim, significa que as quebras de segurança nos domínios de responsabilidade da Comissão devem ser tratadas em conformidade com a política da Comissão em matéria de acções disciplinares e a sua política de cooperação com os Estados-Membros no domínio da justiça penal.

Entende-se por transparência a necessidade de clareza em todas as regras e disposições de segurança, de um equilíbrio entre os diferentes serviços e domínios (segurança física e protecção das informações) e de uma política coerente e estruturada de sensibilização para as questões de segurança. Implica, igualmente, a necessidade de dispor de directrizes escritas claras para a aplicação das medidas de segurança.

Entende-se por responsabilidade a necessidade, não apenas de uma definição clara das responsabilidades no domínio da segurança, mas também de uma verificação regular da correcta execução das mesmas.

Entende-se por subsidiariedade, ou proporcionalidade, que a segurança deve ser organizada ao nível mais baixo possível e tão próximo quanto possível das direcções-gerais e serviços da Comissão. O conceito implica, igualmente, que as actividades de segurança se devem limitar aos elementos que, de facto, se justifiquem. Finalmente, significa que as medidas de segurança devem ser proporcionais aos interesses a proteger e às ameaças reais ou potenciais a esses interesses, para que a protecção exercida cause um mínimo de perturbação.

3. BASES DA SEGURANÇA

As bases da boa segurança são:

a) No interior de cada Estado-Membro, uma organização nacional de segurança responsável:

   1. pela recolha e registo de informações sobre espionagem, sabotagem, terrorismo e outras actividades subversivas e

   2. por informar e aconselhar o Governo respectivo e, através dele, a Comissão, sobre a natureza das ameaças à segurança e os meios de protecção contra essas ameaças;

b) No interior de cada Estado-Membro, e no interior da Comissão, uma autoridade técnica INFOSEC, que deverá trabalhar com a autoridade de segurança pertinente a fim de informar e aconselhar sobre ameaças técnicas à segurança e os meios de protecção contra essas ameaças;

c) Uma colaboração regular entre ministérios e os serviços competentes das instituições europeias, a fim de estabelecer e recomendar, consoante o caso:

   1. as pessoas, informações e recursos que deverão ser protegidos e

   2. as normas comuns de protecção;

d) Uma cooperação estreita entre a►**M2** Direcção de Segurança da Comissão ◄ e os serviços de segurança das outras instituições europeias e com o Serviço de Segurança da NATO (NOS).

▼B

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

4.1. **Objectivos**

A segurança da informação tem os seguintes objectivos principais:

a) Salvaguardar as informações classificadas da UE dos riscos de espionagem, fuga ou divulgação não-autorizada;

b) Salvaguardar as informações da União Europeia tratadas em sistemas e redes de comunicações das ameaças à sua confidencialidade, integridade e disponibilidade;

c) Salvaguardar as instalações da Comissão onde existam informações da União Europeia dos riscos de sabotagem ou de dano intencional;

d) Em caso de falha, avaliar os danos causados, limitar as suas consequências e adoptar as medidas correctivas necessárias.

4.2. **Definições**

Nas presentes regras, entende-se por:

a) «Informações classificadas da UE», qualquer informação ou material cuja divulgação não-autorizada possa causar vários graus de prejuízo aos interesses da União Europeia, ou a um ou mais dos seus Estados-Membros, quer essa informação provenha da União Europeia ou de Estados-Membros, Estados terceiros ou organizações internacionais.

b) «Documento», qualquer carta, nota, minuta, relatório, memorando, sinal/ /mensagem, esboço, fotografia, diapositivo, filme, mapa, tabela, plano, bloco de notas, stencil, papel químico, máquina de escrever ou fita impressora, fita magnética, cassete, disco de computador, CD-ROM ou outro meio fisico no qual tenha sido registada informação.

c) «Material», «documento» tal como definido na alínea b), bem como qualquer peça de equipamento, já fabricada ou em vias de o ser.

d) «Necessidade de tomar conhecimento», a necessidade de uma determinada pessoa ter acesso a informações classificadas da UE para a execução de uma função ou tarefa.

e) «Autorização», uma decisão do ►M2 director da Direcção de Segurança da Comissão ◄ de conceder acesso individual a informações classificadas da UE até um determinado nível, com base no resultado positivo de um inquérito de segurança efectuado por uma autoridade nacional de segurança em conformidade com o direito nacional.

f) «Classificação», a atribuição de um nível apropriado de segurança a informação cuja divulgação não-autorizada possa prejudicar em determinado grau os interesses da Comissão ou dos seus Estados-Membros.

g) «Desgraduação», uma redução do nível de classificação.

h) «Desclassificação», a eliminação de qualquer nível de classificação.

i) «Entidade de origem», o autor, devidamente autorizado, de um documento classificado. Na Comissão, incumbe aos chefes dos serviços autorizar os seus subordinados a produzir informações classificadas da UE.

j) «Serviços da Comissão», as unidades e outros serviços da Comissão, incluindo os Gabinetes, em todos os locais de trabalho, incluindo o Centro Comum de Investigação, as Representações e Gabinetes na União e as Delegações em países terceiros.

4.3. **Classificação**

a) No que respeita à confidencialidade, é necessário cuidado e experiência na selecção das informações e materiais que deverão ser protegidos e na avaliação do grau de protecção que os mesmos requerem. É fundamental que o grau de protecção corresponda à importância securitária de cada elemento de informação ou peça de material a proteger. A fim de assegurar o bom fluxo da informação, deverão ser tomadas medidas para evitar sobreclassificações e subclassificações.

b) O sistema de classificação constitui o instrumento para pôr em prática estes princípios; deve ser utilizado um sistema semelhante de classificação no planeamento e organização da luta contra a espionagem, a sabotagem, o terrorismo e outras ameaças, de forma a dar o maior grau de protecção às instalações mais importantes onde existam informações classificadas e aos pontos mais sensíveis no interior dessas instalações.

c) A responsabilidade pela classificação das informações incumbe exclusivamente à entidade de origem.

d) O nível de classificação basear-se-á apenas no conteúdo da informação em causa.

▼B

e) Quando forem reunidos vários elementos de informação, o nível de classificação a aplicar ao conjunto será pelo menos idêntico à classificação mais elevada entre os elementos em causa. A um conjunto de informações pode, porém, ser atribuída uma classificação mais elevada dos que a das suas partes constituintes.

f) As classificações serão atribuídas e mantidas apenas quando e durante o período necessário.

4.4. **Objectivos das medidas de segurança**

As medidas de segurança devem:

a) Abranger todas as pessoas que tenham acesso a informações classificadas, os suportes das informações classificadas, os locais onde se encontrem essas informações e as instalações importantes.

b) Ser concebidas para detectar as pessoas cuja localização possa pôr em perigo a segurança de informações classificadas e de instalações importantes onde se encontrem informações classificadas e proceder à sua exclusão ou afastamento.

c) Impedir qualquer pessoa não-autorizada de aceder a informações classificadas ou a instalações que as contenham.

d) Assegurar que as informações classificadas apenas sejam difundidas às pessoas que delas necessitem de tomar conhecimento, princípio fundamental em todos os aspectos da segurança.

e) Assegurar a integridade (ou seja, impedir a deterioração, a alteração não-autorizada ou a eliminação não-autorizada) e a disponibilidade (ou seja, assegurar que o acesso não seja negado às pessoas com necessidade e autorização de acesso) de todas as informações, tanto classificadas como não-classificadas, especialmente das informações armazenadas, tratadas ou transmitidas de forma electromagnética.

5. ORGANIZAÇÃO DA SEGURANÇA

5.1. **Normas mínimas comuns**

A Comissão deve assegurar que todos os destinatários de informações classificadas da UE, no interior da instituição ou sob a sua competência (por exemplo, os seus serviços e os prestadores de serviços à Comissão), cumpram normas mínimas comuns de segurança, de forma que as informações classificadas da UE possam ser transmitidas com a certeza de que serão tratadas com iguais precauções. Essas normas mínimas devem incluir critérios para a habilitação do pessoal em matéria de segurança e procedimentos para a protecção das informações classificadas da UE.

A Comissão só autorizará o acesso de entidades externas a informações classificadas da UE se as mesmas garantirem que, ao lidarem com essas informações, serão respeitadas disposições pelo menos estritamente equivalentes às referidas normas mínimas.

▼M3

Essas normas mínimas serão também aplicáveis sempre que a Comissão confie, por contrato ou convenção de subvenção, a entidades industriais ou outras, tarefas que envolvam, impliquem e/ou contenham informações classificadas UE: essas normas mínimas comuns constam da secção 27 da parte II.

▼B

5.2. **Organização**

No interior da Comissão, a segurança encontra-se organizada a dois níveis:

a) Ao nível da Comissão no seu todo, existe a►M2 Direcção de Segurança da Comissão ◄, que integra uma Autoridade de acreditação de segurança (SAA) — que também desempenha as funções de Autoridade cripto (CrA) e de Autoridade TEMPEST — e uma autoridade INFOSEC (IA) e um ou mais registos centrais de informações classificadas da UE, cada um deles com um ou mais Responsáveis do controlo do registo (RCO).

b) Ao nível dos serviços da Comissão, a segurança está entregue a um ou mais Responsáveis locais de segurança (LSO), a um ou mais Responsáveis centrais da segurança informática (CISO) e responsáveis locais da segurança informática (LISO) e a Registos locais de informações classificadas da UE, com um ou mais Responsáveis do controlo do registo.

c) Os órgãos de segurança centrais dirigem operacionalmente os órgãos de segurança locais.

▼B

6. SEGURANÇA DO PESSOAL

6.1. **Habilitação do pessoal em matéria de segurança**

Todas as pessoas que necessitem de ter acesso a informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior deverão ser adequadamente habilitadas a fazê-lo antes de o acesso ser autorizado. Será exigida uma habilitação de segurança semelhante no caso das pessoas cujas funções envolvam a operacionalidade ou a manutenção técnicas de sistemas de comunicações ou informáticos que contenham informações classificadas. Essa habilitação de segurança deverá ser concebida de forma a determinar se os indivíduos em questão:

a) São de lealdade inquestionável;

b) Possuam um carácter e uma discrição que não deixem dúvidas quanto à sua integridade ao lidarem com informações classificadas; ou

c) Podem ser vulneráveis a pressões de origem estrangeira ou outras.

No procedimento de habilitação será dada especial atenção às pessoas:

d) A quem for dado acesso a informações com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄;

e) Que ocupem posições que impliquem o acesso regular a um volume considerável de informações com a classificação ►**M1** SECRET UE ◄;

f) Cujas funções lhes dêem acesso especial a sistemas de comunicações ou informáticos protegidos e, por conseguinte, a oportunidade de obter acesso não-autorizado a grandes quantidades de informações classificadas da UE ou de prejudicar seriamente a missão da mesma através de actos de sabotagem técnica.

Nas circunstâncias referidas nas alíneas d), e) e f), deverão ser utilizadas ao máximo as possibilidades práticas da técnica de investigação de antecedentes.

As pessoas sem uma necessidade válida de tomar conhecimento de informações classificadas da UE que desempenhem funções nas quais possam ter acesso a esse tipo de informações (mensageiros, agentes de segurança, pessoal de manutenção e de limpeza, etc.) deverão ser previamente objecto de uma habilitação adequada em matéria de segurança.

6.2. **Registos do pessoal habilitado em matéria de segurança**

Todos os serviços da Comissão que lidem com informações classificadas da UE ou nos quais existam sistemas de comunicações ou informáticos protegidos deverão manter um registo do seu pessoal ao qual tiver sido concedida uma habilitação em matéria de segurança. Todas as habilitações deverão ser oportunamente verificadas, para determinar a sua adequação às funções actuais da pessoa em questão; serão reexaminadas com carácter prioritário sempre que houver novas informações que indiquem que a continuação do trabalho, da pessoa em questão, com informações classificadas deixou de ser compatível com os interesses da segurança. O responsável local de segurança do serviço da Comissão manterá um registo das habilitações concedidas no seu domínio.

6.3. **Formação do pessoal em matéria de segurança**

Todo o pessoal ocupado em funções nas quais possa ter acesso a informações classificadas receberá uma formação completa ao assumir funções, e a intervalos regulares, sobre as necessidades de segurança e os meios de a conseguir. Esse pessoal atestará por escrito ter lido e compreendido totalmente as presentes disposições de segurança.

6.4. **Responsabilidades dos gestores**

Os gestores deverão saber quais os membros do seu pessoal que trabalham com informações classificadas ou que têm acesso a sistemas de comunicações ou informáticos protegidos e deverão registar e relatar todos os incidentes e vulnerabilidades aparentes, susceptíveis de afectar a segurança.

6.5. **Estatuto de segurança do pessoal**

Serão definidos procedimentos para garantir que, ao ter-se conhecimento de informações desfavoráveis relativamente a uma pessoa, se possa saber se trabalha com informações classificadas ou tem acesso a sistemas de comunicações ou informáticos protegidos, e que seja informado a►**M2** Direcção de Segurança da Comissão ◄. Se se determinar que essa pessoa constitui um risco para a segurança, deverá ser afastada ou proibida de desempenhar funções em que possa pôr em perigo a segurança.

▼B

7. SEGURANÇA FÍSICA

7.1. **Necessidade de protecção**

O grau das medidas de segurança física a aplicar para assegurar a protecção das informações classificadas da UE deverá ser proporcional à classificação, ao volume e às ameaças para as informações e material existentes. Todos os detentores de informações classificadas da UE deverão seguir práticas uniformes em matéria de classificação dessas informações e respeitar normas comuns de protecção em matéria de armazenagem, transmissão e eliminação de informações e material que necessitem de ser protegidos.

7.2. **Controlo de instalações**

Antes de abandonarem locais onde existam informações classificadas da UE, as pessoas responsáveis pela guarda das mesmas devem assegurar que essas informações se encontram guardadas em condições de segurança e que todos os dispositivos de segurança foram activados (fechaduras, alarmes, etc.). Deverão ser efectuadas acções de controlo independentes após as horas de serviço.

7.3. **Segurança de edifícios**

Deve ser impedido o acesso não-autorizado aos edifícios onde existam informações classificadas da UE ou sistemas de comunicações ou informáticos protegidos. A natureza da protecção concedida às informações classificadas da UE, por exemplo janelas com grades, fechaduras nas portas, guardas nas entradas, sistemas automatizados de controlo de acesso, controlo e rondas de segurança, sistemas de alarme, sistemas de detecção de intrusão e cães de guarda, dependerá:

a) Da classificação, volume e localização no interior do edifício das informações e material a proteger;

b) Da qualidade dos contentores de segurança dessas informações e material; e

c) Da natureza física e localização do edifício.

A natureza da protecção conferida a sistemas de comunicações e informáticos deverá igualmente depender de uma avaliação do que for necessário proteger e dos danos potenciais em caso de falha de segurança, da natureza física e localização do edifício em que o sistema se encontrar e da localização do sistema no interior do edifício.

7.4. **Planos de emergência**

Deverão existir planos pormenorizados para a protecção das informações classificadas em caso de emergências locais ou nacionais.

8. SEGURANÇA DA INFORMAÇÃO

A segurança da informação (INFOSEC) diz respeito à identificação e aplicação de medidas de segurança destinadas a proteger as informações classificadas da UE, tratadas, armazenadas ou transmitidas através de sistemas de comunicações ou informáticos ou de outros sistemas electrónicos, contra perdas de confidencialidade, integridade ou disponibilidade, quer acidental, quer intencional. Deverão ser tomadas contramedidas adequadas para impedir o acesso a informações classificadas da UE a pessoas não-autorizadas, a recusa de acesso a pessoas autorizadas e a deterioração ou a alteração ou eliminação não-autorizadas desse tipo de informações.

9. MEDIDAS DE LUTA CONTRA A SABOTAGEM E CONTRA OUTRAS FORMAS DE DANOS INTENCIONAIS

As precauções físicas de protecção das instalações importantes onde existam informações classificadas constituem a melhor salvaguarda contra a sabotagem e outras formas de danos intencionais, não constituindo a habilitação do pessoal em matéria de segurança, por si só, uma alternativa eficaz. A instância nacional competente deverá facultar informações relativas às acções de espionagem, sabotagem e terrorismo e outras actividades subversivas.

10. DIVULGAÇÃO DE INFORMAÇÕES CLASSIFICADAS A PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

A decisão de divulgar informações classificadas da UE provenientes da Comissão a um país terceiro ou a uma organização internacional será tomada pelo colégio dos membros da Comissão. Se a origem das informações que se pretendam divulgar não for a Comissão, esta deverá obter o consentimento prévio da entidade de origem para a divulgação das mesmas. Se não for possível identificar a entidade de origem, a Comissão assumirá a responsabilidade em seu lugar.

▼B

Se a Comissão receber informações classificadas de países terceiros, organizações internacionais ou outros terceiros, essas informações beneficiarão de protecção adequada à sua classificação, equivalente às normas definidas nas presentes disposições para as informações classificadas da UE ou a normas mais estritas eventualmente solicitadas pelo terceiro que divulgar as informações. Podem ser previstas acções de controlo mútuas.

Os princípios acima enunciados serão postos em prática em conformidade com as normas de execução constantes da secção 26 da parte II e dos apêndices 3, 4 e 5.

PARTE II: ORGANIZAÇÃO DA SEGURANÇA NA COMISSÃO

11. MEMBRO DA COMISSÃO RESPONSÁVEL PELAS QUESTÕES DE SEGURANÇA

O membro da Comissão responsável pelas questões de segurança:

a) Executa a política de segurança da Comissão;

b) Estuda os problemas de segurança que lhe forem submetidos pela Comissão ou pelas instâncias competentes desta;

c) Analisa as questões que envolvam alterações da política de segurança da Comissão, em estreita ligação com as autoridades nacionais de segurança (ou outras autoridades competentes) dos Estados-Membros (adiante designadas por «NSA»).

Compete, nomeadamente, ao membro da Comissão responsável pelas questões de segurança:

a) Coordenar todos os aspectos da segurança relacionados com as actividades da Comissão;

b) Dirigir às autoridades designadas dos Estados-Membros pedidos para que as NSA procedam à habilitação em matéria de segurança do pessoal da Comissão, nos termos da secção 20;

c) Investigar ou mandar investigar qualquer fuga de informações classificadas da UE que pareça ter ocorrido na Comissão;

d) Solicitar às autoridades de segurança competentes que iniciem investigações quando se afigurar ter havido fuga, da Comissão, de informações classificadas da UE e coordenar as investigações quando se encontrar envolvida mais do que uma autoridade de segurança;

e) Examinar periodicamente as disposições de segurança para a protecção das informações classificadas da UE;

f) Manter uma ligação estreita com todas as autoridades de segurança competentes, tendo em vista uma coordenação global da segurança;

g) Manter em constante revisão a política e os procedimentos de segurança da Comissão e, se necessário, elaborar as recomendações adequadas. Nesse sentido, apresentará à Comissão o plano anual de inspecção elaborado pela►**M2** Direcção de Segurança da Comissão ◄.

12. GRUPO CONSULTIVO DA POLÍTICA DE SEGURANÇA DA COMISSÃO

Será criado um Grupo consultivo da política de segurança da Comissão. O grupo será constituído pelo membro da Comissão responsável pelas questões de segurança, que presidirá, ou por um seu delegado, e por representantes da NSA de cada Estado-Membro. Podem ser convidados representantes de outras instituições europeias. Quando forem tratadas questões que lhes digam respeito, também podem ser convidados a participar nas reuniões representantes das entidades descentralizadas da União Europeia.

O Grupo consultivo da política de segurança da Comissão reunir-se-á a pedido do seu presidente ou de qualquer dos seus membros. Competirá ao grupo analisar e avaliar todas as questões de segurança pertinentes e, se necessário, apresentar recomendações à Comissão.

▼M2

13. COMITÉ DE SEGURANÇA DA COMISSÃO

É criado um Comité de Segurança da Comissão. O Comité é constituído pelo director-geral do pessoal e da administração, que exerce a presidência, por um membro do Gabinete do Membro da Comissão responsável pelas questões de segurança, por um membro do Gabinete do Presidente, pelo secretário-geral adjunto que preside ao Grupo de Gestão de Crises da Comissão, pelos directores-gerais responsáveis pelo Serviço Jurídico, pelas Relações Externas, pela Justiça, Liberdade e Segurança, pelo Centro Comum de Investigação, pela Informática e

▼**M2**

pelo Serviço de Auditoria Interna e director da direcção de segurança da Comissão ou pelos respectivos representantes. Podem ser convidados outros funcionários da Comissão. Compete ao Comité avaliar as medidas de segurança no interior da Comissão e formular recomendações nesse domínio ao membro da Comissão responsável pelas questões de segurança.

▼**B**

14. ►**M2** DIRECÇÃO DE SEGURANÇA DA COMISSÃO ◄

Para dar cumprimento às incumbências referidas na secção 11, o membro da Comissão responsável pelas questões de segurança terá à sua disposição a►**M2** Direcção de Segurança da Comissão ◄, para a coordenação, supervisão e implementação das medidas de segurança.

O ►**M2** director da Direcção de Segurança da Comissão ◄ será o principal conselheiro do membro da Comissão responsável pelas questões de segurança e desempenhará as funções de secretário do Grupo consultivo da política de segurança. Nesse sentido, dirigirá a actualização das regras de segurança e coordenará as medidas de segurança com as autoridades competentes dos Estados-Membros e, se necessário, com organizações internacionais ligadas à Comissão por acordos de segurança. Para o efeito, agirá como elemento de ligação.

Incumbe ao ►**M2** director da Direcção de Segurança da Comissão ◄ a acreditação das redes e sistemas informáticos da Comissão. O ►**M2** director da Direcção de Segurança da Comissão ◄ decidirá, em acordo com a NSA pertinente, da acreditação de redes e sistemas informáticos que envolvam, por um lado, a Comissão e, por outro, qualquer outro destinatário de informações classificadas da UE.

15. INSPECÇÕES DE SEGURANÇA

A►**M2** Direcção de Segurança da Comissão ◄ efectuará inspecções periódicas das disposições de segurança para a protecção das informações classificadas da UE.

A►**M2** Direcção de Segurança da Comissão ◄ poderá ser assistido nessa tarefa pelos serviços de segurança de outras instituições da União Europeia em que existam informações classificadas da UE ou pelas autoridades nacionais de segurança dos Estados-Membros ([1]).

A pedido de um Estado-Membro, a sua NSA pode inspeccionar informações classificadas da UE no interior da Comissão, conjuntamente com a►**M2** Direcção de Segurança da Comissão ◄ e em acordo mútuo com este.

16. CLASSIFICAÇÕES, DESIGNADORES DE SEGURANÇA E MARCAÇÕES

16.1. **Níveis de classificação** ([2])

As informações serão classificadas nos seguintes níveis (ver também o apêndice 2):

►**M1** TRES SECRET UE/EU TOP SECRET ◄: esta classificação apenas se aplica a informações e material cuja divulgação não-autorizada possa prejudicar de forma excepcionalmente grave os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros.

►**M1** SECRET UE ◄: esta classificação apenas se aplica a informações e material cuja divulgação não-autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros.

►**M1** CONFIDENTIEL UE ◄: esta classificação apenas se aplica a informações e material cuja divulgação não-autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros.

►**M1** RESTREINT UE ◄: esta classificação apenas se aplica a informações e material cuja divulgação não-autorizada possa ser desvantajosa para os interesses da União Europeia ou de um ou vários dos seus Estados-Membros.

Não é permitida qualquer outra classificação.

([1]) Sem prejuízo da Convenção de Viena sobre Relações Diplomáticas, de 1961, e do Protocolo relativo aos Privilégios e Imunidades das Comunidades Europeias, de 8 de Abril de 1965.

([2]) Consta do apêndice 1 um quadro comparativo das classificações de segurança da UE, da NATO, da UEO e dos Estados-Membros.

▼B

16.2. **Designadores de segurança**

Para limitar no tempo a validade de uma classificação (significando a desgraduação ou desclassificação automática das informações classificadas) pode ser utilizado um designador de segurança acordado. Esse designador será «ATÉ … (hora/data)» ou «ATÉ …(ocorrência)».

Serão aplicados designadores de segurança adicionais, tais como CIFRADO ou qualquer outro designador de segurança reconhecido a nível da União Europeia, sempre que forem necessários uma distribuição limitada e um tratamento especial, além do indicado pela classificação de segurança.

Os designadores de segurança só podem ser utilizados associados a uma classificação.

16.3. **Marcações**

Poderá ser aposta uma marcação para indicar o domínio abrangido pelo documento, uma distribuição específica com base no princípio da «necessidade de tomar conhecimento» ou (no caso de informações não-classificadas) para indicar o final de uma proibição.

As marcações não constituem uma classificação e não podem ser utilizadas como alternativas a esta.

A marcação PESD será aposta nos documentos e cópias dos mesmos que digam respeito à segurança e defesa da União Europeia ou de um ou vários dos seus Estados-Membros ou à gestão militar ou civil de crises.

16.4. **Aposição da classificação**

A classificação será aposta do seguinte modo:

a) Nos documentos com a classificação ►**M1** RESTREINT UE ◄, por meios mecânicos ou electrónicos;

b) Nos documentos com a classificação ►**M1** CONFIDENTIEL UE ◄, por meios mecânicos ou manualmente, ou por impressão em papel pré-carimbado, consignado num registo;

c) Nos documentos com a classificação ►**M1** SECRET UE ◄ e ►**M1** TRES SECRET UE/EU TOP SECRET ◄, por meios mecânicos ou manualmente.

16.5. **Aposição de designadores de segurança**

Os designadores de segurança serão apostos imediatamente abaixo da classificação, por meios idênticos aos utilizados na aposição desta última.

17. GESTÃO DAS CLASSIFICAÇÕES

17.1. **Disposições gerais**

As informações apenas serão classificadas em caso de necessidade. A classificação será indicada de forma clara e correcta e apenas será mantida enquanto as informações necessitarem de protecção.

A responsabilidade pela classificação de informações ou por qualquer desgraduação ou desclassificação subsequentes incumbe exclusivamente à entidade de origem.

Os funcionários e outros agentes da Comissão só poderão proceder à classificação, desgraduação ou desclassificação de informações mediante instruções do seu superior hierárquico, ou com o acordo deste.

A concepção dos procedimentos pormenorizados para o tratamento de documentos classificados deve garantir que estes estejam sujeitos a uma protecção adequada às informações que contenham.

O número de pessoas autorizadas a produzir documentos com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄ será o mais reduzido possível e os nomes das mesmas constarão de uma lista elaborada pela►**M2** Direcção de Segurança da Comissão ◄.

17.2. **Aplicação das classificações**

A classificação de um documento será determinada pelo nível de sensibilidade do seu conteúdo, em conformidade com o definido na secção 16. É importante que a classificação seja utilizada de forma correcta e comedida. Esta última disposição aplica-se, especialmente, à classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄.

A entidade de origem de um documento a classificar deverá ter em mente as regras atrás indicadas e abster-se de proceder a qualquer sobreclassificação ou subclassificação.

▼B

Consta do apêndice 2 um guia prático da classificação.

Cada uma das páginas, parágrafos, secções, anexos, apêndices, adendas e elementos juntos de um determinado documento pode exigir classificações diferentes, devendo ser classificada em conformidade. A classificação do documento no seu todo deverá ser a da sua parte com a classificação mais elevada.

A classificação de uma carta ou nota de envio de elementos juntos será a classificação mais elevada dos elementos juntos. A entidade de origem indicará claramente em que nível essa carta ou nota deverá ser classificada quando separada dos elementos juntos que acompanha.

O Regulamento (CE) n.º 1049/2001 continua a reger o acesso público.

17.3. **Desgraduação e desclassificação**

Os documentos classificados da União Europeia só podem ser desgraduados ou desclassificados com a autorização da entidade de origem e, se necessário, após discussão com as outras partes interessadas. A desgraduação ou desclassificação serão confirmadas por escrito. A entidade de origem terá a responsabilidade de informar os seus destinatários da alteração, sendo estes, por seu turno, responsáveis por informar dessa alteração quaisquer destinatários subsequentes a quem tenham enviado o documento ou facultado uma cópia do mesmo.

Se possível, as entidades de origem especificarão nos documentos classificados a data, período ou ocorrência após a qual ou o qual o conteúdo do mesmo pode ser objecto de uma desgraduação ou desclassificação. Caso contrário, deverão passar em revista os documentos de cinco em cinco anos, no máximo, a fim de verificar se é necessário manter a classificação original.

18. SEGURANÇA FÍSICA

18.1. **Disposições gerais**

Os principais objectivos das medidas de segurança física consistem em impedir o acesso de pessoas não-autorizadas a informações e/ou material classificados da União Europeia, o roubo ou degradação de equipamentos e outros bens e o assédio ou qualquer outro tipo de agressão aos funcionários, outros agentes e a visitantes.

18.2. **Requisitos de segurança**

Todas as instalações, áreas, edifícios, compartimentos, sistemas de comunicações e informáticos, etc. onde estiverem armazenados e/ou se lidar com informações e material classificados da União Europeia deverão ser protegidos por medidas adequadas de segurança física.

Ao decidir o grau de segurança física necessário, deverão ser tomados em consideração todos os factores pertinentes, tais como:

a) A classificação das informações e/ou do material;

b) A quantidade e a forma (por exemplo cópias em papel, suportes digitais) das informações em questão;

c) A avaliação local da ameaça constituída por serviços de espionagem que tenham como alvo a União Europeia, os Estados-Membros e/ou outras instituições ou terceiros detentores de informações classificadas da UE, em virtude de actos de sabotagem, de terrorismo ou de outras actividades subversivas e/ /ou criminosas.

As medidas de segurança física aplicadas deverão ser concebidas por forma a:

a) Impedir a entrada sub-reptícia ou forçada de intrusos;

b) Dissuadir, impedir e detectar acções por parte de pessoal desleal;

c) Impedir o acesso a informações classificadas da UE a pessoas que não necessitem de tomar conhecimento das mesmas.

18.3. **Medidas de segurança física**

18.3.1. *Áreas de segurança*

As áreas onde forem tratadas e armazenadas informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior serão organizadas e estruturadas de modo a corresponderem a uma das seguintes categorias:

a) Área de segurança de classe I: uma área onde as informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior são tratadas e armazenadas de tal modo que a entrada nessa área constitui, para todos os efeitos práticos, acesso a informações classificadas. Essa área deverá ter:

   i) um perímetro claramente definido e protegido, com controlo de todas as entradas e saídas,

▼B

ii) um sistema de controlo de entradas que admita apenas as pessoas devidamente habilitadas e especialmente autorizadas a entrar nessa área,

iii) uma indicação da classificação das informações normalmente existentes nessa área, ou seja, às quais a entrada dá acesso.

b) Área de segurança de classe II: uma área onde as informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior são tratadas e armazenadas de tal modo que podem ser protegidas contra o acesso por pessoas não-autorizadas através de meios de controlo estabelecidos internamente, por exemplo, instalações onde se situem serviços nos quais sejam regularmente tratadas ou armazenadas informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior. Essa área deverá ter:

i) um perímetro claramente definido e protegido, com controlo de todas as entradas e saídas,

ii) um sistema de controlo de entradas que admita sem escolta apenas as pessoas devidamente habilitadas e especialmente autorizadas a entrar nessa área. Para todas as outras pessoas, deverão ser previstas escoltas ou um sistema de controlo equivalente que impeça o acesso não-autorizado a informações classificadas da UE e a entrada sem controlo nas áreas sujeitas a inspecções técnicas de segurança.

As áreas não ocupadas por pessoal em serviço 24 horas por dia deverão ser inspeccionadas imediatamente após as horas normais de serviço, para verificar se as informações classificadas da UE estão devidamente protegidas.

18.3.2. *Áreas administrativas*

Poderão ser estabelecidas áreas administrativas de menor segurança adjacentes ou envolventes das áreas de segurança de classe I ou II. Essas áreas administrativas deverão ter um perímetro visivelmente definido, que permita o controlo de pessoal e veículos. Nessas áreas administrativas só poderão ser tratadas e armazenadas informações com a classificação ►**M1** RESTREINT UE ◄ ou não-classificadas.

18.3.3. *Controlo das entradas e saídas*

As entradas e saídas nas e das áreas de segurança de classe I e II deverão ser controladas através de um sistema de passes ou de reconhecimento de pessoas aplicável a todo o pessoal que normalmente nelas trabalhar. Deverá também ser criado um sistema de controlo dos visitantes concebido para impedir o acesso não-autorizado a informações classificadas da UE. Os sistemas de passes poderão basear-se numa identificação automatizada, que deverá ser considerada um complemento, mas não um substituto total, do pessoal de vigilância. Qualquer alteração do nível de ameaça poderá implicar um reforço das medidas de controlo das entradas e saídas, por exemplo durante a visita de altas personalidades.

18.3.4. *Rondas*

Fora das horas normais de serviço, as áreas de segurança de classe I e II devem ser patrulhadas, com o objectivo de proteger os bens da União Europeia contra fugas, danos ou perdas. A frequência das rondas será determinada pelas circunstâncias locais, mas, de um modo geral, deverão ter lugar de duas em duas horas.

18.3.5. *Contentores de segurança e casas-fortes*

Serão utilizados três tipos de contentores para guardar as informações classificadas da UE:

— classe A: contentores acreditados a nível nacional para guardar informações com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄ nas áreas de segurança de classe I ou II;

— classe B: contentores acreditados a nível nacional para guardar informações com a classificação ►**M1** SECRET UE ◄ e ►**M1** CONFIDENTIEL UE ◄ nas áreas de segurança de classe I ou II,

— classe C: mobiliário de escritório adequado para guardar apenas informações com a classificação ►**M1** RESTREINT UE ◄.

As paredes, chãos, tectos, portas e fechaduras das casas-fortes construídas nas áreas de segurança de classe I ou II, e de todas as áreas de segurança de classe I onde forem guardadas em prateleiras abertas ou apresentadas em quadros, mapas, etc. informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior, deverão ser certificados por uma NSA como garantidoras de um grau de protecção equivalente à classe do contentor de segurança acreditado para guarda de informações com a mesma classificação.

18.3.6. *Fechaduras*

As fechaduras utilizadas nos contentores de segurança e nas casas-fortes em que forem guardadas informações classificadas da UE deverão cumprir as seguintes normas:

▼B

— grupo A: acreditadas a nível nacional para contentores da classe A,

— grupo B: acreditadas a nível nacional para contentores da classe B,

— grupo C: apenas adequadas para mobiliário de escritório da classe C.

18.3.7. *Controlo das chaves e dos segredos das fechaduras*

As chaves dos contentores de segurança não deverão ser levadas para fora dos edifícios da Comissão. As combinações dos contentores de segurança deverão ser memorizadas pelas pessoas que precisarem de as conhecer. Para utilização em casos de emergência, o responsável local de segurança do serviço da Comissão em questão deverá possuir duplicados das chaves e um registo escrito de cada combinação; estes últimos serão guardados em envelopes separados, opacos e fechados. As chaves habituais, os duplicados das chaves e as combinações deverão ser mantidos em contentores de segurança distintos. Essas chaves e combinações deverão ser objecto de uma protecção de segurança pelo menos equivalente à do material ao qual derem acesso.

As combinações dos contentores de segurança apenas deverão ser conhecidas pelo número mais restrito possível de pessoas. As combinações deverão ser mudadas:

a) Sempre que for recebido um novo contentor;

b) Sempre que houver uma mudança de pessoal;

c) Sempre que tiver ocorrido ou houver suspeita de ter ocorrido uma fuga;

d) De preferência de seis em seis meses, ou, pelo menos, uma vez em cada período de 12 meses.

18.3.8. *Dispositivos de detecção de intrusão*

Quando forem utilizados sistemas de alarme, circuitos fechados de televisão ou outros dispositivos eléctricos para proteger informações classificadas da UE, deverá existir uma fonte de energia eléctrica de emergência capaz de garantir o funcionamento contínuo do sistema em caso de interrupção do fornecimento de energia eléctrica principal. Outro requisito básico é o de que um mau funcionamento ou qualquer intervenção não-autorizada nesses sistemas ponha em funcionamento um alarme ou outro dispositivo de alerta fiável que advirta o pessoal de vigilância.

18.3.9. *Equipamento acreditado*

A►**M2** Direcção de Segurança da Comissão ◄ deverá manter listas actualizadas, por tipo e modelo, do equipamento de segurança que tiver acreditado para a protecção de informações classificadas nas várias circunstâncias e condições específicas. A►**M2** Direcção de Segurança da Comissão ◄ tomará por base dessas listas, nomeadamente, as informações prestadas pelas NSA.

18.3.10. *Protecção física das fotocopiadoras e das telecopiadoras*

As fotocopiadoras e as telecopiadoras deverão ser fisicamente protegidas de modo a garantir que só serão utilizadas com informações classificadas por pessoas autorizadas a fazê-lo e que todos os produtos classificados das mesmas estejam sujeitos a um controlo adequado.

18.4. **Protecção contra visão e escuta não-autorizadas**

18.4.1. *Visão não-autorizada*

Deverão ser tomadas todas as medidas, tanto de dia como de noite, para assegurar que as informações classificadas da UE não sejam vistas, mesmo acidentalmente, por qualquer pessoa não-autorizada.

18.4.2. *Escuta não-autorizada*

Sempre que o risco o justificar, os serviços e as áreas em que forem regularmente discutidas informações com a classificação ►**M1** SECRET UE ◄ ou superior deverão ser protegidos contra actos passivos e activos de escuta não-autorizada. A avaliação do risco desses actos será da responsabilidade da►**M2** Direcção de Segurança da Comissão ◄, após consulta, se necessário, das NSA.

18.4.3. *Introdução de equipamento electrónico e de registo*

Não é permitida a introdução de telemóveis, computadores privados, equipamentos de registo, máquinas fotográficas ou de filmar ou outros equipamentos electrónicos ou de registo em áreas de segurança ou áreas tecnicamente seguras sem autorização prévia do ►**M2** director da Direcção de Segurança da Comissão ◄.

Para definir as medidas de protecção que deverão ser tomadas nas instalações sensíveis às escutas passiva (por exemplo, isolamento de paredes, portas, chãos e tectos, medição dos níveis sonoros emitidos) e activa (por exemplo, busca de microfones), a►**M2** Direcção de Segurança da Comissão ◄ poderá pedir a assistência de peritos das NSA.

▼B

Do mesmo modo, sempre que as circunstâncias o exigirem, o equipamento de telecomunicações e o equipamento de escritório eléctrico ou electrónico de qualquer tipo utilizado durante as reuniões de nível ►M1 SECRET UE ◄ ou superior poderão ser verificados por especialistas técnicos de segurança das NSA, a pedido do ►M2 director da Direcção de Segurança da Comissão ◄.

18.5. **Áreas tecnicamente seguras**

Certas áreas poderão ser designadas como áreas tecnicamente seguras. Será feito um controlo especial das entradas nessas áreas, que deverão estar fechadas por um método acreditado quando não estiverem ocupadas, devendo as chaves ser tratadas como chaves de segurança. Essas áreas deverão ser sujeitas a inspecções físicas regulares, que também serão feitas depois de qualquer entrada não-autorizada ou suspeita dessa ocorrência.

Será mantido um inventário pormenorizado do equipamento e mobiliário, a fim de controlar os movimentos dos mesmos. Não será introduzida numa área com tais características nenhuma peça de mobiliário ou de equipamento que não tenha sido objecto de uma inspecção cuidadosa por pessoal de segurança especialmente treinado, com o objectivo de detectar quaisquer dispositivos de escuta. Como regra geral, não será permitida a instalação de linhas de comunicações em áreas tecnicamente seguras sem autorização prévia da autoridade competente.

19. REGRAS GERAIS SOBRE O PRINCÍPIO DA NECESSIDADE DE TOMAR CONHECIMENTO E A HABILITAÇÃO EM MATÉRIA DE SEGURANÇA DO PESSOAL DA UNIÃO EUROPEIA

19.1. **Disposições gerais**

O acesso a informações classificadas da UE só será autorizado às pessoas que delas necessitem de tomar conhecimento para o desempenho das suas funções ou tarefas. O acesso a informações com a classificação ►M1 TRES SECRET UE/ /EU TOP SECRET ◄, ►M1 SECRET UE ◄ e ►M1 CONFIDENTIEL UE ◄ só será autorizado a pessoas que tenham a habilitação adequada em matéria de segurança.

A responsabilidade por determinar a «necessidade de tomar conhecimento» incumbirá ao serviço no qual a pessoa em questão deva trabalhar.

A solicitação da habilitação do pessoal será da responsabilidade de cada serviço.

A habilitação em matéria de segurança dará lugar à emissão de um «certificado de segurança do pessoal da União Europeia», que indicará o nível de informações classificadas ao qual a pessoa habilitada poderá ter acesso e a data de expiração do mesmo.

O certificado de segurança do pessoal da União Europeia para uma dada classificação poderá conferir ao seu detentor acesso a informações com classificação inferior.

As pessoas que não sejam funcionários, nem outros agentes, por exemplo prestadores de serviços, peritos ou consultores externos, com quem seja necessário discutir ou a quem seja necessário dar conhecimento de informações classificadas da UE devem possuir uma habilitação em matéria de segurança do pessoal da União Europeia para efeitos de informações classificadas da UE e ser informados das suas responsabilidades nesse domínio.

O Regulamento (CE) n.º 1049/2001 continua a reger o acesso público.

19.2. **Regras específicas de acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄**

Todas as pessoas que devam ter acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ deverão ser previamente sujeitas a um inquérito de segurança com vista ao acesso a essas informações.

Todas as pessoas que devam ter acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ deverão ser designadas pelo membro da Comissão responsável pelas questões de segurança e os seus nomes serão mantidos no registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ adequado. Incumbirá à►M2 Direcção de Segurança da Comissão ◄ criar e manter esse registo.

Antes de terem acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄, todas as pessoas devem assinar uma declaração de que tomaram conhecimento dos procedimentos de segurança da Comissão e reconhecem inteiramente a sua especial responsabilidade pela salvaguarda de informações classificadas ►M1 TRES SECRET UE/EU TOP SECRET ◄, conhecendo as consequências previstas na regulamentação da União Europeia e na legislação ou regulamentação administrativa nacionais no caso de informações classificadas serem facultadas a pessoas não-autorizadas, quer intencionalmente, quer por negligência.

▼B

No caso das pessoas que tiverem acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ em reuniões, etc., o responsável do controlo competente do serviço ou entidade em que a pessoa trabalhar deverá notificar a instância responsável pela reunião de que as pessoas em questão estão autorizadas a fazê-lo.

Os nomes de todas as pessoas que deixarem de desempenhar tarefas que exijam acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ deverão ser removidos da lista ►M1 TRES SECRET UE/EU TOP SECRET ◄. Além disso, deverá ser chamada a atenção de todas essas pessoas para a sua especial responsabilidade pela salvaguarda das informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄. Devem, igualmente, assinar uma declaração de que não utilizarão, nem divulgarão, quaisquer informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ que possam estar em seu poder.

19.3. **Regras específicas de acesso a informações com a classificação ►M1 SECRET UE ◄ e ►M1 CONFIDENTIEL UE ◄**

Todas as pessoas que devam ter acesso a informações com a classificação ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄ deverão ser previamente sujeitas a um inquérito de segurança ao nível adequado.

Todas as pessoas que devam ter acesso a informações com a classificação ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄ deverão ter conhecimento das disposições de segurança adequadas e estar conscientes das consequências de uma eventual negligência.

No caso das pessoas que tiverem acesso a informações com a classificação ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄ em reuniões, etc., o responsável de segurança da entidade em que a pessoa trabalhar deverá notificar a instância responsável pela reunião de que as pessoas em questão estão autorizadas a fazê-lo.

19.4. **Regras específicas de acesso a informações com a classificação ►M1 RESTREINT UE ◄**

Às pessoas com acesso a informações com a classificação ►M1 RESTREINT UE ◄ deve ser dado conhecimento das presentes regras de segurança e das consequências de eventuais actos de negligência.

19.5. **Transferências**

Quando um membro do pessoal for transferido de um lugar que envolva o tratamento de material classificado da União Europeia, o registo deverá supervisionar a transferência adequada desse material, do funcionário que partir para o funcionário que o substituir.

Quando um membro do pessoal for transferido para outro lugar que envolva o tratamento de material classificado da União Europeia, o responsável local de segurança transmitir-lhe-á as instruções adequadas.

19.6. **Instruções especiais**

As pessoas que tenham de lidar com informações classificadas da UE devem, ao assumir as suas funções, e posteriormente de forma periódica, ser informadas:

a) Dos perigos para a segurança decorrentes de conversas indiscretas;

b) Das precauções a tomar nas suas relações com a imprensa e com representantes de grupos de interesses;

c) Da ameaça que as actividades dos serviços de espionagem que têm por alvo a União Europeia e os Estados-Membros representam para as informações classificadas e as actividades da União Europeia;

d) Da obrigação de relatar imediatamente às autoridades de segurança competentes qualquer abordagem ou manobra que dê lugar a suspeitas de uma actividade de espionagem ou quaisquer circunstâncias pouco usuais em matéria de segurança.

Todas as pessoas que normalmente estejam expostas a contactos frequentes com representantes de países cujos serviços de espionagem visem as informações classificadas e as actividades da União Europeia e dos seus Estados-Membros devem ser informadas das técnicas habitualmente empregues pelos vários serviços de espionagem.

Não existem disposições de segurança da Comissão em matéria de viagens de carácter privado para qualquer destino por parte do pessoal habilitado a aceder a informações classificadas da UE. Todavia, a►M2 Direcção de Segurança da Comissão ◄ dará a conhecer aos funcionários e outros agentes sob a sua responsabilidade as regras de viagem a que possam estar sujeitos.

▼B

20. PROCEDIMENTO DE HABILITAÇÃO EM MATÉRIA DE SEGURANÇA DOS FUNCIONÁRIOS E OUTROS AGENTES DA COMISSÃO

a) Só terão acesso a informações classificadas na posse da Comissão os funcionários e outros agentes da Comissão, ou pessoas que trabalhem na Comissão, que, devido às suas funções e em conformidade com as necessidades do serviço, necessitarem de tomar conhecimento ou de utilizar tais informações.

b) Para terem acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ e ►M1 CONFIDENTIEL UE ◄, as pessoas referidas na alínea a) devem ser autorizadas nos termos das alíneas c) e d).

c) A autorização apenas será concedida a pessoas que tiverem sido objecto de um inquérito de segurança pelas autoridades nacionais competentes dos Estados-Membros (NSA) nos termos das alíneas i) a n).

d) A concessão das autorizações referidas nas alíneas a), b) e c) competirá ao ►M2 director da Direcção de Segurança da Comissão ◄.

e) Esse responsável concederá a autorização após ter obtido o parecer das autoridades nacionais competentes dos Estados-Membros no âmbito do inquérito de segurança efectuado nos termos das alíneas i) a n).

f) A►M2 Direcção de Segurança da Comissão ◄ manterá uma lista actualizada de todos os lugares sensíveis, indicados pelos serviços pertinentes da Comissão, e de todas as pessoas a quem tiver sido concedida uma autorização (eventualmente temporária).

g) A autorização, que será válida por um período de cinco anos, não poderá exceder a duração das tarefas com base nas quais for concedida. Poderá ser renovada nos termos da alínea e).

h) A autorização será retirada pelo ►M2 director da Direcção de Segurança da Comissão ◄ sempre que este considerar que existem motivos fundamentados para o fazer. Qualquer decisão de retirar uma autorização deverá ser notificada à pessoa em questão, que poderá pedir para ser ouvida pelo ►M2 director da Direcção de Segurança da Comissão ◄, e à autoridade nacional competente.

i) O inquérito de segurança será efectuado com a assistência da pessoa interessada e a pedido do ►M2 director da Direcção de Segurança da Comissão ◄. A autoridade nacional competente na matéria será a do Estado-Membro cuja nacionalidade a pessoa em questão tiver. Se a pessoa não tiver a nacionalidade de um dos Estados-Membros, o ►M2 director da Direcção de Segurança da Comissão ◄ solicitará a realização do inquérito de segurança ao Estado-Membro da União Europeia no qual a mesma tiver o seu domicílio ou residir habitualmente.

j) No âmbito do inquérito de segurança, a pessoa em questão deverá preencher um formulário de informação pessoal.

k) O ►M2 director da Direcção de Segurança da Comissão ◄ deverá especificar no seu pedido o tipo e o nível de informações classificadas a que a pessoa em questão terá acesso, para que as autoridades nacionais competentes possam proceder ao inquérito de segurança e dar o seu parecer quanto ao nível de autorização que será adequado conferir a essa pessoa.

l) Todo o processo de inquérito de segurança, bem como os resultados obtidos, estarão sujeitos às regras e regulamentos pertinentes em vigor no Estado-Membro em questão, incluindo em matéria de recurso.

m) Se as autoridades nacionais competentes do Estado-Membro derem parecer positivo, o ►M2 director da Direcção de Segurança da Comissão ◄ poderá conceder a autorização à pessoa em questão.

n) O parecer negativo das autoridades nacionais competentes será notificado à pessoa, que poderá pedir para ser ouvida pelo ►M2 director da Direcção de Segurança da Comissão ◄. Caso o considere necessário, este poderá pedir às autoridades nacionais competentes qualquer esclarecimento adicional que as mesmas possam fornecer. Se o parecer negativo for confirmado, a autorização não será concedida.

o) Todas as pessoas a quem for concedida uma autorização na acepção das alíneas d) e e) deverão, no momento em que lhes for concedida a autorização e, posteriormente, a intervalos regulares, receber as instruções necessárias sobre a protecção de informações classificadas e os meios de assegurar essa protecção. Essas pessoas deverão assinar uma declaração de que confirmam ter recebido tais instruções e se comprometem a respeitá-las.

p) O ►M2 director da Direcção de Segurança da Comissão ◄ deverá tomar todas as medidas necessárias para pôr em prática a presente secção, em especial no que diz respeito às regras de acesso à lista das pessoas autorizadas.

q) Excepcionalmente, e por necessidades de serviço, o ►M2 director da Direcção de Segurança da Comissão ◄ poderá conceder uma autorização temporária por um período não superior a seis meses, sujeita aos resultados

▼B

do inquérito de segurança referido na alínea i), depois de ter notificado as autoridades nacionais competentes e na condição de não ter obtido resposta destas no prazo de um mês.

r) As autorizações provisórias e temporárias assim concedidas não darão acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄; esse acesso será limitado aos funcionários que tiverem sido habilitados com base num inquérito de segurança nos termos da alínea i). Na pendência dos resultados do inquérito, os funcionários para quem tiver sido pedida habilitação ao nível ►M1 TRES SECRET UE/EU TOP SECRET ◄ poderão ser autorizados, de forma temporária e provisória, a ter acesso a informações classificadas até ao nível ►M1 SECRET UE ◄, inclusive.

21. ELABORAÇÃO, DISTRIBUIÇÃO, TRANSMISSÃO, HABILITAÇÃO EM MATÉRIA DE SEGURANÇA DO PESSOAL DE TRANSPORTE, CÓPIAS, TRADUÇÕES E EXTRACTOS DE DOCUMENTOS CLASSIFICADOS DA UNIÃO EUROPEIA

21.1. **Elaboração**

1. As classificações UE serão aplicadas conforme o estabelecido na secção 16; no caso do nível ►M1 CONFIDENTIEL UE ◄ ou superior, deverão ser apostas no topo e no fundo de cada página, centradas, devendo ainda todas as páginas ser numeradas. Todos os documentos classificados da União Europeia deverão ostentar um número de referência e uma data. No caso dos documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ e ►M1 SECRET UE ◄, esse número de referência deverá figurar em cada página. Caso devam ser distribuídos em vários exemplares, cada um destes deverá ostentar um número de cópia, que deverá ser aposto na primeira página juntamente com a indicação do número total de páginas. Os documentos com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior deverão ostentar na primeira página uma enumeração de todos os anexos ou elementos juntos que os acompanharem.

2. Os documentos com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior só poderão ser dactilografados, traduzidos, armazenados, fotocopiados, reproduzidos magneticamente ou microfilmados por pessoas que estiverem habilitadas a ter acesso a informações classificadas da UE pelo menos até ao nível de classificação de segurança do documento em questão.

3. As disposições relativas à produção informática de documentos classificados constam da secção 25.

21.2. **Distribuição**

1. As informações classificadas da UE só serão distribuídas às pessoas que delas necessitarem de tomar conhecimento e que possuírem uma habilitação em matéria de segurança adequada. A entidade de origem indicará a distribuição inicial.

2. Os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ serão distribuídos através de registos ►M1 TRES SECRET UE/ /EU TOP SECRET ◄ (ver a secção 22.2). No caso das mensagens com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄, o registo competente poderá autorizar o chefe do Centro de Comunicações a produzir o número de cópias indicado na lista de destinatários.

3. Os documentos com a classificação ►M1 SECRET UE ◄ ou inferior poderão ser redistribuídos pelo destinatário inicial a outros destinatários, com base no princípio da «necessidade de tomar conhecimento». As entidades de origem deverão, todavia, indicar claramente quaisquer advertências que desejem impor. Sempre que tais advertências sejam impostas, os destinatários só podem redistribuir os documentos com a autorização da entidade de origem.

4. Todos os documentos com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior deverão, ao entrar ou sair de uma direcção-geral ou serviço, ser averbados no registo local de informações classificadas da UE. As indicações a registar (referências, data e, se for caso disso, o número da cópia) deverão permitir identificar os documentos e ser averbadas num livro de registo ou num meio informático especialmente protegido (ver a secção 22.1).

21.3. **Transmissão de documentos classificados da União Europeia**

21.3.1. *Embalagem e recibos*

1. Os documentos com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior deverão ser transmitidos em envelopes duplos, resistentes e opacos. O envelope interior deverá ostentar a classificação de segurança da União Europeia adequada, bem como, se possível, indicações pormenorizadas quanto às funções e endereço do destinatário.

▼B

2. O envelope interior só poderá ser aberto por um responsável de controlo do registo (ver a secção 22.1), ou seu substituto, que deverá acusar a recepção dos documentos nele contidos, excepto se o envelope for endereçado a uma pessoa concreta. Nesse caso, a chegada do envelope deverá ser averbada no registo adequado (ver a secção 22.1) e somente a pessoa a quem for endereçado poderá abrir o envelope interior e acusar a recepção dos documentos nele contidos.

3. O envelope interior conterá um formulário de aviso de recepção. O aviso de recepção, que não será classificado, deverá ostentar o número de referência, a data e o número de cópia do documento, mas nunca o assunto do mesmo.

4. O envelope interior deverá ser inserido num envelope exterior, que ostentará um número de expedição para efeitos de recepção. A classificação de segurança nunca deverá ser aposta no envelope exterior, seja em que circunstâncias for.

5. No caso de documentos com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior, os mensageiros ou estafetas deverão obter recibos da entrega, dos quais deverão constar os números de expedição respectivos.

21.3.2. *Transmissão no interior de um edifício ou de um grupo de edifícios*

No interior de um dado edifício ou grupo de edifícios, os documentos classificados poderão ser transportados num envelope selado que ostente apenas o nome do destinatário, desde que esse envelope seja transportado por uma pessoa com habilitação em matéria de segurança do mesmo nível que os documentos.

21.3.3. *Transmissão no interior de um país*

1. No interior de um país, os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ apenas deverão ser enviados através de um serviço oficial de estafetas ou transportados por pessoas habilitadas a ter acesso a informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Sempre que for utilizado um serviço de estafetas para a transmissão de um documento com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ fora do perímetro de um edifício ou grupo de edifícios, será necessário respeitar as disposições em matéria de expedição e recepção constantes do presente capítulo. Os serviços de entrega deverão ser estruturados de molde a assegurar que as embalagens que contiverem documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ estejam permanentemente sob controlo directo de um funcionário responsável.

3. Excepcionalmente, os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ podem ser transportados por funcionários, que não estafetas, fora do perímetro de um edifício ou grupo de edifícios para uso local em reuniões e discussões, desde que:

   a) O portador esteja habilitado para o acesso a esses documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄;

   b) O modo de transporte satisfaça as regras em matéria de transmissão de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄;

   c) O funcionário não deixe, em nenhuma circunstância, os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ sem guarda;

   d) Sejam tomadas disposições para que uma lista dos documentos assim transportados fique no registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ que tem a guarda de tais documentos e seja averbada num livro de registo, devendo o seu retorno ser verificado por tal averbamento.

4. No interior de um país, os documentos com a classificação ►M1 SECRET UE ◄ e ►M1 CONFIDENTIEL UE ◄ poderão ser enviados pelo correio, se esse envio for permitido pela regulamentação nacional e conforme com as disposições da mesma, ou por um serviço de estafetas ou por pessoas habilitadas para o acesso a informações classificadas da UE.

5. A►M2 Direcção de Segurança da Comissão ◄ deverá elaborar instruções sobre o transporte pessoal de documentos classificados da União Europeia, com base nas presentes regras. O portador deverá ler e assinar essas instruções. Em especial, as instruções deverão indicar claramente que, em nenhuma circunstâncias, os documentos poderão:

   a) Deixar de estar na posse do portador, salvo se forem guardados de forma segura, segundo o disposto na secção 18;

   b) Ser deixados sem guarda em transportes públicos ou veículos privados ou em locais como restaurantes ou hotéis; também não poderão ser guardados em cofres de hotéis, nem deixados sem guarda em quartos de hotel;

   c) Ser lidos em locais públicos, como aviões ou comboios.

▼B

21.3.4. *Transmissão de um Estado para outro*

1. O material com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior deverá ser enviado por serviços de estafetas militares ou mala diplomática da União Europeia.

2. Todavia, poderá ser autorizado o transporte pessoal de material ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄ se as disposições em matéria de transporte forem de molde a garantir que este não poderá chegar às mãos de pessoas não-autorizadas.

3. O membro da Comissão responsável pelas questões de segurança pode autorizar o transporte pessoal quando não estiverem disponíveis mala diplomática ou serviços de estafetas militares, ou, sendo o material urgentemente necessário ao destinatário, a utilização desses tipos de transporte puder resultar num atraso susceptível de prejudicar as operações da União Europeia. A►M2 Direcção de Segurança da Comissão ◄ deverá elaborar instruções que abranjam o transporte internacional pessoal de material classificado até ao nível ►M1 SECRET UE ◄, inclusive, por pessoas que não sejam correios diplomáticos, nem militares. Essas instruções deverão estipular que:

   a) O portador tenha a habilitação de segurança adequada;

   b) Todo o material assim transportado esteja averbado num registo ou serviço competente;

   c) As embalagens ou sacos com material da União Europeia ostentem um selo oficial, para impedir ou desencorajar a inspecção pelos serviços aduaneiros, e rótulos com identificação e instruções para as pessoas que os possam eventualmente encontrar;

   d) O portador disponha de um certificado de correio e/ou de uma ordem de missão, reconhecida por todos os Estados-Membros da União Europeia, que o autorize a transportar a embalagem identificada;

   e) Não sejam atravessados territórios ou fronteiras de Estados não-membros da União Europeia, por via terrestre, a menos que o Estado de envio receba garantias específicas desses Estados;

   f) As condições de viagem do portador, no tocante a destinos, rotas a seguir e meios de transporte a utilizar, sejam conformes com a regulamentação da União Europeia ou, se a regulamentação nacional na matéria for mais restritiva, conformes com essa regulamentação;

   g) O material não deixe de estar na posse do portador, excepto se for guardado de forma segura segundo o disposto na secção 18;

   h) O material não seja deixado sem guarda em transportes públicos ou veículos privados, nem em locais como restaurantes ou hotéis; também não deve ser guardado em cofres de hotéis, nem deixado sem guarda em quartos de hotel;

   i) Se o material a transportar contiver documentos, estes não sejam lidos em locais públicos (por exemplo, aviões, comboios, etc.).

4. A pessoa designada para transportar o material classificado deve ler e assinar uma informação de segurança que contenha, no mínimo, as instruções acima enumeradas e os procedimentos a seguir em caso de emergência ou no caso de a embalagem com material classificado ser inspeccionada pelos serviços aduaneiros ou funcionários de segurança dos aeroportos.

21.3.5. *Transmissão de documentos com a classificação* ►M1 *RESTREINT UE* ◄

Não são estabelecidas disposições especiais para o transporte de documentos com a classificação ►M1 RESTREINT UE ◄, excepto que será necessário assegurar que tais documentos não cheguem às mãos de pessoas não-autorizadas.

21.4. **Habilitação em matéria de segurança do pessoal de transporte**

Todos os mensageiros e estafetas que transportem documentos com as classificações ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄ deverão possuir uma habilitação em matéria de segurança adequada.

21.5. **Transmissão electrónica ou por outros meios técnicos**

1. As medidas de segurança das comunicações serão concebidas de modo a assegurar a transmissão segura de informações classificadas da UE. As normas de execução em matéria de transmissão de tais informações constam da secção 25.

2. Apenas poderão transmitir informações com a classificação ►M1 CONFIDENTIEL UE ◄ e ►M1 SECRET UE ◄ os centros e redes e/ou os terminais e sistemas de comunicações acreditados.

▼B

21.6. **Cópias, traduções e extractos de documentos classificados da União Europeia**

1. Apenas a entidade de origem poderá autorizar a cópia ou a tradução de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄.
2. Se houver pessoas sem habilitação em matéria de segurança para o nível ►M1 TRES SECRET UE/EU TOP SECRET ◄ que precisem de informações que não tenham essa classificação, mas estejam contidas num documento ►M1 TRES SECRET UE/EU TOP SECRET ◄, o responsável do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ (ver a secção 22.2) poderá ser autorizado a produzir o número de extractos necessário de tal documento. Simultaneamente, deverá tomar as medidas necessárias para garantir que seja atribuída a esses extractos uma classificação de segurança adequada.
3. Os documentos com a classificação ►M1 SECRET UE ◄ ou inferior poderão ser reproduzidos e traduzidos pelo destinatário, no âmbito das presentes disposições de segurança e na condição de ser respeitado estritamente o princípio da «necessidade de tomar conhecimento». As medidas de segurança aplicáveis ao documento original serão igualmente aplicáveis às reproduções e/ou às traduções do mesmo.

22. REGISTOS, INVENTÁRIOS, VERIFICAÇÕES, ARQUIVAGEM E DESTRUIÇÃO DE INFORMAÇÕES CLASSIFICADAS DA UNIÃO EUROPEIA

22.1. **Registos locais de informações classificadas da UE**

1. Em cada serviço da Comissão, e em função das necessidades, serão constituídos um ou mais registos locais de informações classificadas da UE, que ficarão responsáveis pelo registo, reprodução, difusão, arquivo e destruição de documentos com as classificações ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄.
2. Se um serviço não dispuser de registo local, será o registo local de informações classificadas da UE do Secretariado-Geral a assumir essas funções.
3. Os registos locais de informações classificadas da UE dependerão do chefe de serviço de quem receberem instruções. Esses registos serão dirigidos por um responsável do controlo do registo.
4. Os registos serão supervisionados pelo responsável local de segurança no respeitante à aplicação das disposições relativas à manipulação de documentos com informações classificadas da UE e das medidas de segurança correspondentes.
5. Os funcionários dos registos locais de informações classificadas da UE serão autorizados a ter acesso a esse tipo de informações em conformidade com a secção 20.
6. Sob a autoridade do chefe de serviço de que dependerem, os registos locais de informações classificadas da UE:
   a) Gerirão as operações relativas ao registo, reprodução, tradução, transmissão, expedição e destruição dessas informações;
   b) Actualizarão a lista das indicações específicas relativas às informações classificadas;
   c) Analisarão periodicamente a necessidade de manter a classificação das informações.
7. Os registos locais de informações classificadas da UE manterão um registo dos seguintes elementos específicos:
   a) A data de elaboração das informações classificadas;
   b) O nível de classificação;
   c) A data de expiração da classificação;
   d) O nome e o serviço do autor;
   e) O destinatário ou destinatários, com o número de série respectivo;
   f) O assunto;
   g) O número;
   h) O número de cópias distribuídas;
   i) A elaboração de inventários das informações classificadas apresentadas ao serviço;
   j) O registo das desclassificações e desgraduações de informações classificadas.
8. As regras gerais previstas na secção 21 são aplicáveis aos registos locais de informações classificadas da UE da Comissão, excepto quando alteradas pelas regras específicas estabelecidas na presente secção.

▼B

22.2. **Registo ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1. *Disposições gerais*

1. O registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ central destina-se a assegurar o arquivo, tratamento e distribuição de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ em conformidade com as presentes disposições de segurança. O responsável do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ será o responsável do controlo do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. O registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ central constituirá a principal autoridade de recepção e expedição da Comissão, relativamente às outras instituições da União Europeia, aos Estados-Membros, às organizações internacionais e aos Estados terceiros com os quais a Comissão tiver acordos sobre procedimentos de segurança, para o intercâmbio de informações classificadas.

3. Sempre que necessário, serão criados sub-registos responsáveis pela gestão interna de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄; esses sub-registos manterão registos actualizados da circulação de cada documento a seu cargo.

4. Os sub-registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ serão criados segundo o disposto na secção 22.2.3 em resposta a necessidades de longo prazo e dependerão de um registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ central. Se apenas for necessário consultar documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ temporária ou ocasionalmente, tais documentos poderão ser disponibilizados sem que seja necessário criar um sub-registo ►M1 TRES SECRET UE/EU TOP SECRET ◄, na condição de serem definidas regras para assegurar que os documentos permaneçam sob o controlo do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ adequado e que sejam cumpridas todas as medidas de segurança física e pessoal.

5. Os sub-registos não podem enviar documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ directamente a outros sub-registos do mesmo registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ central sem a aprovação expressa deste último.

6. Todos os intercâmbios de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ entre sub-registos que não dependam do mesmo registo central deverão ter lugar através dos registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ centrais.

22.2.2. *Registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ central*

Na sua qualidade de responsável do controlo, incumbirá ao responsável do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ central providenciar:

a) A transmissão de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ segundo as disposições da secção 21.3;

b) A manutenção de uma lista de todos os sub-registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ dependentes do seu registo central, juntamente com os nomes e as assinaturas dos responsáveis do controlo nomeados e dos substitutos autorizados destes últimos;

c) A conservação de recibos dos vários registos para todos os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ distribuídos pelo registo central;

d) A manutenção de um registo dos documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ arquivados e distribuídos;

e) A manutenção de uma lista actualizada de todos os registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ centrais com os quais normalmente trabalhe, juntamente com os nomes e as assinaturas dos responsáveis do controlo nomeados dos mesmos e dos substitutos autorizados destes últimos;

f) A salvaguarda física de todos os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ arquivados no registo, segundo as regras da secção 18.

22.2.3. *Sub-registos ►M1 TRES SECRET UE/EU TOP SECRET ◄*

Na sua qualidade de responsável do controlo, incumbirá ao responsável de um sub-registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ providenciar:

a) A transmissão de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ segundo as disposições da secção 21.3;

b) A manutenção de uma lista actualizada de todas as pessoas autorizadas a ter acesso às informações com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ sob o seu controlo;

▼B

c) A distribuição de documentos com a classificação ►M1 TRES SECRET UE/ /EU TOP SECRET ◄ segundo as instruções da entidade de origem ou segundo o princípio de «necessidade de tomar conhecimento», devendo verificar previamente se o destinatário possui a necessária habilitação em matéria de segurança;

d) A manutenção de um registo actualizado de todos os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ arquivados ou que circulem sob o seu controlo ou que tiverem sido enviados a outros registos ►M1 TRES SECRET UE/EU TOP SECRET ◄, e a guarda de todos os recibos correspondentes;

e) A manutenção de uma lista actualizada dos registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ com os quais estiver autorizado a fazer intercâmbio de documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄, juntamente com os nomes e as assinaturas dos responsáveis do controlo dos mesmos e dos substitutos autorizados destes últimos;

f) A salvaguarda física de todos os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ arquivados no sub-registo, segundo as regras da secção 18.

22.3. **Inventários e verificações de documentos classificados da União Europeia**

1. Os registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ referidos na presente secção farão, cada um deles, todos os anos, um inventário exaustivo dos documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄. Considerar-se-á que foi dada conta de um documento se estiver fisicamente inscrito no registo, ou se este último possuir um recibo do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄ para o qual o documento tiver sido transferido, um certificado de destruição do documento ou uma ordem para a desgraduação ou desclassificação do mesmo. Os registos enviarão os resultados do inventário anual ao membro da Comissão responsável pelas questões de segurança, até ao dia 1 de Abril de cada ano.

2. Os sub-registos ►M1 TRES SECRET UE/EU TOP SECRET ◄ enviarão os resultados do seu inventário anual ao registo central de que dependerem, numa data indicada por este.

3. Os documentos classificados da União Europeia com classificação inferior a ►M1 TRES SECRET UE/EU TOP SECRET ◄ serão objecto de verificações internas de acordo com as instruções do membro da Comissão responsável pelas questões de segurança.

4. Essas operações deverão permitir que os detentores dos documentos possam dar a sua opinião sobre:

   a) A possibilidade de desgraduar ou desclassificar certos documentos;

   b) Documentos a destruir.

22.4. **Arquivagem de informações classificadas da UE**

1. As informações classificadas da UE devem ser arquivadas em conformidade com as disposições pertinentes da secção 18.

2. Para reduzir os problemas de arquivagem, os responsáveis do controlo de todos os registos serão autorizados a arquivar documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ e ►M1 CONFIDENTIEL UE ◄ sob a forma de microfilmes ou de gravação magnética ou óptica, desde que:

   a) O processo de microfilmagem/gravação seja realizado por pessoal com uma habilitação em matéria de segurança correspondente ao nível de classificação do material tratado;

   b) O microfilme/suporte de gravação possua o mesmo grau de segurança que os documentos originais;

   c) A microfilmagem/gravação de qualquer documento com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ seja comunicada à entidade de origem;

   d) Cada rolo de filme ou outro suporte contenha apenas documentos com o mesmo grau de classificação (►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄);

   e) A microfilmagem/gravação de um documento com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ ou ►M1 SECRET UE ◄ seja claramente indicada no registo utilizado para o inventário anual;

   f) Os documentos originais passados para microfilme ou gravados noutros suportes sejam destruídos em conformidade com as regras estabelecidas na secção 22.5.

▼B

3. Estas regras também são aplicáveis a qualquer outra forma de gravação autorizada, tais como meios electromagnéticos e disco óptico.

22.5. **Destruição de documentos classificados da UE**

1. Para impedir a acumulação desnecessária de documentos classificados da União Europeia, os que forem considerados pelo responsável da entidade detentora como desactualizados ou excedentários deverão ser destruídos logo que possível, da seguinte maneira:

   a) Os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ só serão destruídos pelo registo central responsável pelos mesmos. Cada documento destruído será enumerado num certificado de destruição, assinado pelo responsável do controlo ►M1 TRES SECRET UE/EU TOP SECRET ◄ e pelo funcionário que testemunhar a destruição, devendo este último possuir habilitação em matéria de segurança ao nível ►M1 TRES SECRET UE/EU TOP SECRET ◄. Será averbada no livro de registo uma nota nesse sentido;

   b) O registo conservará durante um período de dez anos os certificados de destruição e as folhas de distribuição. Só serão enviadas cópias à entidade de origem ou ao registo central adequado se estas forem explicitamente solicitadas;

   c) Os documentos com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄, incluindo todos os resíduos classificados resultantes da preparação de documentos com a classificação ►M1 TRES SECRET UE/ /EU TOP SECRET ◄, tais como cópias estragadas, rascunhos, notas dactilografadas e disquetes, serão destruídos, sob a supervisão do responsável do controlo do registo ►M1 TRES SECRET UE/EU TOP SECRET ◄, através de combustão, redução a pasta, retalhamento ou outro processo que os reduza a uma forma irreconhecível e não-reconstituível.

2. Os documentos com a classificação ►M1 SECRET UE ◄ serão destruídos pelo registo responsável pelos mesmos, sob a supervisão de uma pessoa habilitada em matéria de segurança, utilizando um dos processos indicados na alínea c) do ponto 1. Os documentos com a classificação ►M1 SECRET UE ◄ destruídos serão enumerados em certificados de destruição assinados, que deverão ser conservados pelo registo, juntamente com as listas de distribuição, pelo menos durante três anos.

3. Os documentos com a classificação ►M1 CONFIDENTIEL UE ◄ serão destruídos pelo registo responsável pelos mesmos, sob a supervisão de uma pessoa habilitada em matéria de segurança, utilizando um dos processos indicados na alínea c) do ponto 1. A sua destruição será registada de acordo com as instruções do membro da Comissão responsável pelas questões de segurança.

4. Os documentos com a classificação ►M1 RESTREINT UE ◄ serão destruídos pelo registo responsável pelos mesmos ou pelo utilizador, de acordo com as instruções do membro da Comissão responsável pelas questões de segurança.

22.6. **Destruição em casos de emergência**

1. Os serviços da Comissão elaborarão, com base nas condições locais, planos para a salvaguarda do material classificado da União Europeia em situações de crise, incluindo, se necessário, a destruição de emergência e planos de evacuação; esses serviços publicarão as instruções consideradas necessárias para impedir que informações classificadas da UE possam chegar às mãos de pessoas não-autorizadas.

2. As disposições para a salvaguarda e/ou destruição de material ►M1 SECRET UE ◄ ou ►M1 CONFIDENTIEL UE ◄ numa situação de crise não deverão prejudicar, em nenhum caso, a salvaguarda ou a destruição de material com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ (incluindo o equipamento de cifragem), cujo tratamento terá prioridade sobre todas as outras tarefas.

3. As medidas a adoptar para a salvaguarda ou destruição do equipamento de cifragem em caso de emergência deverão ser objecto de instruções específicas.

4. As instruções estarão imediatamente acessíveis, em envelope selado. Existirão os meios/utensílios necessários para a destruição.

23. MEDIDAS DE SEGURANÇA A APLICAR POR OCASIÃO DE REUNIÕES ESPECÍFICAS REALIZADAS FORA DAS INSTALAÇÕES DA COMISSÃO E QUE ENVOLVAM INFORMAÇÃO CLASSIFICADA DA UE

23.1. **Disposições gerais**

Quando forem realizadas reuniões da Comissão ou outras reuniões importantes fora das instalações da Comissão e sempre que tal se justifique devido aos requisitos especiais de segurança relacionados com a alta sensibilidade das questões

▼B

ou das informações tratadas, deverão ser tomadas as medidas de segurança seguidamente descritas. Estas medidas dizem apenas respeito à protecção das informações classificadas da UE; poderá ser necessário planear outras medidas de segurança.

23.2. **Responsabilidades**

23.2.1. ►M2 *Direcção de Segurança da Comissão* ◄

A►M2 Direcção de Segurança da Comissão ◄ cooperará com as autoridades competentes do Estado-Membro em cujo território tem lugar a reunião (o Estado-Membro de acolhimento) a fim de garantir a segurança das reuniões da Comissão ou outras reuniões importantes e a segurança dos delegados e respectivo pessoal. Em matéria de segurança, o Estado-Membro de acolhimento deverá especialmente assegurar que:

a) Sejam elaborados planos para fazer face às ameaças à segurança e aos incidentes relacionados com a segurança, os quais devem abranger em especial a guarda segura dos documentos classificados da UE em gabinetes;

b) Sejam tomadas medidas para facultar o acesso ao sistema de comunicações da Comissão para a recepção e transmissão de mensagens classificadas da UE. Será igualmente pedido ao Estado-Membro de acolhimento que faculte o acesso, se necessário, a sistemas telefónicos seguros.

A►M2 Direcção de Segurança da Comissão ◄ deverá agir como consultor em matéria de segurança para a preparação da reunião; deverá estar representado no local a fim de ajudar e aconselhar o Responsável da Segurança da Reunião (MSO) e as delegações, consoante as necessidades.

Será pedido a cada uma das delegações a uma reunião que designe um responsável de segurança, a quem competerá tratar as questões de segurança no interior da sua delegação e manter o contacto com o responsável da segurança da reunião e com o representante da►M2 Direcção de Segurança da Comissão ◄, consoante as necessidades.

23.2.2. *Responsável da Segurança da Reunião (MSO)*

Será nomeado um Responsável da Segurança da Reunião, que será responsável pela preparação geral e controlo das medidas gerais de segurança interna e pela coordenação com as outras autoridades competentes em matéria de segurança. As medidas tomadas pelo MSO incidirão, em geral:

a) Em medidas de protecção no local da reunião destinadas a garantir que esta se processa sem qualquer incidente que possa comprometer a segurança de qualquer informação classificada da UE que aí seja utilizada;

b) No controlo do pessoal a quem é permitido aceder ao local da reunião, áreas das delegações e salas de conferência, e à verificação de todo o equipamento;

c) Na constante coordenação com as autoridades competentes do Estado-Membro de acolhimento e com a►M2 Direcção de Segurança da Comissão ◄;

d) Na inclusão de instruções de segurança no dossier da reunião, tendo em conta as exigências das presentes regras de segurança e quaisquer outras instruções de segurança consideradas necessárias.

23.3. **Medidas de segurança**

23.3.1. *Áreas de segurança*

Serão criadas as seguintes áreas de segurança:

a) Uma área de segurança da classe II, constituída por uma sala de redacção, os escritórios e equipamento de reprografia da Comissão e os escritórios das delegações, conforme as necessidades;

b) Uma área de segurança da classe I, constituída pela sala de conferência e pelos gabinetes dos intérpretes e dos técnicos de som;

c) Áreas administrativas, constituídas pela área de imprensa e pelas instalações utilizadas para a administração, a restauração e o alojamento, bem como a área imediatamente adjacente ao Centro de Imprensa e ao local da reunião.

23.3.2. *Passes*

O MSO fornecerá cartões adequados, conforme os pedidos das delegações, e segundo as suas necessidades. Quando necessário, deverá ser feita uma distinção no que toca ao acesso às várias áreas de segurança.

As instruções de segurança para a reunião exigirão que todas as pessoas abrangidas ostentem de forma visível os seus cartões sempre que estejam dentro do local de reunião, de forma a poderem ser controladas pelo pessoal de segurança, na medida do necessário.

▼B

Além dos participantes que possuem um cartão, o número de pessoas a admitir no local de reunião será o mais reduzido possível. O MSO só permitirá que as delegações nacionais recebam visitantes durante a reunião mediante pedido dessas delegações. Deve ser dado um cartão de visitante a cada visitante. Será igualmente preenchido um passe de entrada do visitante, com o seu nome e com o nome da pessoa que este visita. Os visitantes serão acompanhados em todas as ocasiões por um guarda de segurança ou pela pessoa que visitam. O passe do visitante será transportado pela pessoa que o acompanha e devolvido ao pessoal encarregado da segurança, quando o visitante sair do local de reunião.

23.3.3. *Controlo do equipamento fotográfico e de som*

Não poderá dar entrada em nenhuma área de segurança da classe I qualquer equipamento audiovisual, com excepção do equipamento utilizado pelos fotógrafos e pelos técnicos de som devidamente autorizados pelo MSO.

23.3.4. *Controlo das pastas, computadores portáteis e embrulhos*

Os detentores de um passe com acesso autorizado a uma área de segurança podem normalmente trazer consigo as suas pastas e computadores portáteis (com a sua própria fonte de energia) sem que seja realizado um controlo. No caso dos embrulhos destinados às delegações, estas podem recebê-los, mas devem ser quer inspeccionados pelo responsável de segurança da delegação, quer visionados em equipamento especial, quer abertos pelo pessoal de segurança para inspecção. Se o MSO o considerar necessário, poderão ser estabelecidas medidas mais restritivas para a inspecção das pastas e embrulhos.

23.3.5. *Segurança técnica*

Uma equipa de segurança técnica deve tornar a sala de reunião tecnicamente segura, podendo igualmente efectuar uma vigilância electrónica durante a reunião.

23.3.6. *Documentos das delegações*

As delegações serão responsáveis por transportar consigo documentos classificados da UE tanto para dentro como para fora das reuniões. Serão igualmente responsáveis pela verificação e pela segurança desses documentos durante a sua utilização nas instalações que lhes forem atribuídas. Pode ser solicitado o auxílio do Estado-Membro de acolhimento para o transporte de documentos classificados para dentro e para fora do local da reunião.

23.3.7. *Guarda segura dos documentos*

Se a Comissão ou as delegações não estiverem em condições de guardar os seus documentos classificados em conformidade com as normas aprovadas, poderão introduzir esses documentos em envelopes selados e entregá-los ao MSO, mediante recibo, para que este os possa guardar segundo as normas aprovadas.

23.3.8. *Inspecção dos gabinetes*

O MSO providenciará para que os gabinetes da Comissão e das delegações sejam inspeccionados no fim de cada dia de trabalho, por forma a garantir que todos os documentos classificados da UE são guardados em local seguro; caso contrário, tomará as medidas necessárias.

23.3.9. *Remoção de resíduos de documentos classificados da UE*

Todos os resíduos serão tratados como resíduos classificados da UE, e todos os cestos ou sacos de lixo de papel devem ser entregues à Comissão ou às delegações para remoção. Antes de abandonar as instalações que lhes foram atribuídas, a Comissão e as delegações devem entregar os seus resíduos ao MSO, que providenciará para a sua destruição segundo as regras.

No fim da reunião, todos os documentos na posse da Comissão ou das delegações mas que já não sejam necessários serão tratados como resíduos. Antes de levantar as medidas de segurança tomadas para a reunião, será feita uma busca exaustiva das instalações ocupadas pela Comissão e pelas delegações. Na medida do possível, os documentos para os quais tenha sido assinado um recibo serão destruídos conforme se encontra previsto no ponto 22.5.

24. QUEBRAS DE SEGURANÇA E FUGAS DE INFORMAÇÕES CLASSIFICADAS DA UE

24.1. **Definições**

Uma quebra de segurança é o resultado de um acto ou uma omissão contrários a uma disposição de segurança da Comissão, susceptível de pôr em perigo as informações classificadas da UE ou propiciar a sua fuga.

▼B

Uma fuga de informações classificadas da UE ocorre quando estas caem no todo ou em parte nas mãos de pessoas não autorizadas, ou seja, pessoas que não possuem a habilitação de segurança adequada ou que não precisam de tomar conhecimento dessas informações, ou quando há a probabilidade de tal ter acontecido.

Pode haver fuga de informações classificadas da UE como resultado de descuido, negligência ou indiscrição, bem como em resultado das actividades de serviços de espionagem que têm por alvo a UE ou os seus Estados-Membros visando as informações classificadas e as actividades da UE, ou das actividades de organizações de carácter subversivo.

24.2. **Comunicação de quebras de segurança**

Todas as pessoas que devam tratar informações classificadas da UE receberão uma informação completa sobre as suas responsabilidades neste domínio e comunicarão imediatamente qualquer quebra de segurança de que possam ter conhecimento.

Quando um responsável local de segurança ou um responsável da segurança da reunião descobrir ou for informado da ocorrência de uma quebra de segurança relacionada com informações classificadas da UE ou com a perda ou desaparecimento de material classificado da UE, tomará imediatamente medidas para:

a) Proteger os elementos de prova;

b) Determinar os factos ocorridos;

c) Avaliar e reduzir os danos verificados;

d) Impedir que tal volte a acontecer;

e) Notificar as autoridades adequadas dos efeitos da quebra de segurança.

Neste contexto, serão fornecidos os seguintes elementos:

i) uma descrição das informações em causa, incluindo a sua classificação, números de referência e de cópia, data, entidade de origem, assunto e âmbito,

ii) uma breve descrição das circunstâncias da quebra de segurança, incluindo a data e o período durante o qual as informações estiveram expostas à fuga,

iii) uma declaração de que a entidade de origem foi ou não informada.

Incumbe a cada autoridade de segurança, imediatamente depois de lhe ter sido notificada a ocorrência de uma quebra de segurança, comunicar o facto imediatamente à►**M2** Direcção de Segurança da Comissão ◄.

Só será necessário comunicar os casos que envolvam informações classificadas de ►**M1** RESTREINT UE ◄ quando estes apresentarem características pouco usuais.

Ao ser informado da ocorrência de uma quebra de segurança, o Membro da Comissão responsável pelas questões de segurança deverá:

a) Notificar a entidade de origem das informações classificadas em questão;

b) Solicitar às autoridades de segurança competentes que procedam a um inquérito;

c) Coordenar os inquéritos, quando estiver envolvida mais do que uma autoridade de segurança;

d) Obter um relatório das circunstâncias da quebra de segurança, o período durante o qual poderá ter ocorrido e a data em que foi descoberta, juntamente com uma descrição pormenorizada do conteúdo e da classificação do material em causa. Serão, igualmente, comunicados os danos causados aos interesses da UE ou de um ou vários dos seus Estados-Membros e tomadas medidas para impedir que tal volte a acontecer.

A entidade de origem deverá informar os destinatários e deverá emitir instruções adequadas.

24.3. **Acções judiciais**

Qualquer indivíduo que seja responsável por uma fuga de informação classificada da UE será passível de acção disciplinar segundo as regras e regulamentos pertinentes, principalmente o Título VI do Estatuto. Essa acção disciplinar não será impeditiva de eventuais acções judiciais.

Se for caso disso, com base no relatório referido no ponto 24.2, o Membro da Comissão responsável pelas questões de segurança tomará todas as medidas necessárias para permitir às autoridades nacionais competentes intentar processos-crime.

▼B

25. PROTECÇÃO DAS INFORMAÇÕES CLASSIFICADAS DA UE TRATADAS EM SISTEMAS INFORMÁTICOS E DE COMUNICAÇÃO

25.1. **Introdução**

25.1.1. *Disposições gerais*

A política e os requisitos de segurança da presente secção aplicar-se-ão a todos os sistemas e redes de comunicação e de informação (adiante designados por sistemas) que tratem informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior. Serão aplicados em suplemento da Decisão C(95) 1510 final, de 23 de Novembro de 1995, relativa à protecção dos sistemas informáticos.

Os sistemas que tratem informações com a classificação ►**M1** RESTREINT UE ◄ necessitam igualmente de medidas de segurança para proteger a confidencialidade dessas informações. Todos os sistemas necessitam de medidas de segurança para proteger a sua integridade e disponibilidade, bem como a das informações que contêm.

A política de segurança informática aplicada pela Comissão comporta os seguintes elementos:

— parte integrante da segurança em geral e complemento de todos os elementos da segurança da informação, da segurança pessoal e da segurança física;

— repartição das responsabilidades pelos proprietários dos sistemas técnicos, proprietários de informações classificadas da UE armazenadas ou tratadas em sistemas técnicos, especialistas da segurança informática e utilizadores;

— descrição dos princípios e requisitos de segurança de cada sistema informático;

— aprovação de tais princípios e requisitos por uma autoridade designada;

— consideração das ameaças e vulnerabilidades específicas na central informática.

25.1.2. *Ameaças aos sistemas e sua vulnerabilidade*

É possível definir uma ameaça como uma quebra potencial, quer acidental quer deliberada, da segurança. No caso dos sistemas, essa quebra envolve a perda de uma ou várias características de confidencialidade, integridade e disponibilidade. A vulnerabilidade pode ser definida como uma fraqueza ou falta de controlo que possa facilitar ou permitir uma ameaça contra um bem ou um alvo específico.

O tratamento de informações classificadas e não classificadas da UE em sistemas de forma concentrada, concebida para permitir a sua rápida localização, comunicação e utilização, é vulnerável a várias ameaças. Estas incluem o acesso à informação por utilizadores não autorizados ou, em sentido inverso, a recusa do acesso aos utilizadores autorizados. Existem igualmente riscos de divulgação, corrupção, alteração ou supressão não autorizadas da informação. Além disso, os equipamentos complexos e muitas vezes frágeis são onerosos e frequentemente de difícil reparação ou substituição.

25.1.3. *Objectivo principal das medidas de segurança*

O objectivo principal das medidas de segurança enumeradas na presente secção é fornecer protecção contra a divulgação não autorizada de informações classificadas da UE (a perda de confidencialidade) e contra a perda de integridade ou disponibilidade das informações. Para alcançar um nível adequado de protecção de segurança de um sistema que trate informações classificadas da UE, a►**M2** Direcção de Segurança da Comissão ◄ especificará normas adequadas de segurança convencional, juntamente com procedimentos e técnicas de segurança especiais e adequados, especialmente concebidos para cada sistema.

25.1.4. *Lista dos requisitos de segurança específicos do sistema (SSRS)*

O proprietário dos sistemas técnicos (TSO, ver ponto 25.3.4) e o proprietário da informação (ver ponto 25.3.5) deverão elaborar uma lista dos requisitos de segurança específicos do sistema (SSRS) para cada um dos sistemas que tratem informações com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior, em colaboração e com assistência, se necessário, da equipa de projecto e da►**M2** Direcção de Segurança da Comissão ◄ (como Autoridade INFOSEC-IA, ver ponto), lista essa que deverá ser aprovada pela Autoridade de Acreditação de Segurança (SAA, ver ponto 25.3.2).

Também será necessária uma lista SSRS sempre que a Autoridade de Acreditação de Segurança (SAA) considerar que é de importância capital a disponibilidade e integridade de informações ►**M1** RESTREINT UE ◄ ou não classificadas.

A lista SSRS será elaborada o mais cedo possível no processo de concepção do projecto e será desenvolvida e aperfeiçoada à medida que o projecto for evoluindo, desempenhando papéis diferentes em fases diferentes do ciclo de vida do projecto e do sistema.

▼B

25.1.5. *Modos seguros de funcionamento*

Todos os sistemas que tratem informações com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior deverão ser acreditados para funcionar num ou, se for caso disso e em períodos diferentes, em vários dos seguintes modos seguros de funcionamento, ou seus equivalentes nacionais:

a) Dedicado;

b) Elevado;

c) Combinado.

25.2. **Definições**

«Acreditação»: autorização e aprovação concedidas a um sistema para tratar informações classificadas da UE no seu ambiente operacional.

Nota:

Esta acreditação deverá ser feita depois de terem sido aplicados todos os procedimentos adequados de segurança e depois de ser alcançado um nível suficiente de protecção dos recursos do sistema. A acreditação deverá normalmente ser feita com base na lista SSRS e incluir os seguintes elementos:

a) Uma indicação dos objectivos pretendidos para a acreditação do sistema, e em particular o(s) nível(eis) de classificação de informações a tratar e o(s) modo (s) seguro(s) de funcionamento proposto(s) para o sistema ou rede;

b) Uma análise de gestão de riscos que identifique as ameaças e as vulnerabilidades existentes e as medidas para as neutralizar;

c) A elaboração de procedimentos operacionais de segurança (SecOPS) com uma descrição pormenorizada das operações propostas (ou seja, modos e serviços a prestar), incluindo uma descrição dos elementos de segurança do sistema, que deverá constituir a base da acreditação;

d) Um plano para pôr em prática e fazer a manutenção dos elementos de segurança;

e) Um plano para testar, avaliar e certificar a segurança do sistema ou da rede, tanto à partida como em regime de acompanhamento;

f) A certificação, quando necessária, juntamente com outros elementos de acreditação.

«Responsável Central da Segurança Informática» (CISO): funcionário que, num serviço informático central, coordena e supervisa as medidas de segurança de sistemas com organização central.

«Certificação»: emissão de uma declaração formal, com base numa análise independente da condução e resultados de uma avaliação, da medida em que um sistema satisfaz os requisitos de segurança, ou da medida em que um produto de segurança informática cumpre objectivos de segurança predefinidos.

«Segurança das Comunicações» (COMSEC): aplicação de medidas de segurança às telecomunicações a fim de recusar às pessoas não autorizadas informações de valor que possam decorrer da posse ou do estudo dessas telecomunicações, ou a fim de assegurar a autenticidade dessas telecomunicações.

Nota:

Estas medidas incluem não só a segurança da cifragem, da transmissão e da emissão, como também a segurança processual, física, do pessoal, documental e informática.

«Segurança Informática» (COMPUSEC): aplicação de elementos de segurança a um sistema informático, tanto no equipamento (hardware) como no firmware e no software, a fim de o proteger contra, ou evitar, actos não autorizados de divulgação, manipulação e modificação/supressão de informações ou de recusa de serviço.

«Produto de Segurança Informática»: elemento genérico de segurança informática destinado a ser incorporado num sistema informático a fim de aumentar ou assegurar a confidencialidade, a integridade ou a disponibilidade das informações tratadas.

«Modo Seguro de Funcionamento Dedicado»: modo de funcionamento em que TODOS os indivíduos com acesso ao sistema estão habilitados para o mais alto nível de classificação das informações tratadas no sistema e têm uma necessidade comum de tomar conhecimento de TODAS as informações tratadas no sistema.

Notas:

(1) A necessidade comum de tomar conhecimento indica que não existe um requisito obrigatório de características de segurança informática que permitam separar as informações no interior do sistema.

▼B

(2) As outras características de segurança (por exemplo, físicas, do pessoal e processuais) deverão cumprir os requisitos para o mais alto nível de classificação e para todas as designações de categoria das informações tratadas no sistema.

«Avaliação»: exame técnico pormenorizado, por uma autoridade competente, dos aspectos de segurança de um sistema ou de um produto de segurança criptográfica ou informática.

Notas:

(1) A avaliação investiga a presença da requerida função de segurança e a ausência de efeitos colaterais prejudiciais nessa função e avalia a incorruptibilidade da mesma.

(2) A avaliação determina em que medida são cumpridos os requisitos de segurança de um sistema, ou as características de segurança de um produto de segurança informática, e estabelece o nível de fiabilidade do sistema, da função criptográfica ou do produto de segurança informática em que é depositada confiança.

«Proprietário da Informação» (IO): autoridade (chefe de serviço) responsável pela criação, o processamento e a utilização da informação, incluindo a decisão sobre as autorizações de acesso a essa informação.

«Segurança da Informação» (INFOSEC): aplicação de medidas de segurança para proteger informações processadas, armazenadas ou transmitidas em sistemas de comunicações, de informações e outros sistemas electrónicos contra a perda de confidencialidade, integridade ou disponibilidade, quer acidental quer intencional, e para prevenir a falta de integridade e disponibilidade dos próprios sistemas.

As «Medidas INFOSEC» incluem a segurança informática, das transmissões, das emissões e da cifragem e a detecção, documentação e neutralização das ameaças às informações e aos sistemas.

«Central Informática»: área que contém um ou mais computadores, as suas unidades locais, periféricas e de memória, as unidades de controlo e equipamento dedicado de rede e de comunicações.

Nota:

Nesta definição não se inclui uma área separada na qual se encontrem dispositivos ou terminais remotos periféricos/estações de trabalho, mesmo que esses dispositivos estejam ligados ao equipamento que se encontra na central informática.

«Rede Informática»: organização geograficamente disseminada de sistemas informáticos interligados para o intercâmbio de dados, que inclui os componentes dos sistemas informáticos interligados e as respectivas interfaces com as redes de dados ou de comunicações que lhes servem de apoio.

Notas:

(1) Uma rede informática pode utilizar os serviços de uma ou várias redes de comunicações para se interligar e proceder ao intercâmbio de dados; várias redes informáticas podem utilizar os serviços de uma rede comum de comunicações.

(2) Uma rede informática é chamada «local» se ligar vários computadores no mesmo local.

«Elementos de Segurança da Rede Informática»: conjunto dos elementos de segurança de cada sistema informático que compõe a rede, mais os componentes e elementos adicionais da rede propriamente dita (por exemplo, comunicações em rede, mecanismos e procedimentos de identificação de segurança e rotulagem, controlos de acesso, programas e pistas de auditoria) necessários para fornecer um nível aceitável de protecção das informações classificadas.

«Sistema Informático»: conjunto de equipamentos, métodos e procedimentos e, se necessário, pessoal, organizado para desempenhar funções de tratamento de informações.

Notas:

(1) Entende-se que esta designação um conjunto de instalações, configurado para tratar informações no interior do sistema;

(2) Estes sistemas poderão servir de apoio a aplicações de consulta, de comando, de controlo, de comunicações, científicas ou administrativas, incluindo o processamento de texto;

(3) As fronteiras de um sistema serão de um modo geral definidas como sendo os elementos sob o controlo de um único proprietário dos sistemas técnicos;

▼B

(4) Um sistema informático pode conter subsistemas, alguns dos quais poderão ser eles próprios sistemas informáticos.

«Elementos de Segurança do Sistema Informático»: compreendem todas as funções, características e elementos do equipamento (hardware), do firmware e do software; os procedimentos operacionais, os procedimentos de responsabilização e os controlos de acesso, a central informática, os terminais remotos/estações de trabalho e as limitações impostas pela gestão, a estrutura física e os dispositivos, o pessoal e os controlos das comunicações necessários para fornecer um nível necessário de protecção das informações classificadas a tratar num sistema informático.

«Responsável Local da Segurança Informática» (LISO): funcionário que, num serviço da Comissão, é responsável pela coordenação e supervisão das medidas de segurança no seu sector.

«Modo Seguro de Funcionamento Combinado»: modo de funcionamento em que NEM TODOS os indivíduos com acesso ao sistema estão habilitados para o mais alto nível de classificação das informações tratadas no sistema e NEM TODOS os indivíduos com acesso ao sistema têm uma necessidade comum de tomar conhecimento das informações tratadas no sistema.

Notas:

(1) Este modo de funcionamento permite o tratamento de informações com diferentes níveis de classificação e com designações mistas de categoria de informações.

(2) O facto de nem todos os indivíduos estarem habilitados para os mais altos níveis de classificação, associado a não haver uma necessidade comum de tomar conhecimento, indica que são necessárias características de segurança informática que permitam um acesso selectivo e a separação das informações no interior do sistema.

«Área de Terminais Remotos/Estações de Trabalho»: área que contém equipamento informático, os seus dispositivos ou terminais periféricos locais/estações de trabalho e qualquer equipamento associado de comunicações, separada de uma central informática.

«Procedimentos Operacionais de Segurança» (SecOPS): procedimentos elaborados pelos Proprietários dos Sistemas Técnicos, que definem os princípios a adoptar em matéria de segurança, os procedimentos operacionais a seguir e as responsabilidades do pessoal.

«Modo Seguro de Funcionamento Elevado»: modo de funcionamento em que TODOS os indivíduos com acesso ao sistema estão habilitados para o mais alto nível de classificação das informações tratadas no sistema, mas NEM TODOS os indivíduos com acesso ao sistema têm uma necessidade comum de tomar conhecimento das informações tratadas no sistema.

Notas:

(1) A ausência de uma necessidade comum de tomar conhecimento indica que são necessárias características de segurança informática que permitam um acesso selectivo e a separação das informações no interior do sistema.

(2) As outras características de segurança (por exemplo, físicas, de pessoal, e processuais) deverão cumprir os requisitos para o mais alto nível de classificação e para todas as designações de categoria das informações tratadas no sistema.

(3) Todas as informações tratadas ou disponíveis no sistema neste modo de funcionamento, juntamente com os resultados produzidos, serão protegidas, até ordem em contrário, como sendo potencialmente da categoria e do nível mais alto de classificação das informações em tratamento, excepto se for possível ter um nível aceitável de confiança em qualquer outra função de classificação presente no sistema.

Lista dos Requisitos de Segurança Específicos do Sistema (SSRS): enumeração completa e explícita dos princípios de segurança a observar e dos requisitos pormenorizados de segurança a cumprir. Tem por base a política de segurança e a avaliação de riscos da Comissão, ou será balizada por parâmetros que incluam o ambiente operacional, o mais baixo nível de habilitação de segurança do pessoal, a mais alta classificação das informações tratadas, o modo seguro de funcionamento ou os requisitos dos utilizadores. A lista SSRS faz parte integrante da documentação de projecto apresentada às autoridades competentes para efeitos de aprovação técnica, orçamental e de segurança. Na sua forma final, a lista SSRS constitui uma enumeração completa dos parâmetros de segurança do sistema.

«Proprietário dos Sistemas Técnicos» (TSO): autoridade responsável pela criação, manutenção, funcionamento e encerramento de um sistema.

▼B

«Contramedidas TEMPEST»: medidas de segurança destinadas a proteger o equipamento e as infra-estruturas de comunicações contra a fuga de informações classificadas resultante de emissões electromagnéticas não intencionais ou da condutividade.

25.3. **Responsabilidades em matéria de segurança**

25.3.1. *Disposições gerais*

As responsabilidades do Grupo Consultivo da Política de Segurança da Comissão, definidas no capítulo 12, incluem as questões INFOSEC. O Grupo organizará as suas actividades de forma a poder prestar aconselhamento técnico sobre essas questões.

A►**M2** Direcção de Segurança da Comissão ◄ será responsável pela emissão de disposições de aplicação INFOSEC, com base no disposto no presente capítulo.

Sempre que surjam problemas de segurança (incidentes, infracções, etc.), serão imediatamente tomadas as medidas adequadas pela►**M2** Direcção de Segurança da Comissão ◄.

A►**M2** Direcção de Segurança da Comissão ◄ disporá de uma unidade INFOSEC.

25.3.2. *Autoridade de Acreditação de Segurança (SAA)*

O ►**M2** director da Direcção de Segurança da Comissão ◄ é a Autoridade de Acreditação de Segurança (SAA) da Comissão. A SAA é responsável pela organização geral da segurança e pelos domínios INFOSEC especializados: segurança das comunicações, segurança Cripto e segurança Tempest.

Competirá à SAA assegurar a conformidade dos sistemas com a política de segurança da Comissão. Uma das suas tarefas será a aprovação de um sistema destinado a tratar as informações classificadas da UE até um determinado nível de classificação no seu ambiente operacional.

A competência da SAA da Comissão abrangerá todos os sistemas que estão em funcionamento nos locais da Comissão. Sempre que diferentes componentes de um sistema passem a ser da competência da SAA da Comissão e de outras SAA, todas as partes em causa poderão nomear um conselho de acreditação conjunto, que será coordenado pela SAA da Comissão.

25.3.3. *Autoridade INFOSEC (IA)*

O chefe da unidade INFOSEC da►**M2** Direcção de Segurança da Comissão ◄ é a Autoridade INFOSEC da Comissão. A Autoridade INFOSEC é responsável por:

— prestar aconselhamento e assistência técnica à SAA,

— contribuir para a elaboração dos SSRS,

— rever os SSRS por forma a assegurar a sua coerência com as presentes regras de segurança e as políticas da INFOSEC e a arquitectura do sistema,

— participar em painéis/conselhos de acreditação sempre que necessário e apresentar à SAA recomendações INFOSEC em matéria de acreditação,

— dar apoio às actividades de formação INFOSEC,

— prestar aconselhamento técnico na investigação de incidentes relacionados com a INFOSEC,

— definir orientações técnicas a fim de garantir que apenas seja utilizado software autorizado.

25.3.4. *Proprietário dos Sistemas Técnicos (TSO)*

O Proprietário dos Sistemas Técnicos (TSO) é responsável pela aplicação e funcionamento dos controlos e dos elementos de segurança especiais de um sistema. Para os sistemas de propriedade central será nomeado um Responsável Central da Segurança Informática (CISO). Cada serviço nomeará, sempre que necessário, um Responsável Local da Segurança Informática (LISO). A responsabilidade de um TSO inclui a criação dos procedimentos operacionais de segurança (SecOPS) e estender-se-á por todo o ciclo de vida do sistema, desde a fase de concepção do projecto até à remoção final.

O TSO definirá as normas e práticas de segurança a respeitar pelo fornecedor do sistema.

O TSO pode delegar parte das suas responsabilidades, sempre que necessário, num Responsável Local pela Segurança Informática. As diversas funções INFOSEC podem ser desempenhadas por uma única pessoa.

▼B

25.3.5. *Proprietário da Informação (IO)*

O Proprietário da Informação (IO) é responsável pelas informações classificadas da UE (e outras informações) a introduzir, processar e produzir nos sistemas técnicos. O IO definirá as condições de acesso a essas informações nos sistemas. O IO pode delegar essa responsabilidade num gestor de informação ou num gestor de bases de dados do seu sector.

25.3.6. *Utilizadores*

Todos os utilizadores deverão assegurar que as suas actividades não sejam nocivas para a segurança do sistema que estão a utilizar.

25.3.7. *Formação INFOSEC*

Serão propostas acções de formação INFOSEC a todos os membros do pessoal que dela necessitem.

25.4. **Medidas de segurança não técnicas**

25.4.1. *Segurança do pessoal*

Os utilizadores do sistema devem possuir habilitação de segurança e ter necessidade de tomar conhecimento que correspondam à classificação e ao conteúdo das informações tratadas no seu sistema específico. Para ter acesso a determinados equipamentos ou informações específicos à segurança dos sistemas é necessária uma habilitação de segurança especial, concedida segundo os procedimentos da Comissão.

A SAA deve designar todos os postos sensíveis e definir o nível de habilitação de segurança e de supervisão necessário para todos os agentes que trabalham nesses postos.

Os sistemas devem ser especificados e concebidos de uma forma que facilite a repartição das tarefas e responsabilidades pelos membros do pessoal, para que nenhuma pessoa possa ter o conhecimento e o controlo completos dos pontos-chave do sistema de segurança.

A central informática e as áreas de terminais/estações de trabalho onde a segurança do sistema possa ser alterada não podem ser ocupadas por um único funcionário autorizado ou outro agente.

Os parâmetros de segurança de um sistema só podem ser alterados por, pelo menos, duas pessoas autorizadas que ajam de modo conjugado.

25.4.2. *Segurança física*

A central informática e as áreas de terminais/estações de trabalho (tal como definidas no ponto 25.2) onde sejam tratadas, por meios informáticos, informações ►M1 CONFIDENTIEL UE ◄ ou com uma classificação superior, ou onde for possível o acesso a tais informações, serão definidas como áreas de segurança UE da classe I ou II, conforme o caso.

25.4.3. *Controlo do acesso a um sistema*

Todas as informações e material que permitam o controlo do acesso a um sistema devem ser protegidos do modo correspondente à classificação mais elevada e à categoria das informações às quais esse sistema possa dar acesso.

Quando já não forem utilizados para esse efeito, as informações e o material de controlo do acesso devem ser destruídos, em conformidade com o disposto no ponto 25.5.4.

25.5. **Medidas de segurança técnicas**

25.5.1. *Segurança das informações*

Compete à entidade de origem das informações identificar e classificar todos os documentos portadores de informações, quer se apresentem sob a forma de cópias impressas ou de suporte informático. Cada página de cópia impressa deverá ser marcada, em cima e em baixo, com a classificação. O produto, quer se apresente sob a forma de cópias impressas ou de suporte informático, deverá ter a mesma classificação que a classificação mais alta atribuída às informações utilizadas para a sua produção. O modo como funciona um sistema também pode ter influência na classificação dos produtos desse sistema.

Compete aos serviços da Comissão e às pessoas que nele são detentores de informações analisar os problemas que surgem quando se agregam elementos de informação, assim como as deduções que podem ser retiradas dos elementos agregados, e determinar se é ou não adequada uma classificação superior para a totalidade da informação.

O facto de a informação consistir num código abreviado, código de transmissão ou qualquer outra forma de representação binária não constitui qualquer protecção de segurança, não devendo portanto influenciar a sua classificação.

▼B

Quando uma informação for transferida de um sistema para outro, deverá ser protegida durante a transferência e no sistema receptor, de uma forma consentânea com a classificação e a categoria originais da informação.

Todos os suportes informáticos deverão ser tratados em conformidade com a classificação mais elevada da informação armazenada ou da identificação do suporte, devendo sempre ser protegidos de forma adequada.

Os suportes informáticos reutilizáveis usados para registar informações classificadas da UE deverão manter a classificação mais elevada que já lhes tenha sido atribuída enquanto essas informações não forem convenientemente desgraduadas ou desclassificadas e os suportes não forem reclassificados em conformidade, ou os suportes não forem desclassificados ou destruídos segundo um procedimento aprovado pela SAA (ver ponto 25.5.4).

25.5.2. *Controlo e responsabilidade pelas informações*

Os acessos às informações classificadas ►M1 SECRET UE ◄ ou nível superior deverão ser averbados num registo manual ou automático (pistas de auditoria). Esses registos deverão ser mantidos em conformidade com as presentes regras de segurança.

O material classificado da UE existente na central informática pode ser tratado como um elemento classificado e não precisa de ser registado, desde que esse material seja identificado, marcado com a respectiva classificação e controlado de forma adequada.

Sempre que o material proveniente de um sistema que trate informações classificadas da UE for transmitido a uma área de terminais remotos/estações de trabalho a partir de uma central informática, deverão ser definidos procedimentos, aprovados pela SAA, para controlar e registar o produto. No que diz respeito ao material com a classificação ►M1 SECRET UE ◄ e superior, tais procedimentos deverão incluir instruções específicas quanto à responsabilidade pelas informações.

25.5.3. *Tratamento e controlo dos suportes informáticos amovíveis*

Todos os suportes informáticos amovíveis com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior deverão ser tratados como material, sendo-lhes aplicadas as regras gerais correspondentes. É necessário adaptar a identificação adequada e as marcações da classificação à natureza física específica do suporte, para permitir que seja claramente reconhecido.

Os utilizadores deverão assumir a responsabilidade de armazenar as informações classificadas da UE em suportes com a devida marcação da classificação e a devida protecção. Deverão ser definidos procedimentos destinados a garantir que, para todos os níveis de informações da UE, o armazenamento de informações em suportes informáticos seja feito segundo as presentes regras de segurança.

25.5.4. *Desclassificação e destruição dos suportes informáticos*

Os suportes informáticos utilizados para registar informações classificadas da UE podem ser desgraduados ou desclassificados, segundo um procedimento a aprovar pela SAA.

Os suportes informáticos que tiverem contido informações►M1 TRES SECRET UE/EU TOP SECRET ◄ ou com uma categoria especial não serão desclassificados nem reutilizados.

Se os suportes informáticos não puderem ser desclassificados ou não forem reutilizáveis, deverão ser destruídos segundo o procedimento supracitado.

25.5.5. *Segurança das comunicações*

O ►M2 director da Direcção de Segurança da Comissão ◄ é a Autoridade Cripto.

Quando as informações classificadas da UE forem transmitidas por meios electromagnéticos, deverão ser aplicadas medidas especiais para proteger a confidencialidade, a integridade e a disponibilidade dessas transmissões. A SAA determinará os requisitos necessários para impedir a detecção e intercepção das transmissões. As informações transmitidas através de um sistema de comunicações deverão ser protegidas com base em requisitos de confidencialidade, integridade e disponibilidade.

Sempre que forem necessários métodos criptográficos para garantir a confidencialidade, a integridade e a disponibilidade, esses métodos e os produtos associados deverão ser especificamente aprovados pela SAA enquanto Autoridade Cripto.

Durante a transmissão, a confidencialidade das informações com classificação ►M1 SECRET UE ◄ e superior deverá ser protegida por métodos ou produtos criptográficos aprovados pelo Membro da Comissão responsável pelas questões de segurança, após consulta do Grupo Consultivo da Política de Segurança da

▼B

Comissão. Durante a transmissão, a confidencialidade das informações com classificação ►M1 SECRET UE ◄ e superior deverá ser protegida por métodos ou produtos criptográficos aprovados pelo Membro da Comissão responsável pelas questões de segurança, após consulta do Grupo Consultivo da Política de Segurança da Comissão.

As regras pormenorizadas aplicáveis à transmissão de informações classificadas da UE deverão ser definidas em instruções de segurança específicas aprovadas pela►M2 Direcção de Segurança da Comissão ◄, após consulta do Grupo Consultivo da Política de Segurança da Comissão.

Em circunstâncias operacionais excepcionais, as informações classificadas ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ e ►M1 SECRET UE ◄ podem ser transmitidas em claro, desde que isso seja explicitamente autorizado caso a caso e devidamente registado pelo Proprietário da Informação. Essas circunstâncias excepcionais são as seguintes:

a) Durante situações de crise iminente ou real, de conflito, ou de guerra;

b) Quando a rapidez da comunicação for de importância fundamental, não estando disponíveis meios de cifragem, e se considere que as informações transmitidas não podem ser exploradas a tempo de influenciar negativamente as operações.

Um sistema deve ter a capacidade de impedir positivamente o acesso às informações classificadas da UE em qualquer dos seus terminais ou estações de trabalho, sempre que necessário, quer através da desconexão física ou de dispositivos informáticos especiais aprovados pela SAA.

25.5.6. *Segurança em matéria de instalação e de radiações*

O caderno de encargos para a instalação inicial dos sistemas e qualquer posterior alteração importante deverá estipular que sejam feitas por instaladores com habilitação de segurança, sob a constante supervisão de pessoal tecnicamente qualificado que esteja habilitado para o acesso a informações classificadas da UE ao nível equivalente à classificação mais alta que o sistema deverá armazenar e tratar.

Os sistemas que tratam informações com a classificação ►M1 CONFIDENTIEL UE ◄ ou superior devem ser protegidos de forma a que a sua segurança não possa ser ameaçada por fugas resultantes de emissões ou da condutividade, cujo estudo e controlo se designam pelo termo «Tempest».

As contramedidas TEMPEST devem ser revistas e aprovadas por uma Autoridade TEMPEST (ver ponto25.3.2).

25.6. **Segurança durante o tratamento**

25.6.1. *Procedimentos Operacionais de Segurança (SecOPS)*

Os Procedimentos Operacionais de Segurança (SecOPS) definem os princípios a adoptar em matéria de segurança, os procedimentos operacionais a seguir e as responsabilidades do pessoal. Os SecOPS serão estabelecidos sob a responsabilidade do proprietário dos sistemas técnicos (TSO).

25.6.2. *Protecção do software/gestão da configuração*

A segurança das aplicações será determinada com base numa avaliação da classificação de segurança do próprio programa e não na classificação das informações a tratar. As versões do software a uso deverão ser verificadas a intervalos regulares para garantir a sua integridade e o seu correcto funcionamento.

Não deverão ser utilizadas versões novas ou alteradas do software para o tratamento de informações classificadas da UE enquanto não forem verificadas pelo TSO.

25.6.3. *Verificação da presença de programas maliciosos/vírus informáticos*

A verificação da presença de programas maliciosos/vírus informáticos deverá ser feita periodicamente segundo os requisitos da SAA.

Antes de serem introduzidos em qualquer sistema, todos os suportes informáticos que dão entrada na Comissão deverão ser controlados a fim de detectar a presença de quaisquer programas maliciosos ou vírus informáticos.

25.6.4. *Manutenção*

Os contratos e os procedimentos relativos à manutenção prevista ou solicitada dos sistemas, para os quais tenha sido elaborada uma lista SSRS, deverão especificar os requisitos e as disposições relativas ao pessoal de manutenção e respectivo equipamento que penetrem numa central informática.

▼B

Os requisitos deverão ser claramente mencionados na lista SSRS e os procedimentos claramente indicados nos SecOPS. A manutenção por contratação que exija procedimentos de diagnóstico de acesso remoto só será permitida em circunstâncias excepcionais, sob um controlo de segurança rigoroso e unicamente com o consentimento da SAA.

25.7. **Contratos públicos**

25.7.1. *Disposições gerais*

Qualquer produto de segurança a utilizar pelo sistema que deva ser obtido por contratação pública deverá ter sido avaliado e certificado, ou estar em processo de avaliação e certificação, por um organismo de avaliação ou de certificação adequado de um dos Estados-Membros da União Europeia com base em critérios reconhecidos a nível internacional (tais como os Critérios Comuns de Avaliação da Segurança Informática — ver ISO 15408). São exigidos procedimentos específicos para obter a aprovação da Comissão Consultiva de Compras e Contratos (CCAM).

Para decidir se o equipamento, designadamente os suportes informáticos, deverá ser alugado em vez de adquirido, há que ter presente que esse equipamento, uma vez utilizado para o tratamento de informações classificadas da UE, não pode abandonar os locais que lhe asseguram a protecção necessária sem primeiro ter sido desclassificado com a aprovação da SAA, aprovação essa que nem sempre é possível.

25.7.2. *Acreditação*

Antes de poderem tratar informações classificadas da UE, todos os sistemas para os quais tenha de ser elaborada uma lista SSRS serão acreditados pela SAA, com base em informações constantes dos SSRS, dos SecOPS e de qualquer outra documentação pertinente. Os sub-sistemas e os terminais/estações de trabalho remotos deverão ser acreditados como parte de todos os sistemas a que estão ligados. Quando um sistema der apoio tanto à Comissão como a outras organizações, a Comissão e as autoridades de segurança competentes deverão dar o seu consentimento mútuo à acreditação.

O processo de acreditação poderá ser conduzido de acordo com uma estratégia de acreditação adequada a um determinado sistema e definida pela SAA.

25.7.3. *Avaliação e certificação*

Antes de se proceder à acreditação, em certos casos, os elementos de segurança do equipamento (hardware), do firmware e do software de um sistema serão avaliados e certificados como capazes de salvaguardar as informações ao nível pretendido de classificação.

Os requisitos de avaliação e certificação deverão ser incluídos na planificação do sistema e claramente mencionados nos SSRS.

A avaliação e certificação serão realizadas de acordo com as directrizes aprovadas e por pessoal tecnicamente qualificado e com a devida habilitação de segurança, agindo em nome do TSO.

As equipas podem ser oriundas de uma autoridade de avaliação ou certificação designada por um Estado-Membro ou dos seus representantes designados, como por exemplo um contratante competente e com habilitação de segurança.

O nível de avaliação e de certificação pode ser reduzido (por exemplo abrangendo apenas aspectos de integração) quando os sistemas se basearem em produtos de segurança informática existentes e já avaliados e certificados a nível nacional.

25.7.4. *Controlos de rotina dos elementos de segurança para prorrogar a acreditação*

O TSO estabelecerá procedimentos de controlo de rotina que deverão garantir que todos os elementos de segurança do sistema continuam válidos.

Os tipos de alterações que possam ocasionar uma nova acreditação, ou que exijam uma aprovação prévia da SAA, serão claramente identificados e mencionados nos SSRS. Na sequência de qualquer alteração, reparação ou falha que possa ter afectado os elementos de segurança do sistema, o TSO providenciará a realização de um controlo para se assegurar do correcto funcionamento dos elementos de segurança. A prorrogação da acreditação do sistema dependerá normalmente dos resultados satisfatórios desses controlos.

Todos os sistemas em que tiverem sido aplicados elementos de segurança serão inspeccionados ou revistos numa base periódica pela SAA. No que diz respeito aos sistemas que tratam informações com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄, essas inspecções devem ser realizadas pelo menos uma vez por ano.

▼B

25.8. **Utilização temporária ou ocasional**

25.8.1. *Segurança dos microcomputadores/computadores pessoais*

Os microcomputadores/computadores pessoais (PCs) dotados de discos fixos (ou outras memórias não voláteis), que funcionem autonomamente ou em rede, assim como os dispositivos informáticos portáteis (por exemplo, PCs portáteis e «agendas electrónicas») com discos duros fixos, serão considerados meios de armazenamento de informações na mesma acepção que as disquetes ou outros suportes informáticos amovíveis.

Estes equipamentos deverão dispor de um nível de protecção, em termos de acesso, tratamento, armazenamento e transporte, correspondente ao nível de classificação mais elevado da informação alguma vez neles armazenada ou tratada (até ser desgraduada ou desclassificada segundo procedimentos aprovados).

25.8.2. *Utilização de equipamento informático privado para trabalhos oficiais da Comissão*

É proibida a utilização de suportes informáticos amovíveis, de programas e de equipamentos informáticos privados (por exemplo PCs e dispositivos informáticos portáteis) dotados de memória, para tratar informações classificadas da UE.

Os equipamentos, programas e suportes informáticos de uso privado não podem ser introduzidos em nenhuma área das categorias I ou II onde sejam tratadas informações classificadas da UE sem autorização escrita do ►**M2** director da Direcção de Segurança da Comissão ◄. Essa autorização só poderá ser dada por motivos técnicos em casos excepcionais.

25.8.3. *Utilização de equipamento informático pertencente a prestadores de serviços ou fornecido por um país para trabalhos oficiais da Comissão*

O ►**M2** director da Direcção de Segurança da Comissão ◄ pode autorizar a utilização de equipamentos e programas informáticos pertencentes a prestadores de serviços em organizações que prestam apoio ao trabalho oficial da Comissão. Também poderá ser autorizada a utilização de equipamentos e programas informáticos fornecidos por um país. Neste caso, o equipamento informático deverá ser controlado e inscrito num inventário adequado da Comissão. Em qualquer dos casos, se o equipamento informático for utilizado para tratar informações classificadas da UE, deverá ser então consultada a SAA, para que os elementos INFOSEC aplicáveis à utilização desse equipamento sejam devidamente analisados e aplicados.

26. DIVULGAÇÃO DE INFORMAÇÕES CLASSIFICADAS DA UE A PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

26.1.1. *Princípios aplicáveis à divulgação de informações classificadas da UE*

A divulgação de informações classificadas da UE a países terceiros ou organizações internacionais será decidida pela Comissão, enquanto Colégio, com base:

— na natureza e conteúdo dessas informações,

— na necessidade de saber do destinatário,

— nas vantagens que isso traz para a UE.

Será pedida autorização à entidade que está na origem das informações classificadas da UE.

Tais decisões serão tomadas caso a caso, com base no seguinte:

— o nível pretendido de cooperação com os Países terceiros ou organizações internacionais em causa,

— a confiança que neles poderá ser depositada — que decorre do nível de segurança que seria aplicado às informações classificadas da UE confiadas a esses Estados ou organizações e da conformidade das regras de segurança que eles aplicam com as aplicadas na UE. O Grupo Consultivo da Política de Segurança da Comissão dará o seu parecer técnico à Comissão sobre este ponto.

A aceitação de informações classificadas da UE por parte de países terceiros ou organizações internacionais implica a garantia de que as informações não serão utilizadas para outros fins que não sejam os que motivaram a divulgação ou troca de informações, e de que garantirão a protecção exigida pela Comissão.

26.1.2. *Níveis*

Tendo a Comissão decidido que as informações classificadas podem ser divulgadas ou trocadas com um determinado Estado ou organização internacional, decidirá também sobre o nível de cooperação possível. Esta depende, em particular, da política de segurança e das regulamentações aplicadas por esse Estado ou organização.

Existem três níveis de cooperação:

▼B

Nível 1

Cooperação com países terceiros ou com organizações internacionais cuja política e regulamentação em matéria de segurança estão muito próximas das da UE.

Nível 2

Cooperação com países terceiros ou com organizações internacionais cuja política e regulamentação em matéria de segurança são significativamente diferentes das da UE.

Nível 3

Cooperação pontual com países terceiros ou com organizações internacionais cuja política e regulamentação em matéria de segurança não podem ser avaliadas.

Cada nível de cooperação determinará os procedimentos e as disposições de segurança, pormenorizadas nos apêndices 3, 4 e 5.

26.1.3. *Acordos de segurança*

Uma vez que tenha decidido que existe uma necessidade permanente ou a longo prazo de trocar informações classificadas entre a Comissão e países terceiros ou outras organizações internacionais, a Comissão concluirá «acordos sobre procedimentos de segurança para a troca de informações classificadas» com a outra parte, que definirão o objectivo da cooperação e as regras recíprocas em matéria de protecção das informações trocadas.

No caso da cooperação pontual do nível 3, que, por definição, é limitada no tempo e no objectivo, o «acordo sobre procedimentos para a troca de informações classificadas» poderá ser substituído por um simples memorando de entendimento que defina a natureza das informações classificadas a trocar e as obrigações recíprocas em relação a essas informações, desde que não sejam classificadas num nível superior ao de ►M1 RESTREINT UE ◄.

Os projectos de acordo sobre procedimentos de segurança ou de memorandos de entendimento serão discutidos pelo Grupo Consultivo da Política de Segurança da Comissão antes de serem apresentados à Comissão para decisão.

O Membro da Comissão responsável pelas questões de segurança pedirá às NSA dos Estados-Membros toda a assistência necessária para garantir que as informações comunicadas serão utilizadas e protegidas em conformidade com o disposto nos acordos sobre procedimentos de segurança ou nos memorandos de entendimento.

▼M3

27. NORMAS MÍNIMAS COMUNS SOBRE SEGURANÇA INDUSTRIAL

27.1. **Introdução**

A presente secção aborda os aspectos da segurança das actividades industriais que sejam exclusivos à negociação e à adjudicação de contratos ou à celebração de convenções de subvenção pelos quais sejam confiadas tarefas que envolvam, impliquem e/ou contenham informações classificadas UE e à sua execução por entidades industriais ou outras, incluindo a disponibilização ou o acesso a informações classificadas UE durante os processos de concurso público e de convite à apresentação de propostas (período de apresentação de candidaturas e negociações pré-contratuais).

27.2. **Definições**

Para efeitos das presentes normas mínimas comuns, entende-se por:

a) «Contrato classificado»: qualquer contrato ou convenção de subvenção de fornecimento de bens, realização de obras, disponibilização de edifícios ou prestação de serviços cuja execução exija ou implique o acesso a informações classificadas UE ou a sua produção;

b) «Subcontrato classificado»: o contrato realizado entre o contratante ou beneficiário de uma subvenção e outro contratante (subcontratante) para o fornecimento de produtos, a realização de obras, a disponibilização de edifícios ou a prestação de serviços cuja execução exija ou implique o acesso a informações classificadas UE ou a sua produção;

c) «Contratante»: um operador económico ou entidade com capacidade jurídica para celebrar contratos ou ser beneficiário de uma subvenção;

▼M3

d) «Autoridade de segurança designada (ASD)»: a autoridade responsável perante a autoridade nacional de segurança (ANS) de qualquer Estado-Membro encarregada de informar as entidades industriais ou outras da política nacional em todas as matérias de segurança industrial e de fornecer orientação e prestar assistência na sua implementação. As funções da ASD podem ser desempenhadas pela ANS;

e) «Certificação de segurança da empresa (CSE)»: a certificação administrativa, emitida pela ASD/ANS, assegurando que, do ponto de vista da segurança, uma empresa está apta a garantir uma protecção de segurança adequada de um nível de classificação de segurança específico às informações classificadas UE e de que o seu pessoal que precise de ter acesso às informações classificadas UE foi devidamente sujeito a um inquérito de segurança e informado dos requisitos de segurança aplicáveis, necessários para ter acesso às informações classificadas UE e garantir a sua protecção;

f) «Entidade industrial ou outra»: um contratante ou subcontratante envolvido no fornecimento de bens, execução de obras ou prestação de serviços; trata-se de entidades industriais, comerciais, de serviços, científicas, de investigação, educativas ou de desenvolvimento;

g) «Segurança industrial»: a aplicação de medidas e procedimentos de protecção para evitar ou detectar perdas ou o comprometimento de informações classificadas UE a que um contratante ou subcontratante tenha acesso no âmbito das negociações pré-contratuais e dos contratos, bem como para recuperar essas informações em caso de perda ou comprometimento;

h) «Autoridade nacional de segurança (ANS)»: a autoridade pública de um Estado-Membro da UE a que cabe em última instância a responsabilidade pela protecção das informações classificadas UE no interior do mesmo;

i) «Nível global de classificação de segurança do contrato»: a determinação da classificação de segurança de todo o contrato ou convenção de subvenção, baseada na classificação das informações e/ou do material que deva ou possa ser produzido, divulgado ou consultado ao abrigo de qualquer parte do contrato geral ou do convenção de subvenção. O nível global de classificação de segurança do contrato não pode ser inferior à classificação mais elevada de qualquer das suas partes, podendo no entanto ser superior, em virtude do efeito de conjunto;

j) «Cláusula adicional de segurança (CAS)»: o conjunto de condições contratuais especiais, emitido pela autoridade contratante, que constitui parte integrante de um contrato classificado que implique o acesso a informações classificadas UE ou a sua produção, no qual são identificados os requisitos de segurança ou as partes do contrato classificado que exigem uma protecção de segurança;

k) «Guia da classificação de segurança (GCS)»: o documento que descreve as partes do programa, contrato ou convenção de subvenção que são classificadas, com os níveis da classificação de segurança. O GCS pode ser alargado durante a vigência do programa, contrato ou convenção de subvenção e as informações podem ser reclassificadas ou passarem para uma classificação inferior. Todas as CAS devem obrigatoriamente integrar um GCS.

27.3. **Organização**

a) Mediante contrato classificado, a Comissão pode confiar a entidades industriais ou outras, registadas num Estado-Membro, tarefas que envolvam, impliquem e/ou contenham informações classificadas UE;

b) Ao adjudicar contratos classificados, a Comissão deve garantir o cumprimento de todos os requisitos derivados das presentes normas mínimas;

c) A Comissão deve implicar a(s) ANS relevante(s) a fim de aplicar as presentes normas mínimas à segurança industrial. A ANS pode confiar estas tarefas a uma ou mais ASD;

d) A responsabilidade pela protecção das informações classificadas no âmbito das entidades industriais ou outras cabe, em última instância, à respectiva administração;

e) Aquando da adjudicação de um contrato ou subcontrato classificado abrangido pelas presentes normas mínimas, a Comissão e/ou a ANS/ASD, conforme o caso, notificará imediatamente a ANS/ASD do Estado-Membro em que o contratante ou o subcontratante está registado.

27.4. **Contratos classificados e decisões de subvenção**

a) A classificação de segurança dos contratos ou convenções de subvenção deve obedecer aos seguintes princípios:

— A Comissão fixa, na medida do necessário, quais os aspectos do contrato classificado que exigem protecção e a consequente classificação de segurança; ao fazê-lo, deve ter em conta a classificação de segurança original atribuída pelo autor à informação produzida antes da adjudicação do contrato;

▼M3

— O nível global de classificação do contrato não pode ser inferior à classificação mais elevada de qualquer das suas partes;

— As informações classificadas UE produzidas no âmbito de actividades contratuais são classificadas de acordo com o GCS;

— Quando se justifique, a Comissão fica responsável pela alteração do nível global de classificação do contrato ou da classificação de segurança de qualquer das suas partes, em consulta com o autor, informando todas as partes interessadas;

— As informações classificadas disponibilizadas ao contratante ou subcontratante ou produzidas no âmbito da actividade contratual não devem ser utilizadas para fins diferentes dos definidos pelo contrato classificado, não podendo ser comunicadas a terceiros sem prévio consentimento escrito da entidade de origem.

b) A Comissão e as ANS/ADS dos Estados-Membros pertinentes são responsáveis por garantir que os contratantes e subcontratantes a quem sejam adjudicados contratos classificados que envolvam informações com a classificação CONFIDENTIEL UE ou superior tomem todas as medidas adequadas para salvaguardar as informações classificadas que lhes tenham sido disponibilizadas ou por eles tenham sido produzidas na execução do contrato classificado, nos termos das disposições legislativas e regulamentares nacionais. Do incumprimento dos requisitos de segurança pode resultar a resolução do contrato classificado.

c) Todas as entidades industriais ou outras que participem em contratos classificados que impliquem o acesso a informações com a classificação CONFIDENTIEL UE ou superior devem possuir uma CSE nacional. A CSE é concedida pela ANS/ADS do Estado-Membro para confirmar que a empresa está em condições de garantir a protecção de segurança adequada às informações classificadas UE ao nível de classificação apropriado.

d) Aquando da adjudicação de um contrato classificado, um oficial de protecção da instalação (OPI), nomeado pela administração do contratante ou subcontratante, fica responsável por pedir uma certificação de segurança pessoal (CSP) para todas as pessoas empregadas em entidades industriais ou outras registadas num Estado-Membro da UE cujas tarefas exijam o acesso a informações com a classificação CONFIDENTIEL UE ou superior, a conceder pela ANS/ADS do referido Estado-Membro nos termos das suas regulamentações nacionais.

e) Os contratos classificados devem incluir uma CAS tal como definido na alínea j) do ponto 27.2. A CAS deve conter um GCS.

f) Antes de iniciar um procedimento de negociação de um contrato classificado, a Comissão contactará as ANS/ADS do Estado-Membro em que estejam registadas as entidades industriais ou outras interessadas, a fim de obter confirmação de que possuem uma CSE válida apropriada ao nível de classificação de segurança do contrato.

g) A autoridade contratante não deve celebrar um contrato classificado com um operador económico escolhido sem ter previamente recebido a CSE válida.

h) Salvo nos casos em que as disposições legislativas e regulamentares nacionais dos Estados-Membros o exijam, não é necessária uma CSE para os contratos que envolvam as informações classificadas RESTREINT UE.

i) No caso de concursos relativos a contratos classificados, os anúncios devem conter uma disposição que exija que os operadores económicos que não apresentem candidatura ou que não sejam seleccionados devem devolver todos os documentos num prazo determinado.

j) Pode ser necessário que um contratante negoceie subcontratos classificados a vários níveis com subcontratantes. Compete ao contratante garantir que todas as actividades de subcontratação respeitam as normas mínimas comuns constantes da presente secção. Todavia, o contratante não pode transmitir a um subcontratante informações ou materiais classificados UE sem o prévio consentimento por escrito da entidade de origem.

k) As condições em que o contratante pode subcontratar devem ser definidas na proposta ou no convite à apresentação de propostas e no contrato classificado. Nenhum subcontrato pode ser celebrado com entidades registadas num Estado que não seja membro da União Europeia sem a expressa autorização por escrito da Comissão.

l) Durante o período de vigência do contrato classificado, a observância de todas as suas disposições de segurança será controlada pela Comissão, juntamente com a ANS/ADS em causa. A notificação de incidentes de segurança será efectuada nos termos das disposições estabelecidas na secção 24 da parte II das presentes regras de segurança. A alteração ou retirada de uma CSE será imediatamente comunicada à Comissão e a qualquer outra ANS/ADS a que tenha sido notificada.

▼M3

m) Em caso de resolução de um contrato ou subcontrato classificado, a Comissão e/ou a ANS/ADS, consoante o caso, notificará prontamente as ANS/ADS do Estado-Membro em que o contratante ou subcontratante estiver registado.

n) As normas mínimas comuns constantes da presente secção continuarão a ser cumpridas e a confidencialidade das informações classificadas será mantida pelos contratantes e subcontratantes após a resolução ou o termo do contrato ou subcontrato classificado.

o) Na CAS ou noutras disposições pertinentes em que se identifiquem requisitos de segurança serão estabelecidas disposições específicas para a eliminação das informações classificadas no termo do contrato classificado.

p) As obrigações e condições referidas na presente secção aplicam-se *mutatis mutandis* a procedimentos de concessão de subvenções por decisão e, nomeadamente, aos beneficiários das mesmas. A decisão de subvenção definirá todas as obrigações dos beneficiários.

27.5. **Visitas**

Quaisquer visitas que representantes da Comissão, no contexto de contratos classificados, efectuem às entidades industriais ou outras dos Estados-Membros que executem contratos classificados UE devem ser organizadas com as ANS/ADS em causa. As visitas de empregados de entidades industriais ou outras que tenham lugar no âmbito de um contrato classificado UE devem ser organizadas entre as ANS/ADS interessadas. Todavia, as ANS/ADS participantes num contrato classificado UE podem aprovar um procedimento segundo o qual as visitas efectuadas por empregados de entidades industriais ou outras podem ser organizadas directamente.

27.6. **Transmissão e transporte de informações classificadas UE**

a) No que se refere à transmissão de informações classificadas UE, aplicar-se-ão as disposições da secção 21 da parte II das presentes regras de segurança. A fim de completar essas disposições, serão aplicados quaisquer procedimentos em vigor entre os Estados-Membros.

b) O transporte internacional de material classificado UE referente a contratos classificados é efectuado nos termos dos procedimentos nacionais dos Estados-Membros. As disposições de segurança para o transporte internacional serão analisadas com base nos seguintes princípios:

— É garantida a segurança em todas as fases do transporte e em todas as circunstâncias, desde o ponto de origem até ao destino final;

— O grau de protecção atribuído a uma remessa é determinado pela classificação mais elevada do material nela contido;

— Se necessário, será obtida uma CSE para as empresas que efectuem o transporte. Nesses casos, o pessoal que manipula a remessa deve ser sujeito a habilitação de segurança, em conformidade com as regras mínimas comuns constantes da presente secção;

— Na medida do possível, os transportes serão directos, efectuando-se tão rapidamente quanto as circunstâncias o permitirem;

— Sempre que possível, os itinerários apenas devem atravessar o território dos Estados-Membros da União Europeia. Só deverão atravessar Estados não membros da União Europeia quando tal for autorizado pelas ANS/ /ADS dos Estados do expedidor e do destinatário;

— Antes de qualquer transporte de material classificado UE, o expedidor elabora um plano de transporte que é aprovado pelas ANS/ADS em causa.

▼**M1**

Apêndice 1

COMPARAÇÃO DAS CLASSIFICAÇÕES NACIONAIS DE SEGURANÇA

Classificação UE	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Classificação UEO	FOCAL TOP SECRET	WEU SECRET	WEU CONFI-DENTIAL	WEU RESTRICTED
Classificação Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFI-DENTIAL	EURA RESTRICTED
NATO classifi-cação	COSMIC TOP SECRET	NATO SECRET	NATO CONFI-DENTIAL	NATO RESTRICTED
Áustria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Bélgica	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Chipre	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
República Checa	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Dinamarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Estónia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Alemanha	Streng geheim	Geheim	VS [1] — Vertraulich	VS — Nur für den Dienstgebrauch
Grécia	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Finlândia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
França	Très Secret Défense [2]	Secret Défense	Confidentiel Défense	
Irlanda	Top Secret	Secret	Confidential	Restricted
Itália	Segretissimo	Segreto	Riservatissimo	Riservato
Letónia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituânia	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburgo	Très Secret	Secret	Confidentiel	Diffusion restreinte
Hungria	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Países Baixos	Stg [3]. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Polónia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Eslovénia	Strogo tajno	Tajno	Zaupno	SVN Interno
Eslováquia	Prísne tajné	Tajné	Dôverné	Vyhradené
Espanha	Secreto	Reservado	Confidencial	Difusión Limitada
Suécia	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

▼**M1**

Reino Unido	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) A classificação «Très Secret Défense», que abrange temas prioritários do Governo, só pode ser alterada com autorização do primeiro-ministro.
([3]) Stg = staatsgeheim.

▼B

Apêndice 2

GUIA PRÁTICO DE CLASSIFICAÇÃO

Este guia é indicativo e não pretende modificar as disposições substantivas apresentadas nas secções 16, 17, 20 e 21.

Classificação	Quando	Quem	Aposições	Desgraduação/desclassificação/destruição	
				Quem	Quando
►**M1** TRES SECRET UE/EU TOP SECRET ◄ Esta classificação apenas se aplica a informações e material cuja divulgação não autorizada possa prejudicar de forma excepcionalmente grave os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros [16].	A fuga de bens com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄ poderia: — ameaçar directamente a estabilidade interna da UE ou de um dos seus Estados-Membros ou de países amigos, — prejudicar de forma excepcionalmente grave as relações com governos amigos, — conduzir directamente a enormes perdas humanas, — prejudicar de forma excepcionalmente grave a eficácia operacional ou a segurança das forças dos Estados-Membros ou de outros contribuintes, assim como a continuação da eficácia de operações extremamente valiosas de segurança ou recolha de informações, — causar graves prejuízos a longo prazo à economia da UE ou dos Estados-Membros.	Pessoas devidamente autorizadas (entidades de origem), directores-gerais, chefes de serviço [17] As entidades de origem devem especificar uma data, um período ou um acontecimento durante o qual os conteúdos podem ser desgraduados ou desclassificados. [16.2] De outro modo, deverão rever os documentos de cinco em cinco anos, no máximo, de forma a assegurar que a classificação inicial é necessária [0].	Deverá ser aposta a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄ em documentos com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄ e, se necessário, introduzido um designador de segurança e/ou a marcação de defesa-ESDP/PESD, por meios mecânicos e à mão [16.4, 0, 16.3]. As classificações UE e os designadores de segurança deverão ser apostos no topo de no fundo de cada página, centradas, devendo todas as páginas ser numeradas. Cada documento deverá possuir um número de referência e uma data; esse número de referência deverá constar de cada página. Se tiverem de ser distribuídos em várias cópias, cada uma dessas cópias deverá ter um número de cópia, que constará da primeira página, juntamente com o número total de páginas. Todos os anexos e apêndices deverão ser enumerados na primeira página [21].	A desclassificação ou a desgraduação são da exclusiva responsabilidade da entidade de origem, que deverá informar de todas as alterações os subsequentes destinatários a quem tiver enviado o documento ou uma cópia [0]. Os documentos com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄ deverão ser destruídos pelo registo central ou pelo sub-registo por eles responsável. Cada documento destruído deverá ser enumerado num certificado de destruição, assinado pelo responsável do controlo ►**M1** TRES SECRET UE/EU TOP SECRET ◄ e pelo funcionário que assistiu à destruição, que deve ter a habilitação ►**M1** TRES SECRET UE/EU TOP SECRET ◄. Será inscrita no livro de registo uma nota nesse sentido. O registo deverá manter os certificados de destruição, juntamente com a folha de distribuição, durante um período de dez anos [0].	As cópias e os documentos excedentários que já não são necessários devem ser destruídos [22.5]. Os documentos com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄, incluindo todos os resíduos classificados resultantes da elaboração de documentos com a classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄, tais como cópias estragadas, rascunhos, notas dactilografadas e papel-químico, deverão ser destruídos, sob a supervisão de um responsável do controlo ►**M1** TRES SECRET UE/EU TOP SECRET ◄, por queima, redução a polpa, retalhamento ou por qualquer outra forma, tornando-os irreconhecíveis e não reconstituíveis [0]
►**M1** SECRET UE ◄: Esta classificação apenas se	A fuga de bens com a classificação ►**M1** SECRET UE ◄	Pessoas devidamente autorizadas (entidades de origem),	Deverá ser aposta a classificação ►**M1** SECRET UE ◄	A desclassificação e a desgraduação são da exclusiva respon-	As cópias e os documentos excedentários que já não são necessá-

Classificação	Quando	Quem	Aposições	Desgraduação/desclassificação/destruição	
				Quem	Quando
aplica a informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros [16].	poderia: — dar origem a tensões internacionais, — prejudicar seriamente as relações com governos amigos, — ameaçar directamente a vida ou prejudicar seriamente a ordem pública ou a segurança ou a liberdade individuais, — causar sérios prejuízos à eficácia operacional ou à segurança das forças dos Estados-Membros ou de outros contribuintes, ou à continuação da eficácia de operações altamente valiosas de segurança ou de recolha de informações, — causar prejuízos materiais substanciais aos interesses financeiros, monetários, económicos e comerciais da UE ou de um dos seus Estados-Membros.	directores-gerais, chefes de serviço [17]. As entidades de origem devem especificar uma data ou um período durante o qual os conteúdos podem ser desgraduados ou desclassificados. [16.2] De outro modo, deverão rever os documentos de cinco em cinco anos, no máximo, de forma a assegurar que a classificação inicial é necessária [0].	em documentos com a classificação ►**M1** SECRET UE ◄ e, se necessário, introduzido um designador de segurança e/ou a marcação de defesa-ESDP/ /PESD, por meios mecânicos e à mão [16.4, 0, 16.3]. As classificações UE e os designadores de segurança deverão ser apostos no topo e no fundo de cada página, centradas, devendo todas as páginas ser numeradas. Cada documento deverá possuir um número de referência e uma data; esse número de referência deverá constar de cada página. Se tiverem de ser distribuídos em várias cópias, cada uma dessas cópias deverá ter um número de cópia, que constará da primeira página, juntamente com o número total de páginas. Todos os anexos e apêndices deverão ser enumerados na primeira página [21].	sabilidade da entidade de origem, que deverá informar de todas as alterações os subsequentes destinatários a quem tiver enviado o documento ou uma cópia [0]. Os documentos com a classificação ►**M1** SECRET UE ◄ deverão ser destruídos pelo registo por eles responsável, sob a supervisão de uma pessoa habilitada em matéria de segurança. Os documentos com a classificação ►**M1** SECRET UE ◄ destruídos serão enumerados em certificados de destruição assinados que deverão ser mantidos pelo registo, juntamente com as listas de distribuição, pelo menos durante três anos [0].	rios devem ser destruídos [0]. Os documentos com a classificação ►**M1** SECRET UE ◄, incluindo todos os resíduos classificados resultantes da elaboração de documentos com a classificação ►**M1** SECRET UE ◄, tais como cópias estragadas, rascunhos, notas dactilografadas e papel-químico, deverão ser destruídos por queima, redução a polpa, retalhamento ou por qualquer outra forma, tornando-os irreconhecíveis e não reconstituíveis [0].
►**M1** CONFIDENTIEL UE ◄ Esta classificação apenas se aplica a informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da União Europeia ou de um ou vários dos seus Estados-Membros [16].	A fuga de bens com a classificação ►**M1** CONFIDENTIEL UE ◄ poderia: — causar prejuízos materiais às relações diplomáticas, ou seja, dar origem a protestos formais ou a outras sanções, — prejudicar a segurança ou a liberdade individuais, — causar prejuízos à eficácia operacional ou à segurança	Pessoas autorizadas (entidades de origem), directores-gerais e chefes de serviço [17]. As entidades de origem devem especificar uma data ou um período durante o qual os conteúdos podem ser desgraduados ou desclassificados. Caso contrário, deverão passar em revista os documentos de cinco em cinco anos, no máximo, a fim de verificar se é	Deverá ser aposta a classificação ►**M1** CONFIDENTIEL UE ◄ em documentos com a classificação ►**M1** CONFIDENTIEL UE ◄, e, se necessário, introduzido um designador de segurança e/ou a marcação de defesa-ESDP/ /PESD, por meios mecânicos e à mão, ou imprimindo-as em papel pré-timbrado registado [16.4, 0 e 16.3].	A desclassificação ou a desgraduação são da exclusiva responsabilidade da entidade de origem, que deverá informar de todas as alterações os subsequentes destinatários a quem tiver enviado o documento ou uma cópia [0]. Os documentos com a classificação ►**M1** CONFIDENTIEL UE ◄ deverão ser destruídos pelo registo por eles respon-	As cópias e os documentos excedentários que já não são necessários devem ser destruídos [0]. Os documentos com a classificação ►**M1** CONFIDENTIEL UE ◄, incluindo todos os resíduos classificados resultantes da elaboração de documentos com a classificação ►**M1** CONFIDENTIEL UE ◄, tais como cópias estragadas, rascunhos, notas dactilografadas e papel-

Classificação	Quando	Quem	Aposições	Desgraduação/desclassificação/destruição	
				Quem	Quando
	das forças dos Estados-Membros ou de outros contribuintes, ou à da eficácia de operações valiosas de segurança ou de recolha de informações, — debilitar substancialmente a viabilidade financeira de organizações importantes, — impedir a investigação ou facilitar o cometimento de crimes graves, — ser substancialmente contrária aos interesses financeiros, monetários, económicos e comerciais da UE ou dos Estados-Membros, — impedir seriamente o desenvolvimento ou o funcionamento de políticas importantes da UE, — paralisar ou de outra forma minar actividades importantes da UE.	necessário manter a classificação original [0].	As classificações UE deverão constar no topo e no fundo de cada página, centradas, devendo cada página ser numerada. Cada documento deverá possuir um número de referência e uma data. Todos os anexos e apêndices deverão ser enumerados na primeira página [21].	sável, sob a supervisão de uma pessoa habilitada. A sua destruição será registada nos termos da regulamentação nacional e, no caso da Comissão ou dos organismos descentralizados da UE, segundo as instruções do ►**M2** membro da Comissão responsável pelas questões de segurança ◄ [0].	químico, deverão ser destruídos por queima, redução a polpa, retalhamento ou por qualquer outra forma, tornando-os irreconhecíveis e não reconstituíveis [0].
►**M1** RESTREINT UE ◄ Esta classificação apenas se aplica a informações e material cuja divulgação não autorizada possa ser desvantajosa para os interesses da União Europeia ou de um ou vários dos seus Estados-Membros [16].	A fuga de bens com a classificação ►**M1** RESTREINT UE ◄ poderia: — afectar negativamente as relações diplomáticas, — causar grande aflição às pessoas, — tornar muito mais difícil manter a eficácia operacional ou a segurança das forças dos Estados-Membros ou de outros	Pessoas autorizadas (entidades de origem), directores-gerais e chefes de serviço [17]. As entidades de origem devem especificar uma data, um período ou um acontecimento durante o qual os conteúdos podem ser desgraduados ou desclassificados [16.2]. Caso contrário, deverão passar em revista os documentos de cinco em cinco anos, no máximo, a fim de verificar se é necessário	Deverá ser aposta a classificação ►**M1** RESTREINT UE ◄ em documentos com a classificação ►**M1** RESTREINT UE ◄ e, se necessário, introduzido um designador de segurança e/ou a marcação de defesa-ESDP/PESD, por meios mecânicos ou electrónicos [16.4, 0 e 16.3]. A classificação UE e os designadores de segurança deverão ser apostos no topo da primeira	A desclassificação é da exclusiva responsabilidade da entidade de origem, que deverá informar de todas as alterações os subsequentes destinatários a quem tiver enviado o documento ou uma cópia [0]. Os documentos com a classificação ►**M1** RESTREINT UE ◄ deverão ser destruídos pelo registo por eles responsável ou pelo utilizador, de acordo com as instruções do	As cópias e os documentos excedentários que já não são necessários devem ser destruídos [0].

▼B

Classificação	Quando	Quem	Aposições	Desgraduação/desclassificação/destruição	
				Quem	Quando
	contribuintes — causar perdas financeiras ou facilitar ganhos ou vantagens ilícitas a indivíduos ou empresas, — violar os devidos compromissos de manter a confidência das informações prestadas por terceiros, — violar as restrições legais em matéria de divulgação da informação, — prejudicar a investigação ou facilitar o cometimento de crimes, — pôr em desvantagem a UE ou os Estados-Membros em negociações comerciais ou políticas com outros, — impedir o efectivo desenvolvimento ou funcionamento de políticas da UE, — Enfraquecer a correcta gestão da UE e das suas operações.	manter a classificação original [0].	página, devendo todas as páginas ser numeradas. Cada documento deverá possuir um número de referência e uma data [21].	►M2 membro da Comissão responsável pelas questões de segurança ◄ [0].	

▼B

Apêndice 3

Orientações para a divulgação de informações classificadas da UE a países terceiros ou organizações internacionais: cooperação de nível 1

PROCEDIMENTOS

1. Compete à Comissão, enquanto Colégio, autorizar a divulgação de informações classificadas da UE a países não membros da União Europeia ou a outras organizações internacionais com políticas e regulamentações de segurança comparáveis às da UE.
2. Na pendência da conclusão de um acordo de segurança, o Membro da Comissão responsável pelas questões de segurança é competente para examinar os pedidos de divulgação de informações classificadas da UE.
3. A esse título, compete-lhe:
   — procurar obter o parecer das entidades que estão na origem das informações classificadas da UE a divulgar,
   — estabelecer os contactos necessários com os órgãos de segurança das organizações internacionais ou países beneficiários a fim de verificar se as respectivas políticas e disposições de segurança são de molde a garantir que as informações classificadas divulgadas serão protegidas de acordo com as presentes disposições de segurança,
   — procurar obter o parecer do Grupo Consultivo da Política de Segurança da Comissão quanto à confiança que é possível depositar nas organizações internacionais ou Estados beneficiários.
4. O Membro da Comissão responsável pelas questões de segurança enviará o pedido à Comissão, para decisão, acompanhado do parecer do Grupo Consultivo da Política de Segurança da Comissão.

DISPOSIÇÕES DE SEGURANÇA A APLICAR PELOS BENEFICIÁRIOS

5. O Membro da Comissão responsável pelas questões de segurança notificará os Estados beneficiários ou as organizações internacionais da decisão da Comissão de autorizar a divulgação das informações classificadas da UE.
6. A decisão de divulgar só entrará em vigor quando os beneficiários tiverem dado garantias por escrito de que:
   — apenas utilizarão as informações para os fins acordados,
   — protegerão as informações de acordo com as presentes disposições de segurança e, em particular, as regras especiais abaixo enunciadas.
7. Pessoal
   a) O número de funcionários com acesso a informações classificadas da UE será estritamente limitado às pessoas cujas funções requeiram esse acesso, com base no princípio da «necessidade de ter conhecimento».
   b) Todos os funcionários ou nacionais autorizados a aceder a informações com classificação ►**M1** CONFIDENTIEL UE ◄ ou superior deverão possuir um certificado de segurança de nível adequado ou a habilitação de segurança equivalente, qualquer deles emitido pelo governo do Estado da sua nacionalidade.
8. Transmissão de documentos
   a) Os procedimentos práticos para a transmissão de documentos serão decididos de comum acordo. Na pendência da conclusão desse acordo, são aplicáveis as disposições da Secção 21. O acordo especificará, em particular, os registos para onde as informações classificadas da UE deverão ser enviadas.
   b) Se as informações classificadas cuja divulgação foi autorizada pela Comissão incluírem elementos com classificação ►**M1** TRES SECRET UE/EU TOP SECRET ◄, o Estado beneficiário ou a organização internacional deverão criar um registo central UE e, se necessário, sub-registos UE. Esses registos aplicarão disposições estritamente equivalentes às da Secção. das presentes disposições de segurança.
9. Registo

   Logo que o registo receba um documento com classificação ►**M1** CONFIDENTIEL UE ◄ ou superior, inscrevê-lo-á num livro especial conservado pela organização, com colunas para a data de recepção, as referências do documento (data, número de referência e número do exemplar), a classifi-

▼B

cação, o título do documento, o nome ou título de quem o recebeu, a data de envio do recibo e a data de destruição ou devolução do documento à entidade da UE que o emitiu.

10. Destruição

a) Os documentos classificados da UE serão destruídos segundo as instruções constantes da Secção das presentes disposições de segurança. O registo UE que enviou os documentos deverá receber uma cópia do certificado de destruição dos documentos com a classificação ►M1 SECRET UE ◄ e ►M1 TRES SECRET UE/EU TOP SECRET ◄.

b) Os documentos classificados da UE serão incluídos nos planos de destruição de emergência previstos para os documentos classificados dos organismos beneficiários.

11. Protecção dos documentos

Serão tomadas todas as disposições para impedir o acesso de pessoas não autorizadas às informações classificadas da UE.

12. Cópias, traduções e extractos

Não poderão ser feitas fotocópias ou traduções nem produzidos extractos de documentos com a classificação ►M1 CONFIDENTIEL UE ◄ ou ►M1 SECRET UE ◄ sem autorização do chefe do serviço de segurança competente, que registará e verificará essas cópias, traduções ou extractos, carimbando-os, se necessário.

A reprodução ou tradução de um documento com a classificação ►M1 TRES SECRET UE/EU TOP SECRET ◄ só poderá ser autorizada pela entidade de origem, que especificará o número de cópias autorizado; se não for possível determinar a entidade de origem, o pedido será remetido para a►M2 Direcção de Segurança da Comissão ◄.

13. Quebras de segurança

No caso de ocorrência ou suspeita de quebra de segurança em que esteja envolvido um documento classificado da UE, deverão ser imediatamente tomadas as seguintes disposições, sob reserva da conclusão de um acordo de segurança:

a) Realização de um inquérito para determinar as circunstâncias em que se verificou a quebra de segurança;

b) Notificação da►M2 direction de la sécurité de la Commission ◄, da autoridade nacional de segurança pertinente e da autoridade de origem, ou indicação clara de que esta última não foi notificada, se o não tiver sido;

c) Adopção de disposições para minimizar os efeitos da quebra de segurança;

d) Reapreciação e implementação de medidas para impedir que o caso se repita;

e) Implementação das medidas recomendadas pela►M2 Direcção de Segurança da Comissão ◄ para impedir que o caso se repita.

14. Inspecções

A►M2 Direcção de Segurança da Comissão ◄ será autorizado, por acordo com os Estados ou organizações internacionais em questão, a proceder a uma avaliação da eficácia das medidas de protecção das informações classificadas da UE que lhes sejam divulgadas.

15. Relatórios

Sob reserva da celebração de um acordo de segurança, enquanto o Estado ou organização internacional tiver na sua posse informações classificadas da UE, deverá apresentar, até uma data a especificar no momento em que for dada autorização para divulgar essas informações, um relatório anual confirmando que foram respeitadas as presentes disposições de segurança.

▼B

Apêndice 4

Orientações para a divulgação de informações classificadas da UE a países terceiros ou organizações internacionais: cooperação de nível 2

PROCEDIMENTOS

1. Compete à entidade de origem autorizar a divulgação de informações classificadas da UE a países terceiros ou organizações internacionais cujas políticas e regulamentações de segurança sejam significativamente diferentes das da UE. Compete à Comissão, enquanto Colégio, autorizar a divulgação de informações classificadas da UE criadas na Comissão.

2. Em princípio, esta competência restringe-se a informações classificadas até ao nível ►M1 SECRET UE ◄ inclusive, excluindo as informações classificadas protegidas por designadores ou marcações de segurança especiais.

3. Na pendência da conclusão de um acordo de segurança, o Membro da Comissão responsável pelas questões de segurança é competente para examinar os pedidos de divulgação de informações classificadas da UE.

4. A esse título, compete-lhe:

   — procurar obter o parecer das entidades que estão na origem das informações classificadas da UE a divulgar,

   — estabelecer os contactos necessários com os órgãos de segurança dos Estados beneficiários ou das organizações internacionais a fim de obter informações sobre as respectivas políticas e disposições de segurança e, em especial, elaborar um quadro comparativo das classificações aplicáveis na UE e no país ou organização interessado,

   — organizar uma reunião do Grupo Consultivo da Política de Segurança da Comissão ou, procurar, por procedimento escrito simplificado se necessário, recolher informações das autoridades nacionais de segurança dos Estados-Membros, com o objectivo de obter o parecer do Grupo Consultivo da Política de Segurança da Comissão.

5. O parecer do Grupo Consultivo da Política de Segurança da Comissão incidirá nos seguintes aspectos:

   — confiança que pode ser depositada nos Estados beneficiários ou nas organizações internacionais, no sentido de avaliar os riscos corridos pela UE ou pelos seus Estados-Membros em matéria de segurança,

   — avaliação da capacidade dos beneficiários para proteger as informações classificadas divulgadas pela UE,

   — propostas de procedimentos práticos para o tratamento das informações classificadas da UE (fornecimento de versões expurgadas de um texto, por exemplo) e dos documentos transmitidos (manutenção ou supressão das menções referentes à classificação UE, marcações específicas, etc.),

   — desgraduação ou desclassificação antes da divulgação das informações aos países beneficiários ou às organizações internacionais.

6. O Membro da Comissão responsável pelas questões de segurança enviará o pedido à Comissão, para decisão, acompanhado do parecer do Grupo Consultivo da Política de Segurança da Comissão.

REGRAS DE SEGURANÇA A APLICAR PELOS BENEFICIÁRIOS

7. O Membro da Comissão responsável pelas questões de segurança notificará os Estados beneficiários ou as organizações internacionais da decisão da Comissão de autorizar a divulgação das informações classificadas da UE e das suas restrições.

8. A decisão de divulgar só entrará em vigor quando os beneficiários tiveram dado garantias por escrito de que:

   — apenas utilizarão as informações para os fins acordados,

   — protegerão as informações segundo as disposições estabelecidas pela Comissão.

9. Serão aplicáveis as regras de protecção adiante enunciadas, salvo se a Comissão, depois de obter o parecer técnico do Grupo Consultivo da Política de Segurança da Comissão, optar por um procedimento específico para o tratamento dos documentos classificados da UE (supressão da menção referente à classificação UE, marcação específica, etc.).

▼B

10. Pessoal

a) O número de funcionários com acesso a informações classificadas da UE será estritamente limitado às pessoas cujas funções requeiram esse acesso, com base no princípio da «necessidade de ter conhecimento».

b) Todos os funcionários ou nacionais autorizados a aceder a informações classificadas divulgadas pela Comissão deverão possuir uma habilitação de segurança nacional ou uma autorização de acesso de nível equivalente ao da UE, conforme indicado no quadro comparativo.

c) Estas habilitações de segurança nacionais ou autorizações serão enviadas, para informação, ao ►**M2** director da Direcção de Segurança da Comissão ◄.

11. Transmissão de documentos

Os procedimentos práticos para a transmissão de documentos serão decididos de comum acordo. Na pendência da conclusão desse acordo, são aplicáveis as disposições da secção. O acordo especificará, em particular, os registos para onde as informações classificadas da UE deverão ser enviadas, os endereços precisos para onde os documentos deverão ser enviados, bem como os serviços postais ou de mensageiro utilizados para a transmissão das informações classificadas da UE.

12. Registo à chegada

A autoridade nacional de segurança (NSA) do Estado destinatário ou a entidade sua homóloga que receber em nome do Governo desse Estado as informações classificadas enviadas pela Comissão, ou o gabinete de segurança da organização internacional receptora, abrirão um registo especial para inscrever as informações classificadas da UE após a sua recepção. Esse registo conterá colunas para a data de recepção, as referências do documento (data, número de referência e número do exemplar), a classificação, o título do documento, o nome ou título do destinatário, a data de envio do recibo e a data de devolução do documento à UE ou da sua destruição.

13. Devolução de documentos

Quando a entidade receptora devolve um documento classificado à Comissão, procederá conforme indicado no ponto «Transmissão de documentos»*supra*.

14. Protecção

a) Os documentos que não estiverem a ser utilizados serão guardados num contentor de segurança aprovado para a armazenagem de material classificado nacional com o mesmo grau de classificação. O contentor não ostentará qualquer indicação do seu conteúdo, a que só terão acesso as pessoas autorizadas a tratar informações classificadas da UE. No caso de serem utilizadas fechaduras de segredo, este só será conhecido dos funcionários do Estado ou organização em causa que estejam autorizados a aceder a informações classificadas da UE guardadas no contentor e será modificado de seis em seis meses, ou antes de decorrido este período em caso de transferência de um funcionário, de retirada da habilitação de segurança de um dos funcionários que conheçam o segredo ou de risco de fuga de informação.

b) Os documentos classificados da UE só serão retirados do contentor de segurança por funcionários habilitados a aceder a documentos classificados da UE e que tenham necessidade de deles ter conhecimento. Estes funcionários serão responsáveis pela guarda desses documentos em condições de segurança enquanto os mesmos estiverem na sua posse e, em particular, por assegurar que nenhuma pessoa não autorizada a eles tenha acesso. Assegurarão também que os documentos sejam fechados num contentor de segurança logo que acabem de os consultar e fora das horas de serviço.

c) Não poderão ser feitas fotocópias de documentos classificados no grau ►**M1** CONFIDENTIEL UE ◄ ou num grau superior, nem deles poderão ser produzidos extractos, sem autorização da►**M2** Direcção de Segurança da Comissão ◄.

d) O procedimento para a destruição rápida e total dos documentos em caso de emergência deverá ser definido e confirmado com a►**M2** Direcção de Segurança da Comissão ◄.

15. Segurança física

a) Quando não estiverem a ser utilizados, os contentores de segurança usados para guardar documentos classificados da UE devem manter-se sempre trancados;

▼B

b) Quando for necessário deixar entrar pessoal de manutenção ou de limpeza para trabalhar numa sala onde estejam guardados contentores de segurança, esse pessoal deverá ser permanentemente acompanhado por um membro do serviço de segurança da organização ou do Estado em questão ou por um funcionário especificamente responsável pela vigilância da segurança da sala;

c) Fora do horário normal de trabalho (de noite, nos fins de semana e nos dias feriados), os contentores de segurança onde estejam guardados documentos classificados da UE deverão ser protegidos por um guarda ou por um sistema de alarme automático.

16. Quebras de segurança

No caso de ocorrência ou suspeita de quebra de segurança em que esteja envolvido um documento classificado da UE, deverão ser imediatamente tomadas as seguintes disposições:

a) Envio imediato de um relatório à►**M2** Direcção de Segurança da Comissão ◄ ou à NSA do Estado-Membro que tomou a iniciativa de enviar os documentos (com cópia para a►**M2** Direcção de Segurança da Comissão ◄);

b) Realização de um inquérito e, logo que este esteja concluído, apresentação de um relatório completo ao organismo de segurança acima referido [ver alínea a)]. Deverão então ser adoptadas as medidas necessárias para corrigir a situação.

17. Inspecções

A►**M2** Direcção de Segurança da Comissão ◄ será autorizado, por acordo com os Estados ou organizações internacionais em questão, a proceder a uma avaliação da eficácia das medidas de protecção das informações classificadas da UE que lhes tenham sido divulgadas.

18. Relatórios

Sob reserva da celebração de um acordo de segurança, enquanto o Estado ou organização internacional tiver na sua posse informações classificadas da UE, deverá apresentar, até uma data a especificar no momento em que for dada autorização para divulgar essas informações, um relatório anual confirmando que foram respeitadas as presentes disposições de segurança.

▼B

Apêndice 5

Orientações para a divulgação de informações classificadas da UE a países terceiros ou organizações internacionais: cooperação de nível 3

PROCEDIMENTOS

1. Ocasionalmente, a Comissão pode desejar cooperar, em circunstâncias especiais, com Estados ou organizações que não possam dar as garantias exigidas pelas presentes regras de segurança, apesar de essa cooperação poder requerer a divulgação de informações classificadas da UE.

2. Compete à entidade de origem autorizar a divulgação de informações classificadas da UE a países terceiros ou organizações internacionais cujas políticas e regulamentações de segurança sejam significativamente diferentes das da UE. Compete à Comissão, enquanto Colégio, autorizar a divulgação de informações classificadas da UE criadas na Comissão.

   Em princípio, esta competência restringe-se a informações classificadas até ao nível ►**M1** SECRET UE ◄ inclusive, excluindo as informações classificadas protegidas por designadores ou marcações de segurança especiais.

3. A Comissão ajuizará da sensatez de autorizar a divulgação das informações classificadas, avaliará a necessidade de o beneficiário delas tomar conhecimento e decidirá sobre a natureza das informações classificadas que poderão ser comunicadas.

4. Se a Comissão for favorável, o Membro da Comissão responsável pelas questões de segurança:

   — procurará obter o parecer das entidades que estão na origem das informações classificadas da UE a divulgar,

   — organizará uma reunião do Grupo Consultivo da Política de Segurança da Comissão ou, procurará, por procedimento escrito simplificado se necessário, recolher informações das autoridades nacionais de segurança dos Estados-Membros, com o objectivo de obter o parecer do Grupo Consultivo da Política de Segurança da Comissão.

5. O parecer do Grupo Consultivo da Política de Segurança da Comissão incidirá nos seguintes aspectos:

   a) Avaliação dos riscos corridos pela UE ou pelos seus Estados-Membros em matéria de segurança;

   b) Nível de classificação das informações que podem ser divulgadas;

   c) Desgraduação ou desclassificação antes da divulgação das informações;

   d) Procedimentos para o tratamento dos documentos a divulgar (ver ponto *infra*);

   e) Métodos de transmissão possíveis (recurso aos serviços públicos de correio, a sistemas de telecomunicações públicos ou securizados, à mala diplomática, a mensageiros devidamente habilitados, etc.).

6. Os documentos divulgados aos Estados ou organizações a que se refere o presente apêndice serão, em princípio, preparados sem referência à sua origem ou à classificação UE. O Grupo Consultivo da Política de Segurança da Comissão poderá recomendar:

   — a utilização de uma marcação específica ou de um nome de código,

   — a utilização de um sistema de classificação específico que associe o grau de sensibilidade das informações às medidas de controlo a aplicar pelo beneficiário em matéria de métodos de transmissão de documentos.

7. O ►**M2** membro da Comissão responsável pelas questões de segurança ◄ enviará o parecer do Grupo Consultivo da Política de Segurança da Comissão à Comissão, para decisão.

8. Uma vez que a divulgação de informações classificadas da UE e os procedimentos práticos de execução tenham sido aprovados pela Comissão, a►**M2** Direcção de Segurança da Comissão ◄ estabelecerá os contactos necessários com os órgãos de segurança do Estado ou organização interessados, a fim de facilitar a aplicação das medidas de segurança previstas.

9. O Membro da Comissão responsável pelas questões de segurança informará os Estados-Membros da natureza e da classificação da informação, estabelecendo uma lista das organizações e países aos quais pode ser divulgada, conforme decisão da Comissão.

▼B

10. A►**M2** Direcção de Segurança da Comissão ◄ tomará todas as medidas necessárias para facilitar a avaliação de eventuais prejuízos ou danos e a reapreciação dos procedimentos.

    A Comissão reexaminará a questão sempre que as condições de cooperação sejam alteradas.

DISPOSIÇÕES DE SEGURANÇA A APLICAR PELOS BENEFICIÁRIOS

11. A decisão da Comissão de autorizar a divulgação de informações classificadas da UE será comunicada aos Estados beneficiários ou às organizações internacionais, acompanhada de uma resenha detalhada das regras de protecção propostas pelo Grupo Consultivo da Política de Segurança da Comissão e aprovadas pela Comissão.

12. A decisão só entrará em vigor quando os beneficiários tiverem dado garantias por escrito de que:

    — apenas utilizarão as informações em causa para efeitos da cooperação decidida pela Comissão,

    — protegerão as informações conforme exigido pela Comissão.

13. Transmissão de documentos

    a) Os procedimentos práticos para a transmissão de documentos serão decididos de comum acordo entre a►**M2** Direcção de Segurança da Comissão ◄ e os órgãos de segurança dos Estados receptores ou das organizações internacionais. Haverá que especificar, em particular, os endereços precisos para onde os documentos deverão ser enviados;

    b) Os documentos com a classificação ►**M1** CONFIDENTIEL UE ◄ ou superior serão transmitidos em duplo envelope. No envelope interior será aposta a marcação específica ou o nome de código que tiver sido decidido, juntamente com uma menção da classificação especial aprovada para o documento. Para cada documento classificado será incluído um recibo, que não será ele próprio classificado, e onde se indicarão apenas as referências do documento (número de referência, data, número do exemplar) e a língua em que se encontra redigido, mas não o título;

    c) O envelope interior será em seguida colocado dentro do envelope exterior, que conterá um número de expedição para efeitos de recepção, mas que não ostentará qualquer classificação de segurança;

    d) Será sempre entregue aos mensageiros um recibo com o número de expedição.

14. Registo à chegada

    A autoridade nacional de segurança (NSA) do Estado destinatário ou a entidade sua homóloga que receber em nome do Governo desse Estado as informações classificadas enviadas pela Comissão, ou o gabinete de segurança da organização internacional receptora, abrirão um registo especial para inscrever as informações classificadas da UE após a sua recepção. Esse registo conterá colunas para a data de recepção, as referências do documento (data, número de referência e número do exemplar), a classificação, o título do documento, o nome ou título do destinatário, a data de envio do recibo e a data de devolução do documento à UE ou da sua destruição.

15. Utilização e protecção das informações classificadas recebidas

    a) As informações de nível ►**M1** SECRET UE ◄ serão tratadas por funcionários especificamente designados, autorizados a ter acesso a informações com este nível de classificação. Serão guardadas em armários de segurança de boa qualidade, que só possam ser abertos pela pessoa autorizada a aceder às informações que contêm. As zonas onde esses armários se encontram deverão ser guardadas em permanência, e será instalado um sistema de controlo para assegurar que só a elas tenham acesso as pessoas devidamente autorizadas. As informações de nível ►**M1** SECRET UE ◄ serão transmitidas por mala diplomática, por serviços de correio de segurança ou por uma rede de telecomunicações securizada. Um documento com a classificação ►**M1** SECRET UE ◄ só poderá ser copiado com autorização dada por escrito pela entidade de origem. Todos os exemplares serão registados e todos os seus movimentos serão anotados. Serão passados recibos para todas as operações relacionadas com documentos com a classificação ►**M1** SECRET UE ◄;

    b) As informações de nível ►**M1** CONFIDENTIEL UE ◄ serão tratadas por funcionários especificamente designados autorizados a tomar conhecimento do assunto em questão. Os documentos serão guardados em armários de segurança trancados colocados em zonas vigiadas;

▼B

As informações de nível ►M1 CONFIDENTIEL UE ◄ serão enviadas por mala diplomática, por correio militar ou por uma rede de telecomunicações securizada; o organismo receptor pode tirar cópias, sendo o seu número e destinatários inscritos num registo especial;

c) As informações de nível ►M1 RESTREINT UE ◄ serão tratadas em instalações que não sejam acessíveis a pessoal não autorizado e serão guardadas em contentores trancados. Os documentos podem ser transmitidos, em duplo envelope, pelos serviços públicos de correio, por correio registado, e, em situações de emergência no decurso de operações, pelas redes públicas de telecomunicações, sem protecção. Os receptores podem deles tirar cópias;

d) As informações não classificadas não requererão medidas de protecção especiais e poderão ser transmitidas pelo correio e pelas redes públicas de telecomunicações. Os destinatários podem dela tirar cópias.

16. Destruição

Os documentos que deixem de ser necessários devem ser destruídos. No caso dos documentos de nível ►M1 RESTREINT UE ◄ e ►M1 CONFIDENTIEL UE ◄, a sua destruição será averbada nos registos especiais. No caso dos documentos de nível ►M1 SECRET UE ◄, serão passados certificados de destruição, que deverão ser assinados por duas pessoas que tenham assistido à operação.

17. Quebras de segurança

Em caso de fuga ou suspeita de fuga de informações de nível ►M1 CONFIDENTIEL UE ◄ ou ►M1 SECRET UE ◄, a NSA do Estado ou o chefe dos serviços de segurança da organização conduzirão um inquérito sobre as circunstâncias dessa fuga. A►M2 Direcção de Segurança da Comissão ◄ será notificado dos resultados desse inquérito. Serão tomadas as medidas necessárias para corrigir procedimentos ou métodos de armazenagem inadequados, se tiverem sido estes a dar origem à fuga.

▼B

Apêndice 6

LISTA DE ABREVIATURAS

CCAM	Comissão Consultiva de Compras e Contratos
CrA	Autoridade Cripto
CISO	Responsável Central da Segurança Informática
COMPUSEC	Segurança Informática
COMSEC	Segurança das Comunicações
CSO	►M2 Direcção de Segurança da Comissão ◄
EUCI	Informações Classificadas da União Europeia
IA	Autoridade INFOSEC
INFOSEC	Segurança da Informação
IO	Proprietário da Informação
ISO	Organização Internacional de Normalização
IT	Tecnologia da Informação
LISO	Responsável Local de Segurança Informática
LSO	Responsável Local de Segurança
MSO	Responsável da Segurança da Reunião
NSA	Autoridade Nacional de Segurança
PC	Computador Pessoal
PESD	Política Europeia de Segurança e de Defesa
RCO	Responsável do Controlo do Registo
SAA	Autoridade de Acreditação de Segurança
SecOPS	Procedimentos Operacionais de Segurança
SSRS	Requisitos de Segurança Específicos do Sistema
TA	Autoridade TEMPEST
TSO	Proprietário dos Sistemas Técnicos

▼M3

ASD	Autoridade de segurança designada
CSE	Certificação de segurança da empresa
OPI	Oficial de protecção da instalação
CSP	Certificação de segurança pessoal
CAS	Cláusula adicional de segurança
GCS	Guia da classificação de segurança