Este documento constitui um instrumento de documentação e não vincula as instituições

►**B**

DECISÃO DO CONSELHO
de 19 de Março de 2001
que aprova as regras de segurança do Conselho

(2001/264/CE)

(JO L 101 de 11.4.2001, p. 1)

Alterada por:

		Jornal Oficial		
		n.º	página	data
►**M1**	Decisão 2004/194/CE do Conselho de 10 de Fevereiro de 2004	L 63	48	28.2.2004

▼B

DECISÃO DO CONSELHO

de 19 de Março de 2001

que aprova as regras de segurança do Conselho

(2001/264/CE)

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia e, nomeadamente, o n.º 3 do seu do artigo 207.º,

Tendo em conta a Decisão 2000/396/CE, CECA, Euratom do Conselho, de 5 de Junho de 2000, que aprova o Regulamento Interno do Conselho ([1]) e, nomeadamente, o seu artigo 24.º,

Considerando o seguinte:

(1) A fim de desenvolver as actividades do Conselho em áreas que exigem confidencialidade, é necessário estabelecer um regime geral de segurança que abranja o Conselho, o seu Secretariado-Geral e os Estados-Membros.

(2) Esse regime deverá combinar num texto único as matérias abrangidas por todas as decisões e disposições anteriores nesta matéria.

(3) Na realidade, a maior parte das informações da UE com classificação «CONFIDENTIEL UE» ou superior dirá respeito à política comum de segurança e de defesa.

(4) A fim de salvaguardar a eficácia do regime de segurança assim estabelecido, os Estados-Membros devem ser associados ao seu funcionamento, tomando as medidas nacionais necessárias para que as disposições da presente decisão sejam respeitadas sempre que as suas autoridades competentes e agentes tratem informações classificadas da UE.

(5) O Conselho congratula-se com a intenção da Comissão de introduzir até à data em que a presente decisão passar a ser aplicável um regime global alinhado pelos anexos da presente decisão, com vista a assegurar o bom funcionamento do processo de tomada de decisões a nível da União.

(6) O Conselho sublinha a importância de associar, sempre que preciso, o Parlamento Europeu e a Comissão às regras e normas de confidencialidade necessárias para proteger os interesses da União e dos seus Estados-Membros.

(7) A presente decisão é aprovada sem prejuízo do artigo 255.º do Tratado nem dos instrumentos que o aplicam.

(8) A presente decisão é aprovada sem prejuízo das práticas existentes nos Estados-Membros quanto a informar os Parlamentos nacionais das actividades da União,

DECIDE:

Artigo 1.º

São aprovadas as regras de segurança do Conselho constantes do anexo.

Artigo 2.º

1. O Secretário-Geral/Alto Representante 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 no interior do Secretariado-Geral do Conselho (adiante designado «SGC») pelos funcionários e outros agentes do SGC, por prestadores de

([1]) JO L 149 de 23.6.2000, p. 21.

▼B

serviços ao SGC e pelo pessoal destacado para o SGC, bem como nas instalações do Conselho e nos organismos descentralizados da UE ([1]).

2. Os Estados-Membros tomam as medidas adequadas, nos termos das disposições nacionais, para assegurar que, quando forem tratadas informações classificadas da UE, as regras a que se refere o artigo 1.º sejam cumpridas nos seus serviços e instalações pelos:

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

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) Pessoal, quer prestadores de serviços quer pessoal destacado, dos Estados-Membros que trate informações classificadas da UE.

Os Estados-Membros informam imediatamente o SGC dessas medidas.

3. As medidas a que se referem os n.ºs 1 e 2 serão tomadas antes de 30 de Novembro de 2000.

Artigo 3.º

Em conformidade com os princípios básicos e com as normas mínimas de segurança contidas na parte I do anexo, o Secretário-Geral/Alto Representante pode tomar medidas nos termos da parte II, secção I, pontos 1 e 2, do anexo.

Artigo 4.º

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

a) A Decisão 98/319/CE do Conselho, de 27 de Abril de 1998, relativa às modalidades segundo as quais os funcionários e agentes do Secretariado-Geral do Conselho podem ser autorizados a aceder a informações classificadas na posse do Conselho ([2]);

b) A Decisão do Secretário-Geral/Alto Representante, de 27 de Julho de 2000, relativa às medidas de protecção das informações classificadas aplicáveis ao Secretariado-Geral do Conselho ([3]);

c) A Decisão n.º 433/97 do Secretário-Geral do Conselho, de 22 de Maio de 1997, relativa ao procedimento de habilitação de segurança dos funcionários encarregados do funcionamento do sistema Cortesy.

Artigo 5.º

1. A presente decisão produz efeitos a partir da data da sua publicação.

2. A presente decisão é aplicável a partir de 1 de Dezembro de 2001.

([1]) Ver conclusões do Conselho de 10 de Novembro de 2000.
([2]) JO L 140 de 12.5.1998, p. 12.
([3]) JO C 239 de 23.8.2000, p. 1.

▼B

ANEXO

REGRAS DE SEGURANÇA DO CONSELHO DA UNIÃO EUROPEIA

▼B

SUMÁRIO

PARTE I

Princípios de base e normas mínimas de segurança . . . . . .

PARTE II . . . . . .

SECÇÃO I

Organização da segurança no Conselho da União Europeia . . . . . .

SECÇÃO II

Classificações e marcações . . . . . .

SECÇÃO III

Gestão das classificações . . . . . .

SECÇÃO IV

Segurança física . . . . . .

SECÇÃO V

Regras gerais sobre o princípio da necessidade de ter conhecimento e sobre habilitação de segurança

SECÇÃO VI

Procedimento para a habilitação de segurança dos funcionários e outros agentes do SGC . . . . . .

SECÇÃO VII

Elaboração, distribuição, transmissão, armazenagem e destruição de material classificado da UE . . . .

SECÇÃO VIII

Registos TRÈS SECRET UE/EU TOP SECRET . . . . . .

SECÇÃO IX

Medidas de segurança a aplicar por ocasião de reuniões específicas realizadas fora das instalações do Conselho e que envolvam questões de alta sensibilidade . . . . . .

SECÇÃO X

Quebras de segurança e fugas de informações classificadas da UE . . . . . .

SECÇÃO XI

Protecção das informações tratadas em sistemas informáticos e de comunicação . . . . . .

SECÇÃO XII

Divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais . .

Apêndices

Apêndice 1

Lista das Autoridades Nacionais de Segurança . . . . . .

Apêndice 2

Comparação das classificações nacionais de segurança . . . . . .

Apêndice 3

Guia prático de classificação . . . . . .

Apêndice 4

Orientações para a divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais — cooperação de nível 1 . . . . . .

Apêndice 5

Orientações para a divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais — cooperação de nível 2 . . . . . .

Apêndice 6

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

▼B

PARTE I

PRINCÍPIOS DE BASE E NORMAS MÍNIMAS DE SEGURANÇA

INTRODUÇÃO

1. As presentes disposições estabelecem os princípios de base e as normas mínimas de segurança que deverão ser respeitadas pelo Conselho, pelo Secretariado-Geral do Conselho (adiante designado «SGC»), pelos Estados-Membros e pelos organismos descentralizados da União Europeia (adiante designados «organismos descentralizados da UE»), de modo a que a segurança seja salvaguardada e possa ser garantida a existência de uma norma comum de protecção.

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

3. Em toda a presente regulamentação, entende-se por:

   a) «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 físico no qual tenha sido registada informação;

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

4. A segurança 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 UE tratadas em sistemas e redes de comunicações e informações das ameaças à sua integridade e disponibilidade;

   c) Salvaguardar as instalações que albergam informações da UE dos riscos de sabotagem ou de danos intencionais;

   d) No caso de uma falha, avaliar os danos causados, limitar as suas consequências e adoptar as medidas necessárias para as remediar.

5. As bases da boa segurança são:

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

      i) pela recolha e registo de informações sobre espionagem, sabotagem, terrorismo e outras actividades subversivas, e

      ii) por informar e de aconselhar o seu Governo e, através dele, o Conselho, 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 do SGC, 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 sobre os meios de protecção contra essas ameaças;

   c) Uma colaboração regular entre ministérios, organismos e os serviços competentes do SGC, a fim de estabelecer e recomendar, conforme adequado:

      i) quais informações, recursos e instalações deverão ser protegidos, e

      ii) as normas comuns de protecção.

6. 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 estes 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 o excesso de classificação. O sistema de classificação constitui o instrumento para pôr em prática estes princípios; deveria 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 que albergam informações classificadas e aos pontos mais sensíveis no interior destas instalações.

▼B

PRINCÍPIOS DE BASE

7. **As medidas de segurança devem:**

   a) Abranger todas as pessoas que tenham acesso a informações classificadas, os suportes que contenham as informações classificadas, os locais que abrigam essas informações e as instalações importantes;

   b) Ser concebidas para detectar as pessoas cuja posição pode pôr em perigo a segurança das informações classificadas e das instalações importantes que albergam 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 são difundidas às pessoas que delas devem tomar conhecimento, princípio que é fundamental a todos os aspectos da segurança;

   e) Assegurar a integridade (ou seja, prevenir a deturpação, a alteração não autorizada ou a supressão não autorizada) e a disponibilidade (ou seja, assegurar que o acesso não é negado às pessoas que têm necessidade e autorização de acesso) de todas as informações, tanto classificadas como não classificadas, e especialmente das informações armazenadas, tratadas ou transmitidas de forma electromagnética.

ORGANIZAÇÃO DA SEGURANÇA

Normas mínimas comuns

8. O Conselho e cada Estado-Membro deverão assegurar que são cumpridas normas mínimas comuns de segurança em todos os ministérios e/ou serviços administrativos, outras instituições da UE, organismos e prestadores de serviços de forma a que as informações classificadas da UE possam ser transmitidas com a certeza de que serão tratadas com igual cuidado. Estas normas mínimas devem incluir critérios para a habilitação do pessoal em matéria de segurança e procedimentos para a protecção das informações classificadas da UE.

SEGURANÇA DO PESSOAL

Habilitação de segurança

9. Todas as pessoas que necessitam de ter acesso a informações com classificação 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 de pessoas cujas funções envolvem o funcionamento técnico ou a manutenção dos sistemas de comunicações e de informação que contenham informações classificadas. Esta habilitação de segurança deverá ser concebida de forma a determinar se esses indivíduos:

   a) Têm uma lealdade inquestionável;

   b) Possuem carácter e discrição que não deixe dúvidas quanto à sua integridade no tratamento das informações classificadas; ou

   c) Podem ser vulneráveis a pressões de fontes estrangeiras ou outras, por exemplo, devido a uma anterior residência ou uma associação anterior que possam constituir um risco para a segurança.

   No procedimento de habilitação de segurança, será dada especial atenção às pessoas:

   d) Que devem ser autorizadas a aceder às informações classificadas TRÈS SECRET UE/EU TOP SECRET;

   e) Que ocupam posições que implicam o acesso regular a um volume considerável de informações SECRET UE;

   f) Cujas funções lhes dão especial acesso a sistemas de comunicações ou informações de importância capital para as missões e, por conseguinte, a oportunidade de obter um acesso não autorizado a grandes quantidades de informações classificadas da UE ou de prejudicar seriamente a missão 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.

10. As pessoas que não possuam uma razão válida para tomar conhecimento de informações classificadas da UE e sejam empregues em funções nas quais possam ter acesso a esse tipo de informações (por exemplo mensageiros,

▼B

agentes de segurança, pessoal de manutenção e de limpeza, etc.) deverão ser previamente objecto de uma habilitação de segurança adequada.

Registos do pessoal habilitado

11. Todos os serviços, órgãos ou estabelecimentos que tratem informações classificadas da UE ou que alberguem sistemas de comunicações ou informações de importância capital para as missões deverão manter um registo do seu pessoal a quem foi concedida habilitação de segurança. Todas as habilitações deverão ser controladas oportunamente para verificar se são adequadas às funções actuais da pessoa em questão; as habilitações serão reexaminadas com carácter prioritário sempre que haja nova informação que indique que a continuação do seu trabalho com informações classificadas já não é compatível com os interesses da segurança. O registo das habilitações será mantido pelo chefe de segurança do serviço, órgão ou estabelecimento em questão.

Formação do pessoal em matéria de segurança

12. Todo o pessoal empregue em funções nas quais possa ter acesso a informações classificadas receberá uma formação completa ao assumir funções, e a intervalos regulares, sobre a necessidade da segurança e os meios de a implementar. Será útil exigir que todo o pessoal em questão ateste por escrito que compreende inteiramente as regras de segurança pertinentes para as suas funções.

Responsabilidades dos gestores

13. Os gestores deverão saber quais os membros do seu pessoal que trabalham com informações classificadas ou que têm acesso a sistemas de comunicações ou informações de importância capital para as missões, assim como deverão registar e relatar quaisquer incidentes ou aparentes vulnerabilidades susceptíveis de afectar a segurança.

Estatuto de segurança do pessoal

14. Serão definidos procedimentos para garantir que, ao ter conhecimento de informações desfavoráveis relativamente a um indivíduo, se possa saber se esse indivíduo trabalha com informações classificadas ou tem acesso a sistemas de comunicações ou informações de importância capital para as missões, e que seja informada a autoridade competente. Se ficar estabelecido que tal indivíduo constitui um risco para a segurança, a pessoa em questão deverá ser afastada ou proibida de desempenhar funções em que possa pôr em perigo a segurança.

SEGURANÇA FÍSICA

Necessidade de protecção

15. 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 ou para o material existente. Por conseguinte, haverá que evitar com cuidado tanto a sobreclassificação como a sub-classificação, bem como rever regularmente a classificação. 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, envio e eliminação de informações e material que necessitem de protecção.

Controlo das instalações

16. Antes de abandonar os locais que contêm informações classificadas da UE, as pessoas responsáveis pela sua guarda devem assegurar que estas informações se encontram guardadas em condições de segurança e que todos os dispositivos de segurança foram activados (fechaduras, alarmes, etc.). Deverão ser efectuados outros controlos independentes após as horas de serviço.

Segurança dos edifícios

17. Os edifícios que albergam informações classificadas da UE ou sistemas de comunicações e de informação de importância capital para as missões devem ser protegidos contra o acesso não autorizado. 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, controlos e patrulhas de segurança, sistemas de alarme, sistemas de detecção de intrusos e cães de guarda, dependerão:

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

▼B

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

c) Da natureza física e localização do edifício.

18. A natureza da protecção concedida aos sistemas de comunicações e de informação deverá igualmente depender de uma avaliação do que é necessário proteger e dos danos potenciais caso haja uma falha na segurança, consoante a natureza física e a localização do edifício em que o sistema se encontra, e consoante a localização do sistema no interior do edifício.

Planos de emergência

19. Deverão ser elaborados previamente planos pormenorizados para a protecção das informações classificadas durante uma emergência local ou nacional.

SEGURANÇA DAS INFORMAÇÕES (INFOSEC)

20. A INFOSEC diz respeito à identificação e aplicação das medidas de segurança destinadas a proteger as informações tratadas, armazenadas ou enviadas através de sistemas de comunicações e informações ou de outros sistemas electrónicos contra a perda de confidencialidade, integridade ou disponibilidade, quer acidental quer intencional. Deverão ser tomadas contramedidas adequadas para impedir o acesso às informações da UE por utentes não autorizados, para impedir a recusa de acesso às informações da UE aos utentes autorizados, e para impedir a deturpação, a alteração ou a supressão não autorizadas de informações da UE.

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

21. As precauções físicas de protecção de instalações importantes que albergam informações classificadas constituem a melhor salvaguarda contra a sabotagem e contra danos intencionais, e a habilitação de segurança do pessoal não constitui por si só uma alternativa eficaz. O órgão nacional competente deverá recolher informações relativas às actividades de espionagem, sabotagem, terrorismo ou outras actividades subversivas.

DIVULGAÇÃO DE INFORMAÇÕES CLASSIFICADAS A PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

22. A decisão de divulgar informações classificadas da UE provenientes do Conselho a um país terceiro ou uma organização internacional será tomada pelo Conselho. Se a origem da informação que se deseja divulgar não for o Conselho, este último deverá obter o consentimento da entidade de origem para a sua divulgação. Se não for possível identificar a entidade de origem, o Conselho assumirá a responsabilidade em seu lugar.

23. Se o Conselho receber informações classificadas de países terceiros e de organizações internacionais ou de terceiros, essas informações beneficiarão da protecção adequada à sua classificação, que será equivalente às normas definidas na presente regulamentação para as informações classificadas da UE, ou a normas mais elevadas que sejam eventualmente solicitadas pelo terceiro que divulgue a informação. Deverão ser previstos controlos mútuos.

24. Os princípios acima enunciados serão postos em prática segundo as disposições de aplicação constantes da parte II.

▼B

PARTE II

SECÇÃO I

ORGANIZAÇÃO DA SEGURANÇA NO CONSELHO DA UNIÃO EUROPEIA

Secretário-Geral/Alto Representante

1. O Secretário-Geral/Alto Representante:

   a) Executa a política de segurança do Conselho;

   b) Estuda os problemas de segurança que lhe forem submetidos pelo Conselho ou pelas suas instâncias competentes;

   c) Analisa as questões que envolvam alterações da política de segurança do Conselho, em estreita ligação com as autoridades nacionais de segurança (ou outras autoridades competentes) dos Estados-Membros (adiante designadas «ANS»). O apêndice 1 contém uma lista destas autoridades.

2. Em especial, o Secretário-Geral/Alto Representante é responsável:

   a) Pela coordenação de todos os aspectos da segurança relacionados com as actividades do Conselho;

   b) Por solicitar a cada Estado-Membro a criação de um registo central TRÈS SECRET UE/EU TOP SECRET e exigir que seja igualmente criado um registo deste tipo, se necessário, nos organismos descentralizados da UE;

   c) Por dirigir às autoridades designadas dos Estados-Membros pedidos para que as ANS procedam à habilitação de segurança do pessoal empregue no SGC, nos termos da secção VI;

   d) Por investigar ou mandar investigar qualquer fuga de informações classificadas da UE que, segundo os indícios evidentes, tenha ocorrido no SGC ou em qualquer dos organismos descentralizados da UE;

   e) Por solicitar às autoridades de segurança competentes que iniciem investigações quando se afigure que houve fuga de informações classificadas da UE fora do SGC ou dos organismos descentralizados da UE, e coordenar as investigações quando se encontrar envolvida mais do que uma autoridade de segurança;

   f) Por efectuar, juntamente e de acordo com a ANS competente, exames periódicos das disposições de segurança destinadas à protecção de informações classificadas da UE nos Estados-Membros;

   g) Por manter uma ligação estreita com todas as autoridades de segurança competentes, a fim de alcançar uma coordenação global da segurança;

   h) Por proceder a uma constante revisão da política e dos procedimentos de segurança do Conselho e, se necessário, pela elaboração de recomendações adequadas. Neste sentido, deverá apresentar ao Conselho o plano anual de inspecção elaborado pelo Serviço de Segurança do SGC.

Comité de Segurança do Conselho

3. Deve ser criado um Comité de Segurança. Este Comité é composto por representantes das ANS de cada Estado-Membro e é presidido pelo Secretário-Geral/Alto Representante ou por um seu delegado. Os representantes dos organismos descentralizados da UE podem também ser convidados a participar nas reuniões quando forem tratadas questões que lhes digam respeito.

4. O Comité de Segurança reúne-se conforme as instruções do Conselho, a pedido do Secretário-Geral/Alto Representante ou de uma ANS. Compete ao comité analisar e avaliar todas as questões de segurança relacionadas com os procedimentos do Conselho, e apresentar recomendações ao Conselho, se necessário. Relativamente à actividade do SGC, compete ao comité fazer recomendações sobre questões de segurança ao Secretário-Geral/Alto Representante.

Serviço de Segurança do Secretariado-Geral do Conselho

5. Para o cumprimento das responsabilidades referidas nos n.os 1 e 2, o Secretário-Geral/Alto Representante tem à sua disposição o Serviço de Segurança do SGC para a coordenação, supervisão e implementação das medidas de segurança.

6. O chefe do Serviço de Segurança do SGC é o principal conselheiro do Secretário-Geral/Alto Representante em questões de segurança e desempenha as funções de secretário do Comité de Segurança. Neste sentido, dirige a actualização das regras de segurança e coordena as medidas de

▼B

segurança com as autoridades competentes dos Estados-Membros e, se necessário, com organizações internacionais ligadas ao Conselho por acordos de segurança. Para o efeito, age como oficial de ligação.

7. O chefe do Serviço de Segurança do SGC é responsável pela aprovação das redes e sistemas informáticos no SGC. O chefe do Serviço de Segurança e a ANS competente decidem em conjunto, sempre que necessário, a aprovação de redes e sistemas informáticos que envolvam o SGC, os Estados-Membros, os organismos descentralizados da UE e/ou terceiros (Estados ou organizações internacionais).

Organismos descentralizados da UE

8. Cada director de um organismo descentralizado da UE é responsável pela implementação da segurança no seu organismo. Normalmente, deverá nomear um membro do seu pessoal como responsável deste domínio perante si. Este membro do pessoal será designado como oficial de segurança.

Estados-Membros

9. Cada Estado-Membro deve designar uma ANS responsável pela segurança das informações classificadas da UE ([1]).

10. No âmbito de cada Estado-Membro, a ANS correspondente é responsável:

   a) Pela segurança das informações classificadas da UE na posse de qualquer serviço, órgão ou organismo nacional, público ou privado, quer dentro quer fora do país;

   b) Por autorizar a criação de registos TRÈS SECRET UE/EU TOP SECRET (esta autoridade pode ser delegada no oficial de controlo de um registro central TRÈS SECRET UE/EU TOP SECRET);

   c) Pela inspecção periódica das disposições de segurança para a protecção das informações classificadas da UE;

   d) Por garantir que todos os nacionais e estrangeiros empregues nos serviços, órgãos ou organismos nacionais que possam ter acesso a informações da UE classificadas de TRÈS SECRET UE/UE TOP SECRET, SECRET UE e CONFIDENTIEL UE foram objecto de uma habilitação de segurança;

   e) Por elaborar os planos de segurança considerados necessários para impedir que as informações classificadas da UE possam ser comunicadas a pessoas não autorizadas.

Inspecções mútuas de segurança

11. O Serviço de Segurança do SGC e as ANS competentes deverão efectuar conjuntamente e de comum acordo inspecções periódicas das disposições de segurança para a protecção das informações classificadas da UE no SGC e nas respectivas Representações Permanentes dos Estados-Membros junto da União Europeia, bem como nas instalações dos Estados-Membros nos edifícios do Conselho ([2]).

12. O Serviço de Segurança do SGC ou, a pedido do Secretário-Geral, a ANS do Estado-Membro de acolhimento efectuarão inspecções periódicas das disposições de segurança para a protecção das informações classificadas da UE nos organismos descentralizados da UE.

([1]) Consta do apêndice 1 uma lista das ANS responsáveis pela segurança das informações classificadas da UE.

([2]) Sem prejuízo da Convenção de Viena de 1961 sobre as relações diplomáticas.

▼B

SECÇÃO II

CLASSIFICAÇÕES E MARCAÇÕES

NÍVEIS DE CLASSIFICAÇÃO ([1])

A informação será classificada aos seguintes níveis:

1. TRÈS 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.

2. 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.

3. 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.

4. 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.

MARCAÇÕES

5. Poderá ser utilizada uma marcação de aviso para indicar o domínio abrangido pelo documento ou uma distribuição específica com base no princípio da «necessidade de ter conhecimento».

6. A marcação ESDP/PESD será aposta nos documentos e respectivas cópias que digam respeito à segurança e defesa da União ou de um ou vários dos seus Estados-Membros, ou que digam respeito à gestão militar ou civil das crises.

7. Certos documentos, nomeadamente os relacionados com sistemas informáticos podem ostentar uma marcação adicional com medidas suplementares de segurança definidas na regulamentação adequada.

APOSIÇÃO DA CLASSIFICAÇÃO E DAS MARCAÇÕES

8. A classificação e as marcações serão apostas do seguinte modo:

   a) Nos documentos RESTREINT UE, por meios mecânicos/electrónicos;

   b) Nos documentos CONFIDENTIEL UE, por meios mecânicos e manualmente ou por impressão em papel pré-impresso, consignado num registo;

   c) Nos documentos SECRET UE e TRÈS SECRET UE/EU TOP SECRET, por meios mecânicos e manualmente.

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

▼B

SECÇÃO III

GESTÃO DAS CLASSIFICAÇÕES

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

2. A responsabilidade pela classificação das informações ou por qualquer subsequente desgraduação ou desclassificação ([1]) incumbe exclusivamente à entidade de origem.

   Os funcionários e outros agentes do SGC só poderão proceder à classificação, desgraduação ou desclassificação das informações mediante instruções do seu director-geral, ou com o acordo deste.

3. Os procedimentos pormenorizados para o tratamento dos documentos classificados devem ser concebidos de forma a garantir que estes estarão sujeitos a uma protecção adequada às informações que contêm.

4. O número de pessoas autorizadas a produzir documentos TRÈS SECRET UE/EU TOP SECRET deverá ser o mais reduzido possível, e os seus nomes deverão constar de uma lista elaborada pelo SGC, por cada um dos Estados-Membros e, se necessário, por cada organismo descentralizado da UE.

APLICAÇÃO DAS CLASSIFICAÇÕES

5. A classificação de um documento será determinada pelo nível de sensibilidade do seu conteúdo, conforme a definição constante dos pontos 1 a 4 da secção II. É importante que a classificação seja utilizada de forma correcta e comedida. Esta última disposição aplica-se especialmente à classificação TRÈS SECRET UE/EU TOP SECRET.

6. O autor de um documento a classificar deverá ter em mente as disposições atrás indicadas e abster-se de proceder a uma sobre ou sub classificação.

   Embora uma alta classificação pareça, à primeira vista, capaz de garantir mais protecção a um documento, uma rotina de sobreclassificação pode dar lugar a uma perda de confiança na validade do sistema de classificação.

   Por outro lado, não se deverão subclassificar documentos com o fim de evitar as restrições relacionadas com a protecção.

   Consta do apêndice 3 um guia prático para a classificação.

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

8. A classificação de uma carta ou nota de envio será tão elevada quanto a mais alta classificação do seu anexo. O autor deverá indicar claramente a que nível deverá ser classificada tal carta ou nota quando separada do anexo.

DESGRADUAÇÃO E DESCLASSIFICAÇÃO

9. Os documentos classificados da UE só podem ser desgraduados ou desclassificados com a autorização do autor e, se necessário, após discussão com as outras partes interessadas. A desgraduação ou a desclassificação deverão ser confirmadas por escrito. A entidade de origem — Instituição, Estado-Membro, serviço, organização sucessora ou autoridade superior — 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 uma cópia do documento.

10. Se possível, a entidade de origem deverá especificar nos documentos classificados a data ou período após o qual o seu conteúdo pode ser objecto de uma desgraduação ou desclassificação. Caso contrário, deverá passar em revista os documentos de cinco em cinco anos, no máximo, a fim de verificar se é necessário manter a classificação original.

([1]) Desgraduação (*déclassement*) significa uma redução do grau de classificação; desclassificação (*déclassification*) significa a perda da confidencialidade, ou seja, a remoção da classificação.

▼B

SECÇÃO IV

SEGURANÇA FÍSICA

GERAL

1. O principal objectivo das medidas de segurança física consiste em impedir o acesso de pessoas não autorizadas às informações e /ou material classificados da UE.

REQUISITOS DE SEGURANÇA

2. Todas as instalações, áreas, edifícios, escritórios, salas, sistemas de comunicações e de informações, etc., onde estejam armazenados e/ou sejam tratados informações e material classificados da UE deverão ser protegidos por medidas adequadas de segurança física.

3. Ao decidir o grau de segurança física necessário, deverão ser tomados em consideração todos os factores relevantes 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 armazenadas;

   c) A avaliação local da ameaça que constituem os serviços de espionagem que têm como alvo a UE, os Estados-Membros e/ou outras instituições ou terceiros detentores de informações classificadas da UE, os actos de sabotagem, o terrorismo e outras actividades subversivas e/ou criminosas.

4. 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 funcionários desleais («o espião interno»);

   c) Impedir o acesso às informações classificadas da UE aos funcionários e outros agentes do SGC, de ministérios e outros serviços dos Estados-Membros e/ou de outras instituições ou terceiros que não têm necessidade de tomar conhecimento das mesmas.

MEDIDAS DE SEGURANÇA FÍSICA

Áreas de segurança

5. As áreas onde são tratadas e armazenadas informações com a classificação CONFIDENTIEL UE ou superior deverão ser organizadas e estruturadas de modo a corresponder a uma das seguintes categorias:

   a) Área de segurança de classe I: uma área onde as informações com a classificação 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,

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

      iii) uma indicação da classificação das informações normalmente tratadas ou armazenadas 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 CONFIDENTIEL UE ou superior são tratadas e armazenadas de tal modo que possam ser protegidas contra o acesso por pessoas não autorizadas através de meios de controlo estabelecidos internamente, ou seja, instalações que contenham gabinetes nos quais são regularmente tratadas ou armazenadas informações com a classificação 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 entrada 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 controlos equivalentes que impeçam o acesso não autorizado às informações classificadas da UE e a entrada sem controlo nas áreas sujeitas a inspecções técnicas de segurança.

▼B

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

Áreas administrativas

6. Poderão ser estabelecidas áreas administrativas de menor segurança adjacentes ou envolventes das áreas de segurança da classe I ou II. Essas áreas administrativas deverão ter um perímetro visivelmente definido que permita o controlo do pessoal e dos veículos. Nas áreas administrativas só poderão ser tratadas e armazenadas informações com a classificação RESTREINT UE.

Controlos de entradas e saídas

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

Patrulhas de guardas

8. As patrulhas das áreas de segurança da classe I e II deverão ter lugar fora das horas normais de serviço, com o objectivo de proteger os bens da UE contra fugas, danos ou perdas. A frequência das patrulhas será determinada pelas circunstâncias locais mas, de um modo geral, estas deverão ter lugar de duas em duas horas.

Contentores de segurança e casas-fortes

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

   — classe A: contentores aprovados a nível nacional para guardar informações classificadas TRÈS SECRET UE/EU TOP SECRET nas áreas de segurança da classe I ou II,

   — classe B: contentores aprovados a nível nacional para guardar informações classificadas SECRET UE e CONFIDENTIEL UE nas áreas de segurança da classe I ou II,

   — classe C: mobiliário de escritório adequado para guardar informações classificadas RESTREINT UE.

10. As paredes, chãos, tectos, portas e fechaduras das casas-fortes construídas nas áreas de segurança da classe I ou II, e de todas as áreas de segurança da classe I onde são guardadas em prateleiras abertas ou apresentadas em quadros, mapas, etc., informações com classificação CONFIDENTIEL UE ou superior deverão ser certificadas por uma ANS como possuindo um grau de protecção equivalente à classe do contentor de segurança aprovado para guarda de informações com a mesma classificação.

Fechaduras

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

   — grupo A: contentores aprovados a nível nacional para a classe A,

   — grupo B: contentores aprovados a nível nacional para a classe B,

   — grupo C: mobiliário de escritório apenas adequado para a classe C.

Controlo das chaves e das fechaduras de segredo

12. As chaves dos contentores de segurança não deverão ser levadas para fora do edifício. As combinações dos contentores de segurança deverão ser memorizadas pelas pessoas que precisam de as conhecer. Em caso de emergência, o oficial de segurança do organismo em questão deverá possuir duplos das chaves e um registo escrito de cada combinação; estes últimos serão guardados em envelopes separados, opacos e fechados. As chaves habituais, os duplos das chaves e as combinações deverão ser mantidos em contentores de segurança distintos. Estas chaves e as combinações deverão ser objecto de uma protecção de segurança pelo menos equivalente à do material ao qual dão acesso.

▼B

13. 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 haja uma mudança de pessoal;

    c) Sempre que tenha ocorrido ou haja suspeita de ter ocorrido uma fuga;

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

Dispositivos de detecção de intrusos

14. Quando forem utilizados sistemas de alarme, circuitos fechados de televisão ou outros dispositivos eléctricos para proteger as informações classificadas da UE, deverá existir uma central eléctrica de emergência capaz de garantir o funcionamento contínuo do sistema em caso de interrupção no fornecimento de energia. Outro requisito básico é o de que o mau funcionamento ou o manuseamento não autorizado desses sistemas ponha em funcionamento um alarme ou outro dispositivo de aviso fiável que advirta o pessoal de vigilância.

Equipamento aprovado

15. As ANS deverão manter, a partir dos seus próprios recursos ou de fontes bilaterais, listas actualizadas por tipo e modelo do equipamento de segurança que aprovaram em várias circunstâncias e condições específicas para a protecção directa ou indirecta de informações classificadas. O Serviço de Segurança do SGC deverá manter uma lista similar baseada, nomeadamente, nas informações prestadas pelas ANS. Os organismos descentralizados da UE deverão consultar o Serviço de Segurança dos SGC e, se necessário, a ANS do seu Estado-Membro de acolhimento antes de adquirirem equipamento de segurança.

Protecção física das fotocopiadoras e dos fax

16. As fotocopiadoras e os fax deverão ser fisicamente protegidos de modo a garantir que só são utilizados por pessoas autorizadas para o fazer e que todos os produtos classificados estão sujeitos aos controlos adequados.

PROTECÇÃO CONTRA VISÃO E ESCUTA NÃO AUTORIZADAS

Visão não autorizada

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

Escuta não autorizada

18. Os gabinetes e as áreas em que são regularmente debatidas informações com classificação SECRET UE ou superior deverão ser protegidos contra actos passivos e activos de escuta não autorizada, sempre que o risco assim o justifique. A avaliação do risco destes actos deverá ser da responsabilidade da autoridade competente de segurança após consulta, se necessário, com as ANS.

19. A fim de definir as medidas de protecção que deverão ser tomadas nas instalações sensíveis à escuta passiva (por exemplo, isolamento das paredes, portas, chãos e tectos, medida dos níveis sonoros comprometedores) bem como às escutas activas (por exemplo, busca de microfones), o Serviço de Segurança do SGC poderá pedir assistência de peritos das ANS. Os oficiais de segurança dos organismos descentralizados da UE podem solicitar que sejam efectuadas inspecções técnicas pelo Serviço de Segurança do SGC e/ /ou a assistência de peritos das ANS.

20. 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 a nível SECRET UE ou a um nível superior poderão ser verificados por especialistas técnicos de segurança das ANS, a pedido do oficial de segurança competente.

ÁREAS TECNICAMENTE SEGURAS

21. 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 aprovado 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 de suspeita dessa possibilidade.

22. Será mantido um inventário pormenorizado do equipamento e mobiliário a fim de controlar os respectivos movimentos. Não será introduzido nessa

▼B

área 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, deverá ser evitada a instalação de linhas de comunicação nas áreas tecnicamente seguras.

▼B

SECÇÃO V

REGRAS GERAIS SOBRE O PRINCÍPIO DA NECESSIDADE DE TER CONHECIMENTO E SOBRE HABILITAÇÃO DE SEGURANÇA

1. O acesso a informações classificadas da UE só será autorizado às pessoas que dela devem tomar conhecimento para o desempenho das suas tarefas ou missões. O acesso às informações classificadas TRÈS SECRET UE/EU TOP SECRET, SECRET UE e CONFIDENTIEL UE só será autorizado às pessoas que tenham habilitação de segurança adequada.

2. A responsabilidade por determinar quem deve tomar conhecimento incumbirá ao SGC, aos organismos descentralizados da UE e ao ministério ou serviço de um Estado-Membro onde a pessoa em questão deverá trabalhar, conforme os requisitos da tarefa.

3. A habilitação de segurança será da responsabilidade do empregador do funcionário, com base nos procedimentos relevantes aplicáveis. No que se refere aos funcionários e outros agentes do SGC, o procedimento para a habilitação de segurança é o previsto na secção VI.

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

   O certificado de segurança para uma dada classificação poderá conferir ao seu detentor acesso a informações com classificação inferior.

4. As pessoas que não sejam funcionários nem outros agentes do SGC ou dos Estados-Membros, por exemplo Membros, funcionários ou agentes de Instituições da UE com quem seja necessário debater, ou a quem seja necessário dar conhecimento de informações classificadas da UE devem possuir uma habilitação de segurança para efeitos de informações classificadas da UE e ser informados da suas responsabilidades em matéria de segurança. A mesma regra se deverá aplicar, em circunstâncias similares, aos prestadores de serviços, aos peritos ou aos consultores.

REGRAS ESPECÍFICAS SOBRE O ACESSO ÀS INFORMAÇÕES CLASSIFICADAS TRÈS SECRET UE/EU TOP SECRET

5. Todas as pessoas que devam ter acesso a informações classificadas TRÈS SECRET UE/EU TOP SECRET deverão ser previamente sujeitas a um inquérito de segurança tendo em vista o acesso a essas informações.

6. Todas as pessoas que devem ter acesso a informações classificadas TRÈS SECRET UE/EU TOP SECRET deverão ser designadas pelo chefe do seu serviço e os seus nomes deverão ser mantidos no registo adequado TRÈS SECRET UE/EU TOP SECRET.

7. Antes de terem acesso a informações classificadas TRÈS SECRET UE/EU TOP SECRET, todas as pessoas devem assinar uma declaração de que tomaram conhecimento dos procedimentos de segurança do Conselho e reconhecem inteiramente a sua especial responsabilidade pela salvaguarda de informações classificadas TRÈS SECRET UE/EU TOP SECRET, bem como as consequências previstas na regulamentação da UE e na legislação ou regulamentação administrativa nacionais no caso de a informação classificada ser facultada a pessoas não autorizadas, quer intencionalmente quer por negligência.

8. No caso das pessoas que têm acesso a informações classificadas TRÈS SECRET UE/EU TOP SECRET em reuniões, etc., o oficial de controlo competente do serviço ou órgão em que essa pessoa trabalha deverá notificar o organismo responsável pela reunião de que as pessoas em questão estão autorizadas a fazê-lo.

9. Os nomes de todas as pessoas que deixam de ser empregues em tarefas que exigem acesso a informações classificadas TRÈS SECRET UE/EU TOP SECRET deverão ser removidos da lista TRÈS SECRET UE/EU TOP SECRET. Além disso, deverá ser chamada a atenção de todas essas pessoas para a sua especial responsabilidade pela salvaguarda de informações classificadas TRÈS SECRET UE/EU TOP SECRET. Devem igualmente assinar uma declaração de que não utilizarão nem divulgarão informações classificadas TRÈS SECRET UE/EU TOP SECRET que estejam na sua posse.

REGRAS ESPECÍFICAS SOBRE O ACESSO ÀS INFORMAÇÕES CLASSIFICADAS SECRET UE E CONFIDENTIEL UE

10. Todas as pessoas que têm acesso a informações classificadas SECRET EU ou CONFIDENTIEL UE devem ser objecto de um inquérito de segurança ao nível adequado.

▼B

11. Todas as pessoas que devem ter acesso a informações classificadas SECRET EU ou CONFIDENTIEL UE devem ter conhecimento da regulamentação de segurança adequada e devem estar conscientes das consequências de uma eventual negligência.

12. No caso das pessoas que têm acesso a informações classificadas de SECRET EU ou CONFIDENTIEL UE em reuniões, etc., o oficial de segurança do órgão em que essa pessoa trabalha deverá notificar o organismo responsável pela reunião de que as pessoas em questão estão autorizadas a fazê-lo.

REGRAS ESPECÍFICAS SOBRE O ACESSO ÀS INFORMAÇÕES CLASSIFICADAS RESTREINT UE

13. Deve ser dado conhecimento das presentes regras de segurança do Conselho adequado e das consequências de eventuais actos de negligência às pessoas que têm acesso a informações classificadas RESTREINT UE.

TRANSFERÊNCIAS

14. Quando um membro do pessoal é transferido de um lugar que envolva o tratamento de material classificado da UE, o registo deverá controlar a transferência adequada desse material do funcionário que parte para o funcionário que o substitui.

INSTRUÇÕES ESPECIAIS

15. As pessoas que têm de tratar 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;

    c) Da ameaça das actividades dos serviços de espionagem que têm por alvo a UE e os Estados-Membros no que se refere às informações classificadas e às actividades da UE;

    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 de quaisquer circunstâncias pouco usuais em matéria de segurança.

16. Todas as pessoas que normalmente estão expostas a contactos frequentes com representantes de países cujos serviços de espionagem visam as informações classificadas e as actividades da UE e dos seus Estados-Membros deverão ser informadas das técnicas habitualmente empregues pelos vários serviços de espionagem.

17. Não existem regras de segurança do Conselho em matéria de viagens de carácter privado para qualquer destino, por parte do pessoal habilitado a aceder a informações classificadas da UE. Todavia, as autoridades competentes em matéria de segurança darão a conhecer aos funcionários e outros agentes sob a sua responsabilidade as regras de viagem a que podem estar sujeitos. Incumbirá aos oficiais de segurança organizar reuniões de funcionários para actualizar estas instruções especiais.

▼B

SECÇÃO VI

PROCEDIMENTO PARA A HABILITAÇÃO DE SEGURANÇA DOS FUNCIONÁRIOS E OUTROS AGENTES DO SGC

1. Só terão acesso a informações classificadas na posse do Conselho os funcionários e outros agentes do SGC, ou pessoas que trabalhem no SGC, que, devido às suas funções e conforme as necessidades do serviço, precisam de ter conhecimento ou de utilizar tais informações.

2. Para terem acesso às informações classificadas TRÈS SECRET UE/EU TOP SECRET, SECRET UE e CONFIDENTIEL UE, as pessoas referidas no ponto 1 devem ser autorizadas nos termos dos pontos 4 e 5.

3. A autorização apenas será concedida às pessoas que foram objecto de um inquérito de segurança pelas autoridades nacionais competentes dos Estados-Membros (ANS), nos termos dos pontos 6 a 10.

4. A autoridade investida do poder de nomeação na acepção do primeiro parágrafo do artigo 2.º do Estatuto dos Funcionários será responsável por conceder as autorizações referidas nos pontos 1, 2 e 3.

   A autoridade investida do poder de nomeação concederá a autorização após ter obtido o parecer das autoridades nacionais competentes dos Estados-Membros, no âmbito do inquérito de segurança efectuado nos termos dos pontos 6 a 12.

5. A autorização, que será válida por um período de cinco anos, não poderá exceder a duração das tarefas com base nas quais é concedida. Poderá ser renovada pela autoridade investida do poder de nomeação nos termos do ponto 4.

   A autorização será retirada pela autoridade investida do poder de nomeação sempre que esta 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 pela autoridade investida do poder de nomeação, e à autoridade nacional competente.

6. O objectivo do inquérito de segurança será o de estabelecer que não existem objecções a autorizar a pessoa em questão a ter acesso a informações classificadas na posse do Conselho.

7. O inquérito de segurança deverá ser efectuado, com a assistência da pessoa interessada e a pedido da autoridade investida do poder de nomeação, pelas autoridades nacionais competentes do Estado-Membro cuja nacionalidade tem a pessoa em questão. No caso de esta residir no território de outro Estado-Membro, as autoridades nacionais competentes poderão solicitar a cooperação das autoridades do Estado de residência.

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

9. A autoridade investida do poder de nomeação deverá especificar no seu pedido o tipo e o nível de informações classificadas a que terá acesso a pessoa em questão, 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.

10. Todo o processo de inquérito de segurança, juntamente com os resultados obtidos, estarão sujeitos às regras e regulamentos pertinentes em vigor no Estado-Membro em questão, incluindo aqueles em matéria de recurso.

11. Quando as autoridades nacionais competentes do Estado-Membro derem um parecer positivo, a autoridade investida do poder de nomeação poderá conceder a autorização à pessoa em questão.

12. O parecer negativo das autoridades nacionais competentes será notificado à pessoa em questão, que poderá pedir para ser ouvida pela autoridade investida do poder de nomeação. Caso o considere necessário, esta autoridade poderá pedir às autoridades nacionais competentes qualquer esclarecimento adicional que estas possam fornecer. Se o parecer negativo for confirmado, não será concedida a autorização.

13. Todas as pessoas a quem for concedida uma autorização na acepção dos pontos 4 e 5 deverá receber as instruções necessárias sobre a protecção de informações classificadas e os meios de assegurar essa protecção, no momento em que lhe for concedida a autorização e posteriormente a intervalos regulares. Estas pessoas deverão assinar uma declaração de que confirmam ter recebido as instruções e se comprometem a respeitá-las.

14. A autoridade investida do poder de nomeação deverá tomar todas as medidas necessárias para pôr em prática a presente secção, em especial no

▼B

que diz respeito às regras que regem o acesso à lista das pessoas autorizadas.

15. Excepcionalmente, e por necessidades de serviço, a autoridade investida do poder de nomeação poderá conceder uma autorização temporária por um período que não exceda seis meses, sujeita aos resultados do inquérito de segurança referido no ponto 7, depois de ter notificado as autoridades nacionais competentes e na condição de não ter obtido resposta sua no prazo de um mês.

16. As autorizações temporárias assim concedidas não darão acesso às informações classificadas TRÈS SECRET UE/EU TOP SECRET; este acesso será limitado aos funcionários que foram aprovados num inquérito de segurança, nos termos do ponto 7. Na pendência dos resultados do inquérito, os funcionários para quem foi pedida habilitação ao nível TRÈS SECRET UE/ /EU TOP SECRET poderão ser autorizados de forma temporária e provisória a aceder a informações classificadas até ao grau de TRÈS SECRET UE/EU TOP SECRET, inclusive.

▼B

SECÇÃO VII

ELABORAÇÃO, DISTRIBUIÇÃO, TRANSMISSÃO, ARMAZENAGEM E DESTRUIÇÃO DE MATERIAL CLASSIFICADO DA UE

Sumário

Disposições gerais

Capítulo I Elaboração e distribuição de documentos classificados da UE . . . . . .

Capítulo II Transmissão de documentos classificados da UE . . . . . .

Capítulo III Meios técnicos de transmissão, eléctricos e outros . . . . . .

Capítulo IV Cópias, traduções e extractos de documentos classificados da UE . . . . . .

Capítulo V Inventários e verificações, armazenagem e destruição de documentos classificados da UE . . . . . .

Capítulo VI Regras específicas aplicáveis aos documentos destinados ao Conselho . . . . . .

▼B

Disposições gerais

A presente secção diz respeito à preparação, distribuição, transmissão, armazenagem e destruição de documentos classificados da UE tais como se encontram definidos na alínea a) do ponto 3 dos princípios de base e normas mínimas de segurança apresentados na parte I do presente anexo. Estas disposições servirão como referência quando as mesmas medidas forem adaptadas a outro material classificado da UE, consoante o seu tipo e numa base caso a caso.

Capítulo I

Elaboração e distribuição de documentos classificados da UE

ELABORAÇÃO

1. As classificações e marcações UE serão aplicadas conforme o estabelecido na secção II e deverão ser apostas no topo e no fundo de cada página, centradas, devendo ainda todas as páginas ser numeradas. Todos os documentos classificados da UE deverão ostentar um número de referência e uma data. No caso dos documentos TRÈS SECRET UE/EU TOP SECRET e SECRET UE, esse número de referência deverá aparecer em cada página. Caso devam ser distribuídos em várias cópias, cada uma destas deverá ostentar um número de cópia, que deverá ser aposto na primeira página, juntamente com a indicação do número total de páginas. Os documentos CONFIDENTIEL UE ou com classificação superior deverão ostentar na primeira página uma enumeração de todos os anexos ou apêndices que os acompanhem.

2. Os documentos CONFIDENTIEL UE ou com classificação superior só poderão ser dactilografados, traduzidos, armazenados, fotocopiados, reproduzidos magneticamente ou microfilmados por pessoas que estejam habilitadas a aceder a informações classificadas da UE pelo menos até ao nível adequado de classificação de segurança do documento em questão, excepto no caso especial descrito no ponto 27 da presente secção.

   Constam da secção XI as disposições relativas à produção informática de documentos classificados.

DISTRIBUIÇÃO

3. As informações classificadas da UE só serão distribuídas às pessoas que precisam de tomar conhecimento delas e que possuem uma habilitação de segurança adequada. A distribuição inicial será indicada pela entidade de origem.

4. Os documentos TRÈS SECRET UE/EU TOP SECRET serão distribuídos através dos registos TRÈS SECRET UE/EU TOP SECRET (ver secção VIII). No caso das mensagens TRÈS 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 dos destinatários.

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

6. Todos os documentos CONFIDENTIEL UE ou com classificação superior deverão, ao entrar ou sair de um serviço ou organismo ser averbados no seu registo. As indicações a registar (referências, data e, se for caso disso, o número da cópia) deverão permitir identificar os documentos e deverão ser averbadas num livro de registo ou num meio informático especialmente protegido.

Capítulo II

Transmissão de documentos classificados da UE

EXPEDIÇÃO

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

8. O envelope interior só poderá ser aberto por um oficial de controlo do registo, ou por um seu substituto, que deverá acusar a recepção dos documentos juntos, excepto se o envelope for endereçado a um indivíduo. Nesse caso, deverá ser averbada no registo adequado a chegada do enve-

▼B

lope, e somente o indivíduo a quem este é endereçado poderá abrir o envelope interior e acusar a recepção do documento que ele contém.

9. No envelope interior será colocado 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 seu assunto.

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

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

TRANSMISSÃO NO INTERIOR DE UM EDIFÍCIO OU DE UM GRUPO DE EDIFÍCIOS

12. 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 de segurança do mesmo nível dos documentos.

TRANSMISSÃO DE DOCUMENTOS DA UE NO INTERIOR DE UM PAÍS

13. No interior de um país, os documentos TRÈS SECRET UE/EU TOP SECRET deverão apenas ser enviados através de um serviço oficial de estafetas ou transportados por pessoas habilitadas a aceder a informações TRÈS SECRET UE/EU TOP SECRET.

14. Sempre que seja utilizado um serviço de estafetas para a transmissão de um documento TRÈS SECRET UE/EU TOP SECRET fora do perímetro de um edifício ou de um 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 contêm documentos TRÈS SECRET UE/EU TOP SECRET estão permanentemente sob controlo directo de um funcionário responsável.

15. Excepcionalmente, os documentos TRÈS SECRET UE/EU TOP SECRET podem ser transportados por funcionários, que não os estafetas, fora do perímetro de um edifício ou de um grupo de edifícios para uso local em reuniões e debates, desde que:

    a) O portador esteja habilitado para o acesso a esses documentos TRÈS SECRET UE/EU TOP SECRET;

    b) O modo de transporte satisfaça as regras nacionais em matéria de transmissão de documentos nacionais classificados MUITO SECRETO;

    c) O funcionário não deixe, em nenhumas circunstâncias, os documentos TRÈS SECRET UE/EU TOP SECRET sem guarda;

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

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

17. Cada Estado-Membro ou cada organismo descentralizado da UE deverá elaborar instruções sobre o transporte pessoal de documentos classificados da UE, com base nas presentes regras. O portador deverá ler e assinar essas instruções. Em especial, as instruções deverão indicar claramente que em nenhumas circunstâncias os documentos poderão:

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

    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 aeronaves ou comboios.

▼B

TRANSMISSÃO DE UM ESTADO-MEMBRO PARA OUTRO

18. O material com classificação CONFIDENTIEL UE ou superior deverá ser enviado de um Estado-Membro para outro por mala diplomática ou por serviços de estafetas militares.

19. Todavia, poderá ser autorizado o transporte pessoal de material SECRET UE ou 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.

20. As ANS podem autorizar o transporte pessoal quando não estejam disponíveis nem a mala diplomática nem os serviços de estafetas militares, ou a utilização destes tipos de transporte possa resultar num atraso susceptível de prejudicar as operações da UE, e quando o material for urgentemente preciso no destinatário previsto. Cada Estado-Membro deverá elaborar instruções que abranjam o transporte internacional pessoal de material classificado até ao nível SECRET UE, inclusive, por pessoas que não sejam correios diplomáticos nem militares. Estas instruções deverão estipular que:

a) O portador tenha a habilitação de segurança adequada concedida pelos Estados-Membros;

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

c) As embalagens ou sacos com material da UE 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 UE, que o autorize a transportar a embalagem assim identificada;

e) Não sejam atravessados nem o território nem as fronteiras de um Estado não membro da UE, por via terrestre, a menos que o Estado de envio receba garantia específica daquele Estado;

f) As condições de viagem do portador, no tocante aos destinos, rotas a seguir e meios de transporte a utilizar, sejam conformes com a regulamentação da UE ou — se a regulamentação nacional para o efeito 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 IV;

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, aeronaves, comboios, etc.).

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.

TRANSMISSÃO DE DOCUMENTOS CLASSIFICADOS RESTREINT UE

21. Não são estabelecidas disposições especiais para o transporte de documentos RESTREINT UE, excepto que será necessário assegurar que tais documentos não caiam em mãos de pessoas não autorizadas para o fazer.

SEGURANÇA DO PESSOAL QUE TRANSPORTA DOCUMENTOS

22. Todos os mensageiros e estafetas que transportam documentos SECRET UE e CONFIDENTIEL UE deverão possuir uma habilitação de segurança adequada.

Capítulo III

Meios técnicos de transmissão, eléctricos e outros

23. As medidas de segurança das comunicações serão concebidas de modo a assegurar a transmissão segura de informações classificadas da UE. As regras de aplicação em matéria de transmissão de tais informações constam da secção XI.

▼B

24. Apenas poderão transmitir informações com classificação CONFIDENTIEL UE e SECRET UE os centros e redes e/ou os terminais e sistemas de comunicações aprovados.

Capítulo IV

Cópias, traduções e extractos de documentos classificados da UE

25. Apenas a entidade de origem poderá autorizar a cópia ou a tradução de documentos TRÈS SECRET UE/EU TOP SECRET.

26. Se houver pessoas sem habilitação de segurança para o nível TRÈS SECRET UE/EU TOP SECRET que precisem de informações que não tenham essa classificação embora contidas num documento TRÈS SECRET UE/EU TOP SECRET, o chefe do registo TRÈS SECRET UE/EU TOP SECRET poderá ser autorizado a produzir o necessário número de extractos de tal documento. Simultaneamente, deverá tomar as medidas necessárias para garantir que seja atribuída a esses extractos uma classificação de segurança adequada.

27. Os documentos SECRET UE ou com classificação inferior poderão ser reproduzidos e traduzidos pelo destinatário, no âmbito da regulamentação nacional de segurança e na condição de ser respeitado estritamente o princípio da «necessidade de ter conhecimento». As medidas de segurança aplicáveis ao documento original devem igualmente ser aplicáveis às reproduções e/ou às traduções do mesmo. Os organismos descentralizados da UE deverão seguir as presentes regras de segurança.

Capítulo V

Inventários e verificações, armazenagem e destruição de documentos classificados da UE

INVENTÁRIOS E VERIFICAÇÕES

28. Todos os anos, cada um dos registos TRÈS SECRET UE/EU TOP SECRET a que é feita referência na secção VIII deverá fazer um inventário exaustivo dos documentos TRÈS SECRET UE/EU TOP SECRET, segundo as regras previstas nos pontos 9 a 11 da secção VIII. Os documentos TRÈS SECRET UE/EU TOP SECRET ou com classificação inferior deverão ser objecto de verificações internas segundo as orientações nacionais e, no caso do SGC ou dos organismos descentralizados da UE, segundo as instruções do Secretário-Geral/Alto Representante.

    Estas 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.

ARQUIVAGEM DE INFORMAÇÕES CLASSIFICADAS DA UE

29. A fim de reduzir os problemas de armazenagem, os oficiais de controlo de todos os registos deverão ser autorizados a arquivar documentos TRÈS SECRET UE/EU TOP SECRET, SECRET UE e CONFIDENTIEL UE sob a forma de microfilmes ou gravação em meios magnéticos ou ópticos, desde que:

    a) O processo de microfilmagem/gravação seja realizado por pessoal com uma habilitação 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 TRÈS SECRET UE/EU TOP SECRET seja comunicada à entidade de origem;

    d) Cada um dos rolos de filme ou outros suportes contenha apenas documentos com o mesmo grau de classificação;

    e) A microfilmagem/gravação de um documento TRÈS SECRET UE/EU TOP SECRET ou 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, conforme as regras estabelecidas nos pontos 31 a 36.

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

▼B

DESTRUIÇÃO ROTINEIRA DE DOCUMENTOS CLASSIFICADOS DA UE

31. A fim de impedir a desnecessária acumulação dos documentos classificados da UE, aqueles que forem considerados pelo chefe do organismo detentor como desactualizados ou excedentários deverão ser destruídos logo que possível, da seguinte maneira:

    a) Os documentos TRÈS 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 oficial de controlo TRÈS SECRET UE/EU TOP SECRET e pelo funcionário que testemunhar a destruição, devendo este último possuir habilitação de segurança ao nível TRÈS SECRET UE/EU TOP SECRET. Será averbada no livro de registo uma nota neste sentido;

    b) O registo manterá 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 quando estas forem explicitamente solicitadas;

    c) Os documentos TRÈS SECRET UE/EU TOP SECRET, incluindo todos os resíduos classificados resultantes da preparação de documentos TRÈS SECRET UE/EU TOP SECRET tais como cópias estragadas, rascunhos, notas dactilografadas e papel químico, serão destruídos sob o controlo de um funcionário TRÈS 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.

32. Os documentos SECRET UE serão destruídos pelo registo responsável por esses documentos, sob o controlo de uma pessoa com habilitação de segurança, utilizando os processos indicados na alínea c) do ponto 31. Os documentos 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.

33. Os documentos CONFIDENTIEL UE serão destruídos pelo registo responsável por esses documentos, sob o controlo de uma pessoa com habilitação de segurança, utilizando os processos indicados na alínea c) do ponto 31. A sua destruição será registada nos termos da regulamentação nacional e, no caso do SGC ou dos organismos descentralizados da UE, segundo as instruções do Secretário-Geral/Alto Representante.

34. Os documentos RESTREINT UE serão destruídos pelo registo responsável por esses documentos ou pelo utilizador, nos termos da regulamentação nacional e, no caso do SGC ou dos organismos descentralizados da UE, segundo as instruções do Secretário-Geral/Alto Representante.

DESTRUIÇÃO EM CASOS DE EMERGÊNCIA

35. O SGC, os Estados-Membros e os organismos descentralizados da UE deverão elaborar, com base nas condições locais, planos para a salvaguarda do material classificado da UE em situação de crise, incluindo, se necessário, a destruição de emergência e planos de evacuação; no âmbito das respectivas estruturas, deverão publicar as instruções consideradas necessárias para impedir que as informações classificadas da UE possam chegar às mãos de pessoas não autorizadas.

36. As disposições para a salvaguarda e/ou destruição de material SECRET UE e CONFIDENTIEL UE numa situação de crise não deverão prejudicar em nenhum caso a salvaguarda ou a destruição do material classificado de TRÈS SECRET UE/EU TOP SECRET, incluindo o equipamento de cifragem, cujo tratamento terá prioridade sobre todas as outras tarefas. As medidas a adoptar para a salvaguarda e a destruição do equipamento de cifragem em caso de emergência deverão ser objecto de instruções *ad hoc*.

Capítulo VI

Regras específicas aplicáveis aos documentos destinados ao Conselho

37. No interior do SGC, um «Serviço das Informações Classificadas» deverá controlar as informações classificadas como SECRET UE ou CONFIDENTIEL UE contida nos documentos destinados ao Conselho.

    Sob a autoridade do director-geral do Pessoal e da Administração, este serviço deverá:

    a) Gerir as operações relativas ao registo, reprodução, tradução, transmissão e destruição dessas informações;

    b) Actualizar a lista das indicações específicas relativas às informações classificadas;

▼B

c) Analisar periodicamente a necessidade de manter a classificação das informações;

d) Definir, em colaboração com o Serviço de Segurança, as condições práticas de classificação e desclassificação das informações;

38. O Serviço das Informações Classificadas deverá manter um registo dos seguintes elementos específicos:

a) A data de elaboração das informações classificadas;

b) O nível de classificação;

c) A data em que expira a classificação;

d) O nome e a designação do serviço do autor;

e) O destinatário ou destinatários, com o respectivo número de série;

f) O assunto;

g) O número;

h) O número de cópias distribuídas;

i) A elaboração de inventários das informações classificadas apresentadas ao Conselho;

j) O registo das desclassificações e das desgraduações de informações classificadas.

39. As regras gerais previstas nos capítulos I a V da presente secção são aplicáveis ao Serviço das Informações Classificadas do SGC, excepto quando alteradas pelas regras específicas estabelecidas no presente capítulo.

▼B

SECÇÃO VIII

REGISTOS TRÈS SECRET UE/EU TOP SECRET

1. Os registos TRÈS SECRET UE/EU TOP SECRET destinam-se a assegurar o arquivo, o tratamento e a distribuição de documentos TRÈS SECRET UE/ /EU TOP SECRET em conformidade com as regras de segurança. O chefe do registo TRÈS SECRET UE/EU TOP SECRET em cada Estado-Membro, no SGC e, se for caso disso, nos organismos descentralizados da UE, será o oficial de controlo TRÈS SECRET UE/EU TOP SECRET.

2. Os registos centrais constituirão a principal autoridade de recepção e despacho nos Estados-Membros, no SGC e nos organismos descentralizados da UE, nos quais tenham sido criados, bem como, se for caso disso, noutras instituições da UE, em organizações internacionais e em países terceiros com os quais o Conselho tenha 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 TRÈS SECRET UE/EU TOP SECRET; esses sub--registos manterão registos actualizados da circulação de cada documento a seu cargo.

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

5. Os sub-registos não podem enviar documentos TRÈS SECRET UE/EU TOP SECRET directamente a outros sub-registos do mesmo registo central TRÈS SECRET UE/EU TOP SECRET sem a aprovação expressa deste último.

6. Todos os intercâmbios de documentos TRÈS SECRET UE/EU TOP SECRET entre sub-registos que não dependam do mesmo registo central deverão ser encaminhados através dos registos centrais.

REGISTOS CENTRAIS TRÈS SECRET UE/EU TOP SECRET

7. Na sua qualidade de oficial de controlo, o chefe de um registo central TRÈS SECRET UE/EU TOP SECRET será responsável:

   a) Pela transmissão de documentos TRÈS SECRET UE/EU TOP SECRET segundo as regras definidas na secção VII;

   b) Por manter uma lista de todos os sub-registos que dependem do seu registo central, juntamente com os nomes e as assinaturas dos oficiais de controlo nomeados e dos seus substitutos autorizados;

   c) Por obter dos vários registos recibos para todos os documentos TRÈS SECRET UE/EU TOP SECRET distribuídos pelo registo central;

   d) Por manter um registo dos documentos TRÈS SECRET UE/EU TOP SECRET arquivados e distribuídos;

   e) Por manter uma lista actualizada de todos os registos centrais TRÈS SECRET UE/EU TOP SECRET com os quais normalmente trabalha, juntamente com os nomes e as assinaturas dos respectivos oficiais de controlo e seus substitutos autorizados;

   f) Pela salvaguarda física de todos os documentos TRÈS SECRET UE/EU TOP SECRET arquivados no registo, segundo as regras contidas na secção IV.

SUB-REGISTOS TRÈS SECRET UE/EU TOP SECRET

8. Na sua qualidade de oficial de controlo, o chefe de um sub-registo TRÈS SECRET UE/EU TOP SECRET será responsável:

   a) Pela transmissão de documentos TRÈS SECRET UE/EU TOP SECRET segundo as regras contidas na secção VII e nos pontos 5 e 6 da secção VIII;

   b) Por manter uma lista actualizada de todas as pessoas autorizadas a aceder às informações TRÈS SECRET UE/EU TOP SECRET sob o seu controlo;

   c) Pela distribuição de documentos TRÈS SECRET UE/EU TOP SECRET segundo as instruções da entidade de origem ou segundo o princípio de

▼B

«necessidade de ter conhecimento», devendo verificar previamente se o destinatário possui a necessária habilitação de segurança;

d) Por manter um registo actualizado de todos os documentos TRÈS SECRET UE/EU TOP SECRET arquivados ou que circulam sob o seu controlo ou que tenham sido enviados a outros registos TRÈS SECRET UE/EU TOP SECRET, e pela guarda de todos os recibos correspondentes;

e) Por manter uma lista actualizada dos registos TRÈS SECRET UE/EU TOP SECRET com os quais está autorizado a fazer intercâmbio de documentos TRÈS SECRET UE/EU TOP SECRET, juntamente com os nomes e assinaturas dos respectivos oficiais do controlo e seus substitutos autorizados;

f) Pela salvaguarda física de todos os documentos TRÈS SECRET UE/EU TOP SECRET arquivados no sub-registo, segundo as regras estabelecidas na secção IV.

INVENTÁRIOS

9. De doze em doze meses, cada registo TRÈS SECRET UE/EU TOP SECRET fará um inventário exaustivo de todos os documentos TRÈS SECRET UE/EU TOP SECRET dos quais é responsável. Considerar-se-á que foram dadas contas do documento se ele estiver fisicamente inscrito no registo, ou se este último possuir um recibo do registo TRÈS SECRET UE/EU TOP SECRET para o qual o documento foi transferido, um certificado de destruição do documento ou uma ordem para a sua desgraduação ou desclassificação.

10. Os sub-registos deverão enviar os resultados do seu inventário anual ao registo central de que dependem, numa data indicada por este.

11. As ANS, bem como as instituições da UE, as organizações internacionais e os organismos descentralizados da UE onde tenha sido criado um registo central TRÈS SECRET UE/EU TOP SECRET deverão enviar os resultados dos inventários anuais efectuados em tais registos ao Secretário-Geral/Alto Representante, o mais tardar em 1 de Abril de cada ano.

▼B

SECÇÃO IX

MEDIDAS DE SEGURANÇA A APLICAR POR OCASIÃO DE REUNIÕES ESPECÍFICAS REALIZADAS FORA DAS INSTALAÇÕES DO CONSELHO E QUE ENVOLVAM QUESTÕES DE ALTA SENSIBILIDADE

DISPOSIÇÕES GERAIS

1. Quando forem realizadas sessões do Conselho Europeu ou do Conselho, reuniões ministeriais ou outras reuniões importantes fora das instalações do Conselho em Bruxelas ou no Luxemburgo e sempre que tal se justifique devido aos requisitos especiais de segurança relacionados com a alta sensibilidade das questões 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.

RESPONSABILIDADES

Estado-Membro de acolhimento

2. O Estado-Membro em cujo território tem lugar a reunião (o Estado-Membro de acolhimento) será responsável, em cooperação com o Serviço de Segurança do SGC, pela segurança do Conselho Europeu, do Conselho, da reunião ministerial ou outras reuniões importantes, e pela segurança física dos principais 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 do Conselho para a recepção e transmissão de mensagens classificadas da UE. O Estado-Membro de acolhimento deverá igualmente fornecer acesso, se necessário, a sistemas telefónicos seguros.

Estados-Membros

3. As autoridades dos Estados-Membros devem tomar as medidas necessárias para assegurar que:

   a) Seja fornecido um certificado adequado de habilitação de segurança aos seus delegados nacionais, se necessário por sinalização ou por fax, quer directamente ao oficial de segurança da reunião ou através do Serviço de Segurança do SGC;

   b) Qualquer ameaça específica seja comunicada às autoridades do Estado-Membro de acolhimento e, se for caso disso, ao Serviço de Segurança do SGC, para que possam ser tomadas as medidas apropriadas.

Oficial de segurança da reunião

4. Deverá ser nomeado um oficial de segurança como 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 devem em geral dizer respeito:

   a) i) Às 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,

      ii) ao 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,

      iii) à constante coordenação com as autoridades competentes do Estado-Membro de acolhimento e com o Serviço de Segurança do SGC;

   b) À 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.

Serviço de Segurança do SGC

5. O Serviço de Segurança do SGC 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 oficial de segurança da reunião e as delegações, consoante as necessidades.

▼B

6. Cada uma das delegações a uma reunião deverá designar um seu oficial de segurança, que será responsável por tratar das questões de segurança no interior da sua delegação e por manter o contacto com o oficial de segurança da reunião e com o representante do Serviço de Segurança do SGC, consoante as necessidades.

MEDIDAS DE SEGURANÇA

Áreas de segurança

7. Deverão ser criadas as seguintes áreas de segurança:

   a) Uma área de segurança da classe II, constituída por uma sala de redacção, os gabinetes e equipamento de reprografia do SGC, e os gabinetes 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.

Passes

8. O oficial de segurança da reunião deverá fornecer 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.

9. As instruções de segurança para a reunião devem exigir 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.

10. Além dos participantes que possuem um cartão, o número de pessoas a admitir no local de reunião deverá ser o mais reduzido possível. As delegações nacionais que desejem receber visitantes durante a reunião devem notificar o oficial de segurança da reunião. Deve ser dado um cartão de visitante a cada visitante. Deverá igualmente ser preenchido um passe de entrada do visitante, com o seu nome e com o nome da pessoa que este visita. Os visitantes devem ser acompanhados em todas as ocasiões por um guarda de segurança ou pela pessoa que estes visitam. O passe do visitante deve ser transportado pela pessoa que o acompanha e devolvido ao pessoal encarregado da segurança, quando o visitante sai do local de reunião.

Controlo do equipamento fotográfico e de som

11. 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 oficial de segurança da reunião.

Controlo das pastas, computadores portáteis e embrulhos

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

Segurança técnica

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

Documentos das delegações

14. As delegações devem ser responsáveis por transportar consigo documentos classificados da UE tanto para dentro como para fora das reuniões. Devem igualmente ser 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.

▼B

Guarda segura dos documentos

15. Se o SGC, 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 oficial de segurança da reunião, mediante recibo, para que este os possa guardar segundo as normas aprovadas.

Inspecção dos gabinetes

16. O oficial de segurança da reunião deve providenciar para que os gabinetes do SGC 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, deverão ser tomadas as medidas necessárias.

Remoção de resíduos de documentos classificados da UE

17. Todos os resíduos devem ser tratados como resíduos classificados da UE, e todos os cestos ou sacos de lixo de papel devem ser entregues ao SGC ou às delegações para remoção. Antes de abandonar as instalações que lhes foram atribuídas, o SGC e as delegações devem entregar os seus resíduos ao oficial de segurança da reunião, que deverá providenciar para a sua destruição segundo a regulamentação.

18. No fim da reunião, todos os documentos na posse do SGC ou das delegações mas que já não sejam necessários deverão ser tratados como resíduos. Antes de levantar as medidas de segurança tomadas para a reunião, deverá ser feita uma busca exaustiva das instalações ocupadas pelo SGC e pelas delegações. Na medida do possível, os documentos para os quais tenha sido assinado um recibo devem ser destruídos conforme se encontra previsto na secção VII.

▼B

SECÇÃO X

QUEBRAS DE SEGURANÇA E FUGAS DE INFORMAÇÕES CLASSIFICADAS DA UE

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

2. 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.

3. 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.

4. É importante que todas as pessoas que devam tratar informações classificadas da UE tenham recebido instruções completas sobre os procedimentos de segurança, os perigos de conversas indiscretas e as suas relações com a imprensa. Essas pessoas deverão estar conscientes da importância de relatar imediatamente qualquer quebra de segurança de que possam ter tido conhecimento à autoridade de segurança do Estado-Membro, da Instituição ou do organismo que as emprega.

5. Quando uma autoridade de segurança descobrir ou for informada da ocorrência de uma quebra de segurança relacionada com informações classificadas da UE ou com a perda ou desaparecimento de material classificado da UE, deverá tomar imediatamente medidas para:

   a) Determinar os factos ocorridos;

   b) Avaliar e reduzir os danos verificados;

   c) Impedir que tal volte a acontecer;

   d) 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.

6. Incumbe a cada autoridade de segurança, imediatamente depois de lhe ter sido notificada a ocorrência de uma quebra de segurança, relatar o facto imediatamente, utilizando o seguinte procedimento: o sub-registo TRÈS SECRET UE/EU TOP SECRET deverá informar o Serviço de Segurança do SGC através do seu registo central TRÈS SECRET UE/EU TOP SECRET; no caso de fuga de informações classificadas da UE no âmbito da competência de um Estado-Membro, essa ocorrência será relatada ao Serviço de Segurança do SGC, tal como se encontra previsto no ponto 5, através da ANS competente.

7. Só será necessário relatar os casos que envolvam informações classificadas de RESTREINT UE quando estes apresentarem características pouco usuais.

8. Ao ser informado da ocorrência de uma quebra de segurança, o Secretário-Geral/Alto Representante 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. Deverão igualmente ser relatados 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.

▼B

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

10. Qualquer indivíduo que seja responsável por uma fuga de informações classificadas da UE será passível de acção disciplinar segundo as regras e regulamentos pertinentes. Essa acção disciplinar não será impeditiva de qualquer acção em justiça.

▼B

SECÇÃO XI

PROTECÇÃO DAS INFORMAÇÕES TRATADAS EM SISTEMAS INFORMÁTICOS E DE COMUNICAÇÃO

Sumário

Capítulo I	Introdução	
Capítulo II	Definições	
Capítulo III	Responsabilidades em matéria de segurança	
Capítulo IV	Medidas de segurança não técnicas	
Capítulo V	Medidas de segurança técnicas	
Capítulo VI	Segurança durante o tratamento	
Capítulo VII	Contratos públicos	
Capítulo VIII	Utilização temporária ou ocasional	

▼B

Capítulo I

Introdução

ASPECTOS GERAIS

1. 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 CONFIDENTIEL UE ou superior.

2. Os SISTEMAS que tratem informações com classificação 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. As medidas de segurança a aplicar a esses sistemas serão determinadas pela Autoridade de Acreditação de Segurança (AAS) competente, serão proporcionais aos riscos avaliados e serão conformes com a política definida nas presentes regras de segurança.

3. A protecção dos sensores de sistemas que contenham SISTEMAS informáticos integrados será determinada e definida no contexto geral dos sistemas a que pertencem, utilizando, na medida do possível, as disposições aplicáveis da presente secção.

AMEAÇAS AOS SISTEMAS E SUA VULNERABILIDADE

4. Em termos gerais, 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 contra um alvo específico. A vulnerabilidade pode consistir numa omissão ou pode estar relacionada com uma deficiência na intensidade, na exaustividade ou na coerência do controlo; ela pode ser de carácter técnico, processual ou operacional.

5. O tratamento de informações classificadas e desclassificadas da UE em SISTEMAS de uma forma concentrada concebida para permitir a sua rápida localização, comunicação e utilização é vulnerável a vários riscos. Estes incluem o acesso à informação por utentes não autorizados ou, em sentido inverso, a recusa do acesso aos utentes 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. Esses SISTEMAS constituem por conseguinte alvos atractivos para operações de espionagem e de sabotagem, especialmente se as medidas de segurança forem consideradas ineficazes.

MEDIDAS DE SEGURANÇA

6. O principal objectivo das medidas de segurança enumeradas na presente secção é fornecer protecção contra a divulgação não autorizada (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, há que especificar normas adequadas de segurança convencional, juntamente com procedimentos e técnicas de segurança especiais e adequados, particularmente concebidos para cada SISTEMA.

7. Será definido e posto em prática um conjunto equilibrado de medidas de segurança a fim de criar um ambiente seguro para o funcionamento do SISTEMA. O âmbito de aplicação destas medidas abrange elementos físicos, o pessoal, procedimentos não técnicos e procedimentos operacionais informáticos e de comunicações.

8. As medidas de segurança informática [características de segurança do material (*hardware*) e dos logiciais (*software*)] deverão respeitar o princípio de quem deve tomar conhecimento e deverão impedir ou detectar a divulgação não autorizada das informações. Saber em que medida será possível confiar nas medidas de segurança informática é um elemento a definir durante o processo de elaboração dos requisitos de segurança. O processo de acreditação deverá determinar a existência de um nível adequado de segurança capaz de justificar esta confiança nas medidas de segurança informática.

▼B

LISTA DOS REQUISITOS DE SEGURANÇA ESPECÍFICOS DO SISTEMA (RSES)

9. A Autoridade Operacional do Sistema Informático (AOSI) deverá elaborar uma lista dos requisitos de segurança específicos do SISTEMA (RSES) para cada um dos sistemas que tratem informações com a classificação CONFIDENTIEL UE ou superior, em colaboração e com assistência, se necessário, da equipa de projecto e da Autoridade INFOSEC, lista essa que deverá ser aprovada pela AAS. Também será necessária uma lista RSES sempre que a AAS considerar que é de importância capital a disponibilidade e integridade de informações RESTREINT UE ou não classificadas.

10. A lista RSES 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.

11. A lista RSES constituirá o acordo vinculativo entre a autoridade responsável pelo funcionamento do sistema informático e a AAS, e servirá de referência para a acreditação do SISTEMA.

12. A lista RSES constitui uma 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 do Conselho, 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 utentes. A lista RSES 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 RSES constitui uma enumeração completa dos parâmetros de segurança do SISTEMA.

MODOS SEGUROS DE FUNCIONAMENTO

13. Todos os SISTEMAS que tratem informações com a classificação 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.

Capítulo II

Definições

MARCAÇÕES ADICIONAIS

14. Serão aplicadas marcações adicionais, tais como CRYPTO (CIFRA) ou qualquer outra designação de tratamento especial reconhecida a nível da UE, sempre que exista uma necessidade de distribuição limitada e de tratamento especial, para além daquilo que for indicado pela classificação de segurança.

15. MODOS SEGURO DE FUNCIONAMENTO «DEDICADO»: um 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.

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

16. MODO SEGURO DE FUNCIONAMENTO «ELEVADO»: um 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.

▼B

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 nível mais alto 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.

17. MODO SEGURO DE FUNCIONAMENTO «COMBINADO»: um 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.

18. INFOSEC: a aplicação de medidas de segurança para proteger informações tratadas, 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 da informática, das transmissões, das emissões e da cifragem, e a detecção, a documentação e a neutralização das ameaças às informações e aos SISTEMAS.

19. SEGURANÇA INFORMÁTICA (COMPUSEC): a aplicação de elementos de segurança a um sistema informático, tanto no material *(hardware)* como nos microprogramas *(firmware)* e nos logiciais *(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.

20. 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.

21. SEGURANÇA DAS COMUNICAÇÕES (COMSEC): a 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, pessoal, documental e informática.

22. AVALIAÇÃO: o 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

▼B

SISTEMA, da função criptográfica ou do produto de segurança informática em que é depositada confiança.

23. CERTIFICAÇÃO: a 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 pré-definidos.

24. ACREDITAÇÃO: a autorização e aprovação concedida 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 RSES 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 (POS) 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.

25. SISTEMA INFORMÁTICO: conjunto de equipamentos, métodos e procedimentos e, se necessário, pessoal, organizado para desempenhar funções de tratamento de informações.

Notas:

1) Considera-se que esta designação significa 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 tratamento de texto;

3) As fronteiras de um sistema serão de um modo geral definidas como sendo os elementos sob o controlo de uma única AOSI;

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

26. ELEMENTOS DE SEGURANÇA DO SISTEMA INFORMÁTICO: compreendem todas as funções, características e elementos do material (*hardware*), dos microprogramas (*firmware*) e dos logiciais (*software*); os procedimentos operacionais, procedimentos de responsabilização e 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.

27. 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.

▼B

28. ELEMENTOS DE SEGURANÇA DA REDE INFORMÁTICA: O 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.

29. CENTRAL INFORMÁTICA: uma 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:

Esta definição não 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.

30. ÁREA DE TERMINAIS REMOTOS/ESTAÇÕES DE TRABALHO: Uma área que contenha equipamento informático, os seus dispositivos ou terminais periféricos locais/estações de trabalho e qualquer equipamento associado de comunicações, separada de uma central informática.

31. Contra-medidas 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.

Capítulo III

Responsabilidades em matéria de segurança

DISPOSIÇÕES GERAIS

32. As responsabilidades do Comité de Segurança, definidas no ponto 4 da secção I, incluem as questões INFOSEC. O Comité de Segurança organizará as suas actividades de forma a poder prestar aconselhamento técnico sobre essas questões.

33. Sempre que surjam problemas de segurança (incidentes, infracções, etc.), serão imediatamente tomadas as medidas adequadas pela autoridade nacional responsável e/ou pelo Serviço de Segurança do SGC. Todos os problemas deverão ser comunicados ao Serviço de Segurança do SGC.

34. O Secretário-Geral/Alto Representante ou, se for caso disso, o chefe de um organismo descentralizado da UE, criarão uma unidade INFOSEC encarregada de dar orientações à autoridade de segurança sobre a criação e controlo de elementos de segurança especiais concebidos como parte dos SISTEMAS.

AUTORIDADE DE ACREDITAÇÃO DE SEGURANÇA (AAS)

35. A AAS deverá ser uma das seguintes autoridades:

— uma ANS,

— a autoridade designada pelo Secretário-Geral/Alto Representante,

— a autoridade de segurança de um organismo descentralizado da UE, ou

— os seus representantes delegados/nomeados, em função do SISTEMA a acreditar.

36. Competirá à AAS assegurar a conformidade dos SISTEMAS com a política de segurança do Conselho. 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. No que se refere ao SGC e, se for caso disso, aos organismos descentralizados da UE, a AAS terá a responsabilidade pela segurança em nome do Secretário-Geral/ /Alto Representante ou dos chefes dos organismos descentralizados.

A competência da AAS do SGC abrangerá todos os SISTEMAS que estão em funcionamento nos locais do SGC. Os SISTEMAS e os componentes de SISTEMAS em funcionamento num Estado-Membro continuarão a ser da competência desse Estado-Membro. Sempre que diferentes componentes de um SISTEMA passem a ser da competência da AAS do SGC e de outras AAS, todas as partes nomearão um conselho de acreditação conjunto que será coordenado pela AAS do SGC.

▼B

AUTORIDADE INFOSEC

37. A Autoridade INFOSEC é responsável pelas actividades da unidade INFOSEC. No que se refere ao SGC e, se for caso disso, aos organismos descentralizados da UE, a Autoridade INFOSEC terá a responsabilidade de:
    - prestar aconselhamento e assistência técnica à AAS,
    - contribuir para a elaboração dos RSES,
    - rever os RSES por forma a assegurar a sua coerência com as presentes regras de segurança e as políticas da INFOSEC e arquitectura do sistema,
    - participar em painéis/conselhos de acreditação sempre que necessário e apresentar à AAS 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 são utilizados programas informáticos autorizados.

AUTORIDADE OPERACIONAL DO SISTEMA INFORMÁTICO (AOSI)

38. A Autoridade INFOSEC deverá delegar o mais cedo possível na AOSI a responsabilidade pela aplicação e funcionamento dos controlos e dos elementos de segurança especiais do SISTEMA. Essa responsabilidade estender-se-á por todo o ciclo de vida do SISTEMA, desde a fase de concepção do projecto até à remoção final.

39. A AOSI será responsável por todas as medidas de segurança que constituam parte do SISTEMA global. Essa responsabilidade inclui a preparação dos POS. A AOSI definirá as normas e práticas de segurança a respeitar pelo fornecedor do SISTEMA.

40. A AOSI pode delegar parte das suas responsabilidades, sempre que necessário, designadamente no oficial de segurança da INFOSEC e no oficial de segurança responsável pelo sítio da INFOSEC. As diversas funções INFOSEC podem ser desempenhadas por uma única pessoa.

UTILIZADORES

41. Todos os utilizadores deverão assegurar que as suas actividades não são nocivas para a segurança do SISTEMA que estão a utilizar.

FORMAÇÃO INFOSEC

42. Serão realizadas, a vários níveis e para o diferente pessoal, acções e de formação INFOSEC no âmbito do SCG, dos organismos descentralizados da UE ou dos órgãos governamentais dos Estados-Membros, conforme adequado.

Capítulo IV

Medidas de segurança não técnicas

SEGURANÇA DO PESSOAL

43. 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 do Conselho.

44. A AAS 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.

45. Os SISTEMAS devem ser especificados e concebidos de uma forma que facilite a repartição das tarefas e responsabilidades entre os membros do pessoal, para que nenhuma pessoa possa ter o conhecimento e o controlo completos dos pontos-chave do sistema de segurança. Pretende-se com isto que, sem a cumplicidade entre duas ou mais pessoas, não seja possível efectuar modificações ou degradar intencionalmente o sistema ou a rede.

SEGURANÇA FÍSICA

46. A central informática e as áreas de terminais/estações de trabalho (tal como definidas nos pontos 29 e 30) onde sejam tratadas, por meios informáticos, informações CONFIDENTIEL UE ou com uma classificação superior, ou

▼B

onde for possível o acesso a tais informações, serão definidas como áreas de segurança UE da classe I ou II ou o seu equivalente a nível nacional, conforme o caso.

47. A central informática ou 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.

CONTROLO DO ACESSO A UM SISTEMA

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

49. 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 nos pontos 61 a 63.

Capítulo V

Medidas de segurança técnicas

SEGURANÇA DAS INFORMAÇÕES

50. 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.

51. Compete a um organismo 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.

52. 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.

53. 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.

54. 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.

55. 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 pelo SGC ou a nível nacional (ver pontos 61 a 63).

CONTROLO E RESPONSABILIDADE PELAS INFORMAÇÕES

56. Os acessos às informações classificadas 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.

57. 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.

58. 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 AAS, para controlar a produção no terminal. No que diz respeito ao material com a classificação SECRET

▼B

UE e superior, tais procedimentos deverão incluir instruções específicas no que diz respeito à responsabilidade pelas informações.

TRATAMENTO E CONTROLO DOS SUPORTES INFORMÁTICOS AMOVÍVEIS

59. Todos os suportes informáticos amovíveis com a classificação 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.

60. 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.

DESCLASSIFICAÇÃO E DESTRUIÇÃO DOS SUPORTES INFORMÁTICOS

61. Os suportes informáticos utilizados para registar informações classificadas da UE podem ser desgraduados ou desclassificados, aplicando os procedimentos aprovados pelo SGC ou a nível nacional.

62. Os suportes informáticos que tiverem contido informações TRÈS SECRET UE/EU TOP SECRET ou com uma categoria especial não serão desclassificados nem reutilizados.

63. Se os suportes informáticos não puderem ser desclassificados ou não forem reutilizáveis, deverão ser destruídos segundo um procedimento aprovado pelo SGC ou a nível nacional.

SEGURANÇA DAS COMUNICAÇÕES

64. 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 AAS 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.

65. Sempre que forem necessários métodos criptográficos para garantir a protecção da confidencialidade, da integridade e da disponibilidade, esses métodos ou produtos associados deverão ser especificamente aprovados pela AAS para o efeito.

66. Durante a transmissão, a confidencialidade das informações com classificação SECRET UE e superior deverá ser protegida por métodos ou produtos criptográficos aprovados pelo Conselho sob recomendação do Comité de Segurança do Conselho. Durante a transmissão, a confidencialidade das informações CONFIDENTIEL UE ou RESTREINT UE deverá ser protegida por métodos ou produtos criptográficos aprovados quer pelo Secretário-Geral/Alto Representante, sob recomendação do Comité de Segurança do Conselho, que por um Estado-Membro.

67. As regras pormenorizadas aplicáveis à transmissão de informações classificadas da UE deverão ser definidas em instruções de segurança específicas aprovadas pelo Conselho sob recomendação do Comité de Segurança do Conselho.

68. Em circunstâncias operacionais excepcionais, as informações classificadas RESTREINT UE, CONFIDENTIEL UE e SECRET UE podem ser transmitidas em claro, desde que isso seja explicitamente autorizado caso a caso. Essas circunstâncias excepcionais são as seguintes:

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

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

69. 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 AAS.

▼B

SEGURANÇA DA INSTALAÇÃO E DAS RADIAÇÕES

70. 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.

71. Todos os equipamentos devem ser instalados de acordo com a actual política de segurança do Conselho.

72. Os SISTEMAS que tratam informações com a classificação CONFIDENTIEL UE ou superior devem ser protegidos de forma a que a sua segurança não possa ser ameaçada por fugas resultantes de emissões, cujo estudo e controlo se designam pelo termo «TEMPEST».

73. As contra-medidas TEMPEST para as instalações do SGC e dos organismos descentralizados da UE devem ser revistas e aprovadas por uma autoridade TEMPEST designada pela autoridade de segurança do SGC. No que diz respeito às instalações nacionais que tratam informações classificadas da UE, a autoridade de aprovação será a autoridade de aprovação TEMPEST reconhecida a nível nacional.

Capítulo VI

Segurança durante o tratamento

PROCEDIMENTOS OPERACIONAIS DE SEGURANÇA

74. Os POS definem os princípios a adoptar em matéria de segurança, os procedimentos operacionais a seguir e as responsabilidades do pessoal. Os POS serão estabelecidos sob a responsabilidade da AOSI.

PROTECÇÃO DOS LOGICIAIS *(SOFTWARE)*/GESTÃO DA CONFIGURAÇÃO

75. 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 dos programas informáticos a uso deverão ser verificadas a intervalos regulares para garantir a sua integridade e o seu correcto funcionamento.

76. Não deverão ser utilizadas versões novas ou alteradas dos programas para o tratamento de informações classificadas da UE enquanto não forem verificadas pela AOSI.

VERIFICAÇÃO DA PRESENÇA DE PROGRAMAS MALIGNOS/VÍRUS INFORMÁTICOS

77. A verificação da presença de programas malignos/vírus informáticos deverá ser feita periodicamente segundo os requisitos da AAS.

78. Antes de serem introduzidos em qualquer SISTEMA, todos os suportes informáticos que dão entrada no SGC, nos organismos descentralizados da UE ou nos Estados-Membros deverão ser controlados a fim de detectar a presença de quaisquer programas malignos ou vírus informáticos.

MANUTENÇÃO

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

80. Os requisitos deverão ser claramente mencionados na lista RSES e os procedimentos claramente indicados nos POS. 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 AAS.

Capítulo VII

Contratos públicos

81. 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 competente para o efeito com base em critérios reconhecidos a nível internacional (tais

▼B

como os Critérios Comuns de Avaliação da Segurança Informática (ver ISO 15408).

82. 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 AAS, aprovação essa que nem sempre é possível.

ACREDITAÇÃO

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

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

AVALIAÇÃO E CERTIFICAÇÃO

85. Antes de se proceder à acreditação, em certos casos, os elementos de segurança do material *(hardware)*, microprogramas *(firmware)* e logiciais *(software)* de um SISTEMA deverão ser avaliados e certificados como capazes de salvaguardar as informações ao nível pretendido de classificação.

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

87. 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 da AOSI.

88. 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.

89. 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.

CONTROLOS DE ROTINA DOS ELEMENTOS DE SEGURANÇA PARA PRORROGAR A ACREDITAÇÃO

90. A AOSI estabelecerá procedimentos de controlo de rotina destinados a garantir que todos os elementos de segurança do SISTEMA continuam válidos.

91. Os tipos de alterações que possam ocasionar uma nova acreditação, ou que exijam uma aprovação prévia da AAS, deverão ser claramente identificados e mencionados nos RSES. Na sequência de qualquer alteração, reparação ou falha que possa ter afectado os elementos de segurança do SISTEMA, a AOSI 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.

92. Todos os SISTEMAS em que tiverem sido aplicados elementos de segurança serão inspeccionados ou revistos numa base periódica pela AAS. No que diz respeito aos SISTEMAS que tratam informações TRÈS SECRET UE/EU TOP SECRET ou com marcações adicionais, essas inspecções devem ser realizadas pelo menos uma vez por ano.

▼B

Capítulo VIII

Utilização temporária ou ocasional

SEGURANÇA DOS MICROCOMPUTADORES/COMPUTADORES PESSOAIS

93. 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.

94. 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).

UTILIZAÇÃO DE EQUIPAMENTO INFORMÁTICO PRIVADO PARA TRABALHOS OFICIAIS DO CONSELHO

95. 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.

96. 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 do chefe do Serviço de Segurança do SCG, de um ministério ou serviço de um Estado-Membro ou do respectivo organismo descentralizado da UE.

UTILIZAÇÃO DE EQUIPAMENTO INFORMÁTICO PERTENCENTE A PRESTADORES DE SERVIÇOS OU DE FORNECIMENTO NACIONAL PARA TRABALHOS OFICIAIS DO CONSELHO

97. O chefe do Serviço de Segurança do SGC, de um ministério ou serviço de um Estado-Membro ou do respectivo organismo descentralizado da UE pode autorizar a utilização de equipamentos e programas informáticos pertencentes a prestadores de serviços em organizações que prestam apoio ao trabalho oficial do Conselho. Também poderá ser autorizada a utilização, por funcionários do SGC ou de um organismo descentralizado da UE, de equipamentos e programas informáticos fornecidos a nível nacional. Neste caso, o equipamento informático deverá ser controlado e inscrito num inventário adequado do SGC. Em qualquer dos casos, se o equipamento informático for utilizado para tratar informações classificadas da UE, deverá ser então consultada a AAS competente, para que os elementos INFOSEC aplicáveis à utilização desse equipamento sejam devidamente analisados e aplicados.

▼B

SECÇÃO XII

DIVULGAÇÃO DE INFORMAÇÕES CLASSIFICADAS DA UE A ESTADOS TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

PRINCÍPIOS APLICÁVEIS À DIVULGAÇÃO DE INFORMAÇÕES CLASSIFICADAS DA UE

1. A divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais será decidida pelo Conselho 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 ao Estado-Membro que está na origem das informações classificadas da UE.

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

   — o nível pretendido de cooperação com os Estados 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 Comité de Segurança do Conselho dará o seu parecer técnico ao Conselho sobre este ponto.

3. A aceitação de informações classificadas da UE por parte de Estados 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 pelo Conselho.

NÍVEIS

4. Tendo o Conselho 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.

5. Existem três níveis de cooperação:

   Nível 1

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

   Nível 2

   Cooperação com Estados terceiros ou com organizações internacionais cuja política e regulamentação em matéria de segurança são sensivelmente 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.

6. Cada nível de cooperação determinará as regulamentações em matéria de segurança, reformuladas caso a caso à luz do parecer técnico do Comité de Segurança do Conselho, que os beneficiários serão chamados a aplicar à protecção das informações classificadas que lhes foram divulgadas. Estes procedimentos e regulamentos em matéria de segurança são explicitados nos apêndices 4, 5 e 6.

ACORDOS

7. Uma vez que tenha constatado que existe uma necessidade permanente ou a longo prazo de trocar informações classificadas entre a UE e Estados terceiros ou outras organizações internacionais, o Conselho 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.

8. 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

▼B

as obrigações recíprocas em relação a essas informações, desde que não sejam classificadas num nível superior ao de RESTREINT UE.

9. Os projectos de acordo sobre procedimentos de segurança ou de memorandos de entendimento serão aprovados pelo Comité de Segurança antes de serem apresentados ao Conselho para decisão.

10. As ANS prestam ao Secretário-Geral/Alto Representante 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.

▼B

Apêndice 1

Lista das Autoridades Nacionais de Segurança

▼M1

BÉLGICA

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P & S 6
Rue des Petits Carmes 15
B-1000 Bruxelles

Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking
Nationale Veiligheidsoverheid (NVO)
Directie Protocol en Veiligheid P&S 6
Karmelietenstraat 15
B-1000 Brussel
Téléphone du secrétariat: (32-2) 519 05 74
Téléphone de la présidence: (32-2) 501 82 20; (32-2) 501 87 10
Télécopieur: (32-2) 519 05 96

REPÚBLICA CHECA

National Security Authority
Na Popelce 2/16
CZ-150 06 Praha 56
Telefon: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DINAMARCA

Politiets Efterretningstjeneste
Klausdalsbrovej 1
DK-2860 Søborg
Telefon (45) 33 14 88 88
Fax (45) 33 43 01 90

ALEMANHA

Bundesministerium des Innern
Referat IS 2
Alt-Moabit 101 D
D-11014 Berlin
Telefon: 49-18 88–681-15 26
Fax: 49-18 88-681-558 06

ESTÓNIA

Ministry of Defence, Republic of Estonia, Department of Security
Sakala 1
EE-15094 Tallinn
Telefon: (372) 717 00 30
Fax: (372) 717 00 01

GRÉCIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ — Β Κλάδος)
Τμήμα Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα: (30) 210 657 20 09 (ώρες γραφείου), (30) 210 657 20 10 (ώρες γραφείου)
Φαξ: (30) 210 642 64 32, (30) 210 657 21 81

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Service (MIS-Bi Branch)
Security Counterintelligence Section
GR-STG 1020 Holargos — Athens
Telephone: (30) 210 657 20 09, (30) 210 657 20 10
Fax: (30) 210 642 64 32, (30) 210 657 21 81

▼**M1**

ESPANHA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,5
E-28023 Madrid
Teléfono: (34-91) 372 57 07, (34-91) 372 50 27
Fax: (34-91) 372 58 08

FRANÇA

Secrétariat général de la défense nationale
Service de sécurité et de défense (SGDN/SSD)
51 boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Téléphone: (33-1) 71 75 81 77
Télécopieur: (33-1) 71 75 82 00

IRLANDA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Ireland
Telephone: (353-1) 478 08 22
Fax: (353-1) 478 14 84

ITÁLIA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Tel.: (39) 066 27 47 75
Fax: (39) 066 14 33 97

CHIPRE

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: (357) 22 80 75 69, (357) 22 80 75 19, (357) 22 80 77 64
Φαξ: (357) 22 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia
Telephone: (357) 22 80 75 69; (357) 22 80 75 19; (357) 22 80 77 64
Fax: (357) 22 30 23 51

LETÓNIA

Constitution Protection Bureau of the Republic of Latvia
Miera Iela 85/A
LV-1001 Riga
Telefon: (371) 702 54 18
Fax: (371) 702 54 06

LITUÂNIA

National Security Authority of the Republic of Lithuania
Gedimino 40/2
LT-2600 Vilnius
Telefon: (370-5) 266 32 05
Fax: (370-5) 266 32 00

LUXEMBURGO

Autorité nationale de sécurité
Ministère d'État

▼**M1**

Boîte Postale 23 79
L-1023 Luxembourg
Téléphone: (352) 478 22 10 (central), (352) 478 22 35 (ligne directe)
Télécopieur: (352) 478 22 43; (352) 478 22 71

HUNGRIA

National Security Authority Republic of Hungary
Pf. 2
HU-1352 Budapest
Telefon: (361) 346 96 52
Fax: (361) 346 96 58

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telefon: (356) 21 24 98 44
Fax: (356) 21 23 53 00

PAÍSES BAIXOS

Ministerie van Binnenlandse Zaken
Postbus 200102500 EA Den Haag
Nederland
Tel.: (31-70) 320 44 00
Fax: (31-70) 320 07 33

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 207012500 ES Den Haag
Nederland
Tel.: (31-70) 318 70 60
Fax: (31-70) 318 79 51

ÁUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: 431-531 15 23 96
Fax: 431-531 15 25 08

POLÓNIA

Military Information Services
National Security Authority — Military Sphere
PL-00-909 Warszawa 60
Telefon: (48-22) 684 61 19
Fax: (48-22) 684 61 72

Internal Security Agency
Department for the Protection of Classified Information
2A Rakowiecka St.
PL-00-993 Warszawa
Telefon: (48-22) 585 73 60
Fax: (48-22) 585 85 09

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira
P-1400-204 Lisboa
Tel.: (351-21) 301 17 10
Fax: (351-21) 303 17 11

ESLOVÉNIA

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information — NSA
Slovenska cesta 5
SVN-1000 Ljubljana
Telefon: (386-1) 426 91 20
Fax: (386-1) 426 91 91

▼**M1**

ESLOVÁQUIA

National Security Authority
Budatínska 30
SK-851 05 Bratislava
Telefon: (421-2) 68 69 95 09
Fax: (421-2) 63 82 40 05

FINLÂNDIA

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu/Maringatan 22
PL/PB 176
FI-00161 Helsinki/Helsingfors
P. (358-9) 16 05 53 38
F. (358-9) 16 05 53 03

SUÉCIA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon (46-8) 405 54 44
Fax (46-8) 723 11 76

REINO UNIDO

National Security Authority
The Secretary for T3P/1
PO Box 56 56
London EC1A 1AH
United Kingdom
Telephone: (44) 20 72 70 87 51
Fax: (44) 20 76 30 14 28

▼B

Apêndice 2

▼M1

Comparação das classificações de segurança

Classificação UE	Très Secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Bélgica	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
República Checa	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dinamarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Alemanha	Streng geheim	Geheim	VS ([2]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estónia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Grécia	Άκρως απόρρητο Abk: ΑΑΠ	Απόρρητο Abk: (ΑΠ)	Εμπιστευτικό ΕΕ Abk: (ΕΜ)	Περιορισμένης χρήσης Abk: (ΠΧ)
Espanha	Secreto	Reservado	Confidencial	Difusión limitada
França	Très Secret Défense ([1])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlanda	Top Secret	Secret	Confidential	Restricted
Itália	Segretissimo	Segreto	Riservatissimo	Riservato
Chipre	Άκρως απόρρητο	Απόρρητο	Εμπιστευτικό ΕΕ	Περιορισμένης χρήσης
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-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett

▼M1

Classificação UE	Très Secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Países Baixos	STG Zeer Geheim	STG Geheim	STG Confidentieel	—
Áustria	Streng geheim	Geheim	Vertraulich	Eingeschränkt
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
Finlândia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Suécia	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Reino Unido	Top Secret	Secret	Confidential	Restricted
Classificação NATO	Cosmic Top Secret	NATO Secret	NATO Confidential	NATO Restricted
Classificação UEO	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

([1]) França: a classificação Très Secret Défense, que abrange as prioridades governamentais, só admite alteração com autorização do primeiro ministro.
([2]) Alemanha: VS = Verschlusssache.

Apêndice 3

Guia prático de classificação

Este guia é indicativo e não pretende modificar as disposições substantivas apresentadas nas secções II e III.

Classificação	Quando	Quem	Marcações	Desgraduação/desclassificação/destruição	
				Quem	Quando
TRÈS 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 (secção II, ponto 1).	A fuga de material ou documentos marcados TRÈS 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.	Estados-Membros: pessoas devidamente autorizadas (entidades de origem) (secção III, ponto 4). SGC: pessoas devidamente autorizadas (entidades de origem) (secção III, ponto 4), SG/AR e SGA. As entidades de origem devem especificar uma data ou um período durante o qual os conteúdos podem ser desgraduados ou desclassificados. De outro modo, deverão rever os documentos pelo menos de cinco em cinco anos, de forma a assegurar que a classificação inicial é necessária (secção III, ponto 10).	Deverá ser atribuída a classificação TRÈS SECRET UE/EU TOP SECRET a documentos TRÈS SECRET UE/EU TOP SECRET e, se necessário, introduzida a marcação de defesa-ESDP/PESD, por meios mecânicos ou à mão (secção II, ponto 8). 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; 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 adendas deverão ser enumerados na primeira página (secção VII, ponto 1).	A desclassificação ou a desgraduação são da exclusiva responsabilidade da entidade de origem ou do SG/AR ou SGA, que deverão informar das alterações os subsequentes destinatários a quem tiverem enviado o documento ou uma cópia (secção VIII, ponto 9). Os documentos TRÈS 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 oficial de controlo TRÈS SECRET UE/EU TOP SECRET e pelo funcionário que assistiu à destruição, que deve ter a habilitação TRÈS 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 (secção VII, ponto 31).	As cópias e os documentos excedentários que já não são necessários devem ser destruídos (secção VII, ponto 31). Os documentos TRÈS SECRET UE/EU TOP SECRET, incluindo todos os resíduos classificados resultantes da elaboração de documentos TRÈS SECRET UE/EU TOP SECRET, tais como cópias estragadas, rascunhos, notas dactilografadas e papel-químico, deverão ser destruídos, sob a supervisão de um funcionário TRÈS SECRET UE/EU TOP SECRET, por queima, redução a polpa, retalhamento ou por qualquer outra forma, tornando-os irreconhecíveis e não reconstituíveis (secção VII, ponto 31).

Classificação	Quando	Quem	Marcações	Desgraduação/desclassificação/destruição	
				Quem	Quando
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 (secção II, ponto 2).	A fuga de material ou documentos marcados SECRET UE 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.	Estados-Membros: pessoas autorizadas (entidades de origem) (secção II, ponto 2). SGC e organismos descentralizados UE: pessoas autorizadas (entidades de origem) (secção II, ponto 2), directores-gerais, SG/AR e SGA. As entidades de origem devem especificar uma data ou um período durante o qual os conteúdos podem ser desgraduados ou desclassificados. De outro modo, deverão rever os documentos pelo menos de cinco em cinco anos, de forma a assegurar que a classificação inicial é necessária (secção III, ponto 10).	Deverá ser atribuída a classificação SECRET UE a documentos SECRET UE e, se necessário, introduzida a marcação de defesa-ESDP/ /PESD, por meios mecânicos ou à mão (secção II, ponto 8). 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; 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 adendas deverão ser enumerados na primeira página (secção VII, ponto 1).	A desclassificação ou a desgraduação são da exclusiva responsabilidade da entidade de origem ou do SG/AR ou SGA, que deverão informar das alterações os subsequentes destinatários a quem tiverem enviado o documento ou uma cópia (secção III, ponto 9). Os documentos SECRET UE deverão ser destruídos pelo registo por eles responsável, sob a supervisão de uma pessoa habilitada ao nível SECRET UE. Os documentos SECRET UE destruídos serão enumerados em certificados de destruição assinados, que devem ser mantidos pelo registo, juntamente com a folha de distribuição, por um período de pelo menos três anos (secção VII, ponto 32).	As cópias e os documentos excedentários que já não são necessários devem ser destruídos (secção VII, ponto 31). Os documentos SECRET UE, incluindo todos os resíduos classificados resultantes da elaboração de documentos 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 (secção VII, pontos 31 e 32).
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 (secção II, ponto 3).	A fuga de material ou documentos marcados 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,	Estados-Membros: pessoas autorizadas (entidades de origem) (secção III, ponto 2). SGC e organismos descentralizados da UE: pessoas autorizadas (entidades de origem) (secção III, ponto 2), directores-gerais,	Deverá ser atribuída a classificação CONFIDENTIEL UE a documentos CONFIDENTIEL UE e, quando adequado, inserida a marcação de defesa-ESDP/ /PESD, por meios mecânicos ou à mão, ou imprimindo-os em papel pré-timbrado registado (secção III, ponto 8). As classificações UE deverão	A desclassificação ou a desgraduação são da exclusiva responsabilidade da entidade de origem ou do SG/AR ou do SGA, que deverão informar de todas as alterações os subsequentes destinatários a quem tiverem enviado o documento ou uma cópia (secção III, ponto 9). Os documentos CONFIDEN-	As cópias e os documentos excedentários que já não são necessários devem ser destruídos (secção VII, ponto 31). Os documentos CONFIDENTIEL UE, incluindo todos os resíduos classificados resultantes da elaboração de documentos CONFIDENTIEL UE, tais como cópias estragadas,

Classificação	Quando	Quem	Marcações	Desgraduação/desclassificação/destruição	
				Quem	Quando
	— causar prejuízo à eficácia operacional ou à segurança das forças dos Estados-Membros ou de outros contribuintes, ou à 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.	SG/AR e SGA. As entidades de origem devem especificar uma data ou um período durante o qual os conteúdos podem ser desgraduados ou desclassificados. De outro modo, deverão rever os documentos pelo menos de cinco em cinco anos, de forma a assegurar que a classificação inicial é necessária (secção III, ponto 10).	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 (secção VII, ponto 1).	TIEL UE deverão ser destruídos pelo registo por eles responsável, sob a supervisão de uma pessoa habilitada. A sua destruição deve ser registada de acordo com as regulamentações nacionais e, no caso do SGC e dos organismos descentralizados da UE, segundo as instruções do SG/AR ou do SGA (secção VII, ponto 33).	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 (secção VII, pontos 31 e 33).
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 (secção II, ponto 4).	A fuga de material ou documentos marcados RESTREINT UE poderia: — afectar negativamente as relações diplomáticas, — casuar grande aflição às pessoas, — tornar muito mais difícil manter a eficácia operacional ou a segurança das	Estados-Membros: pessoas autorizadas (entidades de origem) (secção III, ponto 2). SGC e organismos descentralizados da UE: pessoas autorizadas (entidades de origem) (secção III,	Deverá ser atribuída a classificação RESTREINT UE a documentos RESTREINT UE e, se necessário, introduzida a marcação de defesa ESDP/ /PESD, por meios mecânicos ou electrónicos (secção II, ponto 8). As classificações UE deverão constar no topo e no fundo de	A desclassificação ou a desgraduação são da exclusiva responsabilidade da entidade de origem ou do SG/AR ou do SGA, que deverão informar das alterações os subsequentes destinatários a quem tiverem enviado o documento ou uma cópia (secção III, ponto 9).	As cópias e os documentos excedentários que já não são necessários devem ser destruídos (secção VII, ponto 31).

▼B

Classificação	Quando	Quem	Marcações	Desgraduação/desclassificação/destruição	
				Quem	Quando
	forças dos Estados-Membros ou de outros 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.	ponto 2), directores-gerais, SG/AR e SGA. As entidades de origem devem especificar uma data ou um período durante o qual os conteúdos podem ser desgraduados ou desclassificados. De outro modo, deverão rever os documentos pelo menos de cinco em cinco anos, de forma a assegurar que a classificação inicial é necessária (secção III, ponto 10).	cada página, centradas, devendo cada página ser numerada. Cada documento deverá possuir um número de referência e uma data (secção VII, ponto 1).	Os documentos classificados RESTREINT UE deverão ser destruídos pelo registo por eles responsável, de acordo com as regulamentações nacionais e, no caso do SGC ou dos organismos descentralizados da UE, segundo as instruções do SG/AR (secção VII, ponto 34).	

▼B

Apêndice 4

Orientações para a divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais

Cooperação de nível 1

PROCEDIMENTOS

1. Cabe ao Conselho a competência para autorizar a divulgação de informações classificadas da UE a países não signatários do Tratado da União Europeia ou a outras organizações internacionais com políticas e regulamentações de segurança comparáveis às da UE.

2. O Conselho pode delegar a decisão de autorizar a divulgação de informações classificadas indicando a natureza das informações cuja divulgação pode ser autorizada e o seu nível de classificação, que não será normalmente superior a CONFIDENTIEL UE.

3. Sob reserva da celebração de um acordo de segurança, os pedidos de divulgação de informações classificadas da UE serão apresentados ao Secretário-Geral/Alto Representante pelos organismos de segurança dos Estados ou organizações nacionais interessados, os quais deverão indicar o fim a que as informações se destinam e a natureza das informações classificadas a divulgar.

   Estes pedidos podem igualmente ser feitos por um Estado-Membro ou um organismo descentralizado da UE que considerem desejável a divulgação de informações classificadas da UE; os interessados deverão indicar os fins a que se destinam essas informações e os benefícios que a sua divulgação trará à UE, especificando a natureza e a classificação das informações a divulgar.

4. O pedido será apreciado pelo SGC, que:

   — procurará obter o parecer do Estado-Membro ou, se for caso disso, do organismo descentralizado que está na origem das informações a divulgar,

   — estabelecerá os contactos necessários com os órgãos de segurança das organizações internacionais ou países beneficiários a fim de verificar se as respectivas políticas e regulamentações de segurança são de molde a garantir que as informações classificadas divulgadas serão protegidas de acordo com as presentes regras de segurança,

   — procurará obter o parecer técnico das ANS dos Estados-Membros quanto à confiança que é possível depositar nas organizações internacionais ou Estados beneficiários.

5. O SGC enviará o pedido ao Conselho, para decisão, acompanhado das recomendações do Serviço de Segurança.

REGRAS DE SEGURANÇA A APLICAR PELOS BENEFICIÁRIOS

6. O Secretário-Geral/Alto Representante notificará as organizações internacionais ou Estados beneficiários da decisão do Conselho de autorizar a divulgação das informações classificadas da UE, enviando-lhes tantos exemplares das presentes regras de segurança quantos forem considerados necessários. Se o pedido tiver sido apresentado por um Estado-Membro, será este a notificar o interessado da autorização de divulgar.

   A decisão de divulgar só entrará em vigor quando os beneficiários derem garantias por escrito de que:

   — apenas utilizarão as informações para os fins acordados,

   — protegerão as informações de acordo com as presentes regras de segurança e, em particular, as disposições 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 da UE com classificação 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.

▼B

8. *Transmissão de documentos*

a) Os procedimentos práticos para a transmissão de documentos serão decididos de comum acordo com base no disposto na secção VII das presentes regras de segurança. Especificar-se-ão, em particular, os registos para onde as informações classificadas da UE deverão ser enviadas.

b) Se as informações classificadas cuja divulgação foi autorizada pelo Conselho incluir elementos TRÈS SECRET UE/EU TOP SECRET, a organização internacional ou o Estado beneficiário deverão criar um registo central UE e, se necessário, sub-registos UE. Estes registos reger-se-ão pelo disposto na secção VIII das presentes regras de segurança.

9. *Registo*

Logo que o registo receba um documento com classificação 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 classificação, 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 ao serviço ou entidade da UE que o emitiu.

10. *Destruição*

a) Os documentos classificados da UE serão destruídos segundo as instruções constantes da secção VI das presentes regras de segurança. O registo UE que enviou os documentos deverá receber uma cópia do certificado de destruição dos documentos SECRET UE e TRÈS 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 classificados de CONFIDENTIEL UE ou 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 TRÈS 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 o Serviço de Segurança do SGC.

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 do Serviço de Segurança do SGC, da ANS 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 pelo Serviço de Segurança do SGC para impedir que o caso se repita.

14. *Inspecções*

O Serviço de Segurança do SGC 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.

▼B

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 regras constantes das presentes regras de segurança.

▼B

Apêndice 5

Orientações para a divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais

Cooperação de nível 2

PROCEDIMENTOS

1. Compete ao Conselho autorizar a divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais cujas políticas e regulamentações de segurança sejam marcadamente diferentes das da UE. Em princípio, esta competência restringe-se a informações classificadas até ao nível SECRET UE inclusive, excluindo a informação nacional especificamente reservada aos Estados-Membros e as categorias de informações classificadas da UE protegidas por marcações especiais.

2. O Conselho pode delegar a decisão de autorizar a divulgação de informações classificadas; ao fazê-lo indicará, com as restrições referidas no n.º 1, a natureza das informações cuja divulgação pode ser autorizada e o seu nível de classificação, que não será superior a RESTREINT UE.

3. Sob reserva da celebração de um acordo de segurança, os pedidos de divulgação de informações das da UE serão apresentados ao Secretário-Geral/ /Alto Representante pelos organismos de segurança dos Estados ou organizações nacionais interessados, os quais deverão indicar o fim a que as informações se destinam e a natureza e a classificação das informações a divulgar.

   Estes pedidos podem igualmente ser feitos por um Estado-Membro ou um organismo descentralizado da UE que considerem desejável a divulgação de informações classificadas da UE; os interessados deverão indicar os fins a que se destinam essas informações e os benefícios que a sua divulgação trará à UE, especificando a natureza e a classificação das informações a divulgar.

4. O pedido será apreciado pelo SGC, que:

   — procurará obter o parecer do Estado-Membro ou, se for caso disso, do organismo descentralizado que está na origem das informações a divulgar,

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

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

5. O parecer técnico do Comité de Segurança do Conselho incidirá sobre os seguintes aspectos:

   — confiança que pode ser depositada nas organizações internacionais ou Estados beneficiários, 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 pela entidade de origem antes de divulgar as informações às organizações internacionais ou países beneficiários ([1]).

6. O Secretário-Geral/Alto Representante enviará o pedido ao Conselho, para decisão, acompanhado do parecer técnico do Comité de Segurança do Conselho obtido pelo Serviço de Segurança do SGC.

([1]) Isto implica que a entidade de origem aplique o procedimento definido na secção III, ponto 9, no caso de todas as cópias distribuídas na UE.

▼B

REGRAS DE SEGURANÇA A APLICAR PELOS BENEFICIÁRIOS

7. A decisão do Conselho de autorizar a divulgação de informações classificadas da UE será comunicada às organizações internacionais ou Estados beneficiários pelo Secretário-Geral/Alto Representante, acompanhada de um quadro comparativo das classificações aplicáveis na UE e nos Estados ou organizações em causa. Se o pedido tiver sido apresentado por um Estado-Membro, será este a notificar o beneficiário da autorização de divulgar as informações pretendidas.

   A decisão de divulgar só entrará em vigor quando os beneficiários derem garantias por escrito de que:

   — apenas utilizarão as informações para os fins acordados,

   — protegerão as informações segundo a regulamentação estabelecida pelo Conselho.

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

   Neste caso, as regras serão adaptadas em conformidade.

9. *Pessoal*

   a) O número de funcionários com acesso às 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 UE deverão possuir uma habilitação de segurança nacional ou uma autorização de acesso a informações classificadas nacionais de nível equivalente ao da UE, conforme indicado no quadro comparativo.

   c) Estas autorizações ou habilitações de segurança nacionais serão enviadas, para informação, ao Secretário-Geral/Alto Representante.

10. *Transmissão de documentos*

   a) Os procedimentos práticos para a transmissão de documentos serão decididos de comum acordo entre o Serviço de Segurança do SGC e os organismos de segurança das organizações internacionais ou Estados receptores, com base nas regras enunciadas na secção VII das presentes regras. Haverá que especificar, em particular, os endereços para onde os documentos deverão ser enviados, bem como os serviços postais ou de mensageiro utilizados para a transmissão das informações classificadas da UE.

   b) Os documentos com a classificação CONFIDENTIEL UE ou superior serão transmitidos em duplo envelope. No envelope interior será aposta a marcação «UE» juntamente com a classificação de segurança. 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 então 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.

11. *Registo à chegada*

   A ANS do Estado destinatário ou a entidade sua homóloga que receber em nome do Governo desse Estado as informações classificadas enviadas pela UE, 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.

12. *Devolução dos documentos*

   Quando a entidade receptora devolve um documento classificado ao Conselho ou ao Estado-Membro que o divulgou, procederá conforme indicado no ponto 10.

▼B

13. *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 CONFIDENTIEL UE ou num grau superior, nem deles poderão ser produzidos extractos, sem autorização do Serviço de Segurança do SGC.

d) O procedimento para a destruição rápida e total dos documentos em caso de emergência deverá ser definido e confirmado com o Serviço de Segurança do SGC.

14. *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) 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.

15. *Quebras de segurança*

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

a) Envio imediato de um relatório ao Serviço de Segurança do SGC ou à ANS do Estado-Membro que tomou a iniciativa de enviar os documentos (com cópia para o Serviço de Segurança do SGC);

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.

16. *Inspecções*

O Serviço de Segurança do SGC 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.

17. *Relatórios*

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 regras de segurança.

▼B

Apêndice 6

Orientações para a divulgação de informações classificadas da UE a Estados terceiros ou organizações internacionais

Cooperação de nível 3

PROCEDIMENTOS

1. Ocasionalmente o Conselho 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». Essa divulgação não incluirá nunca informações nacionais, especificamente reservadas aos Estados-Membros.

2. Em tais circunstâncias, os pedidos de cooperação com a «UE», sejam eles provenientes de Estados terceiros ou organizações internacionais ou propostos pelos Estados-Membros ou, se for caso disso, por organismos descentralizados da «UE», serão primeiro apreciados em substância pelo Conselho, que, se necessário, pedirá o parecer do Estado-Membro ou do organismo descentralizado que emitiu a informação. O Conselho 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.

3. Se a decisão do Conselho for favorável, caberá ao Secretário-Geral/Alto Representante convocar o Comité de Segurança do Conselho ou informar-se junto das «ANS» dos Estados-Membros, por procedimento escrito simplificado se tal for adequado, a fim de obter o parecer técnico do Comité de Segurança.

4. O parecer técnico do Comité de Segurança do Conselho incidirá sobre os seguintes aspectos:

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

   b) Classificação das informações que podem ser divulgadas, se for caso disso, em função da sua natureza;

   c) Desgraduação ou desclassificação das informações pela entidade de origem antes de as divulgar às organizações internacionais ou países interessados ([1]);

   d) Procedimentos para o tratamento dos documentos a divulgar (ver ponto 5 adiante);

   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.).

5. 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 Comité de Segurança do Conselho 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 (ver exemplos no ponto 14).

6. O Serviço de Segurança do SGC submeterá o parecer técnico do Comité de Segurança à apreciação do Conselho, juntando-lhe, se for caso disso, as propostas de delegação de poderes necessárias para a realização da operação, especialmente em casos urgentes.

7. Uma vez que a divulgação de informações classificadas da «UE» e os procedimentos de execução prática tenham sido aprovados pelo Conselho, o Serviço de Segurança do «SGC» estabelecerá os contactos necessários com o organismo de segurança do Estado ou organização interessados, a fim de facilitar a aplicação das medidas de segurança previstas.

8. A título de elemento de referência, o Serviço de Segurança do «SGC» enviará a todos os Estados-Membros e, se for caso disso, aos organismos descentralizados da «UE» interessados um quadro-resumo do tipo e classifi-

([1]) Isto implica que a entidade de origem aplique o procedimento previsto na secção III, ponto 9, a todas as cópias distribuídas na UE.

▼B

cação das informações, com indicação das organizações e países aos quais pode ser divulgada, conforme decisão do Conselho.

9. A «ANS» do Estado-Membro que procede à divulgação das informações ou o Serviço de Segurança do «SGC» tomarão todas as medidas necessárias para facilitar a avaliação de eventuais prejuízos ou danos e a reapreciação dos procedimentos.

10. O Conselho será chamado a pronunciar-se novamente sempre que as condições de cooperação sejam alteradas.

REGRAS DE SEGURANÇA A APLICAR PELOS BENEFICIÁRIOS

11. A decisão do Conselho de autorizar a divulgação de informações classificadas da «UE» será comunicada às organizações internacionais ou Estados beneficiários pelo Secretário-Geral/Alto Representante, acompanhada de uma resenha detalhada das regras de protecção propostas pelo Comité de Segurança do Conselho e aprovadas por este último. Se o pedido tiver sido apresentado por um Estado-Membro, será este a notificar o beneficiário de que foi autorizada a divulgação das informações pretendidas.

    A decisão só entrará em vigor quando os beneficiários derem garantias por escrito de que:

    — as informações em causa apenas serão utilizadas para efeitos da cooperação decidida pelo Conselho,

    — protegerão as informações conforme exigido pelo Conselho.

12. *Transmissão de documentos*

    a) Os procedimentos práticos para a transmissão de documentos serão decididos de comum acordo entre o Serviço de Segurança do «SGC» e os organismos de segurança das organizações internacionais ou Estados receptores. Haverá que especificar, em particular, os endereços para onde os documentos deverão ser enviados.

    b) Os documentos com a classificação «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 então 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.

13. *Registo à chegada*

    A ANS do Estado destinatário ou a entidade sua homóloga que receber em nome do Governo desse Estado as informações classificadas enviadas pela «UE», 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.

14. *Utilização e protecção das informações classificadas recebidas*

    a) As informações de nível «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 «SECRET UE» serão transmitidas por mala diplomática, por serviços de correio de segurança ou por uma rede de telecomunicações securizada. Um documento «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 «SECRET UE».

    b) As informações de nível «CONFIDENTIEL UE» serão tratadas por funcionários especificamente designados autorizados a tomar conheci-

▼B

mento do assunto em questão. Os documentos serão guardados em armários de segurança trancados colocados em zonas vigiadas.

As informações de nível «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 «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, através dos serviços públicos, 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.

15. *Destruição*

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

16. *Quebras de segurança*

Em caso de fuga ou suspeita de fuga de informações de nível «CONFIDENTIEL UE» ou «SECRET UE», a «ANS» do Estado ou o chefe dos serviços de segurança da organização conduzirão um inquérito sobre as circunstâncias dessa fuga. Se o inquérito produzir resultados positivos, a autoridade de origem será notificada. Serão tomadas as medidas necessárias para corrigir procedimentos ou métodos de armazenagem inadequados, se tiverem sido estes a dar origem à fuga. O Secretário-Geral/Alto Representante ou a «ANS» do Estado-Membro que transmitiu a informação em causa poderão pedir ao beneficiário que lhes forneça pormenores do inquérito.