1.4.2014 PT Jornal Oficial da União Europeia C 96/1

II

(Comunicações)

COMUNICAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

PARLAMENTO EUROPEU

DECISÃO DA MESA DO PARLAMENTO EUROPEU

de 15 de abril de 2013

sobre as regras que regem o tratamento de informações confidenciais pelo Parlamento Europeu

(2014/C 96/01)

A MESA DO PARLAMENTO EUROPEU,

Tendo em conta o artigo 23.º, n.º 12, do Regimento do Parlamento Europeu,

CONSIDERANDO O SEGUINTE:

(1) Tendo em conta o Acordo-Quadro sobre as relações entre o Parlamento Europeu e a Comissão Europeia ([1]), assinado em 20 de outubro de 2010 («Acordo-Quadro»), e o Acordo Interinstitucional entre o Parlamento Europeu e o Conselho sobre a transmissão ao Parlamento Europeu e o tratamento pelo mesmo de informações classificadas na posse do Conselho sobre assuntos distintos dos que se inscrevem no âmbito da política externa e de segurança comum ([2]), assinado em 12 de março de 2014 («Acordo Interinstitucional»), é necessário estabelecer regras específicas sobre o tratamento de informações confidenciais pelo Parlamento Europeu.

(2) O Tratado de Lisboa confere novas competências ao Parlamento Europeu e, para que este possa desenvolver atividades em domínios que exigem um certo grau de confidencialidade, é necessário estabelecer princípios de base, normas mínimas de segurança e procedimentos adequados para o tratamento de informações confidenciais, incluindo informações classificadas, pelo Parlamento Europeu.

(3) As regras previstas na presente decisão destinam-se a garantir normas equivalentes de proteção e a compatibilidade com as regras adotadas por outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou pelos EstadosMembros, a fim de facilitar o bom funcionamento do processo decisório a nível da União Europeia.

(4) As disposições da presente decisão são adotadas sem prejuízo das regras atuais e futuras sobre o acesso aos documentos, adotadas nos termos do artigo 15.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

([1]) JO L 304 de 20.11.2010, p. 47.
([2]) JO C 95, 1.4.2014, p. 1.

(5) As disposições da presente decisão são adotadas sem prejuízo das regras atuais e futuras sobre a proteção dos dados pessoais, adotadas nos termos do artigo 16.º do TFUE.

ADOPTOU A PRESENTE DECISÃO:

Artigo 1.º

Objetivo

A presente decisão rege a gestão e o tratamento de informações confidenciais pelo Parlamento Europeu, nomeadamente a sua produção, receção, transmissão e armazenamento, a fim de proteger de forma adequada a sua natureza confidencial. A presente decisão dá aplicação ao Acordo Interinstitucional e ao Acordo-Quadro, nomeadamente o Anexo II.

Artigo 2.º

Definições

Para efeitos da presente decisão, entende-se por:

a) «Informação», uma informação oral ou escrita, seja qual for o seu suporte ou o seu autor;

b) «Informações confidenciais», informações classificadas e outras informações confidenciais não classificadas;

c) «Informações classificadas», informações classificadas da UE e informações classificadas equivalentes;

d) «Informações classificadas da UE» (ICUE), informações ou materiais classificados como «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET», «CONFIDENTIEL UE/EU CONFIDENTIAL» ou «RESTREINT UE/EU RESTRICTED», cuja divulgação não autorizada possa causar prejuízos de diversos níveis aos interesses da União ou de um ou vários dos seus EstadosMembros, quer tais informações tenham ou não origem nas instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados. Neste contexto, informações ou materiais classificados como:

— «TRÈS SECRET UE/EU TOP SECRET», são informações e materiais cuja divulgação não autorizada possa prejudicar de forma excecionalmente grave os interesses essenciais da União ou de um ou vários dos seus EstadosMembros,

— «SECRET UE/EU SECRET», são informações e materiais cuja divulgação não autorizada possa prejudicar gravemente os interesses essenciais da União ou de um ou vários dos seus EstadosMembros,

— «CONFIDENTIEL UE/EU CONFIDENTIAL», são informações e materiais cuja divulgação não autorizada possa prejudicar os interesses essenciais da União ou de um ou vários dos seus EstadosMembros,

— «RESTREINT UE/EU RESTRICTED», são informações e materiais cuja divulgação não autorizada possa ser desfavorável aos interesses da União ou de um ou vários dos seus EstadosMembros;

e) «Informações classificadas equivalentes», informações classificadas, emitidas pelos EstadosMembros, por países terceiros ou por organizações internacionais, que ostentem uma marca de classificação de segurança equivalente a uma das marcas de classificação de segurança utilizadas para as ICUE e que tenham sido transmitidas ao Parlamento Europeu pelo Conselho ou pela Comissão;

f) «Outras informações confidenciais», outras informações não classificadas, incluindo informações abrangidas por regras relativas à proteção de dados ou pela obrigação de sigilo profissional, produzidas no Parlamento Europeu ou transmitidas ao Parlamento Europeu por outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou pelos EstadosMembros;

g) «Documento», uma informação registada, independentemente da sua forma física ou das suas características;

h) «Material», um documento ou parte de maquinaria ou equipamento, produzido ou em processo de produção;

i) «Necessidade de tomar conhecimento», a necessidade de uma pessoa aceder a informações confidenciais para desempenhar uma função oficial ou para executar uma tarefa;

j) «Autorização», uma decisão adotada pelo Presidente, se disser respeito a deputados ao Parlamento Europeu, ou pelo Secretário-Geral, se disser respeito a funcionários do Parlamento Europeu e a outros agentes do Parlamento Europeu ao serviço dos grupos políticos, de conceder acesso individual a informações classificadas até um determinado nível, com base no resultado favorável de um inquérito de segurança (procedimento de habilitação) efetuado por uma autoridade nacional nos termos da lei nacional e do Anexo I, Parte 2;

k) «Desgraduação», uma redução do nível de classificação;

l) «Desclassificação», a supressão de uma classificação;

m) «Marca», um sinal afixado em outras informações confidenciais a fim de identificar instruções específicas preestabelecidas quanto ao seu tratamento, ou quanto ao âmbito de um determinado documento. Este sinal pode também ser afixado em informações classificadas, a fim de impor requisitos adicionais ao seu tratamento;

n) «Desmarcação», a supressão de uma marca;

o) «Entidade de origem», o autor devidamente autorizado de informações classificadas;

p) «Indicações de segurança», as medidas de aplicação estabelecidas no anexo II;

q) «Instruções de tratamento», instruções técnicas fornecidas aos serviços do Parlamento Europeu sobre a gestão de informações confidenciais.

Artigo 3.º

Princípios de base e normas mínimas

1. O tratamento de informações confidenciais pelo Parlamento Europeu obedece aos princípios de base e às normas mínimas estabelecidos no Anexo I, Parte 1.

2. O Parlamento Europeu cria um sistema de gestão da segurança das informações (SGSI) em conformidade com esses princípios de base e essas normas mínimas. O SGSI é composto pelas indicações de segurança, pelas instruções de tratamento e pelas normas aplicáveis do Regimento e tem por objetivo facilitar o trabalho parlamentar e administrativo e, simultaneamente, assegurar a proteção das informações confidenciais tratadas pelo Parlamento Europeu, respeitando plenamente as regras estabelecidas pela entidade de origem das informações que figuram nas indicações de segurança.

O tratamento de informações confidenciais por meio dos sistemas de comunicação e informação (SCI) automatizados do Parlamento Europeu é efetuado de acordo com o conceito de garantia da informação (GI), tal como estabelecido na indicação de segurança n.º 3.

3. Os deputados ao Parlamento Europeu podem consultar informações classificadas até ao nível RESTREINT UE/EU RESTRICTED, inclusive, sem necessidade de habilitação de segurança.

4. É concedido acesso a informações classificadas no nível CONFIDENTIEL UE/EU CONFIDENTIAL, ou equivalente, aos deputados ao Parlamento Europeu que tenham sido autorizados pelo Presidente nos termos do n.º 5 ou após terem assinado uma declaração sob compromisso de honra de que não divulgarão o conteúdo dessas informações a terceiros, de que respeitarão a obrigação de proteger as informações classificadas no nível CONFIDENTIEL UE/EU CONFIDENTIAL e de que conhecem as consequências de um eventual incumprimento.

5. É concedido acesso a informações classificadas no nível SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou equivalente, aos deputados ao Parlamento Europeu que tenham sido autorizados pelo Presidente após:

a) Terem sido habilitados com uma habilitação de segurança nos termos do Anexo I, Parte 2, da presente decisão, ou

b) Ter sido recebida uma notificação de uma autoridade nacional competente atestando que os deputados em causa estão devidamente autorizados por força das funções que exercem nos termos da lei nacional.

6. Antes de lhes ser concedido acesso a informações classificadas, os deputados ao Parlamento Europeu são informados da responsabilidade, que reconhecem, de proteger tais informações nos termos do Anexo I, bem como dos meios para assegurar essa proteção.

7. Os funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos podem consultar informações confidenciais se tiverem uma razão válida para delas tomar conhecimento, e podem consultar informações classificadas num nível superior a RESTREINT UE/EU RESTRICTED se dispuserem do nível de habilitação de segurança adequado. Só lhes será facultado acesso a informações classificadas se tiverem sido informados e lhes tiverem sido fornecidas instruções escritas sobre a sua responsabilidade de proteger tais informações, bem como sobre os meios para assegurar a sua proteção, e se tiverem assinado uma declaração pela qual acusam a receção das referidas instruções e se comprometem a cumpri-las de acordo com as presentes regras.

Artigo 4.º

Produção de informações confidenciais e tratamento administrativo pelo Parlamento Europeu

1. O Presidente do Parlamento Europeu, os presidentes das comissões parlamentares interessadas e o Secretário-Geral e/ou qualquer pessoa por este devidamente autorizada por escrito podem produzir informações confidenciais e/ou informações classificadas, tal como estabelecido nas indicações de segurança.

2. Ao produzir informações classificadas, a entidade de origem aplica o nível adequado de classificação, em conformidade com as normas e definições internacionais que figuram no Anexo I. Regra geral, a entidade de origem indica igualmente os destinatários que podem ser autorizados a consultar as informações em função do nível de classificação. Esta informação é comunicada à Unidade de Informações Classificadas (UIC) quando os documentos forem depositados na UIC.

3. As outras informações confidenciais abrangidas pelo sigilo profissional são tratadas em conformidade com os Anexos I e II e com as instruções de tratamento.

Artigo 5.º

Receção de informações confidenciais pelo Parlamento Europeu

1. As informações confidenciais recebidas pelo Parlamento Europeu são comunicadas do seguinte modo:

a) Informações com a classificação RESTREINT EU/EU RESTRICTED ou equivalente e outras informações confidenciais: ao secretariado da instância parlamentar/titular de um cargo que apresentou o pedido, ou diretamente à UIC;

b) Informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET ou equivalente: à UIC.

2. O registo, o armazenamento e a rastreabilidade das informações confidenciais são assegurados, consoante o caso, pelo secretariado da instância parlamentar/ titular de um cargo que tenha recebido as informações, ou pela UIC.

3. As modalidades a estabelecer por comum acordo para preservar a confidencialidade das informações, no caso de informações confidenciais transmitidas pela Comissão nos termos do ponto 3.2 do Anexo II do Acordo-Quadro, ou no caso de informações classificadas transmitidas pelo Conselho nos termos do artigo 5.º, n.º 4, do Acordo Interinstitucional, são depositadas, juntamente com as informações confidenciais, no secretariado da instância parlamentar/titular de um cargo ou na UIC, consoante o caso.

4. As modalidades referidas no n.º 3 podem ser igualmente aplicadas, com as necessárias adaptações, à transmissão de informações confidenciais por outras instituições, órgãos, organismos e agências estabelecidos por força ou com base nos Tratados ou pelos EstadosMembros.

5. A Conferência dos Presidentes cria um comité de supervisão encarregado de garantir um nível de proteção adequado à classificação TRÈS SECRET UE/EU TOP SECRET, ou equivalente. A transmissão de informações com a classificação TRÈS SECRET UE/EU TOP SECRET ou equivalente ao Parlamento Europeu está sujeita a outras modalidades, a acordar entre o Parlamento Europeu e a instituição da União que comunica essas informações.

Artigo 6.º

Transmissão de informações classificadas a terceiros pelo Parlamento Europeu

O Parlamento Europeu pode, sob reserva do consentimento por escrito da entidade de origem ou da instituição da União que tenha comunicado as informações classificadas, consoante o caso, transmitir essas informações classificadas a terceiros, desde que estes assegurem que, aquando do tratamento dessas informações, sejam aplicadas, nos seus serviços e instalações, regras equivalentes às previstas na presente decisão.

Artigo 7.º

Instalações seguras

1. Para efeitos da gestão de informações confidenciais, o Parlamento Europeu cria uma zona securizada e salas de leitura segura.

2. A zona securizada dispõe de instalações para o registo, consulta, arquivo, transmissão e tratamento de informações classificadas. A zona securizada compreende, nomeadamente, uma sala de leitura e uma sala de reuniões para a consulta de informações classificadas, e é administrada pela UIC.

3. Podem ser criadas, fora da zona securizada, salas de leitura segura a fim de permitir a consulta de informações classificadas do nível RESTREINT UE/EU RESTRICTED ou equivalente e de outras informações confidenciais. Estas salas de leitura segura são geridas pelos serviços competentes do secretariado da instância parlamentar/titular de um cargo ou pela UIC, consoante o caso. As salas de leitura segura não podem conter fotocopiadoras, telefones, fax, scanners ou qualquer outro equipamento técnico de reprodução ou transmissão de documentos.

Artigo 8.º

Registo, tratamento e armazenamento de informações confidenciais

1. As informações com a classificação RESTREINT UE/EU RESTRICTED, ou equivalente, e outras informações confidenciais podem ser registadas e armazenadas pelos serviços competentes do secretariado da instância parlamentar/titular de um cargo ou pela UIC, em função de quem tiver recebido as informações.

2. Aplicam-se as seguintes condições ao tratamento de informações com a classificação RESTREINT UE/EU RESTRICTED, ou equivalente, e de outras informações confidenciais:

a) Os documentos em papel são entregues pessoalmente ao responsável pelo secretariado, que os regista e acusa a sua receção;

b) Quando não estiverem a ser efetivamente utilizados, esses documentos são guardados em locais fechados à chave, sob a responsabilidade do secretariado;

c) As informações não podem, em circunstância alguma, ser gravadas noutro suporte nem transmitidas a terceiros. Esses documentos podem ser reproduzidos por meio de equipamento devidamente acreditado, tal como estabelecido nas indicações de segurança;

d) O acesso a essas informações é limitado às pessoas designadas pela entidade de origem ou pela instituição da União que comunicou as informações ao Parlamento Europeu, em conformidade com as modalidades referidas no artigo 4.º, n.º 2, ou no artigo 5.º, n.ºs 3, 4 e 5;

e) O secretariado da instância parlamentar/titular de um cargo mantém um registo das pessoas que consultaram as informações e da data e hora das consultas, e transmite o registo à UIC aquando do depósito das informações na UIC.

3. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET/EU TOP SECRET, ou equivalente, são registadas, tratadas e armazenadas pela UIC na zona securizada, em conformidade com o nível específico de classificação e tal como estabelecido nas indicações de segurança.

4. Em caso de infração às regras estabelecidas nos n.ºs 1 a 3, o funcionário responsável do secretariado da instância parlamentar/titular de um cargo, ou da UIC, informa o Secretário-Geral, o qual submete o assunto ao Presidente caso esteja envolvido um deputado ao Parlamento Europeu.

Artigo 9.º

Acesso às instalações seguras

1. Só têm acesso à zona securizada as seguintes pessoas:

a) As pessoas que, nos termos do artigo 3.º, n.ºs 4 a 7, estejam autorizadas a consultar as informações nela contidas e tenham apresentado um pedido nos termos do artigo 10.º, n.º 1;

b) As pessoas que, nos termos do artigo 4.º, n.º 1, estejam autorizadas a produzir informações classificadas e tenham apresentado um pedido nos termos do artigo 10.º, n.º 1;

c) Os funcionários da UIC do Parlamento Europeu;

d) Os funcionários do Parlamento Europeu responsáveis pela gestão dos SCI;

e) Se necessário, os funcionários do Parlamento Europeu responsáveis pela segurança e pela prevenção de incêndios;

f) O pessoal de limpeza, sempre na presença e sob a apertada vigilância de um funcionário da UIC.

2. A UIC pode recusar o acesso à zona securizada a todas as pessoas não autorizadas a entrar nela. Qualquer objeção a uma recusa de acesso é apresentada ao Presidente, no caso de um pedido de acesso apresentado por um deputado ao Parlamento Europeu, ou ao Secretário-Geral, nos restantes casos.

3. O Secretário-Geral pode autorizar a realização de uma reunião destinada a um número limitado de pessoas na sala de reuniões situada na zona securizada.

4. Só têm acesso a uma sala de leitura segura as seguintes pessoas:

a) Os deputados ao Parlamento Europeu, os funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos, devidamente identificados para efeitos da consulta e produção de informações confidenciais;

b) Os funcionários do Parlamento Europeu responsáveis pela gestão dos SCI, os funcionários do secretariado da instância parlamentar/titular de um cargo que tenham recebido as informações, e os funcionários da UIC;

c) Se necessário, os funcionários do Parlamento Europeu responsáveis pela segurança e pela prevenção de incêndios;

d) O pessoal de limpeza, sempre na presença e sob a apertada vigilância de um funcionário do secretariado da instância parlamentar/titular de um cargo ou da UIC, consoante o caso.

5. O secretariado competente da instância parlamentar/titular de um cargo ou a UIC, consoante o caso, pode recusar o acesso à sala de leitura segura a todas as pessoas não autorizadas a entrar nela. Qualquer objeção a uma recusa de acesso é apresentada ao Presidente, no caso de um pedido de acesso apresentado por um deputado ao Parlamento Europeu, ou ao Secretário-Geral, nos restantes casos.

Artigo 10.º

Consulta ou produção de informações confidenciais em instalações seguras

1. Uma pessoa que pretenda consultar ou criar informações confidenciais na zona securizada comunica com antecedência o seu nome à UIC. A UIC comprova a identidade dessa pessoa e verifica se a pessoa está autorizada, nos termos do artigo 3.º, n.os 3 a 7, do artigo 4.º, n.º 1, ou do artigo 5.º, n.os 3, 4 e 5, a consultar ou produzir informações confidenciais.

2. Uma pessoa que pretenda aceder, nos termos do artigo 3.º, n.os 3 e 7, a informações confidenciais com a classificação RESTREINTUE/EU RESTRICTED, ou equivalente, ou a outras informações confidenciais numa sala de leitura segura, comunica com antecedência o seu nome aos serviços competentes do secretariado da instância parlamentar/titular de um cargo, ou à UIC.

3. Salvo em circunstâncias excecionais (por exemplo, caso tenha sido apresentado um número elevado de pedidos de consulta num curto período), a consulta de informações confidenciais numa instalação segura só é autorizada a uma pessoa de cada vez, na presença de um funcionário do secretariado da instância parlamentar/titular de um cargo ou da UIC.

4. Durante a consulta não são permitidos contactos com o exterior (inclusive por meio de telefones ou de outros aparelhos), nem tomar notas ou fazer fotocópias ou fotografias das informações confidenciais consultadas;

5. Antes de autorizar uma pessoa a abandonar a sala de leitura segura, o funcionário do secretariado da instância parlamentar/titular de um cargo ou da UIC certifica-se de que as informações confidenciais consultadas se mantêm presentes, intactas e completas.

6. Em caso de infração às regras acima definidas, o funcionário do secretariado da instância parlamentar/titular de um cargo ou da UIC informa o Secretário-Geral, o qual submete o assunto ao Presidente caso esteja envolvido um deputado ao Parlamento Europeu.

Artigo 11.º

Normas mínimas aplicáveis à consulta de informações confidenciais em reuniões à porta fechada fora das instalações seguras

1. As informações confidenciais com a classificação RESTREINT UE/EU RESTRICTED ou equivalente e outras informações confidenciais podem ser consultadas por membros das comissões parlamentares ou de outras instâncias políticas e administrativas do Parlamento Europeu em reuniões à porta fechada realizadas fora das instalações seguras.

2. Nas circunstâncias previstas no n.º 1, o secretariado da instância parlamentar/titular de um cargo responsável pela reunião assegura que sejam cumpridas as seguintes condições:

a) Só são autorizadas a entrar na sala de reuniões pessoas designadas para participar na reunião pelo presidente da comissão ou da instância competente;

b) Os documentos são todos numerados, distribuídos no início da reunião e recolhidos no final, e não são tomadas notas nem feitas fotocópias ou fotografias desses documentos;

c) A ata da reunião não menciona o conteúdo do debate sobre as informações apreciadas. Só pode ser lavrada em ata a decisão, caso exista;

d) As informações confidenciais prestadas oralmente a destinatários no Parlamento Europeu são sujeitas a um nível de proteção equivalente ao aplicado às informações confidenciais escritas;

e) Não podem estar presentes nas salas de reuniões documentos suplementares;

f) São distribuídas cópias dos documentos apenas no número necessário aos participantes e aos intérpretes, no início da reunião;

g) O presidente da reunião esclarece o estatuto da classificação/marcação dos documentos no início da reunião;

h) Os participantes não retiram documentos da sala de reuniões;

i) As cópias dos documentos são todas recolhidas e controladas no final da reunião pelo secretariado da instância parlamentar/titular de um cargo; e

j) Não são introduzidos aparelhos eletrónicos de comunicação nem outros aparelhos eletrónicos na sala de reuniões onde as informações confidenciais em causa são consultadas ou discutidas.

3. Caso, de acordo com as exceções estabelecidas do Anexo II, ponto 3.2.2, do Acordo-Quadro e no artigo 6.º, n.º 5, do Acordo Interinstitucional, sejam discutidas informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou equivalente, numa reunião realizada à porta fechada, o secretariado da instância parlamentar/titular de um cargo responsável pela reunião assegura que, além do disposto no n.º 2, as pessoas designadas para participar na reunião cumpram os requisitos do artigo 3.º, n.ºs 4 e 7.

4. No caso previsto no n.º 3, a UIC fornece ao secretariado da instância parlamentar/titular de um cargo responsável pela reunião à porta fechada o número de cópias necessário dos documentos a discutir, que serão devolvidas à UIC finda a reunião.

Artigo 12.º

Arquivo de informações confidenciais

1. É assegurado um sistema de arquivo seguro no interior da zona securizada. A gestão do arquivo seguro é assegurada pela UIC, em conformidade com as normas de arquivo habituais.

2. As informações classificadas depositadas a título definitivo na UIC e as informações com a classificação RESTREINT UE/EU RESTRICTED ou equivalente, depositadas no secretariado da instância parlamentar/titular de um cargo são transferidas para o arquivo seguro na zona securizada seis meses após a última consulta e, no máximo, um ano depois de terem sido depositadas. As outras informações confidenciais são arquivadas, a não ser que tenham sido depositadas na UIC, pelo secretariado da instância parlamentar/titular de um cargo em causa, de acordo com as normas gerais sobre gestão de documentos.

3. As informações confidenciais guardadas nos arquivos seguros podem ser consultadas nas seguintes condições:

a) Só são autorizadas a consultar essas informações as pessoas identificadas nominalmente, ou por força das suas funções, na ficha de acompanhamento preenchida aquando do depósito das informações confidenciais;

b) O pedido de consulta de informações confidenciais é apresentado à UIC, a qual assegura a transferência do documento em questão para a sala de leitura segura;

c) Aplicam-se os procedimentos e as condições de consulta de informações confidenciais estabelecidos no artigo 10.º.

Artigo 13.º

Desgraduação, desclassificação e desmarcação das informações classificadas

1. As informações confidenciais só podem ser desgraduadas, desclassificadas ou desmarcadas com a autorização prévia da entidade de origem e, se necessário, após discussão com as outras partes interessadas.

2. A desgraduação ou a desclassificação são confirmadas por escrito. A entidade de origem tem a responsabilidade de informar da alteração os seus destinatários, e estes, por seu turno, são responsáveis por informar da alteração quaisquer destinatários subsequentes aos quais tenham enviado o documento ou facultado um exemplar do mesmo. Se possível, as entidades de origem especificam nos documentos classificados a data, o período ou a ocorrência após os quais os conteúdos podem ser desgraduados ou desclassificados. Caso contrário, devem rever os documentos de cinco em cinco anos, no máximo, a fim de verificar se é necessário manter a classificação original.

3. As informações confidenciais guardadas nos arquivos seguros são examinadas em tempo útil, e o mais tardar 25 anos após a data da sua produção, a fim de determinar devem ou não ser desclassificadas, desgraduadas ou desmarcadas. O exame e a publicação destas informações são realizados nos termos do Regulamento (CEE, Euratom) n.º 354/83 do Conselho, de 1 de fevereiro de 1983, relativo à abertura ao público dos arquivos históricos da Comunidade Económica Europeia e da Comunidade Europeia da Energia Atómica ([1]). A desclassificação é efetuada pela entidade de origem das informações classificadas ou pelo serviço que no momento seja competente para o efeito, em conformidade com o Anexo I, Parte 1, ponto 10.

4. Após a desclassificação, as informações classificadas contidas no arquivo seguro são transferidas para os arquivos históricos do Parlamento Europeu para conservação permanente e tratamento ulterior segundo as normas aplicáveis.

5. Após a desmarcação, as outras informações confidenciais ficam sujeitas às normas do Parlamento Europeu em matéria de gestão de documentos.

Artigo 14.º

Quebra de segurança, perda ou exposição a risco de informações confidenciais

1. As quebras de confidencialidade em geral e as violações da presente decisão em particular implicam, no caso dos deputados ao Parlamento Europeu, a aplicação das disposições em matéria de sanções previstas no Regimento do Parlamento Europeu.

2. As quebras de confidencialidade cometidas por membros do pessoal do Parlamento Europeu implicam a aplicação dos procedimentos e sanções previstos, respetivamente, pelo Estatuto dos Funcionários e pelo Regime Aplicável aos Outros Agentes da União Europeia, estabelecidos no Regulamento (CEE, Euratom, CECA) n.º 259/68 ([2]) («Estatuto dos Funcionários»).

([1]) JO L 43, 15.2.1983, p. 1
([2]) JO L 56, 4.3.1968, p. 1

3. O Presidente e/ou o Secretário-Geral, consoante o caso, determinam os inquéritos necessários em caso de infração, nos termos da indicação de segurança n.º 6.

4. Se as informações confidenciais tiverem sido comunicadas ao Parlamento Europeu por uma instituição da União ou por um Estado-Membro, o Presidente e/ou o Secretário-Geral, consoante o caso, informam a instituição da União ou o Estado-Membro em causa de qualquer prova ou suspeita de perda ou exposição a risco de informações classificadas e dos resultados do inquérito, bem como das medidas tomadas para evitar novas ocorrências.

Artigo 15.º

Adaptação da presente decisão e das suas normas de execução e relatório anual sobre a aplicação da presente decisão

1. O Secretário-Geral propõe as adaptações necessárias da presente decisão e dos anexos que lhe dão execução e transmite essas propostas à Mesa para decisão.

2. O Secretário-Geral é responsável pela aplicação da presente decisão pelos serviços do Parlamento Europeu e emite as instruções de tratamento relativas aos assuntos da alçada do SGSI, em conformidade com os princípios estabelecidos pela presente decisão.

3. O Secretário-Geral apresenta à Mesa um relatório anual sobre a aplicação da presente decisão.

Artigo 16.º

Disposições transitórias e finais

1. Para efeitos da presente decisão, as informações não classificadas existentes na UIC ou em qualquer outro arquivo do Parlamento Europeu, consideradas confidenciais e com data anterior a 1 de abril de 2014, são consideradas como «outras informações confidenciais». A sua entidade de origem pode, a qualquer momento, reconsiderar o seu nível de confidencialidade.

2. Em derrogação ao artigo 5.º, n.º 1, alínea a), e ao artigo 8.º, n.º 1, da presente decisão, por um período de doze meses a partir de 1 de abril de 2014, as informações fornecidas pelo Conselho nos termos do Acordo Interinstitucional com a classificação RESTREINT UE/EU RESTRICTED, ou equivalente, são depositadas, registadas e armazenadas na UIC. Estas informações podem ser consultadas nos termos do artigo 4.º, n.º 2, alíneas a) e c), e do artigo 5.º, n.º 4, do Acordo Interinstitucional.

3. A Decisão da Mesa, de 6 de junho de 2011, sobre as regras que regem o tratamento de informações confidenciais pelo Parlamento Europeu, é revogada.

Artigo 17.º

Entrada em vigor

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

ANEXO I

Parte 1

PRINCÍPIOS DE BASE E NORMAS MÍNIMAS DE SEGURANÇA PARA A PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS

1. **INTRODUÇÃO**

As presentes disposições estabelecem os princípios de base e as normas mínimas de segurança para a protecção de informações confidenciais que devem ser respeitados e/ou cumpridos pelo Parlamento Europeu em todos os seus locais de trabalho, bem como por todos os destinatários de informações classificadas e de outras informações confidenciais, de modo a que a segurança seja salvaguardada, e que todas as pessoas interessadas possam ter a certeza de que foi estabelecida uma norma comum de proteção. As presentes disposições são completadas pelas indicações de segurança constantes do Anexo II e por outras disposições que regem o tratamento de informações confidenciais pelas comissões parlamentares e por outras instâncias parlamentares/titulares de um cargo.

2. **PRINCÍPIOS DE BASE**

A política de segurança do Parlamento Europeu é parte integrante da sua política geral de gestão interna e baseia-se, portanto, nos princípios que regem essa política geral. Esses princípios compreendem a legalidade, a transparência, a responsabilidade, a subsidiariedade e a proporcionalidade.

O princípio de legalidade implica a necessidade de que a execução das funções de segurança se mantenha estritamente dentro do quadro jurídico, e de respeitar as exigências legais aplicáveis. Significa, igualmente, que as responsabilidades em matéria de segurança devem assentar em disposições jurídicas apropriadas. Aplicam-se na íntegra as disposições do Estatuto dos Funcionários, nomeadamente o artigo 17.º, relativo à obrigação de o pessoal se abster de qualquer revelação não autorizada de informações recebidas no exercício das suas funções, e o título VI, relativo às medidas disciplinares. Por último, significa que as quebras de segurança nos domínios de responsabilidade do Parlamento Europeu devem ser tratadas em conformidade com o seu Regimento e com a sua política em matéria de medidas disciplinares.

O princípio de transparência implica a necessidade de clareza em todas as regras e disposições de segurança, a fim de se obter um equilíbrio entre os diferentes serviços e os diferentes domínios (segurança física em comparação com a proteção das informações, etc.), e de uma política coerente e estruturada de sensibilização para as questões de segurança. Significa, igualmente, que são necessárias diretrizes escritas claras para a aplicação das medidas de segurança.

O princípio de responsabilidade significa que as responsabilidades no domínio da segurança devem ser claramente definidas. Além disso, implica a necessidade de verificar regularmente se essas responsabilidades foram adequadamente cumpridas.

O princípio de subsidiariedade significa que a segurança deve ser organizada ao nível mais baixo e tão próximo quanto possível das direções-gerais e dos serviços do Parlamento Europeu.

O princípio de proporcionalidade significa que as atividades de segurança devem limitar-se estritamente ao mínimo necessário, e que as medidas de segurança devem ser proporcionais aos interesses a proteger e às ameaças reais ou potenciais a esses interesses, a fim de permitir que estes sejam defendidos de um modo que cause o mínimo de perturbação possível.

3. **BASES DA SEGURANÇA DA INFORMAÇÃO**

As bases de uma boa segurança da informação são:

a) Sistemas de comunicação e informação (SCI) adequados. Estes sistemas são responsabilidade da Autoridade de Segurança do Parlamento Europeu (definida na indicação de segurança n.º 1);

b) No Parlamento Europeu, a Autoridade de Garantia da Informação (definida na indicação de segurança n.º 1), encarregada de trabalhar com a Autoridades de Segurança para prestar informações e aconselhamento sobre ameaças técnicas aos SCI e sobre os meios de proteção contra essas ameaças;

c) Uma estreita cooperação entre os serviços do Parlamento Europeu responsáveis pela segurança e os serviços de segurança das outras instituições da União;

4. **PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO**

4.1. ***Objetivos***

Os objetivos principais da segurança da informação são os seguintes:

a) Salvaguardar as informações confidenciais dos riscos de espionagem, exposição ou divulgação não autorizada;

b) Salvaguardar as informações classificadas tratadas em sistemas e redes de comunicação e informação das ameaças à sua confidencialidade, integridade e disponibilidade;

c) Salvaguardar as instalações do Parlamento Europeu que albergam informações classificadas dos riscos de sabotagem ou de danos intencionais;

d) Em caso de falha, avaliar os danos causados, limitar as suas consequências, realizar inquéritos de segurança e adotar as medidas corretivas necessárias.

4.2. ***Classificação***

4.2.1. No que respeita à confidencialidade, é necessário cautela e experiência na seleção das informações e dos materiais a proteger e na avaliação do grau de proteção requerido. É fundamental que o grau de proteção corresponda à importância securitária de cada elemento de informação e de cada peça de material a proteger. A fim de assegurar o bom fluxo da informação, devem ser evitadas tanto a sobreclassificação como a subclassificação.

4.2.2. O sistema de classificação é o instrumento que permite pôr em prática os princípios definidos na presente secção. É utilizado um sistema semelhante de classificação no planeamento e na organização da luta contra a espionagem, a sabotagem, o terrorismo e outras ameaças, por forma a garantir a máxima proteção das instalações mais importantes que alberguem informações classificadas e dos pontos mais sensíveis no interior dessas instalações;

4.2.3. A responsabilidade pela classificação das informações incumbe exclusivamente à entidade de origem das mesmas;

4.2.4. O nível de classificação baseia-se exclusivamente no conteúdo das informações em causa;

4.2.5. Quando vários elementos de informação estiverem agrupados, a classificação do conjunto deve ser pelo menos idêntica à classificação mais elevada aplicada a um dos seus elementos. A um conjunto de informações pode, porém, ser atribuída uma classificação mais elevada do que a atribuída às suas partes constituintes.

4.2.6 As classificações são atribuídas e mantidas apenas quando e durante o período necessário.

4.3. ***Objetivos das medidas de segurança***

As medidas de segurança devem:

a) Abranger todas as pessoas que tenham acesso a informações classificadas, aos suportes das informações classificadas e a outras informações confidenciais, bem como todos os locais que alberguem essas informações e instalações importantes;

b) Ser concebidas de modo a permitir identificar as pessoas cuja posição (em termos de acesso, relações ou outros) possa pôr em perigo a segurança dessas informações e das instalações importantes que as alberguem, e proceder à sua exclusão ou afastamento;

c) Impedir que pessoas não autorizadas tenham acesso a essas informações ou a instalações que as alberguem;

d) Assegurar que essas informações apenas sejam difundidas às pessoas que delas precisem de tomar conhecimento, princípio fundamental em todos os aspetos da segurança;

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

5. NORMAS MÍNIMAS COMUNS

O Parlamento Europeu deve assegurar que todos os destinatários de informações classificadas, tanto no interior da instituição como dependentes da sua competência, nomeadamente todos os seus serviços e prestadores de serviços, cumpram normas mínimas comuns de segurança, por forma a que essas informações possam ser transmitidas com a certeza de que serão tratadas com iguais precauções. Estas normas mínimas devem incluir critérios para a habilitação de segurança de funcionários do Parlamento Europeu e de outros agentes do Parlamento Europeu ao serviço dos grupos políticos, e procedimentos para a proteção das informações confidenciais.

O Parlamento Europeu só autorizará o acesso de entidades externas a essas informações, na condição de estas serem tratadas de acordo com disposições pelo menos estritamente equivalentes às normas mínimas comuns.

Estas normas mínimas serão igualmente aplicadas quando o Parlamento Europeu confiar a entidades industriais ou outras, por contrato ou convenção de subvenção, tarefas que envolvam informações confidenciais.

6. MEDIDAS DE SEGURANÇA APLICÁVEIS AOS FUNCIONÁRIOS DO PARLAMENTO EUROPEU E A OUTROS AGENTES DO PARLAMENTO EUROPEU AO SERVIÇO DOS GRUPOS POLÍTICOS

6.1. *Instruções de segurança aplicáveis aos funcionários do Parlamento Europeu e a outros agentes do Parlamento Europeu ao serviço dos grupos políticos*

Os funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos que ocupem lugares em que possam ter acesso a informações classificadas receberão instruções completas, ao assumirem as suas funções e, posteriormente, a intervalos regulares, sobre a necessidade de segurança e sobre os meios de a conseguir. Essas pessoas devem atestar por escrito ter lido e compreendido totalmente as disposições de segurança aplicáveis.

6.2. *Responsabilidades dos gestores*

Os gestores devem saber quais os membros do seu pessoal que trabalham com informações classificadas ou que têm acesso a sistemas de comunicação ou informação protegidos, e devem registar e relatar todos os incidentes e vulnerabilidades manifestas, suscetíveis de afetar a segurança.

6.3. *Estatuto de segurança dos funcionários do Parlamento Europeu e dos outros agentes do Parlamento Europeu ao serviço dos grupos políticos*

Devem ser definidos procedimentos para garantir que, quando forem comunicadas informações desfavoráveis relativamente a um funcionário do Parlamento Europeu ou a um agente do Parlamento ao serviço dos grupos políticos, sejam tomadas medidas para determinar se o trabalho dessa pessoa a põe em contacto com informações classificadas ou se tem acesso a sistemas de comunicação ou de informação protegidos, e para que o serviço competente do Parlamento Europeu seja informado. Se a Autoridade Nacional de Segurança indicar que essa pessoa constitui um risco para a segurança, deverá ser afastada ou proibida de desempenhar funções em que possa pôr em perigo a segurança.

7. SEGURANÇA FÍSICA

Entende-se por segurança física a aplicação de medidas de proteção física e técnica para impedir o acesso não autorizado a informações classificadas.

7.1. ***Necessidade de proteção***

O grau das medidas de segurança física a aplicar para assegurar a proteção das informações classificadas deve ser proporcional à classificação, ao volume e às ameaças a que estão expostos os materiais e as informações existentes. Todos os detentores de informações classificadas devem aplicar práticas uniformes em matéria de classificação dessas informações e respeitar normas comuns de proteção no que se refere ao armazenamento, à transmissão e à eliminação de informações e de materiais que necessitem de proteção.

7.2. ***Controlo***

Antes de abandonarem locais onde existam informações classificadas, as pessoas responsáveis pela guarda das mesmas devem assegurar que essas informações se encontram guardadas em condições de segurança e que todos os dispositivos de segurança foram ativados (fechaduras, alarmes, etc.). Devem ser efetuadas outras ações de controlo independentes após as horas de serviço.

7.3. ***Segurança dos edifícios***

Deve ser impedido o acesso não autorizado aos edifícios onde existam informações classificadas ou sistemas de comunicação e informação protegidos.

A natureza da proteção concedida às informações classificadas, por exemplo, janelas com grades, fechaduras nas portas, guardas nas entradas, sistemas automatizados de controlo de acesso, controlo e rondas de segurança, sistemas de alarme, sistemas de deteção de intrusão e cães de guarda, dependerá:

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

b) Da qualidade dos contentores de segurança das informações e dos materiais em causa; e

c) Das características físicas e da localização do edifício.

A natureza da proteção concedida aos sistemas de comunicação e informação dependerá da avaliação do valor das informações e dos materiais em causa e dos danos potenciais em caso de falha de segurança, das características físicas e da localização do edifício em que o sistema se encontrar, e da localização desse sistema no interior do edifício.

7.4. ***Planos de emergência***

É necessário elaborar com antecedência planos pormenorizados para a proteção das informações classificadas em caso de emergência.

8. **INDICADORES DE SEGURANÇA, MARCAS, APOSIÇÃO E GESTÃO DA CLASSIFICAÇÃO**

8.1. ***Indicadores de segurança***

Não são permitidas outras classificações para além das definidas no artigo 2.º, alínea d), da presente decisão.

Pode ser utilizado um indicador de segurança acordado para limitar no tempo a validade de uma classificação (ou seja, o momento da desgraduação ou da desclassificação automática das informações classificadas).

Os indicadores de segurança só podem ser utilizados em associação com uma classificação.

Os indicadores de segurança são regulados na indicação de segurança n.º 2 e são definidos nas instruções de tratamento.

8.2. ***Marcas***

É aposta uma marca para indicar instruções concretas, estabelecidas previamente, sobre o tratamento das informações confidenciais. Uma marca pode indicar também o domínio abrangido por um documento ou uma distribuição específica com base no princípio da necessidade de tomar conhecimento, ou (no caso de informações não classificadas) o fim de uma proibição.

As marcas não constituem uma classificação e não devem ser utilizadas como uma alternativa à classificação.

Os indicadores de segurança são regulados na indicação de segurança n.º 2 e são definidos nas instruções de tratamento.

8.3. ***Aposição das classificações e dos indicadores de segurança***

A aposição das classificações e indicadores de segurança e das marcas é efetuada em conformidade com a indicação de segurança n.º 2, secção E, e com as instruções de tratamento.

8.4. ***Gestão da classificação***

8.4.1 *Generalidades*

As informações são classificadas apenas em caso de necessidade. A classificação deve ser indicada de forma clara e correta e só será mantida enquanto as informações necessitarem de proteção.

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

Os funcionários do Parlamento Europeu procedem à classificação, desgraduação ou desclassificação das informações mediante instruções ou por delegação do Secretário-Geral.

Os procedimentos pormenorizados para o tratamento de documentos classificados devem ser concebidos de modo a garantir que estes sejam objeto de uma proteção adequada às informações que contenham.

O número de pessoas autorizadas a produzir informações com a classificação TRÈS SECRET UE/EU TOP SECRET deve ser o mais reduzido possível, e os seus nomes devem constar de uma lista elaborada pela UIC.

8.4.2 *Aplicação da classificação*

A classificação de um documento é determinada pelo nível de sensibilidade do seu conteúdo, em conformidade com as definições contidas no artigo 2.º, alínea d). É importante que as classificações sejam atribuídas de forma correta e comedida.

A classificação de uma carta ou nota de envio de documentos deve ser equivalente ao nível mais alto de classificação dos documentos anexos. A entidade de origem deve indicar claramente em que nível essa carta ou nota de envio deve ser classificada quando for separada dos documentos anexos.

A entidade de origem de um documento a classificar deve ter em conta as regras acima indicadas e abster-se de proceder a sobreclassificações ou subclassificações.

Cada uma das páginas, parágrafos, secções, anexos, apêndices, adendas e documentos anexos de um determinado documento pode exigir uma classificação diferente, e deve ser classificado em conformidade. A classificação do documento no seu todo deve ser a da sua parte com a classificação mais elevada.

9. **INSPEÇÕES**

A Direção da Segurança e Avaliação de Riscos do Parlamento Europeu, que pode solicitar assistência às autoridades de segurança do Conselho ou da Comissão, efetua inspeções internas periódicas das medidas de segurança tomadas para proteger as informações classificadas.

As autoridades de segurança e os serviços competentes das instituições da União podem levar a cabo, como parte de um processo acordado, iniciado por uma das partes, avaliações inter pares das disposições de segurança para a proteção das informações classificadas que tenham sido objeto de intercâmbio no quadro dos acordos interinstitucionais pertinentes.

10. **PROCEDIMENTOS DE DESCLASSIFICAÇÃO E DE DESMARCAÇÃO**

10.1. A UIC examina as informações confidenciais contidas no seu registo e apresenta à entidade de origem propostas de desclassificação ou de desmarcação de um documento o mais tardar no 25.º aniversário da sua produção. Os documentos que não tenham sido desclassificados ou desmarcados aquando de um primeiro exame devem ser reexaminados periodicamente pelo menos de cinco em cinco anos. Além de se aplicar a documentos efetivamente guardados nos arquivos seguros na zona securizada e devidamente classificados, o processo de desmarcação pode abranger também outras informações confidenciais existentes na instância parlamentar/titular de um cargo ou no serviço responsável pelos arquivos históricos do Parlamento.

10.2 A decisão relativa à desclassificação ou à desmarcação de um documento é, regra geral, da exclusiva competência da entidade de origem, ou, a título excecional, é tomada em conjunto com a instância parlamentar/titular de um cargo detentor dessas informações, antes que as informações contidas no documento sejam transferidas para o serviço encarregado dos arquivos históricos do Parlamento. A desclassificação ou desmarcação de informações classificadas só pode ser efetuada após consentimento prévio por escrito da entidade de origem. No caso de outras informações confidenciais, o secretariado da instância parlamentar/titular de um cargo detentor dessas informações decidirá, em conjunto com a entidade de origem, se o documento pode ser desmarcado.

10.3. Cabe à UIC informar, em nome da entidade de origem, os destinatários do documento da alteração de classificação ou de marcação, e estes, por seu turno, são responsáveis por informar os destinatários subsequentes aos quais tenham enviado o documento ou facultado um exemplar do mesmo.

10.4. A desclassificação não afeta nenhum dos indicadores de segurança nem nenhuma das marcas que possam aparecer no documento.

10.5. Em caso de desclassificação, a classificação inicial que figura no cimo e no fundo de cada página deve ser barrada. A primeira página (capa) do documento deve ser carimbada e completada com a referência da UIC. Em caso de desclassificação, a classificação inicial que figura no cimo de cada página deve ser barrada.

10.6. O texto do documento desclassificado ou desmarcado deve ser anexado à ficha eletrónica ou ao sistema equivalente em que tenha sido registado.

10.7. No caso dos documentos abrangidos pelas exceções relativas à vida privada e à integridade dos indivíduos ou aos interesses comerciais das pessoas singulares ou coletivas, e no caso dos documentos sensíveis, aplica-se o disposto no artigo 2.º do Regulamento (CEE, Euratom) n.º 354/83.

10.8. Além do disposto nos pontos 10.1. a 10.7, aplicam-se as seguintes regras:

a) No que diz respeito aos documentos de terceiros, a UIC consulta os terceiros em causa antes de proceder à desclassificação ou desmarcação;

b) No que diz respeito à exceção relativa à vida privada e à integridade dos indivíduos, o processo de desclassificação ou de desmarcação tem em conta, em particular, o consentimento da pessoa em causa, ou, consoante o caso, a impossibilidade de identificar a pessoa em causa;

c) No que diz respeito aos interesses comerciais das pessoas singulares ou coletivas, a pessoa em causa pode ser notificada mediante publicação no *Jornal Oficial da União Europeia* e dispor de um prazo de quatro semanas para apresentar observações.

Parte 2

PROCEDIMENTO DE HABILITAÇÃO DE SEGURANÇA

11. **PROCEDIMENTO DE HABILITAÇÃO DE SEGURANÇA PARA OS DEPUTADOS AO PARLAMENTO EUROPEU**

11.1. Para acederem às informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou equivalente, os deputados ao Parlamento Europeu devem ter sido autorizados para o efeito, nos termos dos pontos 11.3 e 11.4 do presente anexo, ou com base numa declaração sob compromisso de honra, nos termos do artigo 3.º, n.º 4, da presente decisão, de que não divulgarão essas informações.

11.2 Para terem acesso a informações com a classificação SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou equivalente, os deputados ao Parlamento Europeu devem ter sido autorizados nos termos dos pontos 11.3. e 11.4.

11.3. A autorização só é concedida aos deputados ao Parlamento Europeu que tenham sido objeto de um inquérito de segurança realizado pelas autoridades nacionais competentes dos EstadosMembros, nos termos dos pontos 11.9 a 11.14. O Presidente é responsável pela concessão da autorização aos deputados.

11.4 O Presidente pode conceder a autorização por escrito, após ter obtido o parecer das autoridades nacionais competentes dos EstadosMembros, com base no inquérito de segurança efetuado nos termos dos pontos 11.8 a 11.13.

11.5. A Direção da Segurança e Avaliação de Riscos do Parlamento Europeu mantém uma lista atualizada de todos os deputados ao Parlamento Europeu aos quais tenha sido concedida uma autorização, incluindo uma autorização temporária nos termos do ponto 11.15.

11.6. A autorização é válida por um período de cinco anos ou enquanto durarem as tarefas para as quais foi concedida, prevalecendo o prazo que for mais curto. Pode ser renovada pelo procedimento estabelecido no ponto 11.4.

11.7. A autorização é retirada pelo Presidente, caso este considere que existem motivos fundamentados para o fazer. Qualquer decisão de retirar uma autorização é notificada ao deputado ao Parlamento Europeu em questão, que pode pedir para ser ouvido pelo Presidente antes de a retirada produzir efeitos, e à autoridade nacional competente.

11.8. O inquérito de segurança é efetuado com a assistência do deputado ao Parlamento Europeu em questão e a pedido do Presidente. A autoridade nacional competente para a realização do inquérito de segurança é a do Estado-Membro de que o deputado em questão for nacional.

11.9. No âmbito do inquérito de segurança, o deputado ao Parlamento Europeu em questão deve preencher um formulário de informação pessoal.

11.10. O Presidente deve especificar no seu pedido às autoridades nacionais competentes o nível de informações classificadas a disponibilizar ao deputado ao Parlamento Europeu em questão, para que aquelas autoridades possam proceder ao inquérito de segurança.

11.11 A integralidade do processo de inquérito de segurança realizado pelas autoridades nacionais competentes, juntamente com os resultados obtidos, deve respeitar a legislação em vigor na matéria no Estado-Membro em questão, inclusive em matéria de recurso.

11.12. Se as autoridades nacionais competentes emitirem um parecer favorável, o Presidente pode conceder a autorização ao deputado em questão.

11.13. Um parecer desfavorável das autoridades nacionais competentes é notificado ao deputado ao Parlamento Europeu, que pode pedir para ser ouvido pelo Presidente. Caso o considere necessário, o Presidente pode pedir esclarecimentos adicionais às autoridades nacionais competentes. Se o parecer desfavorável for confirmado, a autorização não é concedida.

11.14. Todos os deputados ao Parlamento Europeu aos quais seja concedida uma autorização nos termos do ponto 11.3 recebem as instruções consideradas necessárias sobre a proteção de informações classificadas e sobre os meios de assegurar essa proteção no momento em que a autorização lhes for concedida e, posteriormente, a intervalos regulares. Esses deputados assinam uma declaração confirmando que receberam essas instruções.

11.15. Em circunstâncias excecionais, o Presidente, depois de ter notificado as autoridades nacionais competentes, e na condição de não ter obtido resposta destas no prazo de um mês, pode conceder uma autorização temporária a um deputado ao Parlamento Europeu por um período não superior a seis meses, sujeita aos resultados do inquérito de segurança referido no ponto 11.11. As autorizações temporárias assim concedidas não dão acesso às informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou equivalente.

12. PROCEDIMENTO DE HABILITAÇÃO DE SEGURANÇA PARA OS FUNCIONÁRIOS DO PARLAMENTO EUROPEU E OUTROS AGENTES DO PARLAMENTO EUROPEU AO SERVIÇO DOS GRUPOS POLÍTICOS

12.1. Só têm acesso a informações classificadas os funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos que, devido às suas funções e às exigências do serviço, necessitem de tomar conhecimento ou de aceder a tais informações.

12.2. Para terem acesso a informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET e, ou equivalente, os funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos devem ter obtido uma autorização nos termos dos pontos 12.3 e 12.4.

12.3. A autorização só é concedida às pessoas referidas no ponto 12.1 que tenham sido objeto de um inquérito de segurança pelas autoridades nacionais competentes dos EstadosMembros, em conformidade com o procedimento referido nos pontos 12.9 a 12.14. O Secretário-Geral é responsável pela concessão da autorização aos funcionários do Parlamento Europeu e aos outros agentes do Parlamento Europeu ao serviço dos grupos políticos.

12.4. O Secretário-Geral pode conceder a autorização por escrito, após ter obtido o parecer das autoridades nacionais competentes dos EstadosMembros, com base no inquérito de segurança efetuado nos termos dos pontos 12.8 a 12.13.

12.5. A Direção da Segurança e Avaliação de Riscos do Parlamento Europeu mantém uma lista atualizada de todos os lugares que exigem uma habilitação de segurança, indicados pelos serviços pertinentes do Parlamento Europeu, e de todas as pessoas às quais tenha sido concedida uma autorização, incluindo uma autorização temporária nos termos do ponto 12.15.

12.6. A autorização é válida por um período de cinco anos ou enquanto durarem as tarefas para as quais foi concedida, prevalecendo o prazo que for mais curto. Pode ser renovada pelo procedimento estabelecido no ponto 12.4.

12.7. A autorização é retirada pelo Secretário-Geral, caso este considere que existem motivos fundamentados para o fazer. Qualquer decisão de retirar uma autorização é notificada ao funcionário do Parlamento Europeu ou outro agente do Parlamento ao serviço do grupo político em questão, que pode pedir para ser ouvido pelo Secretário-Geral antes de a retirada produzir efeitos, e à autoridade nacional competente.

12.8. O inquérito de segurança é efetuado com a assistência do funcionário do Parlamento Europeu ou de outros agentes do Parlamento Europeu ao serviço dos grupos políticos, a pedido do Secretário-Geral. A autoridade nacional competente para a realização do inquérito de segurança é a do Estado-Membro de que a pessoa em questão for nacional. Quando as disposições legislativas e regulamentares nacionais o permitirem, as autoridades nacionais competentes podem realizar inquéritos em relação a cidadãos estrangeiros que solicitem o acesso a informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET.

12.9. No âmbito do inquérito de segurança, o funcionário do Parlamento Europeu ou outro agente do Parlamento ao serviço do grupo político em questão deve preencher um formulário de informação pessoal.

12.10. O Secretário-Geral deve especificar no seu pedido às autoridades nacionais competentes o nível de informações classificadas a disponibilizar à pessoa em questão, para que aquelas autoridades possam proceder ao inquérito de segurança e dar o seu parecer quanto ao nível de autorização que será adequado conceder a essa pessoa.

12.11. A integralidade do processo de inquérito de segurança realizado pelas autoridades nacionais competentes, juntamente com os resultados obtidos, devem respeitar a legislação em vigor no Estado-Membro em questão, inclusive em matéria de recurso.

12.12. Se as autoridades nacionais competentes emitirem um parecer favorável, o Secretário-Geral pode conceder a autorização em causa ao funcionário do Parlamento Europeu ou a outro agente do Parlamento ao serviço do grupo político em causa.

12.13. Um parecer desfavorável das autoridades nacionais competentes é notificado ao funcionário do Parlamento Europeu ou outro agente do Parlamento ao serviço do grupo político em questão, que pode pedir para ser ouvido pelo Secretário-Geral. Caso o considere necessário, o Secretário-Geral pode pedir esclarecimentos adicionais às autoridades nacionais competentes. Se o parecer desfavorável for confirmado, a autorização não é concedida.

12.14. Todos os funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos aos quais seja concedida uma autorização nos termos dos pontos 12.4 e 12.5 recebem as instruções consideradas necessárias sobre a proteção de informações classificadas e os meios de assegurar essa proteção no momento em que a autorização lhes for concedida e, posteriormente, a intervalos regulares. Esses funcionários e agentes assinam uma declaração confirmando que receberam essas instruções e comprometem-se a respeitá-las.

12.15. Em circunstâncias excecionais, o Secretário-Geral, depois de ter notificado as autoridades nacionais competentes, e na condição de não ter obtido resposta destas no prazo de um mês, pode conceder uma autorização temporária a um funcionário do Parlamento Europeu ou a outro agente do Parlamento ao serviço de um grupo político por um período não superior a seis meses, sujeita aos resultados do inquérito de segurança referido no ponto 12,11. As autorizações temporárias assim concedidas não dão acesso às informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou equivalente.

ANEXO II

INTRODUÇÃO

As presentes disposições estabelecem as indicações de segurança que regem e garantem o tratamento e a gestão seguros das informações confidenciais pelo Parlamento Europeu. Estas indicações de segurança, juntamente com as instruções de tratamento, constituem o sistema de gestão da segurança das informações (SGSI) do Parlamento Europeu a que se faz referência no artigo 3.º, n.º 2, da presente decisão.

INDICAÇÃO DE SEGURANÇA n.º 1

Organização da segurança no Parlamento Europeu para a proteção de informações confidenciais

INDICAÇÃO DE SEGURANÇA n.º 2

Gestão de informações confidenciais

INDICAÇÃO DE SEGURANÇA n.º 3

Tratamento de informações confidenciais por meio de sistemas de comunicação e informação (SCI) automatizados

INDICAÇÃO DE SEGURANÇA n.º 4

Segurança física

INDICAÇÃO DE SEGURANÇA n.º 5

Segurança industrial

INDICAÇÃO DE SEGURANÇA n.º 6

Quebra da segurança, perda ou exposição a risco de informações confidenciais

INDICAÇÃO DE SEGURANÇA n.º 1

ORGANIZAÇÃO DA SEGURANÇA NO PARLAMENTO EUROPEU PARA A PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS

1. O Secretário-Geral é responsável pela aplicação geral e coerente da presente decisão.

O Secretário-Geral adota todas as medidas necessárias para assegurar que, para efeitos do tratamento ou armazenamento de informações confidenciais, os deputados ao Parlamento Europeu, os funcionários do Parlamento Europeu, outros agentes do Parlamento Europeu ao serviço dos grupos políticos e os contratantes, apliquem a presente decisão nas instalações do Parlamento.

2. O Secretário-Geral é a Autoridade de Segurança (AS). Nesta qualidade, o Secretário-Geral é responsável por:

2.1. coordenar todos os assuntos de segurança relativos às atividades do Parlamento em matéria de proteção de informações confidenciais;

2.2. aprovar a instalação de uma zona securizada, de salas de leitura segura e de equipamentos seguros;

2.3. aplicar decisões que autorizem, nos termos do artigo 6.º da presente Decisão, o Parlamento a transmitir informações classificadas a terceiros;

2.4. investigar ou ordenar uma investigação sobre qualquer fuga de informações confidenciais que, à primeira vista, tenha ocorrido no Parlamento, em colaboração com o Presidente do Parlamento Europeu, quando se encontrar envolvido um deputado ao Parlamento Europeu;

2.5. manter um contacto estreito com as autoridades de segurança de outras instituições e com as autoridades nacionais de segurança dos EstadosMembros, a fim de garantir uma coordenação otimizada das políticas de segurança em matéria de informações classificadas;

2.6. sujeitar as políticas e os procedimentos de segurança do Parlamento a uma revisão permanente e adotar as recomendações pertinentes resultantes dos mesmos;

2.7. informar a Autoridade Nacional de Segurança (ANS) que realizou o procedimento de inquérito de segurança, nos termos do Anexo I, Parte 2, ponto 11.3, em casos que envolvam informações desfavoráveis, suscetíveis de afetar essa autoridade.

3. Se estiverem envolvidos deputados ao Parlamento Europeu, o Secretário-Geral exercerá as suas responsabilidades em estreita colaboração com o Presidente do Parlamento Europeu.

4. No cumprimento das suas responsabilidades nos termos dos n.os 2 e 3, o Secretário-Geral é assistido pelo Secretário-Geral Adjunto, pela Direção da Segurança e Avaliação de Riscos, pela Direção das Tecnologias da Informação (DIT) e pela Unidade de Informações Classificadas (UIC).

4.1. A Direção da Segurança e Avaliação de Riscos é responsável por adotar medidas de proteção pessoal e, em particular, pelo procedimento de habilitação de segurança previsto no Anexo I, Parte 2. Compete à Direção da Segurança e Avaliação de Riscos, em particular:

a) Servir de ponto de contacto para as autoridades de segurança das demais instituições da União e para as ANS sobre questões relativas aos procedimentos de habilitação de segurança destinados aos deputados ao Parlamento Europeu, funcionários do Parlamento Europeu e outros agentes do Parlamento Europeu ao serviço dos grupos políticos;

b) Facultar as informações gerais necessárias em matéria de segurança no que diz respeito à obrigação de proteger informações classificadas e das consequências de um eventual incumprimento;

c) Controlar o funcionamento da zona securizada e das salas de leitura seguras nas instalações do Parlamento, em cooperação, se for caso disso, com os serviços de segurança de outras instituições da União e as ANS;

d) Proceder à auditoria, em colaboração com os serviços de segurança de outras instituições da União e as ANS, dos procedimentos de gestão e armazenamento das informações classificadas, da zona securizada e das salas de leitura segura nas instalações do Parlamento em que sejam tratadas informações classificadas;

e) Propor ao Secretário-Geral as instruções de tratamento adequadas.

4.2. A DIT é responsável pelos sistemas informáticos seguros que efetuam o tratamento de informações confidenciais pelo Parlamento Europeu.

4.3. A UIC é responsável:

a) Por identificar as necessidades em matéria de segurança com vista à eficaz proteção de informações confidenciais, em estreita colaboração com a Direção da Segurança e Avaliação de Riscos e a DIT, e com as autoridades de segurança das outras instituições da União;

b) Por identificar todos os aspetos relacionados com a gestão e o armazenamento de informações confidenciais no Parlamento, tal como estabelecido nas instruções de tratamento;

c) Pelo funcionamento da zona securizada;

d) Pela gestão ou consulta de informações confidenciais na zona securizada ou na sala de leitura segura da UIC, nos termos do artigo 7.º, n.os 2 e 3, da presente decisão;

e) Pela gestão do registo da UIC;

f) Por informar a AS sobre qualquer prova ou suspeita de violação de segurança, perda ou exposição a risco em relação às informações confidenciais depositadas na UIC e contidas na zona securizada ou na sala de leitura segura da UIC.

5. Além disso, o Secretário-Geral, na sua qualidade de AS, procede à nomeação das seguintes autoridades:

a) Autoridade de Acreditação de Segurança (AAS);

b) Autoridade Operacional de Garantia da Informação (AOGI);

c) Autoridade de Distribuição Criptográfica (ADC);

d) Autoridade TEMPEST (AT);

e) Autoridade de Garantia da Informação (AGI).

O exercício destas funções não implica a existência de entidades orgânicas únicas. Terão mandatos independentes. Contudo, aquelas funções, e as responsabilidades que lhes estão associadas, podem ser combinadas ou integradas na mesma entidade orgânica ou divididas em diferentes entidades orgânicas, desde que sejam evitados quaisquer conflitos internos de interesses ou a duplicação de funções.

6. A AAS aconselha sobre todos os assuntos de segurança relacionados com a acreditação de cada sistema e rede de tecnologia da informação no Parlamento, cabendo-lhe o seguinte:

6.1. Garantir a conformidade dos SCI com as políticas de segurança e as pertinentes diretrizes técnicas de segurança, emitir uma declaração de aprovação dos SCI para o tratamento de ICUE até um determinado nível de classificação, no seu ambiente operacional, enunciando os termos e condições da acreditação e os critérios segundo os quais é exigida nova aprovação;

6.2. Definir um processo de acreditação de segurança, nos termos das políticas pertinentes, em que sejam claramente estabelecidas as condições de aprovação dos SCI sob a sua autoridade;

6.3. Definir uma estratégia de acreditação de segurança em que se estabeleça para o processo de acreditação um grau de pormenor proporcional ao nível de garantia exigido;

6.4. Analisar e aprovar documentação em matéria de segurança, nomeadamente as declarações de gestão de risco e de risco residual, a documentação de verificação da execução e os procedimentos operacionais de segurança, e garantir a conformidade desta documentação com as regras e políticas de segurança do Parlamento;

6.5. Verificar a execução das medidas de segurança relativamente aos SCI, realizando ou promovendo avaliações, inspeções ou controlos de segurança;

6.6. Definir requisitos de segurança (por exemplo, níveis de credenciação do pessoal) para posições sensíveis relativamente aos SCI;

6.7. Aprovar a interconexão de um SCI com outro SCI, ou, se for caso disso, participar na aprovação conjunta dessa interconexão;

6.8. Aprovar as normas de segurança do equipamento técnico previsto para o tratamento e proteção seguros de informações classificadas;

6.9. Garantir que os produtos criptográficos utilizados no Parlamento estão incluídos na lista UE de produtos aprovados; e

6.10. Consultar o fornecedor do sistema, os intervenientes e os representantes dos utilizadores no domínio da segurança a respeito da gestão de risco, em especial do risco residual, e dos termos e condições da declaração de aprovação.

7. Cabe à AOGI:

7.1. Elaborar documentação em matéria de segurança de acordo com as políticas e diretrizes na matéria, nomeadamente a declaração de risco residual, os procedimentos operacionais de segurança e o plano criptográfico no processo de acreditação do SCI;

7.2. Tomar parte na seleção e no ensaio das medidas técnicas de segurança, dispositivos e programas informáticos específicos do sistema, a fim de supervisionar a sua implementação e garantir a segurança da sua instalação, configuração e manutenção, nos termos da documentação de segurança pertinente;

7.3. Acompanhar a execução e aplicação dos procedimentos operacionais de segurança e, se necessário, delegar no detentor do sistema, a saber, a UIC, quaisquer responsabilidades em matéria de segurança operacional;

7.4. Gerir e manusear os produtos criptográficos, assegurar a guarda de elementos cifrados e controlados e, se necessário, assegurar a geração de variáveis criptográficas;

7.5. Proceder a revisões das análises de segurança e a ensaios, em especial para a elaboração dos relatórios de risco exigidos pela AAS;

7.6. Fornecer à UIC formação específica em matéria de garantia da informação;

7.7. Executar e pôr em prática medidas de segurança específicas em relação ao SCI.

8. Cabe à ADC:

8.1. Gerir e prestar contas pelo material criptográfico da União;

8.2. Garantir, em estreita cooperação com a AAS, a aplicação dos procedimentos e a criação dos canais adequados para prestar contas pelo material criptográfico da União e proceder ao seu tratamento, armazenamento e distribuição em condições de segurança; e

8.3. Assegurar as transferências de material criptográfico da União para as pessoas singulares ou os serviços que o utilizem, e as transferências deles provenientes.

9. A AT é responsável pela garantia da conformidade dos SCI com as políticas e diretrizes TEMPEST. A AT procede à aprovação de contramedidas TEMPEST aplicáveis a instalações e produtos destinados a proteger as informações classificadas, no seu ambiente operacional, até um determinado nível de classificação.

10. A AGI é responsável por todos os aspetos da gestão e do tratamento de informações confidenciais no Parlamento, cabendo-lhe, em particular:

10.1 Definir a segurança em matéria de garantia da informação e as respetivas diretrizes de segurança, e acompanhar a sua eficácia e pertinência;

10.2. Salvaguardar e administrar as informações técnicas relativas aos produtos criptográficos;

10.3. Garantir que as medidas em matéria de garantia da informação selecionadas para proteção das informações confidenciais estejam em consonância com as políticas pertinentes que regem a sua elegibilidade e seleção;

10.4. Garantir que os produtos criptográficos sejam selecionados em conformidade com as políticas que regem as suas elegibilidade e seleção;

10.5. Consultar o fornecedor do sistema, os intervenientes e os representantes dos utilizadores em matéria de segurança da garantia da informação;

INDICAÇÃO DE SEGURANÇA n.º 2

GESTÃO DE INFORMAÇÕES CONFIDENCIAIS

A. **INTRODUÇÃO**

1. Esta indicação de segurança estabelece as disposições com vista à gestão de informações confidenciais pelo Parlamento.

2. Ao produzir informações confidenciais, a entidade de origem avalia o nível de confidencialidade e toma uma decisão baseada nos princípios estabelecidos na presente indicação no que diz respeito à classificação ou marcação dessas informações.

B. **CLASSIFICAÇÃO DAS ICUE**

3. A decisão de classificar um documento é feita antes da sua produção. Neste contexto, a classificação de informações como «informações classificadas» implica uma avaliação prévia do seu nível de confidencialidade e a decisão da entidade de origem de que a divulgação não autorizada dessas informações causaria vários graus de prejuízo aos interesses da UE, ou a um ou mais dos seus EstadosMembros, ou a particulares.

4. Uma vez tomada a decisão de classificar a informação, segue-se uma segunda avaliação prévia a fim de determinar o nível de classificação apropriado. A classificação de um documento é determinada pelo nível de sensibilidade do seu conteúdo.

5. A responsabilidade pela classificação das informações incumbe exclusivamente à entidade de origem. Os funcionários do Parlamento procedem à classificação das informações mediante instruções ou por delegação do Secretário-Geral.

6. A classificação deve ser utilizada de forma correta e comedida. A entidade de origem de um documento a classificar deve ter em mente as regras atrás indicadas e abster-se de proceder a sobreclassificações ou subclassificações.

7. O nível de classificação atribuído à informação determinará o nível de proteção que lhe é conferida nos domínios da segurança do pessoal, segurança física, segurança dos procedimentos e garantia da informação.

8. A informação que careça de classificação será marcada e tratada como tal, independentemente do respetivo suporte físico. A sua classificação será comunicada aos respetivos destinatários com clareza, quer mediante uma marcação (se for transmitida por escrito, quer em papel quer em suporte informático), quer mediante anúncio (se for transmitida oralmente, como, por exemplo, numa conversa ou numa reunião realizada à porta fechada). O material classificado será marcado fisicamente de forma a permitir a fácil identificação da sua classificação de segurança.

9. As ICUE em formato eletrónico só podem ser produzidas no quadro de um SCI acreditado. As próprias informações classificadas, bem como a designação do ficheiro e o dispositivo de armazenamento (se for externo, CD-ROM ou memória USB) ostentam a marca de segurança pertinente.

10. As informações são classificadas assim que adquirem forma. Por exemplo, notas pessoais, projetos ou mensagens de correio eletrónico que contenham informações que careçam de classificação levam a marcação ICUE desde o início, e devem ser apresentadas e tratadas em conformidade com a presente Decisão e as suas instruções de tratamento em termos físicos e técnicos. Estas informações podem depois converter-se num documento oficial que, por seu turno, obterá a marcação e o tratamento adequados. Durante o seu processo de elaboração, um documento oficial pode carecer de uma nova avaliação e ser-lhe atribuído um nível de classificação superior ou inferior, em consequência da sua evolução.

11. A entidade de origem pode decidir atribuir um nível de classificação convencional às categorias de informação que essa mesma entidade produz de forma regular. No entanto, a entidade de origem deve certificar-se de que, ao fazê-lo, não está a proceder a sobreclassificações ou subclassificações sistemáticas de elementos de informação.

12. As ICUE ostentarão sempre uma marca de segurança correspondente à classificação do seu nível de segurança.

B.1. ***Níveis de classificação***

13. As ICUE são classificadas num dos seguintes níveis:

— «TRÈS SECRET UE/EU TOP SECRET», na aceção do artigo 2.º, alínea d), da presente decisão, classificação que, a ser comprometida, poderia:

a) Ameaçar diretamente a estabilidade interna da União ou de um ou mais dos seus EstadosMembros ou de países terceiros ou de organizações internacionais,

b) Causar prejuízos excecionalmente graves às relações com países terceiros ou com organizações internacionais,

c) Conduzir diretamente a enormes perdas humanas,

d) Causar prejuízos excecionalmente graves à eficácia operacional ou à segurança dos efetivos destacados dos EstadosMembros ou de outros, assim como à continuação da eficácia de operações extremamente valiosas de segurança ou de recolha de informações,

e) Causar graves prejuízos a longo prazo à economia da União ou dos EstadosMembros;

— «TRÈS SECRET UE/EU TOP SECRET», na aceção da alínea d) do artigo 2.º da presente decisão, classificação que, a ser comprometida, poderia:

a) Elevar as tensões internacionais a um grau significativo;

b) Causar graves prejuízos às relações com os países terceiros e as organizações internacionais;

c) Ameaçar diretamente a vida ou prejudicar gravemente a ordem pública ou a segurança ou a liberdade individuais;

d) Comprometer importantes negociações de natureza comercial ou política, causando problemas operacionais significativos à União ou aos EstadosMembros;

e) Causar graves prejuízos à segurança dos EstadosMembros ou à eficácia de operações de segurança ou de informação sumamente importantes;

f) Causar substanciais prejuízos materiais aos interesses financeiros, monetários, económicos e comerciais da União ou dos EstadosMembros;

g) Debilitar substancialmente a viabilidade financeira de organizações ou operadores importantes; ou

h) Entravar gravemente o desenvolvimento ou o funcionamento de políticas da União com importantes consequências de ordem económica, comercial ou financeira;

— «CONFIDENTIEL UE/EU CONFIDENTIAL», na aceção do artigo 2.º, alínea d), da presente decisão, classificação que, a ser comprometida, poderia:

a) Lesar significativamente as relações diplomáticas, originando, por exemplo, um protesto formal ou outras sanções;

b) Colocar em risco a segurança ou a liberdade individuais;

c) Pôr gravemente em risco os resultados de negociações de natureza comercial ou política; causar problemas operacionais à União ou aos EstadosMembros;

d) Causar prejuízos à segurança operacional dos EstadosMembros ou à eficácia de operações de segurança ou de recolha de informações;

e) Debilitar substancialmente a viabilidade financeira de organizações ou operadores importantes;

f) Impedir a investigação ou facilitar o cometimento de crimes ou de atividades terroristas;

g) Lesar substancialmente os interesses financeiros, monetários, económicos e comerciais da União ou dos EstadosMembros; ou

h) Entravar gravemente o desenvolvimento ou o funcionamento de políticas da União com importantes consequências de ordem económica, comercial ou financeira;

— «RESTREINT UE/EU RESTRICTED», na aceção da alínea d) do artigo 2.º da presente decisão, classificação que, a ser comprometida, poderia:

a) Ter consequências desfavoráveis para os interesses gerais da União;

b) Afetar negativamente as relações diplomáticas;

c) Causar grande aflição às pessoas ou empresas,

d) Ter consequências desfavoráveis para a União ou para um ou vários dos seus EstadosMembros em negociações de natureza comercial ou política;

e) Tornar mais difícil manter uma segurança eficaz na União ou nos EstadosMembros;

f) Impedir o efetivo desenvolvimento ou funcionamento de políticas da União;

g) Enfraquecer a correta gestão da União e das suas operações;

h) Violar os compromissos assumidos pelo Parlamento a fim de manter a natureza classificada das informações fornecidas por terceiros;

i) Violar as restrições legais em matéria de divulgação da informação;

j) Causar perdas financeiras ou facilitar ganhos ou vantagens ilícitas a indivíduos ou a empresas; ou

k) Prejudicar a investigação ou facilitar o cometimento de crimes.

B.2. ***Classificação de coletâneas, páginas de rosto e extratos***

14. A classificação de uma carta ou nota de envio de documentos deve ser equivalente ao nível mais alto de classificação dos documentos anexos. A entidade de origem deve indicar claramente em que nível essa carta ou nota de envio deverá ser classificada quando for separada dos documentos anexos. Quando a carta ou nota de envio não carece de classificação, incluirá a seguinte frase no final: «A presente nota ou carta não será classificada quando for separada dos respetivos documentos anexos.»

15. Sempre que possível, os documentos ou dossiês que contenham componentes com diferentes níveis de classificação devem ser estruturados de forma a permitir que os componentes com diferentes níveis de classificação sejam identificados facilmente e, se necessário, separados. O nível de classificação geral de um documento ou dossiê deve ser, pelo menos, tão elevado quanto a do componente desse documento classificado ao nível mais elevado.

16. Cada uma das páginas, parágrafos, secções, anexos, apêndices, adendas e documentos anexos de um determinado documento pode exigir uma classificação diferente, e deve ser classificado em conformidade. Nos documentos que contenham ICUE, podem ser utilizadas abreviaturas normalizadas para indicar o nível de classificação de secções ou blocos do texto com menos de uma página.

17. Quando forem coligidas informações provenientes de várias fontes, o produto final será analisado para determinar o seu nível geral de classificação de segurança, uma vez que poderá justificar uma classificação mais elevada que a das partes que o compõem.

C. **OUTRAS INFORMAÇÕES CONFIDENCIAIS**

18. «Outras informações confidenciais» são marcadas em conformidade com o ponto E da presente indicação de segurança e com as instruções de tratamento.

D. **PRODUÇÃO DE INFORMAÇÕES CONFIDENCIAIS**

19. Só as pessoas devidamente autorizadas pela presente Decisão ou autorizadas pela AS podem produzir informações confidenciais.

20. As informações confidenciais não figuram nos sistemas de gestão de documentos na Internet ou Intranet.

D.1. ***Produção de ICUE***

21. A fim de produzir ICUE com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, ou TRÈS SECRET UE/EU TOP SECRET, a pessoa em questão deve ser autorizada pela presente decisão a dispor de uma autorização nos termos do artigo 4.º, n.º 1 da presente Decisão.

22. As ICUE com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, devem ser produzidas apenas dentro da zona securizada.

23. São aplicáveis as seguintes regras à produção de ICUE:

a) Cada página é marcada claramente com o nível de classificação aplicável;

b) Cada página é numerada e indica o número total de páginas;

c) O documento ostentará um número de referência na primeira página e uma indicação do respetivo assunto, o que, em si, não constituirá informação classificada, a menos que isso seja indicado como tal;

d) O documento ostentará uma data na primeira página;

e) A primeira página de qualquer documento com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, deverá ostentar a lista de todos os anexos ou apêndices que o acompanhe;

f) Os documentos com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, que devam ser distribuídos em vários exemplares, ostentarão um número de exemplar em todas as páginas. Cada página ostentará também na primeira página o número total de exemplares e de páginas; e

g) Se o documento fizer referência a outros documentos que contêm informações classificadas recebidas de outras instituições da União, ou se contém informações classificadas provenientes desses documentos, ostentará o mesmo nível de classificação que esses documentos, e, sem o prévio consentimento por escrito da respetiva entidade de origem, só pode ser distribuído às pessoas indicadas na lista de distribuição relativa ao documento original ou aos documentos que contenham informações classificadas.

24. A entidade de origem conserva o controlo sobre as ICUE que criou. Deve ser solicitado o prévio consentimento por escrito da entidade de origem antes que as ICUE sejam:

a) Desgraduadas ou desclassificadas;

b) Utilizadas para fins diferentes dos estabelecidos pela entidade de origem;

c) Transmitidas a um país terceiro ou organização internacional;

d) Teveladas a uma pessoa, instituição, país ou organização internacional que não seja o destinatário originalmente autorizado pela entidade de origem a consultar as informações em questão;

e) Reveladas a um contratante ou possível contratante estabelecido num país terceiro;

f) Copiadas ou traduzidas, se as informações tiverem a classificação TRÈS SECRET UE/ EU TOP SECRET;

g) Destruídas;

D.2. ***Produção de outras informações confidenciais***

25. O Secretário-Geral, na sua qualidade de AS, pode decidir se autoriza ou não a produção de outras informações confidenciais por uma dada função, serviço e/ou pessoa.

26. Outras informações confidenciais ostentarão uma das marcas definidas nas instruções de tratamento.

27. São aplicáveis as seguintes regras à produção de outras informações confidenciais:

a) A sua classificação é indicada no cimo da primeira página do documento;

b) Cada página é numerada e indica o número total de páginas;

c) O documento ostentará um número de referência na primeira página e uma indicação do respetivo assunto;

d) O documento ostentará uma data na primeira página;

e) A última página do documento contém a lista de todos os anexos e apêndices.

28. A produção de outras informações confidenciais está sujeita a regras e a procedimentos específicos estabelecidos nas instruções de tratamento.

E. **INDICADORES E MARCAS DE SEGURANÇA**

29. O objetivo dos indicadores e marcas de segurança em documentos é controlar o fluxo de informação e restringir o acesso às informações confidenciais com base no princípio da necessidade de tomar conhecimento.

30. Quando se utiliza ou ostenta indicadores e/ou marcas de segurança, devem ser tomadas providências para evitar confusões com as classificações de segurança aplicáveis às ICUE RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET.

31. Nas instruções de tratamento são estabelecidas regras específicas sobre a utilização dos indicadores e marcas de segurança, juntamente com a lista das marcas de segurança aprovadas pelo Parlamento Europeu.

E.1. ***Indicadores de segurança***

32. Os indicadores de segurança só podem ser utilizados conjuntamente com uma classificação de segurança e não se aplicam separadamente aos documentos. Pode ser aplicado um indicador de segurança às ICUE a fim de:

a) Fixar limites à validade de uma classificação (no caso de informações classificadas, implicará a desgraduação ou desqualificação automática);

b) Limitar a distribuição de ICUE em causa;

c) Estabelecer modalidades específicas de tratamento, para além das que correspondem à classificação do nível de segurança.

33. Os controlos adicionais aplicáveis ao tratamento e armazenamento dos documentos que contêm ICUE impõem encargos adicionais a todas as partes envolvidas. Para minimizar o trabalho necessário neste sentido, constitui uma boa prática, aquando da produção desse documento, estabelecer um prazo ou acontecimento, após o qual a classificação caducará automaticamente e as informações contidas no documento serão desgraduadas ou desclassificadas.

34. Quando um documento se ocupe de um âmbito de trabalho específico e a sua distribuição deva ser limitada e/ou vá ser sujeita a modalidades de tratamento especiais, pode ser acrescentada à sua classificação uma declaração para esse efeito, a fim de ajudar a identificar o público a que se dirige.

E.2. ***Marcas***

35. As marcações não constituem uma classificação de segurança. Servem apenas para fornecer instruções concretas sobre o tratamento de um documento e não serão utilizadas para descrever o conteúdo desse documento.

36. As marcas podem ser aplicadas aos documentos separadamente ou utilizadas conjuntamente com uma classificação de segurança.

37. Em regra geral, as marcas são aplicadas às informações abrangidas pelo sigilo profissional (artigo 339.º do TFUE, artigo 17.º do Estatuto dos funcionários, ou que, por razões legais, têm de ser protegidas pelo Parlamento), mas que não carecem de classificação (ou que não podem ser classificadas).

E.3 ***Utilização de marcas na UIC***

38. As regras relativas à utilização das marcas são também aplicáveis às UIC acreditadas.

39. Cabe à Autoridade de Acreditação de Segurança definir regras específicas relativas à utilização das marcas nas UIC acreditadas.

F. **RECEÇÃO**

40. A UIC é a única instância do Parlamento autorizada a receber informações de terceiros com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET ou com classificação equivalente.

41. Para as informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outra informações confidenciais, tanto a UIC como a instância parlamentar/titular de um cargo competente podem assumir a responsabilidade de as receber de terceiros e de aplicar os princípios estabelecidos na presente indicação de segurança.

G. **REGISTO**

42. Por «registo», entende-se a aplicação de procedimentos que registem o ciclo de vida das informações confidenciais, incluindo a sua difusão, consulta e destruição.

43. Para efeitos da presente indicação de segurança, «Livro de Registos» é o livro em que se inscreve, nomeadamente, a data e a hora em que as informações confidenciais:

a) Dão entrada ou saída no secretariado da instância parlamentar/titular de um cargo ou na UIC, consoante o caso;

b) São consultadas por pessoas com credenciação de segurança ou a elas transmitidas; e

c) São destruídas.

44. A entidade de origem das informações classificadas assume a responsabilidade pela marcação da declaração inicial, uma vez produzido o documento que contenha essas informações. Essa declaração será comunicada à UIC quando o documento estiver criado.

45. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET ou com classificação equivalente, apenas podem ser registadas pela UIC para fins de segurança. As informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais recebidas de terceiros são registadas, para fins administrativos, pelo serviço encarregado da receção oficial do documento, que será a UIC ou o secretariado da instância parlamentar/titular de um cargo. Outras informações confidenciais produzidas no Parlamento serão registadas pela entidade de origem, para fins administrativos.

46. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET ou com classificação equivalente, são registadas, em especial, quando:

a) São produzidas;

b) Dão entrada ou saída na UIC; e

c) Quando dão entrada ou saída num SIC.

47. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, ou com classificação equivalente ou superior, são registadas especialmente quando:

a) São produzidas;

b) Dão entrada ou saída no secretariado da instância parlamentar/titular de um cargo ou na UIC, consoante o caso; e

c) Quando dão entrada ou saída num SCI;

48. O registo de informações confidenciais pode ser efetuado em papel ou em livros de registos eletrónicos/SCI.

49. Para as informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais, procede-se ao registo, pelo menos, do seguinte:

a) A data e a hora de entrada ou saída no secretariado da instância parlamentar/titular de um cargo ou na UIC, consoante o caso;

b) O título do documento, o nível de classificação ou marcação, a data de expiração da classificação ou da marcação e todo o número de referência atribuído ao documento.

50. Para as informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, procede-se ao registo, pelo menos, do seguinte:

a) A data e a hora de entrada ou saída na UIC;

b) O título do documento, o nível de classificação ou marcação, todo o número de referência atribuído ao documento e a data de expiração da classificação ou da marcação;

c) A identificação da entidade de origem;

d) A relação das pessoas a quem tenha sido concedido acesso ao documento e a hora em que este tenha sido consultado;

e) A indicação de todas as cópias ou traduções efetuadas do documento;

f) A data e a hora de entrada ou saída na UIC de todos os exemplares ou traduções do documento, e a indicação do local para onde foram enviadas e de quem as devolveu;

g) A data e a hora em que o documento foi destruído, e por quem, em conformidade com as regras de segurança do Parlamento em matéria de destruição; e

h) A desclassificação e desgraduação do documento.

51. Os livros de registos podem ser classificados ou marcados, consoante o mais apropriado. Os livros de registos relativos às informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, são registados ao mesmo nível.

52. As informações classificadas podem ser registadas:

a) Num único livro de registos; ou

b) Em livros de registos individuais, consoante o respetivo nível de classificação, segundo dão entrada ou saída, e em função da sua origem ou destino.

53. Em caso de tratamento eletrónico dentro de um determinado SCI, o procedimento de registo pode ser efetuado por meios internos ao próprio SCI que respeitem requisitos equivalentes aos acima descritos. Quando as ICUE saem do perímetro do SCI, aplica-se o procedimento de registo acima descrito.

54. A UIC manterá um registo de todas as informações classificadas facultadas pelo Parlamento a terceiros, bem como das informações classificadas recebidas pelo Parlamento de terceiros.

55. Uma vez completado o registo das informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, a UIC comprovará se o destinatário dispõe de uma autorização de segurança válida. Se for esse o caso, a UIC informará o destinatário. A consulta de informações classificadas só pode ter lugar depois de o documento que as contém ter sido registado.

H. **DISTRIBUIÇÃO**

56. A entidade de origem estabelece a lista inicial de distribuição para as ICUE que tiver produzido.

57. As informações com a classificação RESTREINT UE/EU RESTRICTED e outras informações confidenciais produzidas pelo Parlamento são distribuídas dentro do Parlamento pela entidade de origem, em conformidade com as pertinentes instruções de tratamento e com base no princípio da necessidade de tomar conhecimento. Para as informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, produzidas pelo Parlamento dentro da zona securizada, a lista de distribuição (e todas as instruções adicionais relativas à distribuição) serão fornecidas à UIC, que é responsável pela sua gestão.

58. Só a UIC pode distribuir a terceiros as ICUE produzidas pelo Parlamento, com base no princípio da necessidade de tomar conhecimento.

59. As informações confidenciais recebidas pela UIC ou por uma instância parlamentar/titular de um cargo que tenha apresentado o pedido a esse respeito são distribuídas em conformidade com as instruções recebidas da entidade de origem.

I. **TRATAMENTO, ARMAZENAMENTO E CONSULTA**

60. O tratamento, armazenamento e consulta de informações confidenciais é realizado em conformidade com a indicação sobre segurança n.º 4 e as instruções de tratamento.

J. **CÓPIA/TRADUÇÃO/INTERPRETAÇÃO DE INFORMAÇÕES CLASSIFICADAS**

61. Os documentos com a classificação TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, não podem ser copiados ou traduzidos sem o prévio consentimento por escrito da entidade de origem. Os documentos com a classificação SECRET UE/EU SECRET, ou equivalente, ou com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, ou equivalente, podem ser copiados ou traduzidos por ordem do respetivo detentor, desde que a entidade de origem tal não tenha proibido.

62. Todos os exemplares de documentos com a classificação TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET EU ou CONFIDENTIEL UE/EU CONFIDENTIAL, ou com classificação equivalente, são registados, para efeitos de segurança.

63. As medidas de segurança aplicáveis ao documento original que contém informações classificadas serão aplicáveis do mesmo modo às respetivas cópias e traduções.

64. Os documentos recebidos do Conselho devem ser recebidos em todas as línguas oficiais.

65. Os exemplares e/ou traduções de documentos que contenham informações classificadas podem ser solicitados pela entidade de origem ou pelo detentor de um exemplar. As cópias dos documentos que contenham informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, apenas podem ser produzidas na zona securizada, utilizando fotocopiadoras que façam parte de um SCI acreditado. As cópias dos documentos que contenham informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais são produzidas dentro das instalações do Parlamento, utilizando um aparelho de reprodução acreditado.

66. Procede-se à devida marcação, numeração e registo de todos os exemplares e traduções de um documento, ou partes de cópia de um documento, que contenha informações confidenciais.

67. Não serão feitas mais cópias do que o número estritamente necessário. No final do período de consulta, todas as cópias serão destruídas em conformidade com as instruções de tratamento.

68. Os intérpretes e tradutores com acesso a informações classificadas são obrigatoriamente funcionários do Parlamento.

69. Os intérpretes e tradutores com acesso a documentos que contenham informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, dispõem da devida habilitação de segurança.

70. Ao trabalharem em documentos que contenham informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, os intérpretes e tradutores permanecerão na zona securizada.

K. **DESGRADUAÇÃO, DESCLASSIFICAÇÃO E ELIMINAÇÃO DA MARCAÇÃO DE INFORMAÇÕES CLASSIFICADAS**

K.1. ***Princípios gerais***

71. Quando já não seja necessária proteção, ou esta não seja requerida ao nível original, as informações confidenciais serão desclassificadas, desgraduadas, ou desmarcadas.

72. A decisão de desgraduação, desclassificação ou desmarcação de informações contidas em documentos produzidos no Parlamento poderá também ser tomada numa base ad hoc, por exemplo, em resposta a um pedido de acesso do público ou de uma outra instituição da União, ou por iniciativa da UIC ou de uma instância parlamentar/titular de um cargo.

73. Aquando da sua criação, a entidade de origem indicará, sempre que possível, se as ICUE em causa podem ser desgraduadas ou desclassificadas em determinada data ou após um dado acontecimento. Quando não for viável fornecer essa informação, a entidade de origem, a UIC ou a instância parlamentar/titular de um cargo detentor da informação procederá à revisão do nível de classificação das ICUE pelo menos de cinco em cinco anos. As ICUE não podem, em caso algum, ser objeto de desgraduação ou de desclassificação sem o prévio consentimento por escrito da entidade de origem.

74. No caso de não ser possível estabelecer ou apurar a entidade de origem de um documento produzido dentro do Parlamento, a AS procederá à revisão do nível de classificação das ICUE com base numa proposta da instância parlamentar/titular de um cargo detentor da informação, podendo consultar a UIC a este respeito.

75. A UIC ou a instância parlamentar/titular de um cargo detentor da informação assume a responsabilidade de informar o(s) destinatário(s) da desclassificação ou desgraduação da informação, e, por seu turno, o(s) destinatário(s) assumem a responsabilidade de informar o(s) destinatário(s) subsequente(s) aos quais tenha(m) enviado o documento ou entregue uma cópia do mesmo.

76. É registada a desclassificação, desgraduação ou desmarcação das informações contidas num documento.

K.2. ***Desclassificação***

77. As ICUE podem ser objeto de uma desclassificação total ou parcial. Podem ser objeto de desclassificação parcial quando deixe de ser considerada necessária a proteção de uma parte específica do documento que a contém, mas continue a justificar-se em relação ao resto do documento.

78. Quando a revisão das ICUE contidas num documento produzido dentro do Parlamento dê lugar à decisão de as desclassificar, deve ponderar-se a questão se o documento pode ser tornado público ou se deve ostentar uma marca de distribuição (ou seja, não ser tornado público).

79. Quando se proceda à desclassificação de ICUE, devem ser inscritas no livro de registos as seguintes informações: a data da desclassificação, a identidade de quem a tiver solicitado e autorizado, o número de referência do documento desclassificado e o seu destino final.

80. As marcas de classificação antigas que o documento desclassificado e todos os seus exemplares apresentarem deverão ser barradas. O documento, e todos os seus exemplares, deverão ser adequadamente armazenados.

81. Uma vez parcialmente desclassificadas as informações classificadas, a parte desclassificada será produzida na forma de extrato e devidamente armazenada. O serviço competente registará:

a) A data da desclassificação parcial;

b) A identidade de quem solicitou e autorizou a desclassificação; e

c) O número de referência do extrato desclassificado.

K.3. ***Desgraduação***

82. Uma vez efetuada a desgraduação das informações classificadas, o documento será registado no livro de registos correspondente, tanto ao nível da antiga como da nova classificação. Deve ainda ficar registada a data da desgraduação, bem como a identidade da pessoa que a tiver autorizado.

83. O documento desgraduado, bem como todos os seus exemplares, devem ser marcados com o novo nível de classificação e adequadamente armazenados.

L. **PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS**

84. As informações confidenciais (tanto em papel como em formato eletrónico) que deixem de ser necessárias serão destruídas ou suprimidas, em conformidade com as instruções de tratamento e as regras pertinentes em matéria de arquivo.

85. As informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou equivalente, ou com a classificação SECRET UE/EU SECRET, ou equivalente, serão destruídas pela UIC, na presença de uma pessoa detentora de uma habilitação de segurança no mínimo correspondente ao nível de classificação das informações que são destruídas.

86. As informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, apenas poderão ser destruídas com o prévio consentimento por escrito da entidade de origem.

87. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, serão destruídas e eliminadas pela UIC, sob as instruções da entidade de origem ou de uma autoridade competente. Os livros de registo e demais registos serão atualizados em conformidade. As informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, serão destruídas e eliminadas pela UIC ou pela instância parlamentar/titular de um cargo pertinente.

88. O funcionário responsável pela destruição e a testemunha assinarão um certificado de destruição, a ser completado e arquivado na UIC. A UIC conserva, juntamente com os impressos de distribuição, os certificados de destruição das informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, por um período não inferior a dez anos, e os das informações com a classificação SECRET UE/EU SECRET, ou com classificação equivalente, e CONFIDENTIEL UE/EU CONFIDENTIAL, ou com classificação equivalente, por um período não inferior a cinco anos.

89. Os documentos que contenham informações classificadas serão destruídos segundo uma modalidade que cumpra as pertinentes regras da União, ou regras equivalentes, por forma a evitar a sua reconstituição, no todo ou em parte.

90. A destruição dos suportes informáticos utilizados para o armazenamento de informações classificadas será efetuada em conformidade com as correspondentes instruções de tratamento.

91. A destruição de informações classificadas é registada no correspondente livro de registos, com as seguintes informações:

a) O dia e a hora da destruição;

b) O nome do funcionário encarregado da destruição;

c) A identificação do documento ou dos exemplares destruídos;

d) O suporte físico original das ICUE destruídas;

e) O meio de destruição; e

f) O lugar de destruição.

M. **ARQUIVO**

92. As informações classificadas, incluindo cartas ou nota de envio, os anexos, o recebo de depósito e outras partes do dossiê, serão transferidas para o arquivo seguro da zona securizada seis meses após a última consulta e, o mais tardar, um ano após ter sido depositada. Nas instruções de tratamento, são estabelecidas regras de pormenor relativas ao arquivo de informações classificadas.

93. Para outras informações confidenciais, são aplicáveis as regras gerais sobre gestão de documentos, sem prejuízo de outras disposições específicas sobre o seu tratamento.

INDICAÇÃO DE SEGURANÇA n.º 3

TRATAMENTO DE INFORMAÇÕES CONFIDENCIAIS POR MEIO DE SISTEMAS DE COMUNICAÇÃO E INFORMAÇÃO (SCI) AUTOMATIZADOS

A. **GARANTIA DAS INFORMAÇÕES CLASSIFICADAS TRATADAS EM SISTEMAS DE INFORMAÇÃO**

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

2. Um sistema de comunicação e informação (SCI) consiste num sistema que permita o tratamento de informações em formato eletrónico. Um sistema de comunicação e informação compreende todos os ativos necessários ao seu funcionamento, designadamente infraestrutura, organização, pessoal e recursos em matéria de informação.

3. Os SCI efetuam o tratamento de informações em conformidade com o conceito de GI.

4. Os SCI são submetidos a um processo de acreditação. A acreditação visa obter a garantia de que foram tomadas todas as medidas de segurança adequadas e de que foi alcançado um nível suficiente de proteção das informações classificadas e do SCI, em conformidade com a presente indicação de segurança. A declaração de acreditação determina o nível máximo de classificação das informações que podem ser tratadas por um SCI, bem como os termos e condições correspondentes.

5. Para a segurança e o correto funcionamento das operações em SCI, são essenciais as seguintes propriedades e conceitos de GI:

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

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

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

d) Integridade: a propriedade de salvaguardar o caráter exato e completo da informação e dos ativos;

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

B. **PRINCÍPIOS DE GARANTIA DA INFORMAÇÃO**

6. As disposições adiante estabelecidas constituem a base da segurança dos SCI em que sejam tratadas informações confidenciais. Nas políticas e diretrizes de segurança em matéria de GI, serão definidos requisitos de pormenor para a execução das presentes disposições.

B.1. ***Gestão dos riscos de segurança***

7. A gestão dos riscos de segurança constitui parte integrante da definição, desenvolvimento, exploração e manutenção do SCI. A gestão dos riscos (avaliação, tratamento, aceitação e comunicação) será conduzida como um processo iterativo em que participem conjuntamente os representantes dos proprietários do sistema, as autoridades de projeto, as autoridades operacionais e as autoridades de aprovação de segurança, seguindo um processo de avaliação do risco comprovado, transparente e plenamente compreensível para todos. O alcance do SCI e os seus ativos serão claramente definidos logo no início do processo de gestão do risco.

8. As autoridades competentes, em conformidade com a instrução de segurança n.º 1, analisarão as potenciais ameaças ao SCI e efetuarão avaliações rigorosas e atualizadas da ameaça que reflitam o ambiente operacional vigente. Atualizarão constantemente o seu conhecimento sobre as questões relacionadas com as vulnerabilidades e procederão periodicamente à reanálise da avaliação das vulnerabilidades, por forma a acompanharem a evolução do ambiente das tecnologias da informação (TI).

9. O objetivo de tratar os riscos de segurança consiste em aplicar um conjunto de medidas de segurança que resulte num compromisso satisfatório entre os requisitos do utilizador, os custos e o risco de segurança residual.

10. A acreditação de um SCI inclui uma declaração formal de risco residual e a aceitação do risco residual por uma autoridade responsável. Os requisitos, a escala e o grau de pormenor específicos determinados pela AAS competente para proceder à acreditação de um SCI serão proporcionais ao risco avaliado, tendo em conta todos os fatores pertinentes, nomeadamente o nível de classificação das informações classificadas tratadas no SCI.

B.2. ***Segurança ao longo do ciclo de vida do SCI***

11. Haverá que garantir a segurança ao longo de todo o ciclo de vida do SCI, desde o início até à retirada de serviço.

12. Para cada fase do ciclo de vida, será identificado o papel de cada um dos intervenientes no SCI e a interação entre eles em termos de segurança do sistema.

13. Os SCI, incluindo as medidas de segurança, de caráter técnico e outras, são sujeitos a ensaios de segurança durante o processo de acreditação, a fim de assegurar o nível de garantia adequado e de verificar se os sistemas estão corretamente implementados, integrados e configurados.

14. São efetuadas periodicamente avaliações, inspeções e análises de segurança durante o funcionamento e a manutenção dos SCI, e quando ocorrem circunstâncias excecionais.

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

16. Os procedimentos de registo cumpridos pelo SCI serão, sempre que necessário, verificados no âmbito do processo de acreditação.

B.3. ***Boas práticas***

17. A AAI desenvolverá boas práticas com vista à proteção das informações classificadas tratadas num SCI. As orientações de boas práticas apresentarão medidas de segurança de natureza técnica, material, organizativa e processual para os SCI, de comprovada eficácia na luta contra determinadas ameaças e vulnerabilidades.

18. A proteção das informações classificadas tratadas num SCI basear-se-á na experiência adquirida pelas entidades envolvidas na GI.

19. A divulgação e a subsequente aplicação das boas práticas ajudarão a atingir um nível de garantia equivalente nos vários SCI que são explorados pelo secretariado do Parlamento em que são tratadas informações confidenciais.

B.4. ***Defesa em profundidade***

20. Para atenuar os riscos que pesam sobre os SCI, será posta em prática uma série de medidas de segurança, de natureza técnica e não técnica, organizadas em múltiplos estratos de defesa. Esses estratos de defesa incluem:

a) Dissuasão: medidas de segurança dissuasivas da concretização de planos hostis de ataque ao SCI;

b) Prevenção: medidas de segurança destinadas a impedir ou bloquear um ataque ao SCI;

c) Deteção: medidas de segurança destinadas a descobrir a ocorrência de um ataque ao SCI;

d) Resistência: medidas de segurança destinadas a limitar o impacto do ataque a um conjunto mínimo de informações ou ativos do SCI e a prevenir mais danos; e

e) Recuperação: medidas de segurança destinadas a restabelecer uma situação segura para o SCI.

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

21. As autoridades competentes, tal como consta da indicação de segurança n.º 1, deverão ter capacidade de resposta a incidentes suscetíveis de ultrapassar as fronteiras de uma organização ou de um país, a fim de coordenarem as respostas e de partilharem informações sobre esses incidentes e os riscos deles resultantes (capacidades de resposta a emergências informáticas).

B.5. ***Princípio da minimalidade e do menor privilégio***

22. A fim de evitar riscos desnecessários, só serão ativadas as funcionalidades, os dispositivos e os serviços essenciais para satisfazer os requisitos operacionais.

23. Para limitar os danos que possam resultar de acidentes, de erros ou da utilização não autorizada dos recursos do SCI, os seus utilizadores e processos automatizados beneficiarão unicamente do acesso, privilégios ou autorizações que forem indispensáveis ao desempenho das suas funções.

B.6. ***Sensibilização para a Garantia da Informação***

24. A sensibilização para os riscos e para as medidas de segurança disponíveis constitui a primeira linha de defesa da segurança dos sistemas de comunicação e informação. Mais concretamente, todos os elementos do pessoal envolvidos no ciclo de vida dos SCI, incluindo os utilizadores, deverão compreender que:

a) As falhas de segurança podem prejudicar consideravelmente os sistemas de comunicação e informação em que são tratadas informações classificadas;

b) A interconexão e a interdependência podem causar prejuízos a terceiros; e

c) Cada um tem a sua parte de responsabilidade e deverá prestar contas pela segurança do SCI, em função do papel que desempenha nos sistemas e processos.

25. A fim de assegurar uma boa perceção das responsabilidades em matéria de segurança, os cursos de formação e sensibilização para a GI serão obrigatórios para todo o pessoal envolvido, incluindo os funcionários que ocupem lugares de direção, os deputados ao Parlamento Europeu e os utilizadores dos SCI.

B.7. ***Avaliação e aprovação de produtos de segurança informática***

26. Os SCI em que sejam tratadas informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, são protegidos de forma a impedir a exposição das informações a riscos devido a emanações eletromagnéticas não intencionais («medidas de segurança TEMPEST»).

27. Quando a proteção das informações classificadas for efetuada mediante produtos criptográficos, esses produtos serão certificados pela AAS enquanto parte dos produtos criptográficos aprovados pela UE.

28. Durante a transmissão de informações classificadas por meios eletrónicos, serão utilizados produtos criptográficos aprovados pela UE. Não obstante este requisito, podem ser aplicados procedimentos específicos, em circunstâncias de emergência, ou configurações técnicas específicas, nos termos dos pontos 41 a 44.

29. O necessário grau de confiança nas medidas de segurança, definido como um nível de garantia, será determinado à luz dos resultados do processo de gestão dos riscos e de acordo com as políticas e diretrizes de segurança relevantes.

30. O nível de garantia será verificado mediante a utilização de metodologias e processos reconhecidos internacionalmente ou aprovados a nível nacional. Neles se incluem principalmente a avaliação, os controlos e as auditorias.

31. A AAS aprovará diretrizes de segurança aplicáveis à qualificação e aprovação de produtos não criptográficos de segurança informática.

B.8. ***Transmissão dentro da Zona Securizada***

32. Quando a transmissão de informações confidenciais se realizar dentro de zonas securizadas, poderá ser utilizada uma distribuição não cifrada ou cifragem a um nível inferior, com base nos resultados de um processo de gestão dos riscos, e sob reserva de aprovação da AAS.

B.9. ***Interconexão segura dos SCI***

33. Por «interconexão» entende-se a conexão direta, unidirecional ou multidirecional, de dois ou mais sistemas informáticos para efeitos de partilha de dados e de outros recursos de informação.

34. O SCI tratará qualquer sistema informático com ele interconectado como não fiável e tomará medidas de proteção para controlar o intercâmbio de informações classificadas com qualquer outro SCI.

35. Todas as interconexões de SCI com outro sistema informático obedecerão aos seguintes requisitos básicos:

a) Os requisitos operacionais ou de atividade dessas interconexões serão determinados e aprovados pelas autoridades competentes;

b) A interconexão será submetida a um processo de gestão dos riscos e de acreditação e deverá ser aprovada pelas AAS competentes;

c) Serão instalados serviços de proteção no perímetro de todos os SCI.

36. Não pode haver interconexão entre um SCI acreditado e uma rede desprotegida ou pública, a não ser que o SCI tenha aprovado um serviço de proteção instalado para esse efeito entre o SCI e a rede desprotegida ou pública. As medidas de segurança aplicáveis a estas interconexões serão avaliadas pela AGI competente e aprovadas pela AAS competente.

37. Quando a rede desprotegida ou pública for exclusivamente utilizada como transmissora e os dados forem cifrados por um produto criptográfico aprovado nos termos do artigo 27.º, não se considerará essa conexão como uma interconexão.

38. É proibida a interconexão direta ou em cascata entre, por um lado, SCI acreditados para tratar informações com a classificação TRÈS SECRET UE/EU TOP SECRET, ou equivalente, ou SECRET UE/EU SECRET, ou equivalente.

B.10. ***Suportes informáticos***

39. Os suportes informáticos devem ser destruídos segundo procedimentos aprovados pela autoridade de segurança competente.

40. Os suportes informáticos serão reutilizados, desgraduados ou desclassificados em conformidade com as instruções de tratamento.

B.11. ***Circunstâncias de emergência***

41. Os procedimentos específicos descritos a seguir podem ser aplicados numa emergência, nomeadamente em situações de crise iminente ou real, de conflito ou de guerra, ou em circunstâncias operacionais excecionais.

42. As informações confidenciais podem ser transmitidas por meio de produtos criptográficos aprovados para um nível de classificação inferior, ou sem cifragem, mediante o consentimento da autoridade competente, se o prejuízo causado por um atraso for claramente mais grave do que o decorrente da eventual divulgação do material classificado, e se:

a) O remetente e o destinatário não dispuserem do dispositivo de cifragem necessário ou não possuírem nenhum dispositivo de cifragem; e

b) O material classificado não puder ser enviado a tempo por outros meios.

43. As informações classificadas transmitidas nas circunstâncias referidas no ponto 41 não ostentarão marcas nem indicações que as distingam de informações não classificadas ou de informações que possam ser protegidas por produtos de cifragem disponíveis. Os destinatários serão imediatamente notificados, por outros meios, do nível de classificação das informações.

44. Em caso de recurso ao disposto nos pontos 41 ou 42, será subsequentemente apresentado um relatório nessa matéria à autoridade competente.

INDICAÇÃO DE SEGURANÇA n.º 4

SEGURANÇA FÍSICA

A. **INTRODUÇÃO**

Esta indicação de segurança estabelece os princípios relativos à segurança, a fim de criar um ambiente seguro que garanta o tratamento de informações confidenciais no Parlamento Europeu. Estes princípios, que incluem a segurança técnica, serão completados pelas instruções de tratamento.

B. **GESTÃO DOS RISCOS DE SEGURANÇA**

1. Os riscos a que estão sujeitas as informações classificadas são geridos como um processo. Esse processo terá por objetivo determinar os riscos de segurança conhecidos, definir as medidas de segurança destinadas a reduzir esses riscos para um nível aceitável, em conformidade com os princípios básicos e as normas mínimas estabelecidos na presente indicação de segurança, e aplicar tais medidas de acordo com o conceito de defesa em profundidade, tal como definido na indicação de segurança n.º 3. A eficácia das medidas será sujeita a avaliação contínua.

2. As medidas de segurança para a proteção de informações confidenciais ao longo do seu ciclo de vida devem ser proporcionais, designadamente, à classificação de segurança, à forma e ao volume da informação ou do material, à localização e construção das instalações que albergam informações confidenciais, e à avaliação local da ameaça de atos mal-intencionados e/ou atividades criminosas, nomeadamente de espionagem, sabotagem e terrorismo.

3. Os planos de emergência têm em conta a necessidade de proteger as informações classificadas em situações de emergência, a fim de evitar o acesso ou a divulgação não autorizados, ou a perda de integridade ou disponibilidade.

4. Os planos de continuidade das atividades incluem medidas de prevenção e recuperação destinadas a minimizar o impacto de quaisquer falhas ou incidentes graves sobre o tratamento e armazenamento de informações classificadas.

C. **PRINCÍPIOS GERAIS**

5. O nível de classificação ou de marcação atribuído à informação determina o nível de proteção que lhe é conferido nos domínios da segurança física.

6. A informação que careça de classificação será marcada e tratada como tal, independentemente do respetivo suporte físico. A sua classificação será comunicada aos respetivos destinatários com clareza, quer mediante uma marcação (se for transmitida por escrito, em papel ou como sistema de comunicação e informação), quer mediante anúncio (se for transmitida oralmente, como uma conversa ou apresentação). O material classificado será marcado fisicamente de forma a permitir a fácil identificação da sua classificação de segurança.

7. Em caso algum, informações confidenciais serão lidas em lugares públicos, onde possam ser intercetadas por quem delas não deva tomar conhecimento, como por exemplo em comboios, aviões, cafetarias, bares, etc.. Tão-pouco serão guardadas em cofres ou em aposentos de hotel. Não serão deixadas sem vigilância em lugares públicos.

D. **RESPONSABILIDADES**

8. A UIC tem a responsabilidade de garantir a segurança física na gestão das informações confidenciais depositadas nas suas instalações. A UIC é também responsável pela gestão das suas instalações.

9. A segurança física na gestão de informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e de outras informações confidenciais é da responsabilidade da respetiva instância parlamentar/titular de um cargo.

10. A Direção da Segurança e Avaliação de Riscos garante a segurança pessoal e a habilitação de segurança necessárias para garantir o tratamento seguro das informações confidenciais no Parlamento Europeu.

11. A Direção das Tecnologias da Informação aconselha e vela por que qualquer SCI criado ou utilizado se conforme plenamente à indicação de segurança n.º 3 e às respetivas instruções de tratamento.

E. **INSTALAÇÕES SEGURAS**

12. Poderão ser criadas instalações securizadas específicas, em conformidade com as normas de segurança técnica e com o nível atribuído às informações confidenciais, tal como determina o artigo 7.º.

13. As instalações seguras serão certificadas pela SAA (Autoridade de Acreditação de Segurança) e homologadas pela Autoridade de Segurança (SA).

F. **CONSULTA DE INFORMAÇÕES CONFIDENCIAIS**

14. Quando informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais forem depositadas nas instalações da UIC e tiverem de ser consultadas fora da zona securizada, a UIC enviará um exemplar ao serviço autorizado competente, que velará por que a consulta e o tratamento dessas informações respeitem o disposto no artigo 8.º, n.º 2, e no artigo 10.º da presente Decisão, bem como as respetivas instruções de tratamento.

15. Caso informações com a classificação RESTREINT UE/EU RESTRICTED, ou equivalente, e outras informações confidenciais sejam depositadas numa instância parlamentar/titular de um cargo que não seja a UIC, o secretariado dessa instância parlamentar/titular de um cargo assegura que a consulta e o tratamento dessas informações respeitem o disposto no artigo 7.º, n.º 3, no artigo 8.º, n.ºs 1, 2 e 4, no artigo 9.º, n.ºs 3, 4 e 5, no artigo 10.º, n.ºs 2 e 6, e no artigo 11.º da presente decisão, bem como as correspondentes instruções de tratamento.

16. Quando informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, tiverem de ser consultadas dentro da zona securizada, a UIC velará por que a consulta e o tratamento dessas informações respeitem o disposto nos artigos 9.º e 10.º da presente Decisão, bem como as respetivas instruções de tratamento.

G. **SEGURANÇA TÉCNICA**

17. As medidas de segurança técnica são da responsabilidade da SAA, que estabelecerá nas respetivas instruções de tratamento as medidas específicas em matéria de segurança técnica que cabe aplicar.

18. As salas de leitura segura para a consulta de informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais, cumprem as medidas específicas em matéria de segurança técnica estabelecidas nas instruções de tratamento.

19. A zona securizada inclui os seguintes serviços:

a) Uma sala de acesso mediante inquérito de segurança (SAS), que será instalada em conformidade com as medidas de segurança técnica estabelecidas nas instruções de tratamento. O acesso a esta sala é registado. A SAS cumpre padrões elevados em termos de identificação de pessoas com direito de acesso, gravação videográfica, espaço seguro para depositar pertences pessoais não autorizados nas salas securizadas (telefones, esferográficas, etc.);

b) Uma sala de comunicações para envio e receção de informações classificadas, incluindo informações classificadas codificadas, em conformidade com a indicação de segurança n.º 3 e as respetivas instruções de tratamento.

c) Um arquivo securizado, no qual contentores homologados e certificados serão utilizados separadamente para as informações com as classificações RESTREINT UE/EU RESTRICTED, ou CONFIDENTIEL UE/EU CONFIDENTIAL, ou SECRET EU/EU SECRET, ou com classificação equivalente. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, serão depositadas numa sala separada, num contentor certificado para esse fim específico. O único material adicional disponível nessa sala será o gabinete de apoio para que a UIC efetue a gestão do arquivo;

d) Uma sala de registo, que fornecerá os instrumentos necessários para garantir que o registo possa ser efetuado em papel ou por meios eletrónicos e que, por isso, será dotada dos serviços securizados necessários para instalar o SCI apropriado. A sala de registo será a única a conter equipamento de reprodução aprovado e acreditado (cópias em papel ou em formato eletrónico). As instruções de tratamento especificam qual é o equipamento de reprodução aprovado e acreditado. A sala de registo disporá também do material acreditado de armazenamento e tratamento necessário para a marcação, reprodução e envio de informações classificadas em suporte físico, por nível de classificação. Todo o material acreditado será definido pela UIC e acreditado pela SAA, segundo parecer da IAOA. Esta sala estará também equipada com um aparelho de destruição acreditado e aprovado para o nível de classificação mais elevado, tal como se descreve nas instruções de tratamento. A tradução das informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, será efetuada na sala de registo, segundo o sistema adequado e acreditado. A sala de registo disporá de postos de trabalho para um máximo de dois tradutores ao mesmo tempo e para um mesmo documento. Um agente da UIC estará presente.

e) Uma sala de leitura para a consulta individual de informações classificadas por pessoas devidamente autorizadas. A sala de leitura disporá de espaço suficiente para duas pessoas, incluindo um agente da UIC, que estará presente durante o tempo que dure cada consulta. O nível de segurança desta sala corresponde ao previsto para as informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, ou com classificação superior. A sala de leitura poderá ter equipamento TEMPEST para consulta eletrónica, se necessário, em conformidade com o nível de classificação da informação.

f) Uma sala de reuniões, com capacidade até 25 pessoas, para discutir informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET, ou com classificação equivalente. A sala de reuniões disporá de instalações tecnicamente seguras e certificadas, necessárias para a interpretação para duas línguas, no máximo. Quando não utilizada para reuniões, a sala de reuniões também poderá ser utilizada como sala de leitura adicional para consultas individuais. Em casos excecionais, a UIC pode permitir a mais do que uma pessoa autorizada a consulta de informações classificadas, desde que o grau de habilitação e a necessidade de tomar conhecimento sejam os mesmos para todas as pessoas na sala. Não poderão consultar informações classificadas mais do que quatro pessoas ao mesmo tempo. Será reforçada a presença de membros do pessoal da UIC.

g) Salas tecnicamente securizadas para depositar todo o equipamento técnico relacionado com a segurança de toda a zona securizada, bem como os servidores securizados de TI.

20. A zona securizada cumprirá as normas internacionais de segurança e será certificada pela Direção da Segurança e Avaliação de Riscos. A zona securizada disporá dos seguintes requisitos técnicos mínimos de segurança:

a) Sistemas de alarme e de controlo de segurança;

b) Equipamento de segurança e sistemas de emergência (duplo sistema de alarme);

c) Sistema de circuito fechado de televisão;

d) Sistema de deteção de intrusos;

e) Controlo de acesso (incluindo um sistema de segurança biométrico);

f) Contentores;

g) Cacifos;

h) Proteção contra a exposição eletromagnética.

21. A SAA pode acrescentar outras medidas de segurança técnica necessárias, em estreita colaboração com a UIC e com a prévia aprovação da SA.

22. Os equipamentos de infraestrutura podem ser ligados aos sistemas gerais de gestão do edifício em que a zona securizada se encontra localizada. Porém, o equipamento de segurança destinado ao acesso ao controlo e ao SCI não dependerá de nenhum outro sistema existente no Parlamento Europeu.

H. **INSPEÇÕES DA ZONA SECURIZADA**

23. A SAA leva a cabo inspeções periódicas à zona securizada e a pedido da UIC.

24. A SAA elabora e mantém atualizada uma lista de controlo para a inspeção de segurança dos pontos a verificar no decurso de uma inspeção, em conformidade com as instruções de tratamento.

I. **TRANSPORTE DE INFORMAÇÕES CONFIDENCIAIS**

25. As informações confidenciais são transportadas fora do alcance visual e sem indicar a natureza confidencial do respetivo conteúdo, em conformidade com as instruções de tratamento.

26. Só os mensageiros ou o pessoal com uma autorização correspondente ao nível de segurança podem transportar informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente.

27. Só se recorrerá ao correio externo ou ao transporte em mão fora de um edifício segundo as condições estabelecidas nas instruções de tratamento.

28. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente, nunca serão enviadas por correio eletrónico ou por fax, inclusive se for instalado um sistema de correio eletrónico securizado ou um fax criptográfico. As informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais podem ser enviadas por correio eletrónico mediante um sistema de codificação acreditado.

J. **ARMAZENAMENTO DE INFORMAÇÕES CONFIDENCIAIS**

29. O nível de classificação ou de marcação conferido à informação determina o nível de proteção conferido para efeitos do seu armazenamento, que deverá ser efetuado no equipamento certificado para o efeito, em conformidade com as instruções de tratamento.

30. As informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais:

a) São armazenadas num armário-padrão, metálico e fechado à chave, colocado num gabinete ou numa zona de trabalho quando não estiverem a ser efetivamente utilizadas;

b) Não serão deixadas sem vigilância, salvo se estiverem devidamente fechadas e armazenadas;

c) Não serão deixadas por cima de uma secretária, mesa, etc., de modo a permitir que as mesmas possam ser lidas ou retiradas por uma pessoa não autorizada, designadamente visitantes, pessoal de limpeza ou pessoal de manutenção, entre outros;

d) Não serão mostradas a uma pessoa não autorizada nem com ela discutidas.

31. As informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, e outras informações confidenciais apenas podem ser arquivadas no secretariado da instância parlamentar/titular de um cargo ou na UIC, em conformidade com as instruções de tratamento.

32. As informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, ou com classificação equivalente:

a) São arquivadas na zona securizada, num contentor de segurança ou numa casa-forte. A título excecional, se por exemplo a UIC estiver encerrada, podem ser armazenadas num cofre aprovado e certificado, localizado nos serviços de segurança;

b) Em momento algum serão deixadas sem vigilância dentro da zona securizada sem que primeiro tenham sido fechadas num cofre aprovado (inclusive durante uma ausência muito breve);

c) Não serão deixadas por cima de uma secretária, mesa, etc., permitindo que as mesmas possam ser lidas ou retiradas por uma pessoa não autorizada, mesmo se o agente da UIC responsável permanecer na sala.

Quando um documento que contenha informações classificadas for editado em formato eletrónico dentro da zona securizada, o computador será bloqueado e o acesso ao ecrã inviabilizado, sempre que a entidade de origem ou o agente da UIC responsável saírem da sala (inclusive durante uma ausência muito breve). Não se considera uma medida suficiente o bloqueio automático de segurança decorridos alguns minutos.

INDICAÇÃO DE SEGURANÇA n.º 5

SEGURANÇA INDUSTRIAL

A. **INTRODUÇÃO**

1. Esta indicação de segurança diz exclusivamente respeito a informações classificadas.

2. Estabelece disposições com vista à aplicação das normas mínimas comuns do Anexo I, Parte I, da presente Decisão.

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

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

B. **ELEMENTOS DE SEGURANÇA DOS CONTRATOS CLASSIFICADOS**

B.1. ***Guia da Classificação de Segurança (GCS)***

5. Antes de abrir concursos públicos ou de celebrar contratos classificados, o Parlamento Europeu determina, enquanto entidade adjudicante, qual a classificação de segurança de todas as informações a fornecer aos proponentes e contratantes, bem como de todas as informações a produzir pelos contratantes. Para o efeito, elabora um guia de classificação de segurança, que deve ser utilizado para a execução do contrato.

6. Para determinar qual a classificação de segurança dos vários elementos de um contrato classificado, são aplicáveis os seguintes princípios:

a) Na elaboração do guia de classificação de segurança, o Parlamento Europeu tem em consideração todos os aspetos de segurança relevantes, nomeadamente a classificação de segurança atribuída às informações fornecidas e aprovadas pela respetiva entidade de origem para utilização no âmbito do contrato;

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

B.2. ***Cláusula sobre aspetos de segurança (CAS)***

7. Os requisitos de segurança específicos de um contrato são descritos numa cláusula sobre aspetos de segurança (CAS). Esta CAS compreenderá, sempre que necessário, o guia de classificação de segurança e faz parte integrante do contrato ou subcontrato.

8. A CAS contém uma disposição em que exige que o contratante e/ou subcontratante cumpra as normas mínimas estabelecidas na presente decisão. O incumprimento dessas normas mínimas pode constituir motivo suficiente para a resolução do contrato.

B.3. ***Instruções de Segurança do Programa/Projeto (ISP)***

9. Em função do âmbito dos programas ou projetos que impliquem acesso, tratamento ou armazenamento de ICUE, a entidade adjudicante designada para efeitos da gestão do programa ou projeto pode elaborar Instruções específicas de Segurança do Programa/Projeto (ISP).

C. **CERTIFICAÇÃO DE SEGURANÇA DAS INSTALAÇÕES (CSI)**

10. A CSI é concedida pela ANS ou por qualquer outra autoridade de segurança competente de um Estado-Membro, a fim de indicar, nos termos das disposições legislativas e regulamentares nacionais, que determinada entidade industrial ou outra está em condições de proteger as ICUE ao nível de classificação adequado (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET) dentro das respetivas instalações. A CSI é apresentada ao Parlamento Europeu, enquanto entidade adjudicante, antes de as ICUE serem fornecidas ao contratante ou subcontratante ou potencial contratante, ou subcontratante ou de lhe ser concedido acesso a essas informações.

11. A habilitação de segurança das instalações:

a) Avalia a integridade da entidade industrial ou outra;

b) Avalia em que medida a propriedade, o controlo e/ou a potencial exposição a influências indevidas podem ser considerados um risco para a segurança;

c) Certifica que a entidade industrial ou outra instalou um sistema de segurança nas instalações que abrange todas as medidas de segurança adequadas à proteção das informações ou material com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, segundo os requisitos da presente decisão;

d) Certifica que o estatuto de segurança da administração, dos proprietários e dos empregados que necessitem de aceder a informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET foi estabelecido segundo os requisitos da presente decisão;

e) Certifica que a entidade industrial ou outra nomeou um Oficial de Segurança da Empresa, responsável perante a respetiva administração pelo cumprimento das obrigações em matéria de segurança na referida entidade.

12. Se necessário, o Parlamento Europeu, enquanto entidade adjudicante, informa a ANS competente, ou qualquer outra autoridade de segurança competente, de que é necessária uma CSI para a fase pré-contratual ou para a execução do contrato. É exigida uma CSI ou uma CSP para a fase pré-contratual quando tiverem de ser fornecidas ICUE com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET durante o processo de apresentação de propostas.

13. A entidade adjudicante não adjudicará nenhum contrato classificado ao proponente preferido antes de ter recebido, da ANS ou de qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante estiver registado, confirmação de que, sendo exigível, foi emitida a CSI adequada.

14. Toda a autoridade de segurança competente que tenha emitido a CSI informa o Parlamento Europeu, enquanto entidade adjudicante, de qualquer alteração que afete a CSI. Em caso de subcontrato, a autoridade de segurança competente será informada do facto.

15. A retirada da CSI pela ANS ou por qualquer outra autoridade de segurança competente constitui motivo suficiente para que o Parlamento Europeu, enquanto entidade adjudicante, ponha termo a um contrato classificado ou exclua um dos proponentes do concurso.

D. **CONTRATOS E SUBCONTRATOS CLASSIFICADOS**

16. Quando forem fornecidas informações classificadas aos proponentes na fase pré-contratual, o aviso de concurso deve compreender uma disposição que obrigue aqueles que não cheguem a apresentar uma proposta ou não sejam selecionados a devolverem todos os documentos classificados num prazo determinado.

17. Uma vez adjudicado um contrato ou subcontrato classificado, o Parlamento Europeu, enquanto entidade adjudicante, informará a ANS ou qualquer outra autoridade de segurança competente do contratante ou subcontratante sobre as disposições de segurança do contrato classificado.

18. Em caso de resolução de contratos desta natureza, o Parlamento Europeu, enquanto entidade adjudicante (e/ou a autoridade de segurança competente, consoante o caso, quando se trate de um subcontrato), informará imediatamente desse facto a ANS ou qualquer outra autoridade de segurança competente do Estado-Membro em que o contratante ou subcontratante estiver registado.

19. Regra geral, no termo do contrato classificado, o contratante ou subcontratante é obrigado a restituir à entidade adjudicante quaisquer informações classificadas que detenha.

20. Serão estabelecidas na CAS disposições específicas relativas à eliminação de informações classificadas durante a fase de execução ou após o termo do contrato.

21. Quando o contratante ou subcontratante for autorizado a conservar informações classificadas após o termo do contrato, as normas mínimas estabelecidas na presente decisão continuarão a ser cumpridas, e a confidencialidade das ICUE protegida pelo contratante ou subcontratante.

22. As condições em que o contratante pode subcontratar são definidas no concurso e no contrato.

23. Antes de procederem à subcontratação de quaisquer partes de contratos classificados, os contratantes deverão obter a autorização do Parlamento Europeu, enquanto entidade adjudicante. Nenhum subcontrato pode ser celebrado com entidades industriais ou outras registadas num país terceiro que não tiverem celebrado um acordo com a União em matéria de segurança das informações.

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

25. Os direitos da entidade de origem sobre as informações classificadas que o contratante ou subcontratante tiver produzido ou manuseado serão exercidos pela entidade adjudicante.

E. **VISITAS ASSOCIADAS A CONTRATOS CLASSIFICADOS**

26. Quando o Parlamento Europeu ou quaisquer contratantes ou subcontratantes necessitarem de aceder a informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET nas instalações uns dos outros, para a execução de um contrato classificado, serão organizadas visitas em articulação com as ANS ou com outras autoridades de segurança competentes a que o assunto diga respeito. Todavia, no contexto de determinados projetos, as ANS podem também aprovar um procedimento, segundo o qual as visitas dessa natureza podem ser organizadas diretamente.

27. Todos os visitantes devem ser titulares de uma CSP ou ter «necessidade de tomar conhecimento» para poderem aceder às informações classificadas relacionadas com o contrato do Parlamento Europeu.

28. Aos visitantes apenas é facultado o acesso às informações classificadas relacionadas com a finalidade da visita.

F. **TRANSMISSÃO E TRANSPORTE DE INFORMAÇÕES CLASSIFICADAS**

29. No que diz respeito à transmissão de informações classificadas por meios eletrónicos, serão aplicadas as disposições pertinentes da indicação de segurança n.º 3.

30. No que toca ao transporte de informações classificadas, serão aplicadas as disposições pertinentes da indicação de segurança n.º 4 e as respetivas instruções de tratamento.

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

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

b) O nível de proteção atribuído a uma remessa é determinado pelo nível de classificação mais elevado do material nela contido;

c) Será obtida uma CSI de nível adequado para as empresas que efetuem o transporte. Nesses casos, o pessoal que manipula a remessa será sujeito a credenciação de segurança, nos termos do Anexo I;

d) Antes de qualquer transporte transfronteiras de material com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, ou equivalente, o expedidor elaborará um plano de transporte, que será aprovado pelo Secretário-Geral;

e) Na medida do possível, o transporte será diretos, efetuando-se tão rapidamente quanto as circunstâncias o permitirem;

f) Sempre que possível, circular-se-á em território de Estados Membros.

G. **TRANSFERÊNCIA DE INFORMAÇÕES CLASSIFICADAS PARA CONTRATANTES ESTABELECIDOS EM PAÍSES TERCEIROS**

32. A transferência de informações confidenciais para contratantes e subcontratantes estabelecidos em países terceiros far-se-á de acordo com as medidas de segurança acordadas entre o Parlamento Europeu, enquanto entidade adjudicante, e o país terceiro em causa em que o contratante se encontre registado.

H. **TRATAMENTO E ARMAZENAMENTO DE INFORMAÇÕES COM A CLASSIFICAÇÃO RESTREINT UE/EU RESTRICTED**

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

34. Na medida do necessário ao abrigo das disposições legislativas e regulamentares nacionais, as ANS ou outras autoridades de segurança competentes serão informadas pelo Parlamento Europeu, na qualidade de entidade adjudicante, dos contratos ou subcontratos que envolvam informações com a classificação RESTREINT UE/EU RESTRICTED.

35. Não será necessário que os contratantes ou subcontratantes e respetivo pessoal possuam CSE nem CSP para a execução de contratos celebrados pelo Parlamento Europeu que envolvam informações com a classificação RESTREINT UE/EU RESTRICTED.

36. Não obstante as exigências de CSE ou CSP eventualmente previstas nas disposições legislativas e regulamentares nacionais, o Parlamento Europeu, enquanto entidade adjudicante, analisará as candidaturas apresentadas em concursos para adjudicação de contratos que exijam acesso a informações com a classificação RESTREINT UE/EU RESTRICTED.

37. As condições em que o contratante pode subcontratar são definidas no concurso e no contrato.

38. Quando um contrato implique o tratamento de informações com a classificação RESTREINT UE/EU RESTRICTED em sistemas de comunicação e informação geridos por um contratante, o Parlamento Europeu, enquanto entidade adjudicante, garantirá que o contrato ou qualquer subcontrato especifique os requisitos técnicos e administrativos necessários para a acreditação dos sistemas de comunicação e informação proporcionais aos riscos avaliados, tendo em conta todos os fatores pertinentes O âmbito da acreditação desses sistemas de comunicação e informação será acordado entre a autoridade adjudicante e a ANS/ASD competente.

INDICAÇÃO DE SEGURANÇA n.º 6

QUEBRA DA SEGURANÇA, PERDA OU EXPOSIÇÃO A RISCO DE INFORMAÇÕES CONFIDENCIAIS

1. Uma quebra da segurança é o resultado de um ato ou uma omissão contrários à presente decisão, suscetíveis de pôr em perigo ou expor informações confidenciais a risco.

2. As informações confidenciais são expostas a risco 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. As informações classificadas podem ser expostas a risco em resultado de descuido, negligência ou indiscrição, bem como em resultado das atividades de serviços que têm por alvo a UE ou das atividades de organizações de caráter subversivo.

4. Quando o Secretário-Geral descubra ou seja informado de um caso, comprovado ou suspeito, de quebra da segurança, perda ou exposição a risco relativo a informações confidenciais, deverá:

a) Determinar os factos ocorridos;

b) Avaliar e reduzir os danos verificados;

c) Tomar medidas para evitar uma nova ocorrência;

d) Notificar a autoridade competente de um terceiro ou do Estado-Membro que tiver produzido ou transmitido informações confidenciais.

Quando se encontrar envolvido um deputado ao Parlamento Europeu, o Secretário-Geral desta instituição agirá em conjunto com o Presidente do Parlamento.

Se a informação tiver sido transmitida pelas outras instituições da União, o Secretário-Geral agirá em conformidade com as medidas de segurança adequadas relativas às informações classificadas e com as disposições estabelecidas ao abrigo do Acordo-Quadro com a Comissão ou do Acordo Interinstitucional com o Conselho.

5. Todas as pessoas que devam tratar informações confidenciais receberão instruções completas sobre os procedimentos de segurança, os perigos de conversas indiscretas e as suas relações com os meios de comunicação social, e, se for caso disso, assinam uma declaração de que não divulgarão a terceiros o conteúdo das informações confidenciais, respeitarão a obrigação de proteger as informações classificadas, e em que reconhecem as consequências resultantes do incumprimento disso. Considera-se quebra da segurança o acesso a informações classificadas por uma pessoa que não tenha recebido as devidas instruções nem assinado a correspondente declaração, ou a utilização de tais informações por essa pessoa.

6. Os deputados ao Parlamento Europeu, os funcionários do Parlamento e outros agentes do Parlamento Europeu ao serviço dos grupos políticos ou contratantes devem notificar imediatamente ao Secretário-Geral toda a quebra da segurança, perda ou exposição de informações confidenciais a risco que cheguem ao seu conhecimento.

7. Qualquer indivíduo que seja responsável por uma exposição de informações confidenciais a risco será passível de ação disciplinar segundo as regras e regulamentos pertinentes. Essa ação disciplinar não será impeditiva de qualquer ação em justiça, em conformidade com a legislação aplicável.

8. Sem prejuízo de outras ações em justiça, os casos de quebra da segurança por funcionários do Parlamento e outros agentes do Parlamento Europeu ao serviço dos grupos políticos darão lugar à aplicação dos procedimentos e sanções previstos no Título VI do Estatuto dos Funcionários.

9. Sem prejuízo de outras ações em justiça, os casos de quebra da segurança por parte de deputados ao Parlamento Europeu serão tramitados em conformidade com o artigo 9.º, n.º 2, e com os artigos 152.º, 153.º e 154.º do Regimento do Parlamento.