DECISÃO (UE) 2022/640 DA COMISSÃO

de 7 de abril de 2022

sobre as regras de execução relativas às funções e responsabilidades dos principais intervenientes no domínio da segurança

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 249.º,

Tendo em conta a Decisão (UE, Euratom) 2015/443 da Comissão, de 13 de março de 2015, relativa à segurança na Comissão ([1]),

Tendo em conta a Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE ([2]),

Considerando o seguinte:

(1) As Decisões (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444 aplicam-se a todos os serviços e instalações da Comissão.

(2) Se necessário, as regras de execução que completam ou apoiam a Decisão (UE, Euratom) 2015/444 devem ser adotadas em conformidade com o artigo 60.º da mesma.

(3) As medidas de segurança destinadas a proteger as informações classificadas da UE ao longo do seu ciclo de vida devem ser proporcionais, em particular, à sua classificação de segurança.

(4) As medidas de segurança para proteger os sistemas de comunicação e informação na Comissão estão estabelecidas na Decisão (UE, Euratom) 2017/46 da Comissão ([3]), em especial no artigo 3.º, relativo aos princípios de segurança informática na Comissão, e no artigo 9.º, relativo aos proprietários de sistemas.

(5) O objetivo das regras de execução relativas às funções e responsabilidades dos principais intervenientes no domínio da segurança consiste em dar orientações sobre os pré-requisitos e deveres estabelecidos para essas funções nas Decisões (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444.

(6) O artigo 36.º, n.º 7, da Decisão (UE, Euratom) 2015/444 estabelece uma série de funções adicionais relacionadas com a segurança a assumir pela Autoridade de Segurança da Comissão. As tarefas relacionadas com estas funções são definidas na presente decisão.

(7) Os responsáveis locais de segurança e os responsáveis do controlo do registo têm responsabilidades específicas pela proteção das informações classificadas da UE nos seus serviços, em conformidade com a Decisão (UE, Euratom) 2015/444.

(8) Em 4 de maio de 2016, a Comissão adotou uma decisão ([4]) que habilita o membro da Comissão responsável pelas questões de segurança a adotar, em nome da Comissão e sob a sua responsabilidade, as regras de execução previstas no artigo 60.º da Decisão (UE, Euratom) 2015/444; posteriormente, em 13 de abril de 2021, o membro da Comissão responsável pelas questões de segurança adotou, em nome da Comissão e sob a sua responsabilidade, uma decisão ([5]) subdelegando estas regras de execução no diretor-geral da Direção-Geral dos Recursos Humanos e da Segurança,

([1]) JO L 72 de 17.3.2015, p. 41.
([2]) JO L 72 de 17.3.2015, p. 53.
([3]) Decisão (UE, Euratom) 2017/46 da Comissão, de 10 de janeiro de 2017, relativa à segurança dos sistemas de comunicação e de informação na Comissão Europeia (JO L 6 de 11.1.2017, p. 40).
([4]) Decisão C(2016) 2797 final da Comissão, de 4 de maio de 2016, relativa a uma habilitação em matéria de segurança.
([5]) Decisão C(2021) 2684 final da Comissão, de 13 de abril de 2021, que subdelega os poderes conferidos pela Decisão C(2016) 2797 da Comissão relativa a uma habilitação em matéria de segurança.

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

Disposições gerais

Artigo 1.º

Objeto e âmbito de aplicação

1. A presente decisão define as funções e responsabilidades dos principais intervenientes no domínio da segurança responsáveis pela proteção das informações classificadas da UE (ICUE) na Comissão ao abrigo das Decisões (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444.

2. A presente decisão é aplicável a todos os serviços e em todas as instalações da Comissão.

CAPÍTULO 2

Direção-Geral dos Recursos Humanos e da Segurança

Artigo 2.º

Autoridade de Segurança da Comissão

1. O diretor da Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança é a Autoridade de Segurança da Comissão (ASC) a que se refere o artigo 7.º da Decisão (UE, Euratom) 2015/444.

2. A ASC desempenha as suas funções nos seguintes domínios, tal como estabelecido na Decisão (UE, Euratom) 2015/444, em conformidade com os artigos 3.º a 7.º da presente decisão:

a) segurança do pessoal;

b) segurança física;

c) gestão das ICUE;

d) acreditação de todos os sistemas de comunicação e informação (SCI) que manuseiam as ICUE;

e) segurança industrial; e

f) troca de informações classificadas.

3. A ASC deve ministrar formação obrigatória aos responsáveis locais de segurança (LSO), aos LSO adjuntos, aos responsáveis do controlo do registo (RCO) e aos RCO adjuntos relativamente às suas responsabilidades e funções.

Artigo 3.º

Autoridade de Garantia da Informação

A Autoridade de Garantia da Informação é responsável pelas seguintes atividades relacionadas com a proteção das ICUE:

a) elaboração de políticas e diretrizes de segurança em matéria de garantia da informação e do controlo da sua eficácia e pertinência;

b) salvaguarda e administração de informações técnicas relativas aos produtos criptográficos;

c) confirmação de que as medidas de garantia da informação estão em conformidade com as políticas de segurança e de adjudicação de contratos da Comissão, conforme adequado;

d) garantia que os produtos criptográficos são selecionados em conformidade com as políticas que regem a sua elegibilidade e seleção;

e) consultas junto dos proprietários dos sistemas, fornecedores de sistemas, intervenientes no domínio da segurança e representantes dos utilizadores no que diz respeito às políticas de segurança da informação e às orientações em matéria de segurança.

Artigo 4.º

Autoridade de Acreditação de Segurança

1. A ASC é responsável pela acreditação das Zonas de Segurança que cumprem os requisitos do artigo 18.º da Decisão 2015/444 e dos SCI que manuseiam ICUE.

2. Os serviços da Comissão consultarão a Autoridade de Acreditação de Segurança, em coordenação com o seu LSO e o seu LISO, conforme adequado, sempre que um serviço tencione:

a) instalar uma Zona de Segurança;

b) implementar um SCI para o manuseamento das ICUE;

c) instalar qualquer outro equipamento para o tratamento de informações classificadas, incluindo ligações a SCI de terceiros.

A Autoridade de Acreditação de Segurança presta aconselhamento no que respeita a estas atividades, tanto durante os processos de planeamento como de construção ou de desenvolvimento.

3. As ICUE não serão manuseadas numa Zona de Segurança ou num SCI antes de a Autoridade de Acreditação de Segurança ter emitido uma acreditação ao nível adequado das ICUE.

4. Os requisitos para a acreditação de uma Zona de Segurança incluem:

a) aprovação dos planos para a Zona de Segurança;

b) aprovação de quaisquer contratos relativos a trabalhos executados por contratantes externos, tendo em conta as disposições em matéria de segurança industrial, tais como eventuais requisitos em matéria de credenciação de segurança dos contratantes e do seu pessoal;

c) disponibilidade de todas as declarações e certificados de conformidade exigidos;

d) uma inspeção física da Zona de Segurança, a fim de verificar se os materiais e métodos de construção, os controlos de acesso, os equipamentos de segurança e quaisquer outros elementos cumprem os requisitos estabelecidos pela ASC;

e) validação das contramedidas contra a radiação eletromagnética para qualquer Zona Tecnicamente Segura;

f) aprovação dos procedimentos operacionais de segurança (SecOP) para a Zona de Segurança.

5. Os requisitos para a acreditação de um SCI que manuseie ICUE devem incluir:

a) a criação de uma estratégia de acreditação do sistema;

b) a validação do plano de segurança do SCI, com base numa abordagem de gestão dos riscos;

c) a validação dos SecOP para o SCI;

d) a validação de toda a outra documentação de segurança exigida, tal como determinado pela Autoridade de Acreditação de Segurança;

e) a aprovação de qualquer utilização de tecnologias de encriptação;

f) a validação das contramedidas contra a radiação eletromagnética para os SCI que manuseiam informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior;

g) uma inspeção do SCI para verificar se as medidas de segurança documentadas são corretamente aplicadas.

6. Uma vez devidamente cumpridos os requisitos de acreditação, a Autoridade de Acreditação de Segurança emite uma autorização formal para o manuseamento das ICUE na Zona de Segurança ou SCI, correspondente a um nível máximo estabelecido de ICUE e por um período máximo de cinco anos, em função dos níveis de ICUE manuseados e dos riscos envolvidos.

7. Após notificação de uma quebra de segurança ou de uma alteração significativa na conceção ou nas medidas de segurança de uma Zona de Segurança ou de um SCI, a Autoridade de Acreditação de Segurança reexamina e, se necessário, pode revogar a autorização de manuseamento das ICUE até que sejam resolvidas quaisquer questões identificadas.

Artigo 5.º

Autoridade TEMPEST

1. São aplicadas medidas de segurança para proteger os SCI que manuseiem informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior, podendo ser aplicadas a informações com classificação RESTREINT UE/EU RESTRICTED.

2. A Autoridade TEMPEST é responsável pela aprovação das medidas de proteção adotadas no intuito de evitar que as ICUE sejam comprometidas devido a emanações eletromagnéticas não intencionais;

3. A pedido de um proprietário de um SCI que manuseie ICUE, a Autoridade TEMPEST emitirá especificações para as medidas de segurança TEMPEST adequadas ao nível de classificação das informações.

4. A autoridade TEMPEST efetua ensaios técnicos durante o processo de acreditação de Zonas de Segurança e SCI para o manuseamento de ICUE ao nível CONFIDENTIAL UE/EU CONFIDENTIAL ou superior e, após a realização de testes positivos, emite um certificado TEMPEST.

5. O certificado TEMPEST deve especificar, pelo menos:

a) a data do teste;

b) uma descrição das medidas de segurança TEMPEST, com planos das instalações;

c) a data de validade do certificado;

d) quaisquer alterações que invalidem a certificação;

e) a assinatura da Autoridade TEMPEST.

6. Um responsável local de segurança (LSO) ou um organizador de reuniões responsável pela organização de uma reunião classificada, em coordenação com o LSO, pode solicitar à autoridade TEMPEST que teste as salas de reunião, a fim de garantir a sua segurança técnica.

Artigo 6.º

Autoridade de Aprovação Criptográfica

1. A Autoridade de Aprovação Criptográfica é responsável pela aprovação da utilização de tecnologias de encriptação.

2. A Autoridade de Aprovação Criptográfica emite orientações sobre os requisitos para a utilização e aprovação de tecnologias de encriptação.

3. A Autoridade de Aprovação Criptográfica aprova a utilização de tecnologias de encriptação com base num pedido do proprietário do sistema. A aprovação deve basear-se, no mínimo, numa avaliação satisfatória do seguinte:

a) as necessidades de segurança das informações a proteger;

b) uma panorâmica geral do SCI envolvido na solução;

c) uma avaliação dos riscos inerentes e residuais;

d) uma descrição da solução pretendida;

e) os SecOP para a solução de encriptação.

4. A Autoridade de Aprovação Criptográfica mantém um registo das soluções de encriptação aprovadas.

Artigo 7.º

Autoridade de Distribuição Criptográfica

1. A Autoridade de Distribuição Criptográfica é responsável pela distribuição de materiais criptográficos utilizados para proteger as ICUE (equipamento de cifragem, chaves criptográficas, certificados e autenticadores conexos) aos seguintes utilizadores:

a) utilizadores ou serviços da Comissão para os SCI administrados por partes externas;

b) utilizadores ou organizações exteriores à Comissão para os SCI administrados pela Comissão.

2. A Autoridade de Distribuição Criptográfica pode delegar a outros serviços a distribuição de materiais criptográficos a terceiros, em conformidade com o artigo 17.º, n.º 3, da Decisão 2015/443.

3. A Autoridade de Distribuição Criptográfica garante que todos os materiais criptográficos sejam enviados através de canais seguros que protejam e revelem provas de qualquer manipulação não autorizada, em conformidade com as regras de segurança aplicáveis ao nível de classificação das ICUE que serão protegidas por esses materiais.

4. A Autoridade de Distribuição Criptográfica fornece orientações ao LSO e, se for caso disso, ao responsável local pela segurança informática de cada serviço da Comissão envolvido na produção, distribuição ou utilização dos materiais criptográficos.

5. A Autoridade de Distribuição Criptográfica assegura o estabelecimento de SecOP adequados para o processo de distribuição.

CAPÍTULO 3

Serviços da Comissão

Artigo 8.º

Chefes de serviço

1. Cada chefe de serviço nomeia:

a) um LSO e um ou mais adjuntos, se for caso disso, para o serviço ou gabinete;

b) um RCO e um ou mais adjuntos, se for caso disso, para cada serviço que proceda à gestão de um registo de ICUE;

c) um proprietário para cada SCI que manuseia ICUE.

2. O chefe de serviço solicita a aprovação do diretor da Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança antes da nomeação de LSO, LSO adjuntos, RCO e RCO adjuntos.

3. O chefe de serviços identifica todos os cargos que necessitam de habilitação para ter acesso às ICUE, em consulta com o LSO. Os candidatos a esses cargos devem ser informados da exigência de habilitação durante o processo de recrutamento.

4. O chefe de qualquer serviço que disponha de ICUE é responsável pela ativação dos planos de destruição e evacuação de emergência, sempre que necessário. Os planos devem incluir uma alternativa para as situações em que o chefe de serviço não possa ser contactado.

Artigo 9.º

Proprietários de SCI que manuseiam ICUE

1. O proprietário do sistema contacta a Autoridade de Acreditação de Segurança o mais rapidamente possível no âmbito de um projeto de implementação de um SCI que manuseie ICUE, a fim de determinar as normas e requisitos de segurança pertinentes e dar início ao processo de acreditação de segurança.

2. O proprietário do sistema garante que as medidas de segurança satisfazem os requisitos da Autoridade de Acreditação de Segurança e que o SCI não manuseia quaisquer ICUE antes de ter sido acreditado.

3. O proprietário do sistema contacta a Autoridade de Aprovação Criptográfica para efeitos de aprovação da utilização de quaisquer tecnologias de encriptação. Os proprietários dos sistemas não podem utilizar tecnologias de encriptação em sistemas de produção sem autorização prévia.

4. O proprietário do sistema consulta o LISO do serviço sobre questões relacionadas com a segurança dos SCI.

5. O proprietário do sistema revê as medidas de segurança aplicadas a um sistema, incluindo o seu plano de segurança, pelo menos uma vez por ano.

6. Sempre que ocorra um incidente de segurança num SCI em que seja indicado que o SCI já não é capaz de proteger adequadamente as ICUE, o proprietário do sistema informa o LSO e contacta imediatamente a Autoridade de Acreditação de Segurança para aconselhamento sobre a forma de proceder. Neste caso, a acreditação pode ser suspensa e o sistema pode ser desativado até que sejam tomadas as medidas corretivas adequadas.

7. O proprietário do sistema apoia plenamente a Autoridade de Acreditação de Segurança, a todo e qualquer momento, nas suas funções relativas à acreditação do SCI.

Artigo 10.º

Autoridade Operacional de Garantia da Informação

A Autoridade Operacional de Garantia da Informação de cada SCI:

a) elabora documentação de segurança em conformidade com as políticas e diretrizes de segurança, em especial o plano de segurança, os SecOP relacionados com o sistema e a documentação criptográfica no âmbito do processo de acreditação do SCI;

b) participa 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;

c) participa na seleção das medidas e dispositivos de segurança TEMPEST, se tal for exigido no plano de segurança, e, em cooperação com a Autoridade TEMPEST, assegura a respetiva instalação e manutenção de forma segura;

d) acompanha a execução e a aplicação dos SecOP relacionados com o funcionamento do sistema;

e) gere e manuseia produtos criptográficos, em colaboração com a Autoridade de Distribuição Criptográfica, a fim de garantir a conservação adequada dos materiais criptográficos e dos produtos controlados e, se necessário, assegurar a geração de variáveis criptográficas;

f) efetua análises, revisões e testes de segurança, em especial para a elaboração dos relatórios de risco pertinentes, conforme exigido pela Autoridade de Acreditação de Segurança;

g) ministra formação em matéria de garantia da informação específica do SCI;

h) executa e põe em prática medidas de segurança específicas do SCI.

CAPÍTULO 4

Responsável local de segurança

Artigo 11.º

Nomeação do LSO

1. O LSO e os LSO adjuntos são funcionários ou agentes temporários.

2. Todos os LSO e os LSO adjuntos devem ser titulares de uma autorização de segurança válida para ter acesso às ICUE até ao nível SECRET UE/EU SECRET e, se necessário, até ao nível TRES SECRET UE/EU TOP SECRET. O LSO ou o LSO adjunto devem obter a autorização de segurança antes da sua nomeação.

3. As Representações da Comissão podem solicitar à ASC que conceda uma derrogação aos requisitos estabelecidos nos n.os 1 e 2.

Artigo 12.º

Procedimentos operacionais de segurança para Zonas de Segurança

1. O LSO do serviço da Comissão em causa elabora SecOP para cada Zona de Segurança sob a sua responsabilidade.

2. O LSO assegura que os SecOP incluem os seguintes requisitos:

a) só os membros do pessoal que disponham de uma autorização de segurança válida e de uma necessidade comprovada de acesso a documentos com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior serão autorizados a aceder sem escolta a uma Zona de Segurança durante as horas de expediente;

b) o acesso sem escolta a uma Zona de Segurança fora do horário de expediente só é concedido ao LSO do serviço, ao(s) RCO(s) da Zona de Segurança, aos seus adjuntos e ao pessoal autorizado da Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança;

c) os dispositivos de registo e comunicação, como telemóveis, computadores, câmaras ou outros dispositivos inteligentes, não são permitidos dentro das Zonas de Segurança sem autorização prévia da ASC; qualquer derrogação deve ser previamente solicitada à ASC; o LSO serve de ponto de contacto;

d) todo o pessoal interno ou externo que necessite de ter acesso a uma Zona de Segurança, mas que não preencha os critérios estabelecidos na alínea a), deve ser permanentemente escoltado e supervisionado por um membro do pessoal devidamente autorizado; qualquer acesso a uma Zona de Segurança deve ser inscrito num livro de registo mantido à entrada da mesma;

e) o LSO garante que os sistemas de deteção de intrusão que monitorizam uma Zona de Segurança estão sempre ativos e a funcionar corretamente, devendo também gerir todas as senhas, chaves, números de identificação pessoal (PIN) ou outros mecanismos de acesso e autenticação conexos.

f) os alarmes numa Zona de Segurança devem ser comunicados à Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança, que notifica imediatamente o LSO;

g) o LSO do serviço em que se situa a Zona de Segurança deve manter um registo de cada intervenção na sequência de um alarme ou de um incidente de segurança;

h) devem ser criados procedimentos para gerir a ocorrência de um alerta ou qualquer outra situação de emergência dentro da Zona de Segurança, incluindo a evacuação de pessoal, que garantam uma resposta rápida por parte de uma equipa de emergência sob a autoridade do ASC e dos serviços de emergência externos, se necessário;

i) o LSO comunica imediatamente à ASC qualquer quebra de segurança que ocorra dentro de uma Zona de Segurança ou que a afete, a fim de determinar a resposta adequada;

j) sempre que sejam deixados sem vigilância, os escritórios, salas e cofres-fortes individuais dentro de uma Zona de Segurança devem permanecer fechados à chave;

k) o pessoal deve evitar debater informações classificadas em corredores ou outras zonas comuns da Zona de Segurança quando pessoas não autorizadas se encontrem nas proximidades.

Artigo 13.º

Chaves de segurança e combinações

1. O LSO é globalmente responsável por assegurar o devido manuseamento e armazenamento das chaves e das combinações utilizadas nas Zonas de Segurança ou para obter o acesso às mesmas. As chaves e combinações devem ser armazenadas num contentor de segurança e dispor pelo menos do mesmo nível de proteção que o material a que dão acesso.

2. O LSO mantém um registo dos contentores de segurança e das caixas-fortes, juntamente com uma lista atualizada de todos os membros do pessoal que tenham acesso sem escolta aos mesmos.

3. O LSO mantém um registo das chaves dos contentores de segurança e das caixas-fortes, incluindo dos membros do pessoal a quem são atribuídas. Deve ser conservado um recibo para cada chave emitida, incluindo a identificação da chave, o destinatário, a data e a hora.

4. As chaves e as combinações só serão emitidas ao pessoal que delas necessitem e que tenham obtido autorização adequada para aceder às ICUE. O LSO recupera as chaves quando essas condições deixarem de ser preenchidas.

5. O LSO conserva chaves sobresselentes e um registo escrito de cada combinação em envelopes individuais selados, opacos, assinados e datados, a fornecer pelo membro do pessoal responsável pelas chaves. Esses envelopes devem ser guardados num contentor de segurança adequado para conter o material como mais elevado grau de classificação armazenado nesse contentor ou caixa-forte pertinente.

6. Se, na sequência de uma alteração da combinação ou após a rotação de chaves, se verificar que um envelope foi manipulado ou danificado, o LSO deve considerar esse facto como um incidente de segurança e informar imediatamente a ASC.

7. As combinações dos contentores de segurança nas Zonas de Segurança devem ser mudadas sob a supervisão do LSO. As combinações devem ser redefinidas, no mínimo, cada 12 meses e sempre que:

a) seja recebido um novo contentor ou instalada uma nova fechadura (em especial, as combinações predefinidas devem ser imediatamente alteradas);

b) se suspeite que a segurança esteja ou tenha sido comprometida;

c) a pessoa que disponha de uma combinação já não necessita de acesso.

8. O LSO deve manter um registo das datas de mudança das combinações a que se refere o n.º 7.

Artigo 14.º

Planos de evacuação de emergência e destruição de ICUE

1. O LSO assiste o chefe de serviço na elaboração de planos de evacuação de emergência e destruição de ICUE, com base nas orientações fornecidas pela Direção-Geral de Recursos Humanos e Segurança (HR.DS).

2. O LSO garante que o equipamento necessário para o funcionamento dos planos previstos no n.º 1 está imediatamente disponível, sendo mantido em bom estado de funcionamento.

3. O LSO, juntamente com os funcionários nomeados nos planos previstos no n.º 1, reexamina o estado de preparação dos planos pelo menos cada 12 meses e toma todas as medidas necessárias para os atualizar.

Artigo 15.º

Autorizações de segurança

1. O LSO mantém um registo de todos os cargos no serviço que exigem uma autorização de segurança da Comissão e do pessoal que ocupa os mesmos. A exigência de uma autorização de segurança deve ser especificada no anúncio de vaga durante o processo de recrutamento e notificada ao candidato durante a entrevista.

2. O LSO supervisiona todos os pedidos de autorizações de segurança para obter acesso às ICUE. O LSO serve de ponto de contacto no serviço e contacta a ASC para as autorizações de segurança.

3. O LSO lança o pedido de abertura do procedimento de autorização de segurança em relação ao membro do pessoal em causa e velará por que este devolva imediatamente o questionário de credenciação de segurança nacional à ASC.

4. O LSO garante que os membros do pessoal com credenciação de segurança no serviço seguem as instruções obrigatórias sobre as ICUE a fim de obterem a sua autorização de segurança.

5. O LSO contacta regularmente a secção de recursos humanos do serviço para obter informações sobre todas as alterações a nível dos cargos que exijam uma autorização de segurança e informa imediatamente a ASC a este respeito.

6. O LSO informa a ASC da chegada de um novo membro do pessoal que seja titular de uma credenciação de segurança existente para assumir funções que exijam um membro do pessoal autorizado em matéria de segurança.

7. O LSO assegura que os membros do pessoal do serviço concluem o procedimento de renovação da credenciação de segurança dentro do prazo fixado. Qualquer membro do pessoal que se recuse a concluir esse procedimento é obrigado a assumir um cargo que não exija um agente autorizado em matéria de segurança.

Artigo 16.º

Registo de ICUE

1. Sempre que um serviço seja responsável pela gestão de um registo de ICUE, o LSO supervisiona as atividades dos RCO no que respeita ao manuseamento das ICUE e ao cumprimento das regras de segurança quanto à sua proteção.

2. O LSO efetua os seguintes controlos pelo menos cada 12 meses e após a substituição de um RCO ou de um RCO adjunto:

a) controlo de uma amostra de documentos no registo de ICUE para confirmar o seu estatuto e a exatidão do registo de documentos classificados;

b) controlo de uma amostra de recibos e fichas de transmissão para a distribuição de ICUE no registo e a partir do mesmo;

c) controlo de uma amostra de certificados de destruição.

3. Pelo menos uma vez por mês o RCO procede a controlos aleatórios do registo de documentos classificados e dos documentos classificados recebidos recentemente, a fim de garantir que os documentos estão a ser corretamente registados.

4. Todos os controlos devem ser inscritos no registo dos documentos classificados.

Artigo 17.º

Outras responsabilidades em matéria de segurança

As outras responsabilidades do LSO em matéria de segurança devem constar de um aviso de segurança que abranja, em especial, a segurança física das pessoas, das instalações e de outros ativos e informações.

CAPÍTULO 5

Responsável do controlo do registo (RCO)

Artigo 18.º

Nomeação do RCO

1. O RCO e os RCO adjuntos são funcionários ou agentes temporários.

2. Todos os RCO e os RCO adjuntos devem ser titulares de uma autorização de segurança válida para ter acesso a ICUE até ao nível SECRET UE/EU SECRET e, se necessário, até ao nível TRES SECRET UE/EU TOP SECRET. O RCO ou o RCO adjunto devem obter a autorização de segurança antes da sua nomeação.

3. As Representações da Comissão podem solicitar à ASC que conceda uma derrogação aos requisitos estabelecidos nos n.os 1 e 2.

Artigo 19.º

Responsabilidades

1. Os RCO registam as informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior para fins de segurança quando:

a) as informações chegam ou saem de um serviço da Comissão; ou

b) as informações chegam ou saem de um SCI.

2. Os RCO registam todos os eventos ocorridos durante o ciclo de vida de todas as informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior. Os RCO asseguram igualmente a manutenção de um registo de todas as informações com a classificação RESTREINT UE/EU RESTRICTED, ou com classificação equivalente, trocadas com países terceiros e organizações internacionais. Tal será feito em coordenação com o registo das ICUE gerido pelo Secretariado-Geral.

3. O RCO regista os documentos com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior no registo de documentos classificados e assegura a sua armazenagem segura no registo de ICUE.

4. O RCO assiste o pessoal da Comissão na criação e transmissão de informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior.

5. Quando os documentos com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior forem recebidos de outros serviços ou terceiros externos, o RCO assegura que o recibo de entrega é devidamente devolvido à entidade de origem.

6. Antes de autorizar um membro do pessoal a aceder a um documento classificado detido no registo de ICUE, o RCO verifica junto do LSO se esse membro do pessoal está autorizado em matéria de segurança pela CSA.

7. O RCO procede ao registo de todo o pessoal que entra e sai do registo de ICUE que não esteja autorizado a ter acesso sem escolta, acompanhando-o durante a sua visita.

8. Quando um membro do pessoal extrair do registo de ICUE um documento para consulta, o RCO assegura-se de que esse membro do pessoal tem conhecimento das medidas de segurança compensatórias pertinentes, devendo devolver o documento logo que deixar de precisar dele. O RCO recorda ao pessoal que deve devolver qualquer documento desse tipo o mais rapidamente possível.

9. O registo de ICUE emite um certificado de estafeta se os documentos classificados forem transportados em mão própria fora do país em que se situa o registo.

10. As instruções pormenorizadas para os RCO sobre o registo de documentos classificados devem constar de um aviso de segurança.

Artigo 20.º

Desgraduação e desclassificação

O RCO assiste os serviços de origem no processo de revisão das ICUE registadas, a fim de verificar se o nível de classificação original continua a ser adequado, ou se o documento pode ser desgraduado ou desclassificado.

Artigo 21.º

Destruição

1. Os RCO são responsáveis pela destruição das informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior por meios aprovados, se for caso disso na presença de testemunhas com credenciação de segurança.

2. Os RCO registam qualquer destruição de informações com a classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior no registo de documentos classificados e conservam os certificados de destruição correspondentes no registo de ICUE.

Artigo 22.º

Tarefas adicionais

1. O RCO presta toda a assistência necessária ao LSO quando este exercer atividades de supervisão no registo de ICUE.

2. O RCO comunica quaisquer incidentes de segurança suspeitos ou reais ao LSO, que, por sua vez, os comunica à ASC.

3. O RCO do registo de ICUE de um serviço da Comissão que organize uma reunião classificada de nível CONFIDENTIEL UE/EU CONFIDENTIAL ou superior prepara as ICUE que serão tratadas durante a reunião e coordena com o organizador da reunião a fim de assegurar que todos os documentos e recibos são tratados em conformidade com as regras aplicáveis.

CAPÍTULO 6

Disposições finais

Artigo 23.º

Transparência

A presente decisão é levada ao conhecimento do pessoal da Comissão e de todas as pessoas às quais se aplica, sendo publicada no *Jornal Oficial da União Europeia*.

Artigo 24.º

O presente regulamento entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 7 de abril de 2022.

Pela Comissão
Em nome da Presidente,
Gertrud INGESTAD
Diretora-Geral
Direção-Geral dos Recursos Humanos e da Segurança