DECISÃO (UE, Euratom) 2018/559 DA COMISSÃO

de 6 de abril de 2018

que estabelece as regras de execução do artigo 6.º da Decisão (UE, Euratom) 2017/46 relativa à segurança dos sistemas de comunicação e informação na Comissão Europeia

A COMISSÃO EUROPEIA,

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

Tendo em conta o Tratado que institui a Comunidade Europeia da Energia Atómica,

Tendo em conta a 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 ([1]), nomeadamente o seu artigo 6.º,

Considerando o seguinte:

(1) A adoção da Decisão (UE, Euratom) 2017/46 torna necessário que a Comissão reveja, atualize e consolide as regras de execução decorrentes da revogação da Decisão C(2006) 3602 da Comissão no que se refere à segurança dos sistemas de comunicação e de informação utilizados pela Comissão.

(2) O membro da Comissão responsável pelas questões de segurança, em plena conformidade com o regulamento interno, foi habilitado a estabelecer regras de execução em conformidade com o artigo 13.º da Decisão (UE, Euratom) 2017/46 ([2]).

(3) As regras de execução da Decisão C(2006) 3602 devem, por conseguinte, ser revogadas,

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. O objeto e o âmbito de aplicação da presente decisão são definidos no artigo 1.º da Decisão (UE, Euratom) 2017/46.

2. As disposições da presente decisão aplicam-se a todos os sistemas de comunicação e informação (SCI). Todavia, as responsabilidades definidas na presente decisão não se aplicam aos SCI que gerem informações classificadas da UE. As responsabilidades correspondentes respeitantes a estes sistemas são determinadas pelo proprietário do sistema e pela Autoridade de Segurança da Comissão, em conformidade com a Decisão (UE, Euratom) 2015/444 da Comissão ([3]).

3. O capítulo 2 da presente decisão apresenta uma panorâmica da implementação prática da organização e das responsabilidades relacionadas com a segurança informática. O capítulo 3 da presente decisão apresenta uma panorâmica dos procedimentos relacionados com o artigo 6.º da Decisão (UE, Euratom) 2017/46.

Artigo 2.º

Definições

As definições constantes do artigo 2.º da Decisão (UE, Euratom) 2017/46 aplicam-se à presente decisão. Para efeitos da presente decisão, são igualmente aplicáveis as seguintes definições:

1) «Autoridade de Aprovação Criptográfica» (AAC): função assumida pela Autoridade de Segurança da Comissão sob a autoridade do Diretor-Geral dos Recursos Humanos e da Segurança.

([1]) JO L 6 de 11.1.2017, p. 40.
([2]) Decisão C(2017) 7428 final da Comissão, de 8 de novembro de 2017, que concede uma habilitação para a adoção de regras de execução, normas e orientações relativas à segurança dos sistemas de comunicação e informação na Comissão Europeia.
([3]) 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 (JO L 72 de 17.3.2015, p. 53).

2) «Ligação às redes externas»: ligação de comunicações eletrónicas entre a rede interna da Comissão e qualquer outra rede, incluindo a Internet. Esta definição exclui as redes de terceiros fornecidas mediante contrato para fazer parte da rede interna da Comissão.

3) «Caução de chave»: procedimento de armazenagem de cópias de chaves criptográficas junto de um ou mais depositários distintos, a fim de garantir a separação de funções e permitir a sua recuperação em caso de perda da cópia operacional. As chaves podem ser divididas em duas ou mais partes, sendo cada uma delas entregue a um depositário diferente a fim de garantir que nenhum deles possui a chave na íntegra.

4) «RASCI»: abreviatura para a atribuição de responsabilidades com base nos seguintes indicadores de atribuição:

   a) «responsável» (R): ter a obrigação de agir e de tomar decisões para obter os resultados desejados;

   b) «responsabilizável» (A): ter a obrigação de responder por atos, decisões e resultados;

   c) «apoia» (S): ter a obrigação de colaborar com a pessoa responsável pelo cumprimento da tarefa;

   d) «consultado» (C): ser solicitado para dar um conselho ou parecer;

   e) «informado» (I): estar ao corrente das informações pertinentes.

CAPÍTULO 2

ORGANIZAÇÃO E RESPONSABILIDADES

Artigo 3.º

Papéis e responsabilidades

Os papéis e as responsabilidades respeitantes aos artigos 4.º a 8.º da presente decisão são definidos no anexo, em conformidade com o modelo RASCI.

Artigo 4.º

Alinhamento com a política de segurança da informação da Comissão

1. A Direção-Geral dos Recursos Humanos e da Segurança examina a política de segurança informática da Comissão, bem como as normas e orientações conexas, a fim de garantir a sua conformidade com as políticas gerais de segurança da Comissão, em especial a Decisão (UE, Euratom) 2015/443 da Comissão ([1]) e a Decisão (UE, Euratom) 2015/444.

2. A pedido de outros serviços da Comissão, a Direção-Geral dos Recursos Humanos e da Segurança pode examinar as suas políticas de segurança informática ou outra documentação de segurança informática, a fim de assegurar a sua coerência com a política de segurança da informação da Comissão. O chefe do serviço da Comissão em causa deve assegurar a eliminação de eventuais incoerências.

3. Enquanto responsável pela segurança da informação, a Direção-Geral dos Recursos Humanos e da Segurança coopera com a Direção-Geral da Informática para assegurar que os procedimentos de segurança informática têm plenamente em conta a classificação e os princípios de segurança previstos na Decisão (UE, Euratom) 2015/443, nomeadamente os artigos 3.º e 9.º.

CAPÍTULO 3

PROCEDIMENTOS DE SEGURANÇA INFORMÁTICA

Artigo 5.º

Tecnologias de encriptação

1. A utilização de tecnologias de encriptação para a proteção das informações classificadas da UE (ICUE) deve estar em conformidade com a Decisão (UE, Euratom) 2015/444.

2. As decisões relativas à utilização de tecnologias de encriptação para a proteção dos dados não ICUE são tomadas pelo proprietário do sistema de cada SCI, tendo em conta tanto os riscos que se pretende atenuar com a utilização da encriptação como os riscos ocasionados por esta última.

3. Qualquer utilização de tecnologias de encriptação requer a aprovação prévia da AAC, a menos que a encriptação seja unicamente utilizada para proteger a confidencialidade dos dados não ICUE em trânsito e utilize protocolos correntes de comunicação em rede.

([1]) Decisão (UE, Euratom) 2015/443 da Comissão, de 13 de março de 2015, relativa à segurança na Comissão (JO L 72 de 17.3.2015, p. 41).

4. Com a exceção indicada no n.º 3, os serviços da Comissão asseguram que as cópias de segurança de todas as chaves de desencriptação são conservadas numa caução de chave para fins de recuperação dos dados memorizados, caso a chave de desencriptação não esteja disponível. A recuperação de dados encriptados utilizando as cópias de segurança das chaves de desencriptação apenas é efetuada quando autorizada em conformidade com a norma definida pela AAC.

5. Os pedidos de aprovação do uso de tecnologias de encriptação devem ser formalmente documentados e incluir informações pormenorizadas sobre os SCI e os dados a proteger, as tecnologias a utilizar e os respetivos procedimentos operacionais de segurança. Os pedidos de aprovação são assinados pelo proprietário do sistema.

6. Os pedidos de aprovação do uso de tecnologias de encriptação devem ser avaliados pela AAC, em conformidade com as normas e requisitos publicados.

Artigo 6.º

Inspeções de segurança informática

1. A Direção-Geral dos Recursos Humanos e da Segurança efetua inspeções de segurança informática para verificar se as medidas de segurança informática são conformes com as políticas de segurança informática da Comissão e para controlar a integridade de tais medidas de controlo.

2. A Direção-Geral dos Recursos Humanos e da Segurança pode efetuar uma inspeção de segurança informática:

a) por sua própria iniciativa;

b) a pedido do Comité Diretor de Segurança da Informação (CDSI);

c) a pedido de um proprietário do sistema;

d) na sequência de um incidente de segurança; ou

e) na sequência da identificação de um risco elevado para um sistema específico.

3. Os proprietários de dados podem solicitar uma inspeção de segurança informática antes de armazenarem as suas informações num SCI.

4. Os resultados das inspeções são consignados num relatório formal dirigido ao proprietário do sistema, com cópia para o responsável local da segurança informática (LISO), incluindo conclusões e recomendações destinadas a melhorar a conformidade do SCI com a política de segurança informática. A Direção-Geral dos Recursos Humanos e da Segurança assinala ao CDSI os principais problemas e recomendações.

5. A Direção-Geral dos Recursos Humanos e da Segurança verifica a aplicação das recomendações.

6. Sempre que adequado, as inspeções de segurança informática devem incluir a inspeção dos serviços, das instalações e dos equipamentos fornecidos ao proprietário do sistema, incluindo os prestadores de serviços internos e externos.

Artigo 7.º

Acesso a partir de redes externas

1. A Direção-Geral dos Recursos Humanos e da Segurança estabelece as regras numa norma que autoriza o acesso entre os SCI da Comissão e as redes externas.

2. As regras devem estabelecer uma distinção entre os diferentes tipos de ligação a redes externas e prever regras de segurança apropriadas para cada tipo de ligação, nomeadamente se a autoridade competente exigir uma autorização prévia para a ligação, como referido no n.º 4.

3. Se necessário, a autorização é concedida com base num pedido oficial e num processo de aprovação. A aprovação é válida por um período determinado e deve ser obtida antes de a ligação ser ativada.

4. A Direção-Geral dos Recursos Humanos e da Segurança tem a responsabilidade geral pela autorização dos pedidos, mas pode, a seu critério, delegar a responsabilidade de autorizar certos tipos de ligação, em conformidade com o artigo 17.º, n.º 3, da Decisão (UE, Euratom) 2015/443, e sob reserva das condições estabelecidas no ponto 8.

5. A entidade que emite a autorização pode impor requisitos de segurança adicionais a título de condição prévia à aprovação, a fim de proteger os SCI e as redes da Comissão contra os riscos de acesso não autorizado ou outras violações da segurança.

6. A Direção-Geral da Informática é o fornecedor habitual de serviços de rede à Comissão. Qualquer outro serviço da Comissão que explore uma rede que não é fornecida pela Direção-Geral da Informática deve obter o acordo prévio do CDSI. O serviço da Comissão documenta a justificação comercial para o pedido e demonstra que os controlos da rede são suficientes para satisfazer os requisitos aplicáveis ao controlo dos fluxos de informação de entrada e de saída.

7. O proprietário de um SCI define os requisitos de segurança para o acesso externo a esse SCI e garante a aplicação das medidas adequadas para proteger a sua segurança, com o apoio do LISO.

8. As medidas de segurança aplicadas às ligações às redes externas devem assentar nos princípios da necessidade de conhecer e do privilégio mínimo, que garantem que cada pessoa apenas recebe as informações e os direitos de acesso necessários ao cumprimento das suas funções oficiais junto da Comissão.

9. Todas as ligações às redes externas devem ser filtradas e monitorizadas para que possam ser detetadas eventuais violações da segurança.

10. Quando são estabelecidas ligações para permitir a externalização de um SCI, a autorização está subordinada à conclusão bem sucedida do procedimento descrito no artigo 8.º.

Artigo 8.º

Externalização de SCI

1. Para efeitos da presente decisão, considera-se que um SCI é externalizado quando é fornecido por força de um contrato com um contratante terceiro, nos termos do qual o SCI está alojado fora das instalações da Comissão. Tal inclui a externalização de um ou vários SCI ou de outros serviços informáticos, centros de dados em instalações fora da Comissão e o tratamento de conjuntos de dados da Comissão por serviços externos.

2. A externalização de SCI deve ter em conta o grau de sensibilidade ou a classificação das informações tratadas de acordo com o seguinte:

a) Os SCI que tratam ICUE são homologados em conformidade com a Decisão (UE, Euratom) 2015/444 e a Autoridade de Acreditação de Segurança (AAS) da Comissão é previamente consultada. Os sistemas que tratam ICUE não são externalizados.

b) O proprietário de um SCI que trata dados não ICUE deve implementar medidas proporcionadas para satisfazer os requisitos de segurança, em conformidade com as obrigações jurídicas pertinentes ou o grau de sensibilidade das informações, tendo em conta os riscos que comporta a externalização. A Direção-Geral dos Recursos Humanos e da Segurança pode impor requisitos adicionais.

c) Os projetos de desenvolvimento externalizados têm em conta a o grau de sensibilidade do código desenvolvido, bem como os dados dos ensaios utilizados durante a fase de desenvolvimento.

3. Para além dos princípios enunciados no artigo 3.º da Decisão (UE, Euratom) 2017/46, aplicam-se os seguintes princípios aos SCI externalizados:

a) os acordos de externalização devem ser concebidos de forma a evitar qualquer dependência de determinados fornecedores;

b) os acordos de externalização da segurança devem reduzir ao mínimo as possibilidades de acesso ou de alteração das informações da Comissão por parte de membros do pessoal dos fornecedores terceiros;

c) os membros do pessoal dos fornecedores terceiros que tenham acesso a um SCI externalizado devem assinar acordos de confidencialidade;

d) a externalização de um SCI deve ser indicada no inventário dos SCI.

4. O proprietário do sistema, com a participação do proprietário dos dados, deve:

a) avaliar e documentar os riscos associados à externalização;

b) fixar os requisitos de segurança pertinentes;

c) consultar os proprietários dos sistemas de todos os outros SCI ligados para garantir a inclusão dos seus requisitos de segurança;

d) assegurar a inclusão no contrato de externalização dos requisitos e dos direitos adequados em matéria de segurança;

e) cumprir quaisquer outros requisitos previstos na norma detalhada, como mencionado no n.º 8.

Estas diligências devem ser efetuadas antes da assinatura do contrato ou de qualquer outro acordo para a externalização de um ou mais SCI.

5. Os proprietários dos sistemas gerem os riscos relacionados com a externalização durante a vigência do SCI, a fim de satisfazer os requisitos de segurança definidos.

6. Os proprietários dos sistemas devem garantir que os contratantes terceiros são obrigados a notificar imediatamente a Comissão de qualquer incidente de segurança informática que afete um SCI da Comissão externalizado.

7. O proprietário do sistema é responsável pela conformidade do SCI, do contrato de externalização e das disposições em matéria de segurança com as regras da Comissão em matéria de segurança da informação e de segurança informática.

8. A Direção-Geral dos Recursos Humanos e da Segurança estabelece a norma detalhada relativa às responsabilidades e atividades enumeradas nos pontos 1 a 7, em conformidade com o artigo 10.º abaixo.

CAPÍTULO 4

DISPOSIÇÕES DIVERSAS E FINAIS

Artigo 9.º

Transparência

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

Artigo 10.º

Normas

1. As disposições da presente decisão são, sempre que necessário, explicadas de forma mais detalhada em normas e/ou orientações que devem ser adotadas em conformidade com a Decisão (UE, Euratom) 2017/46 e a Decisão C(2017) 7428. As normas e orientações em matéria de segurança informática contêm informações mais detalhadas sobre estas regras de execução e a Decisão (UE, Euratom) 2017/46 para domínios de segurança específicos, em conformidade com a norma ISO 27001: 2013, anexo A. Estas normas e orientações baseiam-se nas melhores práticas do setor e são selecionadas de acordo com as características do ambiente informático da Comissão.

2. As normas são, sempre que necessário, elaboradas em conformidade com a norma ISO 27001: 2013, anexo A, nos seguintes domínios:

(1) organização da segurança da informação;

(2) segurança dos recursos humanos;

(3) gestão de ativos;

(4) controlo do acesso;

(5) criptografia;

(6) segurança física e ambiental;

(7) segurança operacional;

(8) segurança das comunicações;

(9) aquisição, desenvolvimento e manutenção dos sistemas;

(10) relações com os fornecedores;

(11) gestão dos incidentes de segurança da informação;

(12) aspetos da segurança da informação na gestão da continuidade das operações;

(13) conformidade.

3. O CDSI aprova as normas referidas nos n.os 1 e 2 antes da sua adoção.

4. As regras de execução da Decisão C(2006) 3602 relativas ao âmbito de aplicação da presente decisão são revogadas.

5. As normas e orientações adotadas nos termos da Decisão C(2006) 3602 de 16 de agosto de 2006 mantêm-se em vigor, na medida em que não entrem em conflito com as presentes normas de execução, até serem revogadas ou substituídas por normas ou orientações a adotar nos termos do artigo 13.º da Decisão (UE, Euratom) 2017/46.

Artigo 11.º

Entrada em vigor

A presente decisão entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 6 de abril de 2018.

Pela Comissão
Em nome do Presidente,
Günther OETTINGER
Membro da Comissão

ANEXO

PAPÉIS E RESPONSABILIDADES (RASCI)

O modelo RASCI atribui funções a entidades com base nas seguintes abreviaturas:

a) R — Responsável (*Responsible*)

b) A — Responsabilizável (*Accountable*)

c) S — Apoia (*Supporting*)

d) C — Consultado (*Consulted*)

e) I — Informado (*Informed*)

Papel / Processo	CDSI	HR (DS)	Serviços da Comissão	Proprietário do sistema	Proprietário dos dados	LISO	DIGIT	Contratantes
Alinhamento com a política da Comissão em matéria de segurança da informação		**A/R**	**S**				**S**	
Tecnologias de encriptação		**C**	**A**	**R**	**I**	**C**		
Inspeções de segurança informática	**I**	**A/R**		**S**	**I**	**I**	**S**	
Acesso a partir das redes externas	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Externalização dos SCI		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] O CDSI é consultado no que diz respeito ao funcionamento das redes internas por qualquer serviço da Comissão, menos a Direção-Geral da Informática.

[2] O proprietário de um SCI externalizado é responsável, e o proprietário de qualquer outro SCI ao qual está ligado um SCI externalizado deve ser consultado.