DECISÕES

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

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,

Considerando o seguinte:

(1) Os sistemas de comunicação e de informação da Comissão fazem parte integrante do seu funcionamento e os incidentes de segurança informática podem ter um impacto grave nas atividades da Comissão, bem como em terceiros, incluindo pessoas, empresas e Estados-Membros.

(2) Há numerosas ameaças suscetíveis de prejudicar a confidencialidade, a integridade ou a disponibilidade dos sistemas de comunicação e de informação da Comissão, bem como das informações neles tratadas. Entre estas ameaças contam-se acidentes, erros, ataques deliberados e acontecimentos naturais, os quais devem ser reconhecidos como riscos operacionais.

(3) Os sistemas de comunicação e informação devem ser dotados de um nível de proteção proporcional à probabilidade, ao impacto e à natureza dos riscos a que estão expostos.

(4) A segurança informática da Comissão deve assegurar que os sistemas de comunicação e informação (SCI) da Comissão protejam as informações que tratam e que funcionem da forma adequada, no momento em que são necessários e sob o controlo de utilizadores legítimos.

(5) A política de segurança informática da Comissão deve ser aplicada de uma forma que seja coerente com as políticas em matéria de segurança na Comissão.

(6) Cabe à Direção de Segurança da Direção-Geral dos Recursos Humanos e da Segurança a responsabilidade geral pela segurança na Comissão sob a autoridade e a responsabilidade do Membro da Comissão responsável pelas questões de segurança.

(7) A abordagem da Comissão deve ter em conta as iniciativas políticas e a legislação da UE em matéria de segurança das redes e da informação, as normas da indústria e as boas práticas, a fim de dar cumprimento a toda a legislação relevante e de permitir a interoperabilidade e a compatibilidade.

(8) Os serviços da Comissão responsáveis pelos sistemas de comunicação e informação devem desenvolver e aplicar medidas adequadas, devendo as medidas de segurança informática para a proteção dos sistemas de comunicação e informação ser coordenadas a nível de toda a Comissão com vista a assegurar a sua eficiência e eficácia.

(9) As regras e os procedimentos que regem o acesso à informação no contexto da segurança informática, incluindo a gestão de incidentes de segurança informática, devem ser proporcionais à ameaça para a Comissão ou para o seu pessoal e estar em conformidade com os princípios estabelecidos no Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho [1] relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados e tendo em conta o princípio do segredo profissional consagrado no artigo 339.º do TFUE.

[1] Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

(10) As políticas e as regras aplicáveis aos sistemas de comunicação e informação que tratam informações classificadas da UE (ICUE), informações sensíveis não classificadas e informações não classificadas devem ser plenamente conformes com as Decisões (UE, Euratom) 2015/443 ([1]) e (UE, Euratom) 2015/444 ([2]) da Comissão.

(11) É necessário que a Comissão proceda à revisão e atualização das disposições relativas à segurança dos sistemas de comunicação e informação utilizados pela Comissão.

(12) Por conseguinte, a Decisão C(2006) 3602 da Comissão deve ser revogada,

ADOTOU A PRESENTE DECISÃO:

CAPÍTULO 1

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. A presente decisão é aplicável a todos os sistemas de comunicação e informação (SCI) detidos, adquiridos, geridos ou explorados pela Comissão, ou por sua conta, e a todas as utilizações desses SCI pela Comissão.

2. A presente decisão estabelece os princípios básicos, os objetivos, a organização e as responsabilidades em matéria de segurança dos referidos SCI e, em particular, dos serviços da Comissão que detêm, adquirem, gerem ou exploram SCI, incluindo os fornecidos por um prestador de serviços informáticos interno. Quando um SCI é fornecido, detido, gerido ou explorado por uma entidade externa com base num contrato ou acordo bilateral celebrado com a Comissão, os termos do acordo ou contrato devem estar em conformidade com a presente decisão.

3. A presente decisão é aplicável a todos os serviços e agências de execução da Comissão. Quando um sistema de comunicação e informação da Comissão é utilizado por outros organismos e instituições com base num acordo bilateral com a Comissão, os termos do acordo devem estar em conformidade com a presente decisão.

4. Sem prejuízo de indicações específicas relativas a determinados grupos de pessoal, a presente decisão é aplicável aos Membros da Comissão, ao pessoal da Comissão abrangido pelo Estatuto dos Funcionários da União Europeia (seguidamente designado o «Estatuto») e pelo Regime aplicável aos Outros Agentes da União (seguidamente designado «o ROA») ([3]), aos peritos nacionais destacados na Comissão (PND) ([4]), aos prestadores de serviços externos e ao seu pessoal, aos estagiários e a qualquer pessoa com acesso ao SCI abrangido pela presente decisão.

5. A presente decisão é aplicável ao Organismo Europeu de Luta Antifraude (OLAF) na medida em que tal seja compatível com a legislação da União e com a Decisão 1999/352/CE, CECA, Euratom da Comissão ([5]). Em particular, as medidas previstas na presente decisão, incluindo instruções, inspeções, inquéritos e medidas equivalentes, podem não ser aplicáveis aos SCI do OLAF se tal não for compatível com a independência da sua função de inquérito e/ou com a confidencialidade das informações obtidas pelo OLAF no exercício dessa função.

Artigo 2.º

Definições

Para efeitos da presente decisão, entende-se por:

1) «Responsável»: ser responsabilizável por ações, decisões e desempenhos.

([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).
([2]) 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).
([3]) Estabelecido pelo Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho, de 29 de fevereiro de 1968, que fixa o Estatuto dos Funcionários das Comunidades Europeias assim como o Regime aplicável aos outros agentes destas Comunidades, e institui medidas especiais temporariamente aplicáveis aos funcionários da Comissão (Estatuto dos Funcionários) (JO L 56 de 4.3.1968, p. 1).
([4]) Decisão da Comissão de 12 de novembro de 2008 relativa ao regime aplicável aos peritos nacionais destacados e aos peritos nacionais em formação profissional nos serviços da Comissão [C(2008) 6866 final].
([5]) Decisão 1999/352/CE, CECA, Euratom da Comissão, de 28 de abril de 1999, que institui o Organismo Europeu de Luta Antifraude (OLAF) (JO L 136 de 31.5.1999, p. 20).

2) «CERT-UE»: Equipa de Resposta a Emergências Informáticas (*Computer Emergency Response Team*) para as instituições e agências da UE. A sua missão consiste em ajudar as instituições europeias a protegerem-se contra ataques intencionais e mal-intencionados que comprometeriam a integridade dos seus bens informáticos e prejudicariam os interesses da UE. As atividades da CERT-UE abrangem a prevenção, a deteção, a resposta e a recuperação.

3) «Serviço da Comissão»: qualquer Direção-Geral ou serviço da Comissão ou qualquer Gabinete de um Membro da Comissão.

4) «Autoridade de Segurança da Comissão»: as funções estabelecidas na Decisão (UE, Euratom) 2015/444.

5) «Sistema de comunicação e informação» ou «SCI»: um sistema que permita o tratamento de informações em formato eletrónico, incluindo todos os meios necessários ao seu funcionamento, bem como a infraestrutura, a organização, o pessoal e os recursos de informação. Esta definição inclui aplicações profissionais, serviços informáticos partilhados, sistemas externalizados e dispositivos para utilizadores finais.

6) «Conselho de Administração Institucional» (*Corporate Management Board* — CMB): o nível mais elevado de supervisão da gestão institucional para questões operacionais e administrativas na Comissão.

7) «Proprietário dos dados»: a pessoa responsável por assegurar a proteção e a utilização de um conjunto de dados específicos tratado por um sistema de comunicação e informação.

8) «Conjunto de dados»: um conjunto de informações que serve uma atividade ou um processo administrativo específicos da Comissão.

9) «Procedimento de emergência»: um conjunto predefinido de métodos e responsabilidades para responder a situações urgentes a fim de evitar um impacto importante na Comissão.

10) «Política de segurança da informação»: um conjunto de objetivos de segurança da informação, que está — ou deve ser — estabelecido, aplicado e verificado. Abrange, nomeadamente, as Decisões (UE, Euratom) 2015/444 e (UE, Euratom) 2015/443.

11) «Comité Diretor de Segurança da Informação» (*Information Security Steering Board* — ISSB): o órgão de governação que apoia o Conselho de Administração Institucional nas suas funções relacionadas com a segurança informática.

12) «Prestador de serviços informáticos interno»: um serviço da Comissão que fornece serviços informáticos partilhados.

13) «Segurança informática» ou «segurança dos SCI»: a preservação da confidencialidade, da integridade e da disponibilidade de sistemas de comunicação e informação e dos conjuntos de dados que tratam.

14) «Orientações de segurança informática»: medidas recomendadas, mas de caráter voluntário, que contribuem para apoiar as normas de segurança informática ou que servem de referência quando não existe uma norma aplicável.

15) «Incidente de segurança informática»: um acontecimento suscetível de prejudicar a confidencialidade, a integridade ou a disponibilidade de um sistema de comunicação e informação.

16) «Medida de segurança informática»: uma medida de caráter técnico ou organizativo destinada a atenuar riscos de segurança informática.

17) «Necessidade de segurança informática»: uma definição precisa e inequívoca dos níveis de confidencialidade, integridade e disponibilidade associados a uma determinada informação ou a um sistema informático para fins de determinação do nível de proteção necessário.

18) «Objetivo de segurança informática»: uma declaração de intenções para combater ameaças específicas e/ou satisfazer determinados requisitos ou pressupostos em matéria de segurança organizativa.

19) «Plano de segurança informática»: a documentação das medidas de segurança informática necessárias para satisfazer as necessidades de segurança de um sistema de comunicação e informação.

20) «Política de segurança informática»: um conjunto de objetivos de segurança informática, que está — ou que deve ser — definido, aplicado e verificado. Inclui a presente decisão e as suas regras de execução.

21) «Requisito de segurança informática»: uma necessidade de segurança informática formalizada através de um processo predefinido.

22) «Risco de segurança informática»: um efeito que uma ameaça à segurança informática possa induzir num sistema de comunicação e informação tirando partido de uma vulnerabilidade. Como tal, um risco de segurança informática é caracterizado por dois fatores: 1) incerteza, isto é, a probabilidade de uma ameaça à segurança informática causar um acontecimento indesejado e 2) impacto, ou seja, as consequências que esse acontecimento indesejado pode ter num sistema de comunicação e informação.

23) «Normas de segurança informática»: medidas de segurança informática obrigatórias específicas que contribuem para a aplicação e execução da política de segurança informática.

24) «Estratégia de segurança informática»: um conjunto de projetos e atividades que visam atingir os objetivos da Comissão e que devem ser definidos, aplicados e verificados.

25) «Ameaça à segurança informática»: um fator suscetível de conduzir a um acontecimento indesejado que pode provocar danos num sistema de comunicação e informação. Estas ameaças podem ser acidentais ou deliberadas e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque.

26) «Responsável local da segurança informática» (*Local Informatics Security Officer*) ou «LISO»: o agente de ligação responsável pela segurança informática de um serviço da Comissão.

27) «Dados pessoais», «tratamento de dados pessoais», «responsável pelo tratamento» e «ficheiro de dados pessoais»: termos com a aceção estabelecida no Regulamento (CE) n.º 45/2001, nomeadamente o artigo 2.º.

28) «Tratamento de informações»: todas as funções de um sistema de comunicação e informação no que diz respeito a conjuntos de dados, incluindo a criação, a alteração, a visualização, o armazenamento, a transmissão, a eliminação e o arquivo de informações. Um sistema de comunicação e informação pode proceder ao tratamento de informações como um conjunto de funcionalidades para os utilizadores e como serviços informáticos para outros SCI.

29) «Segredo profissional»: a proteção de informações comerciais do tipo abrangido pela obrigação de segredo profissional, em especial as informações respeitantes a empresas, às suas relações comerciais ou os seus componentes de custos, conforme previsto no artigo 339.º do TFUE.

30) «Responsável»: ter a obrigação de atuar e tomar decisões para obter os resultados exigidos.

31) «Segurança na Comissão»: a segurança de pessoas, bens e informações na Comissão e, em particular, a integridade física de pessoas e bens, a integridade, a integridade, confidencialidade e disponibilidade das informações e dos sistemas de comunicação e informação, bem como o funcionamento sem entraves das funções da Comissão.

32) «Serviço informático partilhado»: o serviço que um sistema de comunicação e informação fornece a outros SCI em termos de tratamento de informações.

33) «Proprietário do sistema»: a pessoa responsável pelo conjunto dos procedimentos de aquisição, desenvolvimento, integração, alteração, funcionamento, manutenção e retirada de serviço de um sistema de comunicação e informação.

34) «Utilizador»: qualquer pessoa que utilize uma funcionalidade fornecida por um sistema de comunicação e informação, tanto no interior como no exterior da Comissão.

Artigo 3.º

Princípios da segurança informática na Comissão

1. A segurança informática na Comissão baseia-se nos princípios da legalidade, da transparência, da proporcionalidade e da responsabilização.

2. As questões de segurança informática devem ser tidas em consideração desde o início do desenvolvimento e da implementação dos SCI da Comissão. Com esse fim em vista, a Direção-Geral da Informática e a Direção-Geral dos Recursos Humanos e da Segurança intervêm no âmbito dos respetivos domínios de competência.

3. Uma segurança informática eficaz assegura níveis adequados de:

a) Autenticidade: a garantia de que a informação é genuína e provém de fontes fidedignas;

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

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

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

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

f) Proteção dos dados pessoais: a prestação de garantias adequadas no que se refere aos dados pessoais, no pleno respeito das disposições do Regulamento (CE) n.º 45/2001;

g) Segredo profissional: a proteção de informações do tipo abrangido pela obrigação de segredo profissional, em especial informações respeitantes a empresas, às suas relações comerciais ou aos seus componentes de custos, conforme estabelecido no artigo 339.º do TFUE.

4. A segurança informática baseia-se num processo de gestão de riscos. Este processo deve ter por objetivo determinar os níveis dos riscos de segurança informática e definir as medidas de segurança destinadas a reduzir esses riscos para um nível adequado e a um custo proporcionado.

5. Todos os SCI são identificados, atribuídos a um proprietário do sistema e registados num inventário.

6. Os requisitos de segurança de todos os SCI são determinados com base nas suas necessidades de segurança e nas necessidades de segurança das informações que tratam. Os SCI que prestam serviços a outros SCI podem ser concebidos de modo a satisfazer níveis específicos de necessidades de segurança.

7. Os planos de segurança informática e as medidas de segurança informática devem ser proporcionais às necessidades de segurança dos SCI.

Os processos relacionados com estes princípios e atividades são apresentados de forma mais pormenorizada nas regras de execução.

CAPÍTULO 2

ORGANIZAÇÃO E RESPONSABILIDADES

Artigo 4.º

Conselho de Administração Institucional (CMB)

O Conselho de Administração Institucional assume a responsabilidade geral pela governação da segurança informática no seu conjunto na Comissão.

Artigo 5.º

Comité Diretor de Segurança da Informação (ISSB)

1. O ISSB é presidido pelo Secretário-Geral Adjunto responsável pela governação da segurança informática na Comissão. Os seus membros representam os interesses a nível empresarial, tecnológico e de segurança em todos os serviços da Comissão e incluem representantes da Direção-Geral da Informática, da Direção-Geral dos Recursos Humanos e da Segurança, da Direção-Geral do Orçamento e, numa base rotativa bianual, representantes de quatro outros serviços da Comissão nos quais a segurança informática constitui uma questão importante para as suas atividades. Os seus membros são gestores dos quadros superiores.

2. O ISSB apoia o Conselho de Administração Institucional nas suas funções em matéria de segurança informática. O ISSB assume a responsabilidade operacional pela governação da segurança informática no seu conjunto na Comissão.

3. O ISSB submete à aprovação da Comissão uma recomendação sobre a política de segurança informática da Comissão.

4. Duas vezes por ano, o ISSB examina e apresenta ao Conselho de Administração Institucional um relatório sobre questões de governação, bem como sobre matérias ligadas à segurança informática, incluindo incidentes graves de segurança informática.

5. O ISSB acompanha e analisa a execução global da presente decisão e mantém o Conselho de Administração Institucional informado sobre a matéria.

6. Sob proposta da Direção-Geral da Informática, o ISSB procede à revisão, aprovação e acompanhamento da execução da estratégia de segurança informática evolutiva. O ISSB mantém o Conselho de Administração Institucional informado sobre a matéria.

7. O ISSB procede ao acompanhamento, avaliação e controlo do ambiente institucional de tratamento dos riscos informáticos em sempre que necessário, pode estabelecer requisitos formais com vista à melhoria.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 6.º

Direção-Geral dos Recursos Humanos e da Segurança

No que se refere à segurança informática, a Direção-Geral dos Recursos Humanos e da Segurança tem as seguintes responsabilidades:

1) Assegurar a coerência entre a política de segurança informática e a política de segurança da informação da Comissão.

2) Definir um quadro para a autorização da utilização de tecnologias de cifragem no que diz respeito ao armazenamento e comunicação de informações pelos SCI.

3) Informar a Direção-Geral da Informática sobre ameaças específicas suscetíveis de ter um impacto significativo na segurança dos SCI e dos conjuntos de dados que tratam.

4) Proceder a inspeções de segurança informática a fim de avaliar a conformidade dos SCI da Comissão com a política de segurança e comunicar os respetivos resultados ao ISSB.

5) Definir um quadro — bem como as respetivas regras de segurança adequadas — para a autorização de acesso aos SCI da Comissão a partir de redes externas e elaborar as orientações e normas de segurança informática conexas em estreita cooperação com a Direção-Geral da Informática.

6) Propor princípios e regras para a externalização de SCI com vista a manter um controlo adequado da segurança da informação.

7) Desenvolver orientações e normas de segurança informática conexas no que diz respeito ao artigo 6.º, em estreita cooperação com a Direção-Geral da Informática.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 7.º

Direção-Geral da Informática

Em relação à segurança informática geral da Comissão, a Direção-Geral da Informática tem as seguintes responsabilidades:

1) Desenvolver orientações e normas de segurança informática, exceto nos casos previstos no artigo 6.º, em estreita cooperação com a Direção-Geral dos Recursos Humanos e da Segurança, a fim de assegurar a coerência entre a política de segurança informática e a política de segurança da informação da Comissão, e submetê-las à aprovação do ISSB.

2) Avaliar os métodos de gestão dos riscos de segurança informática, e os respetivos processos e resultados, de todos os serviços da Comissão e do mesmo informar regularmente o ISSB.

3) Propor uma estratégia de segurança informática evolutiva para revisão e aprovação pelo ISSB e posterior adoção pelo Conselho de Administração Institucional e propor um programa que inclua, nomeadamente, o planeamento de projetos e atividades de execução da estratégia de segurança informática.

4) Proceder ao acompanhamento da execução da estratégia de segurança informática da Comissão e do mesmo informar regularmente o ISSB.

5) Proceder ao acompanhamento dos riscos de segurança informática e das medidas de segurança informática aplicadas nos SCI e do mesmo informar regularmente o ISSB.

6) Informar regularmente o ISSB sobre a aplicação geral e o cumprimento das disposições da presente decisão.

7) Após consulta à Direção-Geral dos Recursos Humanos e da Segurança, solicitar aos proprietários de sistemas que tomem medidas de segurança informática específicas a fim de atenuar os riscos de segurança informática para os SCI da Comissão.

8) Assegurar que seja colocado à disposição dos proprietários de sistemas e dos proprietários de dados um catálogo adequado dos serviços de segurança informática da Direção-Geral da Informática para fins de cumprimento das suas responsabilidades em matéria de segurança informática e das normas e política de segurança informáticas.

9) Facultar documentação adequada aos proprietários de sistemas e de dados e consultá-los, conforme adequado, sobre medidas de segurança informática aplicadas aos seus serviços informáticos, a fim de facilitar o cumprimento da política de segurança informática e de apoiar os proprietários de sistemas na gestão dos riscos informáticos.

10) Organizar reuniões regulares da rede LISO e apoiar os LISO no exercício das suas funções.

11) Definir as necessidades de formação e coordenar os programas de formação sobre segurança informática, em cooperação com os serviços da Comissão, e desenvolver, aplicar e coordenar campanhas de sensibilização sobre segurança informática em estreita cooperação com a Direção-Geral dos Recursos Humanos.

12) Assegurar que os proprietários de sistemas, os proprietários de dados e outros responsáveis pela segurança informática nos serviços da Comissão sejam informados sobre a política de segurança informática.

13) Informar a Direção-Geral dos Recursos Humanos e da Segurança sobre ameaças específicas à segurança informática, incidentes e exceções à política de segurança informática da Comissão notificados pelos proprietários de sistemas e que sejam suscetíveis de ter um impacto significativo na segurança no interior da Comissão.

14) No que se refere à sua função de prestador de serviços informáticos interno, fornecer à Comissão um catálogo de serviços informáticos partilhados que oferecem níveis de segurança definidos. Tal será concretizado procedendo sistematicamente à avaliação, à gestão e ao controlo dos riscos de segurança informática para a aplicação das medidas de segurança com vista a atingir o nível de segurança definido.

Os processos conexos e as responsabilidades são definidos de forma mais pormenorizada nas regras de execução.

Artigo 8.º

Serviços da Comissão

No que diz respeito à segurança informática nos seus serviços, cabe aos chefes de serviço da Comissão:

1) Nomear formalmente, para cada SCI, um proprietário do sistema, que é funcionário ou agente temporário, e que será responsável pela segurança informática do SCI em questão, bem como nomear formalmente um proprietário dos dados para cada conjunto de dados tratados num SCI, o qual deve pertencer à mesma entidade administrativa que o responsável pelo tratamento de dados para os conjuntos de dados abrangidos pelo Regulamento (CE) n.º 45/2001.

2) Nomear formalmente um responsável local da segurança informática (LISO) que possa assumir as responsabilidades de forma independente em relação aos proprietários de sistemas e aos proprietários de dados. Um LISO pode ser nomeado para um ou mais serviços da Comissão.

3) Assegurar que foram devidamente estabelecidos e executados planos de segurança informática e avaliações de riscos informáticos.

4) Assegurar que seja comunicado regularmente à Direção-Geral da Informática um resumo dos riscos e das medidas de segurança informática.

5) Assegurar, com o apoio da Direção-Geral da Informática, a aplicação de soluções, processos e procedimentos adequados para garantir a eficiência na deteção, na comunicação de informações e na resolução de incidentes de segurança relacionados com os seus SCI.

6) Lançar um procedimento de emergência para situações de emergência em matéria de segurança informática.

7) Assumir a responsabilidade última pela segurança informática, incluindo as responsabilidades do proprietário do sistema e do proprietário dos dados.

8) Assumir os riscos associados aos seus próprios SCI e conjuntos de dados.

9) Resolver eventuais diferendos entre os proprietários de dados e os proprietários de sistemas e, em caso de persistência de um diferendo, submeter a questão ao ISSB para resolução.

10) Assegurar que as medidas e os planos de segurança informática são aplicados e que os riscos estão cobertos de forma adequada.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 9.º

Proprietários de sistemas

1. O proprietário do sistema é responsável pela segurança informática do SCI e responde perante o chefe do serviço da Comissão.

2. No que se refere à segurança informática, cabe ao proprietário do sistema:

a) Garantir a conformidade do SCI com a política de segurança informática;

b) Assegurar que o SCI está corretamente registado no inventário relevante;

c) Avaliar os riscos de segurança informática e determinar as necessidades de segurança informática de cada SCI, em colaboração com os proprietários dos dados e em consulta com a Direção-Geral da Informática;

d) Preparar um plano de segurança, incluindo, quando adequado, informações pormenorizadas sobre os riscos avaliados e as medidas de segurança adicionais eventualmente necessárias;

e) Aplicar medidas de segurança informática adequadas, proporcionais aos riscos de segurança informática identificados, e seguir as recomendações validadas pelo ISSB;

f) Identificar eventuais dependências em relação a outros SCI ou serviços informáticos partilhados e aplicar medidas de segurança conforme adequado com base nos níveis de segurança propostos por esses SCI ou serviços informáticos partilhados;

g) Gerir e controlar os riscos de segurança informática;

h) Informar regularmente o chefe do serviço da Comissão sobre o perfil de risco de segurança informática do seu SCI e informar a Direção-Geral da Informática sobre os riscos associados, as atividades de gestão dos riscos e as medidas de segurança adotadas;

i) Consultar o LISO do(s) serviço(s) competente(s) da Comissão sobre aspetos de segurança informática;

j) Publicar instruções dirigidas aos utilizadores sobre a utilização do SCI e dados associados, bem como sobre as responsabilidades dos utilizadores relativamente ao SCI;

k) Solicitar a autorização da Direção-Geral dos Recursos Humanos e da Segurança, na qualidade de Autoridade Criptográfica, para os SCI que utilizam tecnologias de cifragem;

l) Consultar previamente a Autoridade de Segurança da Comissão sobre qualquer sistema que trate informações classificadas da UE;

m) Assegurar que as cópias de segurança de eventuais chaves de decifração sejam armazenadas numa conta bloqueada. A recuperação de dados cifrados é efetuada somente quando autorizada em conformidade com o quadro definido pela Direção-Geral dos Recursos Humanos e da Segurança;

n) Respeitar as instruções dadas pelo(s) responsável(is) pelo tratamento de dados em questão quanto à proteção de dados pessoais e à aplicação das regras de proteção de dados à segurança do tratamento;

o) Notificar a Direção-Geral da Informática de quaisquer exceções à política de segurança informática da Comissão, incluindo as justificações relevantes;

p) Comunicar ao chefe do serviço da Comissão eventuais diferendos impossíveis de resolver entre o proprietário dos dados e o proprietário do sistema e comunicar os incidentes de segurança informática às partes relevantes, de forma atempada e consoante adequado em função da sua gravidade, conforme estabelecido no artigo 15.º;

q) Relativamente aos sistemas externalizados, garantir que sejam incluídas nos contratos de externalização disposições adequadas em matéria de segurança informática e que os incidentes de segurança informática ocorridos nos SCI externalizados sejam comunicados em conformidade com o disposto no artigo 15.º;

r) Velar por que os SCI que prestam serviços informáticos partilhados atinjam um nível de segurança definido e claramente documentado e por que sejam aplicadas medidas de segurança para que esses SCI atinjam o nível de segurança definido.

3. Os proprietários de sistemas podem delegar formalmente a totalidade ou parte das suas funções em matéria de segurança informática, mas continuam a ser responsáveis pela segurança informática dos seus SCI.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 10.º

Proprietários de dados

1. O proprietário dos dados é responsável, perante o chefe de serviço da Comissão, pela segurança informática de um conjunto de dados específico e pela confidencialidade, integridade e disponibilidade do conjunto de dados.

2. Em relação a esse conjunto de dados, o proprietário dos dados:

a) Assegura que todos os conjuntos de dados sob a sua responsabilidade estão adequadamente classificados de acordo com as Decisões (UE, Euratom) 2015/443 e (UE, Euratom) 2015/444;

b) Define as necessidades de segurança das informações e informa os proprietários de sistemas relevantes dessas necessidades;

c) Participa no sistema de avaliação de riscos do SCI;

d) Informa o chefe do serviço da Comissão sobre eventuais diferendos impossíveis de resolver entre o proprietário dos dados e o proprietário do sistema;

e) Comunicar os incidentes de segurança informática, conforme previsto no artigo 15.º.

3. Os proprietários de dados podem delegar formalmente a totalidade ou parte das suas funções em matéria de segurança informática, mas mantêm as suas responsabilidades conforme definidas no presente artigo.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 11.º

Responsáveis Locais da Segurança Informática (LISO)

No que se refere à segurança informática, cabe ao LISO:

a) Identificar proativamente os proprietários de sistemas, os proprietários de dados e outros responsáveis da segurança informática nos serviços da Comissão e informá-los sobre a política de segurança informática;

b) Assegurar a ligação com a Direção-Geral da Informática, no âmbito da rede LISO, sobre questões relacionadas com a segurança informática nos serviços da Comissão;

c) Assistir às reuniões regulares dos LISO;

d) Manter uma visão global do processo de gestão dos riscos de segurança da informação e da elaboração e execução de planos de segurança dos sistemas de informação;

e) Aconselhar os proprietários de dados, os proprietários de sistemas e os chefes dos serviços da Comissão sobre questões relacionadas com a segurança informática;

f) Cooperar com a Direção-Geral da Informática na divulgação de boas práticas em matéria de segurança informática e propor programas de sensibilização e formação específicos;

g) Informar o(s) chefe do(s) serviço(s) da Comissão sobre a segurança informática, as lacunas identificadas e as melhorias possíveis.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 12.º

Utilizadores

1. No que se refere à segurança informática, os utilizadores devem:

a) Respeitar a política de segurança informática e as instruções emitidas pelo proprietário do sistema sobre a utilização de cada SCI;

b) Comunicar os incidentes de segurança informática, conforme previsto no artigo 15.º.

2. A utilização dos SCI da Comissão em violação da política de segurança informática ou das instruções emitidas pelo proprietário do sistema é passível de processo disciplinar.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

CAPÍTULO 3

REQUISITOS E OBRIGAÇÕES EM MATÉRIA DE SEGURANÇA

Artigo 13.º

Execução da presente decisão

1. A adoção das regras de execução referidas no artigo 6.º, bem como das normas e orientações conexas, será objeto de uma decisão de delegação de poderes da Comissão no Membro da Comissão responsável pelas questões de segurança.

2. A adoção de todas as outras regras de execução ligadas à presente decisão, bem como das normas e orientações conexas em matéria de segurança informática, será objeto de uma decisão de delegação de poderes da Comissão no Membro da Comissão responsável pela informática.

3. O ISSB aprova as regras de execução, as normas e as orientações referidas nos n.os 1 e 2, antes da sua adoção.

Artigo 14.º

Obrigação de cumprimento

1. O cumprimento das disposições expostas na política de segurança informática e nas normas é obrigatório.

2. O incumprimento da política e das normas em matéria de segurança informática é passível de sanções disciplinares nos termos dos Tratados, do Estatuto e do ROA, bem como de sanções contratuais e/ou de ação judicial ao abrigo da legislação e regulamentação nacionais.

3. A Direção-Geral da Informática deve ser notificada de quaisquer exceções à política de segurança informática.

4. Caso o ISSB decida que existe um risco inaceitável persistente para um SCI da Comissão, a Direção-Geral da Informática, em colaboração com o proprietário do sistema, propõe medidas de atenuação ao ISSB para aprovação. As referidas medidas podem, nomeadamente, incluir um reforço do controlo e da comunicação de informações, e limitações, ou mesmo interrupção, do serviço.

5. O ISSB impõe, quando necessário, a aplicação de medidas de atenuação aprovadas. O ISSB pode igualmente recomendar ao Diretor-Geral da Direção-Geral dos Recursos Humanos e da Segurança a abertura de um inquérito administrativo. A Direção-Geral da Informática comunica ao ISSB todas as situações em que sejam impostas medidas de atenuação.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

Artigo 15.º

Gestão de incidentes de segurança informática

1. A Direção-Geral da Informática é responsável pela disponibilização da principal capacidade de resposta operacional a incidentes de segurança informática na Comissão Europeia.

2. A Direção-Geral dos Recursos Humanos e da Segurança, na qualidade de parte interessada que contribui para a resposta a incidentes de segurança informática:

a) Tem o direito de acesso a informações resumidas de todos os registos de incidentes e aos registos completos, mediante pedido;

b) Participa nos grupos de gestão de crises de incidentes de segurança informática e nos procedimentos de emergência em matéria de segurança informática;

c) É responsável pelos contactos com os serviços de controlo do cumprimento da lei e com os serviços de informações;

d) Procede à análise forense relativa à cibersegurança, em conformidade com o disposto no artigo 11.º da Decisão (UE, Euratom) 2015/443;

e) Decide da necessidade de iniciar um inquérito formal;

f) Informa a Direção-Geral da Informática de todos os incidentes de segurança informática suscetíveis de constituir um risco para outros SCI.

3. Serão realizadas comunicações periódicas entre a Direção-Geral da Informática e a Direção-Geral dos Recursos Humanos e da Segurança para trocar informações e coordenar a gestão dos incidentes de segurança, em especial de incidentes de segurança informática que possam exigir um inquérito formal.

4. Pode recorrer-se aos serviços de coordenação de incidentes da Equipa de Resposta a Emergências Informáticas para as instituições, organismos e agências da UE (CERT-UE) a fim de apoiar o processo de gestão de incidentes, quando adequado, e de permitir a partilha de conhecimentos com outras instituições e agências da UE que possam ser afetadas.

5. Cabe aos proprietários de sistemas implicados num incidente de segurança informática:

a) Notificar imediatamente o seu chefe de serviço da Comissão, a Direção-Geral da Informática, a Direção-Geral dos Recursos Humanos, o LISO e, quando adequado, o proprietário dos dados de quaisquer incidentes importantes de segurança informática, em especial os que impliquem uma violação da confidencialidade dos dados;

b) Cooperar com as autoridades competentes da Comissão e seguir as instruções dessas autoridades no que diz respeito à comunicação de incidentes, à resposta e à remediação.

6. Os utilizadores devem comunicar atempadamente todos os incidentes de segurança informática — quer sejam reais ou supostos — ao *Helpdesk* Informático relevante.

7. Os proprietários de dados devem comunicar atempadamente todos os incidentes de segurança informática — quer sejam reais ou supostos — às equipas de resposta a incidentes de segurança informática competentes.

8. A Direção-Geral da Informática, com o apoio das outras partes interessadas, é responsável pelo tratamento de qualquer incidente de segurança informática detetado relativamente aos SCI da Comissão que não sejam sistemas externalizados.

9. A Direção-Geral da Informática informa os serviços da Comissão afetados, os LISO e, quando adequado, a CERT-UE, sobre eventuais incidentes de segurança informática na medida em que estes tenham «necessidade de tomar conhecimento».

10. A Direção-Geral da Informática informa regularmente o ISSB sobre incidentes de segurança informática graves que afetem os SCI da Comissão.

11. O LISO competente tem acesso, mediante pedido, aos registos de incidentes de segurança informática relativos ao SIC do serviço da Comissão.

12. Em caso de incidentes de segurança informática graves, a Direção-Geral da Informática é o ponto de contacto para a gestão das situações de crise, coordenando os grupos de gestão de crises de incidentes de segurança informática.

13. Em caso de emergência, o Diretor-Geral da Direção-Geral da Informática pode decidir lançar um procedimento de emergência em matéria de segurança informática. A Direção-Geral da Informática elabora os procedimentos de emergência a aprovar pelo ISSB.

14. A Direção-Geral da Informática comunica ao ISSB e aos chefes dos serviços da Comissão afetados informações sobre a execução de procedimentos de emergência.

Os processos relacionados com estas responsabilidades e atividades são apresentados de forma mais pormenorizada nas regras de execução.

CAPÍTULO 4

DISPOSIÇÕES FINAIS

Artigo 16.º

Transparência

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

Artigo 17.º

Relação com outros atos

As disposições da presente decisão são adotadas sem prejuízo da Decisão (UE, Euratom) 2015/443, da Decisão (UE, Euratom) 2015/444, do Regulamento (CE) n.º 45/2001, do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho ([1]), da Decisão 2002/47/CE, CECA, Euratom da Comissão ([2]), do Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho ([3]) e da Decisão 1999/352/CE, CECA, Euratom.

Artigo 18.º

Revogação e medidas de transição

É revogada a Decisão C(2006) 3602 de 16 de agosto de 2006.

As regras de execução e as normas de segurança informática adotadas nos termos do artigo 10.º da Decisão C(2006) 3602 mantêm-se em vigor na medida em que não entrem em conflito com a presente decisão, até serem substituídas pelas regras de execução e as normas a adotar nos termos do artigo 13.º da presente decisão. Qualquer referência ao artigo 10.º da Decisão C(2006) 3602 deve ser entendida como referência ao artigo 13.º da presente decisão.

Artigo 19.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 10 de janeiro de 2017.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

([1]) Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

([2]) Decisão 2002/47/CE, CECA, Euratom da Comissão, de 23 de janeiro de 2002, que altera o seu regulamento interno (JO L 21 de 24.1.2002, p. 23).

([3]) Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho, de 11 de setembro de 2013, relativo aos inquéritos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF) e que revoga o Regulamento (CE) n.º 1073/1999 do Parlamento Europeu e do Conselho e o Regulamento (Euratom) n.º 1074/1999 do Conselho (JO L 248 de 18.9.2013, p. 1).